IJCSIS Vol. 12 No. 3, March 2014
ISSN 1947-5500

International Journal of Computer Science & Information Security


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

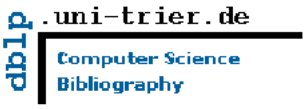

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


ProQuest

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS
International Journal of Computer Science and Information Security (IJCSIS)
January-December 2014 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: see web site
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

Editorial
Message from Managing Editor

The ***International Journal of Computer Science and Information Security*** *(IJCSIS) is an international forum for scientists and engineers involved in all aspects of computer science and technology to publish high quality refereed-papers. As a scholarly open access peer-reviewed international journal, IJCSIS encourages emerging scholars and academicians globally to disseminate their professional knowledge, innovative ideas and research in the fields of computer science, engineering, technology and related disciplines. The objective of IJCSIS is to bridge the research community and technology developers from academia and industry through submitting/publishing their research–based papers, articles and case reviews on various topics of current concern on Computer Science, Security and Technology.*

IJCSIS archives all publications in major academic/scientific databases; abstracting/indexing, editorial board and other important information are available online on homepage. Indexed by the following International agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported increased in number cited papers published in IJCSIS. This journal supports the Open Access policy of distribution of published manuscripts, ensuring "free availability on the public Internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of [published] articles".

IJCSIS editorial board, consisting of international experts, ensures a rigorous peer-reviewing process. We look forward to your collaboration. For further questions please do not hesitate to contact us at ***ijcsiseditor@gmail.com****.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 12, No. 3, March 2014 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

1. Paper 28021449: Privacy and Security Concerns in Cloud Computing (pp. 1-4)

Hamoud Alshammari
Department of Computer Science and Engineering
221 University Ave, University of Bridgeport,
Bridgeport, CT, USA

Abstract — In Cloud Computing environment, when clients or providers want to authenticate themselves to the cloud, they face some problems like the security level of their credential information to be stolen or by illegal using of their decrypted messages by attackers during the communication process. The service providers and clients delegate a third party to monitor and enforce the datacenter in the infrastructure level of cloud. However, the third party might not be a trusted enough for one of them or for both, so they need to manage their data by themselves. In this paper, I will go over one technique for each issue to solve the privacy problem. Web Service Security model for encrypted and decrypted messages, and Private Virtual Infrastructure model for monitoring the data over cloud.

Keywords— Cloud Computing, Cloud Security, Locator Bot, Virtual Private Infrastructure, Web Service Security.

2. Paper 28021427: A knowledge-Based DSS for Egypt's Water Security (pp. 5-10)

Ahmed Mohamed Omran, Computer Science Department, FCI, Fayoum University, Fayoum, Egypt
Nisreen Laham, Information and Decsion Support Centre, Egyptian Cabinet, Cairo,Egypt

Abstract — In Egypt, water security tops the national agenda whereby studies reveal that estimations of available water and water needs for different purposes are heading towards an increasing gap between water supply and demand. This paper is the first to integrate RT-Delphi with ontology KB, explanation, scenario methods and structural analysis. It provides a strategic planning methodology based on a multi-participatory approach. Moreover, this paper introduces a tailored methodology for a successful scenarios building process in Egypt. It discusses how the futures studies methods could be integrated into the decision analysis and making process in Egypt. Final, this Research builds on our research to support policy/decision makers in Information and Decision Support Centre (IDSC)-Egyptian Cabinet for the Egypt's water security research.

Keywords - Knowledge-based DSS, Eyptian Water Security, RTDelphi, Ontology-based, Secnario-based, Explanation.

3. Paper 28021412: A Study on the Radio Spectrum Management in South Asian Countries: Challenges and Opportunities (pp. 11-15)

Md. Kabir Uddin and M Abdus Sobhan
School of Engineering and Computer Science, Independent University, Bangladesh, Bashundhara, Dhaka

Abstract — The enhancing cumbersome intricacy of wireless communications technologies and inclusion in a wide range of miscellaneous applications mean the related spectrum management issues are being more complex. Pursuant to this spectrum complexity relates equally to private and public sector use of the spectrum. Changes from an industrial to an informational based society and the associated demand for enhanced communications services push the need for seamless access further. It is likely that removing unnecessary regulatory distinctions between government and non-government spectrum will become increasingly important to maximize the overall benefit derived from use of the spectrum. Many applications of practical interest stem from the capability to monitor and store packet-level traces in a WiFi, WiMAX, 3G and 4G networks. In this approach, yields strong practical benefits, given the costs and complication of accessing network equipments, especially in the Radio Access Network as well

as pondering of security. The author of this paper discusses the opportunities to exploit in and addresses challenges faced by the key players in South Asian region and seeks the spectrum commons approach in South Asian countries and concludes that, even in the face of enormous challenges, the potential benefits and opportunities are noteworthy adequate to necessitate grim thoughtfulness by telecommunications policy–makers in their function as spectrum managers.

Keywords — Spectrum, Regulatory, RFID, DSA

4. Paper 28021416: On the Implications of Current Radio Spectrum Management Issues in Bangladesh (pp. 16-21)

Md. Kabir Uddin and M Abdus Sobhan
School of Engineering and Computer Science, Independent University, Bangladesh, Bashundhara, Dhaka

Abstract — The brisk and mammoth yield of wireless mobile community, coupled with their demands for high speed, wideband, multimedia services, stands in clear contrast to the limited radio spectrum allocated in international agreements. Advanced mobile services combine the innovation potential of reckoning, data communications, and the wireless industry. So, Current Radio Spectrum Management (CRSM) [1] remains as a key challenge to the efficient engineering of mobile wireless networks. Different types of innovation scenarios can be distinguished, depending on the constellation of sunk cost and the cost of coordination between suppliers along the value chain. No single spectrum management framework supports all equally well, although spectrum use markets seem to be most broadly compatible. A mixed approach is possibly superior to any given individual class of spectrum management. Broadening the literature on spectrum policy, the author of this Paper focuses on implications and issues of Current Radio Spectrum Management regimes for rolling out in mobile services in Bangladesh with the current status of Radio Spectrum Management (RSM) polices and outline the key issues in RSM for next generation mobile wireless networks although the development of 3G in many countries new directions are being researched.

Keywords — CRSM, RSM, QoS, ISM, Spectrum

5. Paper 28021420: Cortex Simulation System Proposal Using Distributed Computer Network Environments (pp. 22-25)

Boris Tomas, University Of Zagreb, Faculty of Organization And Informatics, Pavlinska 2, Varazdin, Croatia

Abstract — In the dawn of computer science and the eve of neuroscience we participate in rebirth of neuroscience due to new technology that allows us to deeply and precisely explore whole new world that dwells in our brains. This review paper is merely insight to what is currently ongoing research in the interdisciplinary field of neuroscience, computer science, and cognitive science.

Index Terms — Artificial neuron, artificial neural networks, neuron simulation

6. Paper 28021422: Chaotic Scheme for Image Encryption Based on Arnold Cat's Map (pp. 26-33)

Ansam Osama Abdul-Majeed
Department of Software Engineering, College of Computer Science and Mathematics / University of Mosul, Mosul, Iraq

Abstract — Digital images are widely used media over the Internet for different purpose. Therefore, security becomes important in the transmission. This paper presents spatial domain multilevel image encryption algorithm based on Arnold cat's map. The algorithm divides the image into different size overlapping blocks along the levels of encryption. The block at level 1 begins at the center of the image and this block is iteratively enlarged in the next levels. In each level of the proposed algorithm, Arnold cat's map is implemented in each level on the block's pixels.

Also, zigzag scan is applied on the whole image to further reducing the correlation between adjacent pixels. In order to achieve the diffusion, the pixel values are xored with different xor values begin at a value, which is generated randomly, beside control parameters and iteration number of Arnold cat's map, by using mid-product algorithm with the secret key as an initial seed. The results of experiments indicated that the proposed algorithm is highly decorrelated the adjacent pixels and it resists the statistical attacks. The values of ciphered image entropy are close to the ideal value. Furthermore, the proposed algorithm is very sensitive to key. It was concluded that the use of zigzag scan beside Arnold cat's map in spatial domain was very efficient to hide the statistical characteristics of the image.

Keywords - Image encryption; Arnold cat's map; Zigzag scan; mid-product.

7. Paper 31101319: An Overview of an Advanced Vehicle Security System (pp. 34-37)

Tariq Alwada'n (1), Adel Hamdan Mohammad (1), Nidhal El-Omari (1), Hamza Aldabbas (2)
(1) Computer Science Department, The world Islamic Sciences and Education University, Amman-Jordan
(2) Prince Abdullah bin Ghazi Faculty of Information and Technology, Al-Balqa' Applied University,Salt-Jordan

Abstract — In the past few decades wireless networks have become increasingly popular, due to the wide availability and rapid introduction of wireless transceivers into a variety of computing devices such as PDAs, laptop and desktop computers. Global Positioning System (GPS) is used to determine position and speed of objects by using the satellite technology. Furthermore, Radio Frequency is another technology which is used to determine the objects' locations. In this paper we have presented an overview for using the previous technologies to track a stolen vehicle by using a system that is resulted from mixing all of those technologies in addition to proposed an enhancement idea that could help the resulted system to determine the cars' thieves by sending their photos to the security agency base to be recognized.

Index: WiMAX, Wi-Fi, GPS, Mobile Cell Phone, Radio Frequency.

8. Paper 30111333: Computational Intelligence Techniques Used In Iris Recognition:A Survey (pp. 38-49)

Shraddha Sharma, UIT, RGPV, Bhopal, India
Shikha Agrawal, UIT, RGPV, Bhopal, India
Sanjay Silakari, UIT, RGPV, Bhopal, India

Abstract - Authentication is a very crucial issue for all security protocols. Biometric based authentication is widely used for security issues such as iris, face, fingerprints etc. Iris Recognition takes into account together of the simplest biometric technique used for human identification and verification, owing to its distinctive feature that disagree from one person to a different, and its importance within the security field. Now-a-days various researchers used many soft computing techniques in the iris recognition system. This paper gives a brief survey of these techniques used for feature extraction such as neural network, genetic algorithm, fuzzy logic and particle swarm optimization.

Keywords - Authentication, iris recognition, Feature Extraction, Neural Network, Genetic Algorithm, particle swarm optimization, Fuzzy Logic.

9. Paper 31101312: Significant Factors Affecting the Use And Integration of Information Technology (IT) Tools in Teaching in South Western Nigerian Polytechnics (pp. 5-61)

Aladesote, O. Isaiah, Agbelusi Olutola, Ojajuni O. James
Computer Science Department, Rufus Giwa Polytechnic, Owo, Ondo State.
Abstract - Information Technology (IT) also referred to as Information and Communication Technology (ICT) can be described as electronic technologies used for information storage and retrieval (Adomi & Kpangban, 2010). This paper examined various factors hindering the use of IT tools in teaching in South Western Nigerian Polytechnics and

also extract the most significant factors that pose serious challenges to the use and integration of IT in teaching using Gain Ratio extraction technique. Questionnaires were distributed to Lecturers and seasoned administrators in the Polytechnic sector to access their knowledge and belief on the stated factors. The responses from the respondents were used to form a dataset. C# Programming was used for the implementation. Also, Microsoft Excel was used for the analysis of the data collected. The result of the analysis shows that seven (7) factors were highly hindering the use and integration of IT tools into teaching.

Keywords: ICT, Gain Ratio, Microsoft Excel, Extraction Technique.

10. Paper 28021410: An Overview of Contemporary Cyberspace Activities and the ChallengingCyberspace Crimes/Threats (pp. 62-100)

Samson Olasunkanmi Oluga, Dr Azizah Bt Haji Ahmad, Ahmad Jamah Ahmad Alnagrat, Haroon Shakirat Oluwatosin, Maryam Omar Abdullah Sawad, Nur Adlya Bt Muktar*
School of Computing (SOC), College of Arts and Sciences (CAS), Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Abstract - One thing that has emanated from the development of the internet technology and popular embrace of social networking is the emergence of a second digital world which is a virtual reality world called the cyberspace. The cyberspace users who can be described as the Cyberians are attracted to the cyberspace from time to time especially because of the various opportunities/activities available via the cyberspace cutting across many spheres of human endeavor. There are however many threats or challenges which may be inimical to the safety of the cyberspace, the cyberspace assets/resources and the interest of the Cyberians, the regular cyberspace users or cyber citizens. This paper, based on extensive examination of contemporary literature on the cyberspace, explores fundamental activities of the cyberspace and explicates various forms of cybercrimes orchestrated by cyber criminals posing great threats to the cyberspace. The basic ideas of the paper are equally captured in vivid illustrative models.

Keywords: Cyberspace, Cyber activities, Cybercrimes/Threats

Privacy and Security Concerns In Cloud Computing

Hamoud Alshammari
Department of Computer Science and Engineering
221 University Ave, University of Bridgeport,
Bridgeport, CT, USA

***Abstract*— In Cloud Computing environment, when clients or providers want to authenticate themselves to the cloud, they face some problems like the security level of their credential information to be stolen or by illegal using of their decrypted messages by attackers during the communication process. The service providers and clients delegate a third party to monitor and enforce the datacenter in the infrastructure level of cloud. However, the third party might not be a trusted enough for one of them or for both, so they need to manage their data by them selves. In this paper, I will go over one technique for each issue to solve the privacy problem. Web Service Security model for encrypted and decrypted messages, and Private Virtual Infrastructure model for monitoring the data over cloud.**

***Keywords*—** Cloud Computing, Cloud Security, Locator Bot, Virtual Private Infrastructure, Web Service Security.

I. INTRODUCTION

In Cloud Computing environment, there are different issues that users should consider when they get the benefits of the Cloud services. Most considered issues are related to the boundaries of the organization, which direct us in deep to the issue of loosing the control of the organization resources within the cloud environment [1]. That happens when the resources are moved to the cloud environment then the owner of these resources losses the monitoring and controlling on their functionality.

One of the most important issues is the inside and outside security threat. The outside threats are similar to the tradition large datacenters [2]. Cloud Computing is not a new concept that we use to provide the information via networks. Since that, the same traditional networks security issues cloud computing has been faced, and we need to figure out these problems. Cloud computing is faced by different challenges to be applied with a high level of security [3]. The responsibility of facing the security issues in the cloud is divided between different parties like the user, service vendor and a third party who located in between of the user and the provider to provide some security services like Service Level Agreement [2].

There are two different security models that support two different levels of services in cloud computing to be secure. The first model is Web-Service Security (WS-Security) that supports working in message level. This model provides Encryption/Decryption concepts, which are using in the security of Authentication, Integrity, and Confidentiality. The second model is Private Virtual Infrastructure (PVI) that discuss the safety of Datacenters in the cloud by distribute the duties between the service provider and the client [4].

Figure 1: Cloud Security Related Issues

II. WEB SERVICE SECURITY MODEL

This part is one of the most significant solutions for the security issue in Web Services, which provides some security services to the cloud like integrity, confidentiality and authentication [5]. This solution explains how to apply the security XML standards, which are XML signature and XML encryption to the SOAP messages.

1) MXL Security Standards

The first stander is the XML Signature, which allows the process of digitally signing the XML fragments to proof authenticity or to ensure the integrity. A simple structure of the XML Signature element is as follows [5]:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

```
<Signature>
    <SignedInfo>
        <CanonicalizationMethod Algorithm="..."/>
                        <SignatureMethod Algorithm="..."/>
                        <Reference URI="..." >

        <DigestMethodAlgorithm="...">

        <DigestValue>...</DigestValue>
                        </Reference>
    </SignedInfo>
    <SignatureValue>...</SignatureValue>
</Signature>
```

The second one is the XML Encryption, which provide the encryption service to the XML fragment to be encrypted to ensure dada confidentiality. The process is as follows an EncryptedData element takes a place of the encrypted fragment containing the ciphertext as a content of the encrypted fragment.

2) Transport Layer Security (TLS)

It has been introduced under its common name "Secure Sockets Layer (SSL)". This layer consists of two main parts [5]:

a. *Record Layer:* which encrypts/decrypts TCP data streams using the algorithms and keys negotiated in the TLS Handshake.
b. *TLS Handshake*: which is used to authenticate the server and the client.

Today, it is considered as the most important cryptographic protocol worldwide, since it is implemented in every web browser.

3) Web Service Security Issues

I will illustrate two main issues that WS-Security model is faced, which are XML Signature element wrapping and web browser security.

a) XML Signature Element Wrapping

Clients are able to connect to cloud computing using a web browser or web service. Although, WS-Security uses XML Signature in order to protect an element's name, it is unable to protect the positions in the document [6].

What is the problem?

An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message.

To solve of the problem

i. Using a WS-Security with XML signature and digital certificated such as X.509 issued by trusted Certificate Authorities.
ii. Servers should create a list of elements that is used in the system and reject any message from unexpected clients.

b) Web Browser Security

Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not [6].

What is the problem?

These days, web browsers are not able to apply WS-Security concepts (XML Signature and XML Encryption). So, they cannot use XML Signature concept to authenticate client's credentials (e.g. username and password). In addition, web browsers have to use SSL/TLS to encrypt the credential and use SSL/TLS handshake process to authenticate the clients. However, SSL/TLS only supports point-to-point encryption which means the message will be encrypted and decrypted many times during the communication process, so the attacker might get a decrypted message in one of the steps, and he can change, delete or manipulate it and resend it again with his information.

To solve of the problem

Providers should create web browsers that support using XML Security concepts [7]. As A result, web browsers are able to use XML Encryption in order to provide end-to-end encryption in SOAP messages. Consequently, SOAP messages don't have to be encrypted and decrypted for many times because it just encrypted and decrypted for one time, so attackers cannot get any decrypted message.

III. PRIVATE VIRTUAL INFRASTRUCTURE (PVI) MODEL

Usually, there is a third party that works with service provider and client to control and save datacenter. In cloud computing, PVI model has been suggested to distribute the responsibility of control and save datacenter between providers and clients. In this model, users would have security over their information in cloud and providers would have security over the fabric of the server [5].

The service level agreement (SLA) between the client and provider is critical to defining the roles and responsibilities of all parties involved in using and providing cloud services. The service level agreement should explicitly call out what security services the provider guarantees and what the client is responsible for providing. Web Service Level Agreement (WSLA) framework is developed for SLA monitoring and enforcement in SOA [8, 9]. In cloud computing environment, the monitoring and enforcement tasks are delegated to a third party to solve the trusted problem [2].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

In order to verify the security within the cloud, each service in the cloud needs to be able to report security properties present and the report must be verifiable. This ability means that clients need visibility into the security settings and configuration of the fabric.

Trusted Computing Techniques have been chosen to verify these settings and report the configuration of the fabric in PVI. Additional requirements for PVI are that communications to and within PVI should be done through virtual private networking and all links should be encrypted with IPSec or SSL tunnels. This step provides confidentiality on the network and prevents other users within the cloud from eavesdropping and modifying communications of PVI [9].

One of the components of the PVI is the PVI Factory; which represents where all the components are replaced on. The PVI Factory should be fully controlled by the owner of the information either being standalone unit or in the site of the owner [4].

TRUSTED COMPUTING

Trusted Computing provides users to verify their security postures in the cloud and control their information, allowing them to achieve the economies of scale, availability, and agility that the cloud promises.

Trusted Platform Model (TPM)

It is a cryptographic component that provides a root of trust for building a trusted computing base. The TPM stores cryptographic keys that can be used to attest the operating state of the platform. The keys are used to measure the platform, which are then stored in the TPM's Platform Configuration Registers (PCRs) [9]. When clients want to attest a platform, clients can request the PCRs and verify that the platform meets its requirements and policy.

What is the problem?

Trusted Platform Model is only works for non-virtualized environments.

To solve of the problem

TPM needs to be virtualized. So, Virtual TPM has been developed and implemented for each virtual machine (VM) on a trusted platform. Individual computing platforms within the cloud each have a TPM owned by the service provider. VTPMs are linked to the physical TPM and used to secure each VM in the cloud [6].

Locator Bot (LoBot) is an architecture that cryptographically secures each VM by tightly coupling a VTPM in its own stub domain. LoBot allows each VM to be verifiable by its owner and provides secure provisioning and migration of the VM within the cloud as well [9]. The LoBot application at the target environment, this probe application, receives and unseals the resource environment. So, if the source environment got changed and unknown tampering within exist transfer, the decryption phase will detect this changes. The probe measures do the measuring of the source environment one more time to make sure that everything is safe and to validate the integrity and to ensure the successfully of lunching process in the target environment.

IV. CONCLUSION

In this paper I represent two solutions for two problems in Cloud Computing. The first model is Web Service Security (XML Signature and XML Encryption) that solves the unauthorized using of decrypted messages. Although, the idea of this model can solve this problem, the web browsers are not able to apply this model. So, we need to develop a web browser that supports the idea of this model.

In the other hand, a third party monitors the datacenters in cloud, so PVI model can determine the responsibilities for client and provider. The problem that I believe is when client wants to know which platform meet his requirements because it will still problem for the client to determine his requirements and control the security side in the infrastructure. The client will cause a number of problems in the datacenter and in the cloud computing system.

REFERENCES

[1] M. Townsend, "Managing a security program in a cloud computing environment," in *2009 Information Security Curriculum Development Conference*, 2009, p. 6.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski*, et al.*, "A view of cloud computing," *Communications of the ACM,* vol. 53, p. 9, 2010.

[3] L. M. Kaufman, "Data security in the world of cloud computing," *Security & Privacy, IEEE,* vol. 7, p. 4, 2009.

[4] A. Nayyar, "Private Virtual Infrastructure (PVI) Model for Cloud Computing," *International Journal of Software Engineering Research and Practices,* vol. 1, p. 5, 2011.

[5] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Cloud Computing, 2009. CLOUD'09. IEEE International Conference*, Horst Gortz Institute for IT Security, Ruhr University Bochum, Germany, 2009, p. 8.

[6] D. Jamil and H. Zaki, "SECURITY ISSUES IN CLOUD COMPUTING AND COUNTERMEASURES," *International Journal of Engineering Science & Technology,* vol. 3, p. 5, 2011.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[7] L. Q. Sumter, "Cloud computing: security risk," in *ACM*, Florida A&M University, 2010, p. 112.

[8] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," in *Informatics and Systems (INFOS), 2010 The 7th International Conference*, Hasso Platter Institute. Postdam, Germany, 2010, p. 8.

[9] F. J. Krautheim, "Private virtual infrastructure for cloud computing," in *Proceedings of the 2009 conference on Hot topics in cloud computing*, University of Maryland, 2009.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A knowledge-Based DSS for Egypt's Water Security

Ahmed Mohamed Omran
Computer Science Department, FCI
Fayoum University
Fayoum, Egypt

Nisreen Laham
Information and Decsion Support Centre,
Egyptian Cabinet
Cairo,Egypt

***Abstract*— In Egypt, water security tops the national agenda whereby studies reveal that estimations of available water and water needs for different purposes are heading towards an increasing gap between water supply and demand. This paper is the first to integrate RT-Delphi with ontology KB, explanation, scenario methods and structural analysis. It provides a strategic planning methodology based on a multi-participatory approach. Moreover, this paper introduces a tailored methodology for a successful scenarios building process in Egypt. It discusses how the futures studies methods could be integrated into the decision analysis and making process in Egypt. Final, this Research builds on our research to support policy/decision makers in Information and Decision Support Centre (IDSC)-Egyptian Cabinet for the Egypt's water security research.**

Keywords:Knowledge-based DSS, Eyptian Water Security,RT-Delphi, Ontology-based, Secnario-based, Explanation.

I. INTRODUCTION

The Nile stands as Egypt's main source of water whereby it secures 80% of Egypt's water yield per year-according to the 1959 Nile Agreement, Egypt's fixed quota of Nile water comes to 55.5 billion m3/year [1]. In Egypt, water security tops the national agenda whereby studies reveal that estimations of available water and water needs for different purposes are heading towards an increasing gap between water supply and demand. Water gap, in Egypt, is likely to increase by time, not only because of the anticipated increase of water demand, but also due to the impact of other factors on the available quantity of Nile water [2].

Different national and international research efforts tried to tackle the problem of water security and the future water gap in Egypt [1, 2, 3, 4, 5, 6]. Uncertainty and Complexity, which are arising from future unprecedented events/ wildcards, represent the main challenges for the previous research [7]. Policy/Decision maker need for two crucial activities, which are explorative the futures and analysis its impacts [4, 7].

Delphi method being an important qualitative tool of future studies applied in discussing a given issue via collective intelligence and scientific forecasts. Using this tool, it is aimed at deriving the knowledge from a group of experts, directing them towards consensus on aspects of the introduced issue, and introducing verifications of the relatively extreme positions [8, 9]. The Delphi method is a powerful and a well structured tool for knowledge acquisition, because its anonymity process. In Delphi method the process for knowledge acquisition from domain participators is done by controlled opinion feedback for a series of questionnaires. It provides the domain participators to move toward consensus [10, 11].

For knowledge elicitation process, the Real-Time (RT-Delphi) Delphi technique is widely-used as a structured and controlled debate. In RT-Delphi, all opinions are made anonymous and the domain experts move toward consensus. it has the following 5 advantages (in comparison to traditional Delphi): Round-less approach then significantly saves time and cost, experts have instantaneous access to the website, flexibility in the number of participants and it can be easily applied to problems formulated in a matrix design[10, 11].

Scenario-based methods are powerful methods for futures anticipation and analysis. It has come through operation analysis and the use of Delphi-methods. The pioneer to use the scenario-based concept in futures studies was Herman Kahn in the 1950's in the RAND Corporation in the U.S.A [10]. MICMAC (Impact Matrix Cross-Reference Multiplication Applied to a Classification) represents a structural analysis based on comparing the hierarchy of issues in the various classifications (direct, indirect and potential), which is a rich source of information to determine the major wildcards of a specific domain [12]. Moreover, domain ontology is major in order to provide an easy way towards the knowledge acquisition process by minimizing the misunderstandings when debating a certain concept or a problem [13]. It plays an important role for reducing the contradiction of the experts' judgments by defining a common language between domain experts. Also, it describes the domain concepts, their attributes and all relationships that hold between these concepts [14].

The core idea of our research paper is to develop an intelligent decision support system (IDSS) to identify the main factors of uncertainty that will affect in the future Egypt's water security, and to anticipate potentials of these uncertainty factors, their different expected impacts. The ontology-based RT-Delphi, scenario based and explanation method are integrated for the developed IDSS. Final, more than 25 experts in the areas of water, economic and political science share in this research.

The paper structure is organized as follows: in Section 2, we discuss the problem addressed. Then in Section 3, our proposed solution is explained in details including the inputs, output and the approach itself. Also, in Section 4, we give the results and discussions. Finally in Section 6, we conclude and suggest possible future work.

II. PROBLEM DEFINITION

Different national research efforts, from literatures, tried to tackle the problem of water security and the future water gap in Egypt. These researches weren't efficient and effective enough to deal appropriately with the long-term uncertainty and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

complexity. The long view of these researches is based on a limited number of participators' views. Also, it have different challenges in handling knowledge acquisition process for instance: dealing with the misunderstanding of some concepts' meaning, handling knowledge contradiction, allowing knowledge gathering from experts in different locations and having an efficient and effectiveness communications between experts. Final, they don't provide policy/decision maker with their need for powerful tools, which deal with studying the futures and analysis its impacts on the Egypt's water security.

III. PROPOSED SOLUTION

The study at hand contributes to foreseeing the future of Egyptian water security, by analyzing the impact of varied factors influencing Egypt's water security in terms of the political, economic, environmental, hydrological, legal and strategic aspects, developing an integrated vision, and forming a new approach for further research in this area and providing comprehensive knowledge. Different Futures studies and knowledge-based methods are enhanced and integrated to develop the intelligent DSS. The following sub-sections discuss in details the solution proposed.

A. The Developed Framework

As shown in figure1, the developed framework consists of three main components, which are model-based, knowledge-based and graphical user interface sub-systems. Model-based component has two sub-components, which are model base and model-base management sub-component. There are different models in model-base system, which are ontology-based RT-Delphi, scenario based and cross impact analysis. The model-base management component provides models integration and execution. In addition, knowledge-based component has two sub-components, which are knowledge-base and knowledge-based management system.

The Knowledge-base component consists of three sub-components which are ontology, explanation and policy sub-components. The explanation sub-component provides "What if" and "Why" explanation, which help for reducing the uncertainties associated with the long-term scenarios and increasing the confidence of policy/decision makers about the consensus results. Furthermore, the domain expert knowledge consists of two main categories, which are experts' judgment and its justifications that represent the core of "Why" explanation. Final, graphical user interface sub-system provides the policy/decision decision maker capabilities for reporting consensus summary information, consensus justifications and the visualization capabilities.

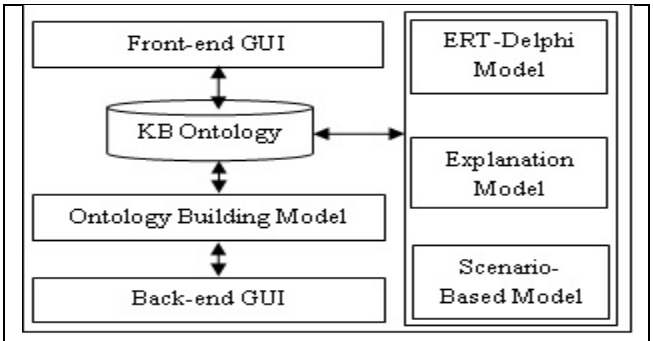


Figure.1."conceptual view of the IDSS framework"

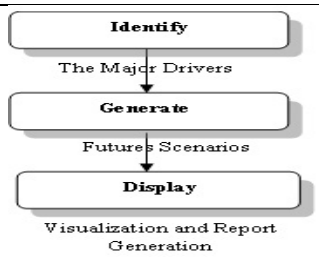


Figure.2. The IDSS Phases

B. Inputs/Outputs

The inputs of the knowledge-based structural analysis approach are based on the knowledge of nominated and weighted experts. Table1 lists the inputs used in our new approach (the usage of each input will be illustrated in the algorithm section). As shown in table 2, the two major outputs of are: the KB-MICMAC Matrix, and "Why" and "What if". Also, based on the KB-MICMAC Matrices, policy/decision makers can determine the influential and dependency drivers with the domain experts' explanation.

Table 1. Inputs of the developed new approach

Short Name	Full Name	Type
MICMx	Structural analysis based on MICMAC Matrix	2D-Matrix

Table 2. Outputs of the developed new approach

Short Name	Full Name	Type
DrMx	Drivers Types Matrix	2D-Matrix

C. The Developed Methodology

The developed system was applied to identify the main factors of uncertainty that will affect in the future Egypt's water security, and to forecast potentials of these uncertainty factors,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

their different expected impacts, and proposed relevant procedures.

Our developed methodology is based on utilizing domain experts' experiences and imagination. It utilized both qualitative and futures studies' models. RT-Delphi is enhanced by integrating ontology component and it is used as a knowledge elicitation tool. Also, Forecasting method which is a compound methodology that does not seek foreseeing or planning for the future, but it rather conducts a set of conditional forecasts or scenarios assuming either the reality or desired ones. The third method is the scenario-based method, which is utilized domain experts knowledge and generated all possible future scenarios.

This methodology is applied to identify the main factors of uncertainty that will affect in the future Egypt's water security, and to forecast potentials of these uncertainty factors, their different expected impacts, and proposed relevant procedures. 25 experts in the areas of water, economic and political science are shared and answered relevant questions. As shown in figure2, our developed methodology consists of two phases of completing this task is as follows:

- 'Identify' Phase

This phase plays a fundamental role in the scenario construction. In addition, in this phase, domain experts identify the main factors affecting Egypt's water security by utilizing experts' knowledge and their imaginations. As shown in figure5, the enhanced ontology-based RT-Delphi [12] is used for knowledge elicitation. The Ontology KB provides to create a repository of Egypt's water security knowledge. The developed ontology KB architecture represents its sub-ontologies and the relationships between their concepts. It consists of six sub-ontologies: model drivers, model variables, participators, questionnaires, planning bedrock, policy, which are consist of different concepts. Moreover, each sub-ontologies consists of different concepts' prosperities (name, description, weight ranking and its impact).

- 'Generate' Phase

Given the aforementioned main factors affecting Egypt's water security, the future of water in the Nile basin will likely be shaped according to three alternative scenarios. 'Generate' phase provides domain experts to generate all possible futures scenarios. Forecasting, scenario-based and RT-Delphi are integrated to generate all possible futures scenarios. Factors are represented in each Political, Economical, Soci-culture, Technical, Ethical, Legal (PESTEEL) issues. As shown in figure3, the integrating two futures studies methods, which are the structural analysis, based on Impact Matrix.

- 'Generate' Phase

Cross-Reference Multiplication Applied to a Classification (MICMAC) and the enhanced RT-Delphi (ERT-Delphi) method, which is used to identify the major drivers. There are two types of information represented in the knowledge acquisition matrices of the ERT-Delphi: the first is a guide-information that contains 4 items for each question: (1) median response of the expert group (2) the number of responses made (3) justifications that the other experts have given for their responses, which are being ordered by values. Moreover, the second type is the judgment information that allows the experts to add a new numerical answer and type his/her justifications for their own answer(s). A group of the domain experts can fill in the structural analysis matrix over a period of time determined by the domain analysts, in the questionnaire's design step. When the relationship is direct influence, the filling-in direct influence is low (1), medium (2) or high (3). In addition, zero value (0), appears if there is not a relation.

- 'Display' Phase

This phase provides policy/decision makers for different visualization and report generation capabilities. The outputs of this phase are (1) the major drivers (2) future scenarios (3) explanation capabilities ("why" and "what if") and finally (4) visualization and report generation. Figure6 and figure7 show the "why" and "what if" explanation flowcharts.

Applying this methodology, the research does not conclude to a determination of achieving any of the aforementioned scenarios as this is an issue that is not related to future planning. But the objective is rather allowing policy/decision makers to learn about the requirements for achieving one of the desired scenarios according to their relevant preference in order to work on giving it precedence over other alternative scenarios.

IV. Results and Discussion

A. Major Drivers

Based on the consensus results of 25 domain experts about the issue of Egypt's water security, the most important drivers affecting Egypt's water security were identified as follows:

- The trend of relations between countries of the Nile basin towards either cooperation or struggle (weight value = 90%, # of accepted experts = 25).
- Impact of external powers stimulating conflicts or cooperation (weight value = 85%, # of accepted experts = 25).
- Shifting of some Nile basin countries to irrigated agriculture and minimizing pressure on the blue water (weight value = 85%, # of accepted experts = 23).
- The nature of change in the economic conditions in countries of the Nile basin (weight value = 80%, # of accepted experts = 20).
- Some of the Nile basin countries constructed water reservoirs or control utilities (weight value = 75%, # of accepted experts = 21).
- High impact of climate change on the water yield of the Nile basin (weight value = 75%, # of accepted experts = 20).
- The impact of the separation of South Sudan on the Egyptian water yield from the Nile basin (weight value = 70%, # of accepted experts = 17).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Political stability or instability in domestic policy of the Nile basin countries (weight value = 70%, # of accepted experts = 17).

Table 3 WRT-MICMAC2 Consensus Results	
Diver	Type
A	Key wildcard event
B	Key wildcard event
C	Key wildcard event
D	High Influence, low Dependent
E	High Influence, Low Dependent
F	Low Influence, Low Dependent
G	Low Influence, Low Dependent
H	Low Influence, Low Dependent

B. Futures Scenarios

Given the aforementioned main factors affecting Egypt's water security, the future of water in the Nile basin will likely be shaped according to three alternative scenarios: business as usual, optimistic scenario, and pessimistic scenario.

- Business as Usual

o *The current situation of struggle relations between Egypt and the Nile Basin Countries, will continue, nevertheless, will not escalate to war because of the experience of political interactions the countries of the Nile basin maintain and the reasonable margin of rationality in its interrelation[15, 16]. They also maintain minimum level of good geographic neighbourhood relations. Also, the domestic political, economic and social circumstances of the Nile basin countries will not permit potential escalation of conflicts and struggle [16].*

o *According to the Consensus results of the developed DSS:*

o *A change in the current situation of cooperation or struggle regarding water is unlikely (because there were no sharp deviations regarding the potential full cooperation or struggles that may escalate to war over water). 46%, 38% and 50% is the probability percentage of increasing the normal yield of Nile water before 2030 via operationalizing the cooperation mechanism when Egypt develops projects in the Ethiopian Plateau, Equatorial Lakes Plateau and Bahr el Ghazal. But the percentage is 48% in the event of reaching an agreement on some of the conflict areas by amending the existing legal agreements of the Nile basin countries.*

o *There is difficulty of benefiting from green water and relieving the pressure off blue water in the countries of Nile basin because of the lack of sufficient funding in the present time.*

o *Probability percentage for Egypt-in cooperation with donor or lender international organizations-to develop projects aimed at assisting other countries in benefiting from green water and thus relieving pressure off blue water in: the Ethiopian, Equatorial Plateaus and Bahr el Ghazal is 49%, 52% and 53% respectively.*

o *It is unlikely for the basin countries to experience an economic boom, as improving the economies of the Nile basin countries requires complete satiability of political regimes which needs attention to the development plans that in turn require local, regional and international capital, capacity building, technical calibers and improvement of institutions and laws. Such issues can only be achieved on the long term.*

o *There is low probability of an impact from the separation of south Sudan on Egypt's normal yield of the Nile water, as the new State in the south will be bound by all past conventions related to the River Nile. Needless to mention, that south Sudan is advantaged with abundant rain which spares it the need for this water. According to Delphi Survey, percentage of the probability of a relevant impact on Egypt's Nile water supply is 45%.*

o *It is likely that climate changes will continue without an impact on the normal yield of Nile water in Egypt, at least, during the coming twenty years. According to a study prepared by the Organization of Economic Cooperation and Development (OECD) in 2004, there is a limited confidence regarding the value and direction change in rain falling in the future on the Nile basin countries. Based on the survey results, the probability percentage that climate changes will move the rain belt far from the Ethiopian, Equatorial Lakes Plateaus or Baher Al Gazal is 40%, 35% and 44% respectively.*

- Optimistic Scenario (Regional Cooperation)

o *This is the scenario of regional cooperation, optimization of available opportunities for developing shared water resources and building a water regional system that is capable of securing the needs of the region's countries. However, this should not undermine the fixed historical and legal rights of some of the countries. Also, this scenario involves the potentiality of expanding cooperation areas among Nile basin countries within the Nile Basin Initiative that combined between collectiveness and consensus, as it included all ten Nile basin countries as members, created an institutional framework for collective cooperation, received governmental and political support, and paid great attention to the projects, programs and mechanisms aiming at building mutual trust among river countries in the basin side by side to capacity building and training projects and mechanisms.*

o *The consensus results of the developed DSS indicate:*

o *There is an increased possibility of establishing water related projects in collaboration with the basin countries via building and connecting dams on a unified electricity network in those countries, in collaboration with international donor*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

organizations, aimed at generating power for agriculture and industrial production purposes rather than storing water and assist in regulating water supply to Egypt.

- *The probability percentage of completing Gongli Canal is 56%, in addition to the possibility of redirecting Congo River to enable benefiting of its water. In this regard, survey results show percentage of probability for Egypt to benefit of water of the Congo River as 60%.*

- Pessimistic Scenario (Conflict)

- *This scenario is based on the possibility that variables motivating struggle will lead to raising chances of conflict of national interests in the Nile basin countries to an extend of inter struggle. The struggle inclination might rise in the Nile interactions given the following variables: 1) A strong and sharp inclination of the Nile basin sources countries towards enforcing the principle of "selling Nile water" to the two countries of the mouth and stream. This strategy on the middle and long term will cause an eruption of international water struggle and wars among the countries.2) Escalated role of the external motivating powers for Nile-Nile struggle based on the following considerations:*

- *It is projected the countryX will play a motivating role for water struggle in the Nile basin in addition to the indirect role of countryY. In this regard, it will work on besieging and pulling the parties of Egyptian policy, on the regional level, in a way that serves coining the countryY power on the political and strategic levels in preparation for an effective the countryX role.*

- *Countries of the upper Nile basin will seek to constitute external coalitions, each according to its powers and strength, aimed at changing the current situation. Ethiopia, Kenya, Tanzania, and Uganda are more prone to changing and stimulating struggle and tension.*

- *Separation of south Sudan will be on the expense of all projects dedicated to exploiting the Nile water wasted in the Egyptian and joint upper parts. This is similar to Gongli Canal project where the implementation of the projects is conditional upon the approval of the infant State of south Sudan.*

- *The political tensions in the Ethiopian Plateau will negatively affect the Egyptian water yield as well as failure to implement any proposed projects. According to the survey, percentage of the probability for a civil war to erupt (because of ethnicity, religion, political or tribal affiliation) in the Ethiopian Plateau and bearing an impact on water projects and management is 53% and 57% respectively.*

- *The probability percentage of Nile basin countries to have an increased demand for the Blue water for the agricultural, industrial, drinking, tourism, and fish wealth purposes by 2030 in the Ethiopian, Equatorial Plateaus and Bahr El Gazal Region is 60%, 61% and 59% respectively. As for the probability percentage for those countries to construct dams or other projects in the Ethiopian, Equatorial Plateaus and Bahr El Gazal Region-aimed at meeting the increased demand for water-that will eventually affect Egypt's Nile water quota by 2030 is 63%, 59% and 54% respectively.*

V. Results and Discussion

1. Complexity and uncertainty of the long-term futures are the major challenges to develop more justifiable estimates for to the quality of long-term view and policies. We can summarize, in this paper, we develop an intelligent decision support system (IDSS).
2. The developed IDSS applied to help policy/decision makers in Egypt for addressing the most important future incidents affecting Egypt's water security. Also, it was used for identifying, analyzing and foreseeing potentials of Egypt's water security as ground to thinking of pilot solutions aimed at evading problems and crisis as well as developing a set of procedures and policies whereby Egypt's water security is attained. The developed IDSS is based on integration of scenario-based, RT-Delphi knowledge-based and explanation modeling capabilities.
3. The consensus results of 18 experts show that: 8 drivers are the major drivers for Egypt's water security. The major drivers are used to generate as usual, optimistic and pessimistic scenarios.
4. The next step in our research is to apply policy generation and evaluation approach to create policies that can help policy/decision makers to manage the future threats. Also, data-mining techniques can be used as a powerful tool for automated ontology building. Data-mining can improve the process of creating a formal ontology of a specific domain. It can help for minimizing the user manual intervention and by combining existing techniques like clustering.

References

[1]AbdulWahhab, A. (2009), “River Nile Basin: Cooperation opportunities and problems”, Cairo, Al Ahram Center for Political and Strategic Studies.

[2]Taye, S. (2007), “Water Security in the Arab Gulf in a Changing World: between Prerequisites of National Interest and Addressing External Threats”, Middle East papers, National Centre for Middle East Studies, Vol. 38.

[3]Shakweer, A., Yousef R.(2007) ,“Futures studies in Egypt: Water Foresight 2025”, foresight, Vol. 9, Iss:4, pp.22-32.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[4]Laham, N.,Saleh, M., Sabry, S. (2009), "Egypt's Water Security – Future Vision 2030 Using Delphi Method", European Foresight Platform, EFP Brief No.252.

[5]Jaïr, V.(2010), "Scenarios for Sudan in 2012: crash or happy take-off?", foresight, V.12 Iss:4.

[6]Brans, H.(1997), "The Scarcity of Water: Emerging Legal and Policy Issues, London, The Hague, Boston, Kluwer International, International Environmental Law and Policy Issues, 21-39.

[7]Jacques, G.(2009), "Uncertainty, the critical basis of risk management", foresight, Vol. 11 Iss: 6, pp.42-55.

[8]Gordon, T.(2003), "The Delphi method, Futures Research Methodology V2", CD ROM, the Millennium Project, American Council for the United Nations University.

[9]Robert, L. (2012),"The Delphi method: a powerful tool for strategic management", An International Journal of Police Strategies & Management, V25, Iss4.

[10]Gordon, T.(2003), "Futures Research Methodology V2", CD ROM, the Millennium Project, American Council for the United Nations University.

[11]Gordon,T., and Pease, A. (2006), "RT-Delphi: An Efficient, "Round-less" Almost Real Time Delphi Method", Technological Forecasting and Social Change, Volume 73, Issue 4.

[12]DiazDelaO, S.(2010),"Structural dynamic analysis using Gaussian process emulators", Engineering Computations, Vol. 27 Iss:5, pp.580-605.

[13]Akerkar, R. and Sajja P. (2010) "Knowledge-Based Systems", Jones & Bartlett Learning.

[14]Eriksson, H.(2003) "Survey of knowledge acquisition techniques and tools and their relationship to software engineering", the journal of systems and software, pp.97-107.

[15]FAO, and Oregon University, (2007), "Atlas of international agreements on fresh waters", UNEP, 2002.

[16]World Bank, (2012), "World Development Indicators, Washington".

AUTHORS PROFILE

Dr.Ahmed Omran

Dr. Ahmed Omran,is an Assisstance Professor in Faculty of Computers and information. Dr.Omran worked as a consultant for information and decision support systems in different national and multi-national organizations for more than 8 years, started his career in UN-FAO. After that he promoted to The Egyptian Cabinet, the Presidency of the Arab Republic of Egypt and League Arab States with increasing responsibility in consulting activities. Dr. Omran now is a member in SRGE (Scientific Research Group in Egypt).

Dr.Nisreen Laham

Dr.Nisreen Laham Researcher in Information & decision Support Center at the Egyptian Capinet. She worked as a researcher for futures studies in The Egyptian Cabinet for more then 10 years.

A Study on the Radio Spectrum Management in South Asian Countries: Challenges and Opportunities

Md. Kabir Uddin[1] and M Abdus Sobhan[2]

School of Engineering and Computer Science

Independent University, Bangladesh, Bashundhara, Dhaka

[1]kabiruddin@gmail.com

[2]sobhan30@gmail.com

***Abstract*— The enhancing cumbersome intricacy of wireless communications technologies and inclusion in a wide range of miscellaneous applications mean the related spectrum management issues are being more complex. Pursuant to this spectrum complexity relates equally to private and public sector use of the spectrum. Changes from an industrial to an informational based society and the associated demand for enhanced communications services push the need for seamless access further. It is likely that removing unnecessary regulatory distinctions between government and non-government spectrum will become increasingly important to maximize the overall benefit derived from use of the spectrum. Many applications of practical interest stem from the capability to monitor and store packet-level traces in a WiFi, WiMAX, 3G and 4G networks. In this approach, yields strong practical benefits, given the costs and complication of accessing network equipments, especially in the Radio Access Network as well as pondering of security. The author of this paper discusses the opportunities to exploit in and addresses challenges faced by the key players in South Asian region and seeks the spectrum commons approach in South Asian countries and concludes that, even in the face of enormous challenges, the potential benefits and opportunities are noteworthy adequate to necessitate grim thoughtfulness by telecommunications policy–makers in their function as spectrum managers.**

***Keywords*— Spectrum, Regulatory, RFID, DSA**

I. INTRODUCTION

The world is appearing frequency spectrum forces as a scarcity of resource treating the spectrum like land. The regime in which spectrum is allocated by frequency or location or power to specific users can be thought of as a static control method "open loop control" for solving the interference problem. Radios for specific uses were engineered specifically for the frequency associated with the ITU [1] licenses and so avoided interference control method. Dynamic Spectrum Access Networks as well as cognitive radio networks will provide high bandwidth to mobile users via heterogeneous wireless architectures and dynamic spectrum assess techniques. The advent of technologies such as WiFi, WiMAX and more recently 3G & 4G, opened up opportunities for broadband access in license-exempt bands, at distances of various ranges. The Authority of South Asian Countries should issue a preliminary ruling on the use of cognitive radio and should convene technical meetings on the topic.

II. CHALLENGES AND OPPORTUNITIES

A. Incorporated Wireless Network

Notwithstanding several wireless communication systems, like Cellular, WiFi, WiMAX and 3G, have developed independently, they should be integrated for seamless access by users. Consequently, in recent years, Cellular/WiFi integrated networks [2], [3] and WiFi/WiMAX integrated networks [4], [5] have been researched actively. In particular, a WiMAX/WiFi integrated network can achieve high-quality communications by using WiMAX and WiFi as complementary access resources. This integrated network enables load balancing between WiMAX and WiFi by using each system selectively in response to the demands of users and the condition of each system. However, this integrated network assumes that each wireless system uses the spectrum band prescribed by law, so that, even if the WiMAX system has unused spectrum temporarily, it cannot be used by WiFi systems. As a possible solution to this problem, cognitive radio is receiving much attention.

B. Intervention

An immense accountability for seeking apposite spectrum and curtailing the interference caused to, and received from, other users. By employing techniques like as intensified frequency re-use, "cognizant" radios, intervention avoidance/cancellation, "smart" antennas, space-division multiplexing and a host of other techniques, in that ways spectrum can be shared on a much more efficient, opportunistic and real-time basis, thereby dramatically increasing the capacity of the resource. Interference among these multiple paths would be avoided by using sophisticated, highly directive, multi-beam antennas and other techniques.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C. The Spectrum

3G spectrum— 120 MHz—stems from two hotly contested decisions in connection with spectrum in the 1.7 and 2.1 GHz bands. Another 130 MHz (or more) of spectrum is now available for broadband mobile services in the 2.5–2.7 GHz band as a result of the existing wireless cable or Multichannel Multipoint Distribution Service (MMDS) and instructional TV (ITFS) licensees to use all of their spectrum to serve mobile devices as well as fixed locations [6].

D. Dynamic Spectrum Access (DSA)

In connection with [7], DSA strategies can be classified in terms of three models namely- the Dynamic Exclusive Use Model (DEUM), the Open Sharing Model (OSM), and the Hierarchical Access Model (HAM), which are depicted below.

1) Dynamic Exclusive Use Model (DEUM): The use of this model hinders the present spectrum regulation policy, in which spectrum bands are licensed to services for exclusive use. The main idea is to commence flexibility to advance spectrum efficiency. Two approaches have been proposed under this model, namely, spectrum property rights and dynamic spectrum assignment. The former approach allows licensees to sell and trade spectrum and to choose freely between technologies. The economy and the market will therefore play major roles in driving towards the most profitable use of this limited resource. On the other hand, the latter approach aims to improve spectrum efficiency through dynamic spectrum assignment by exploiting the spatial and temporal traffic statistics of the various services.

2) Open Sharing Model (OSM): This model employs open sharing among peer users as the basis for managing a spectral region. Advocates of this model draw support from the phenomenal success of wireless services operating in the unlicensed Industrial, Scientific, and Medical radio band.

3) Hierarchical Access Model (HAM): This model adopts a hierarchical access structure with primary users (licensees) and secondary users. The key idea is to open licensed spectrum to secondary users while limiting the interference perceived by primary users. Two approaches to spectrum sharing between primary and secondary users have been considered, namely, spectrum underlay and spectrum overlay. The former approach imposes severe constraints on the transmission power of secondary users so that they operate below the noise floor of primary users. By spreading transmitted signals over a wide frequency band (i.e., using an Ultra-Wideband system), secondary users can potentially achieve short-range high data rates with extremely low transmission power. Alternatively, the latter approach does not necessarily impose severe restrictions on the transmission power of secondary users, but rather on when and where they may transmit. It directly targets spatial and temporal white space in the spectrum by allowing secondary users to identify and exploit local and instantaneous spectrum availability in a nonintrusive manner.

E. Harmonization of RFID Frequencies

Nonetheless DSA, Harmonization of RFID is more significant to have spectrum available in all relevant markets if it is to work in South Asian Countries. While harmonized frequency bands for RFID systems are important, it is also important to have a workable authorization regime and licensing framework for each of the relevant markets when harmonization is not practicable. There could be benefits in reduced costs to harmonizing spectrum on a global basis in a small number of frequency ranges. On the other hand, using more complex hardware and software, it is technically possible for individual tags and readers to operate with multiple frequency bands within different markets. It is vital to give manufacturers and operators flexibility in spectrum options, particularly for the diverse set of RFID applications [8].

F. Co-ordination with South Asian Countries

The effective use of radio spectrum will typically require careful co-ordination with neighboring countries in South Asian Countries, to intricate the extent of harmful interference. The Government must weigh up the benefits of co-ordinate and harmonized use of spectrum across South Asian neighbor countries against the constraints which this imposes on spectrum management. South Asian markets 3G and other mobile broadband technologies are commonplace. There are very high penetration rates of Smartphones and tablets, relatively high Average Revenue Per User (ARPU) and a highly competitive market. The result is a staggering increase in network traffic without a corresponding increase in revenue - a trend that cannot be sustained. The solution to this needs to include creative ways to break out of the flat-rate tariff model while creating mobile plans that make sense to the subscriber. Developing markets such as Indonesia, India and Bangladesh have very large populations and lower ARPU. The rapid increase in Smartphone penetration, not higher usage, is what driving data traffic volumes on 3G networks. Innovative pricing and packaging is not top priority - their challenges are based on pure scalability, efficiency and operational cost structures.

G. Satellite Radio

To create the Satellite Digital Radio Service (SDRS), a comparatively small amount of spectrum (12.5 MHz) was awarded to each of two licensees, now known as XM Radio and Sirius. Both companies began to roll out service in 2002. With each MHz of SDRS spectrum able to deliver at least ten

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

channels of CD quality across the United States, the radio business will be transformed.

H. Regulatory Failure

The reasons of regulatory failures may arise from:

- the lack of information available to the regulator about the costs, revenues and economic trade-offs facing business, government entities and individuals;
- the cost of analyzing data may be prohibitive for the regulator;
- changing technology and demand, which makes it difficult for the regulator and regulation to keep pace with change;
- a lack of incentives for the regulator to make the right decisions, compared to those for industry;
- overly stringent rules by the regulator that hamper innovation and prevent resources from being use in the most valuable way;
- excessive complexity;
- risk aversion; for example, the desire to eradicate rather than manage risk;
- the creation of distortions; that is, the creation of incentives that result in diversion of resources to less efficient activities; and
- regulatory duplication; that is, more than one scheme designed to produce the same outcome.

I. Cost and Affordability

In accordance with 4G Network cost and affordability are a number of issues to consider that reflect some degree of risk, as well as opportunity, so that these networks are successful once rolled out to the general public, and in general, 4G Networks are designed in order to create an environment that supports high-speed data transmission and increased profit margins for organizations that utilize these capabilities. Developing a successful 4G Network platform is a positive step towards the creation of a wireless and broadband environment that possesses rapid transmission speeds, data integrity modules, and other related events that encourage users to take additional risks in promoting successful utilization of these 4G tools.

J. Capabilities and Features

Even though the 4G Network platform is not brand new, many telecommunications providers have not yet developed their own alternatives that will support this network in full. 4G is intended to replace the current 3G systems within few years. The ambitious goal of IP based 4G, unlike 3G is to allow the provided connection with higher bandwidth, data rate, lower authentication overhead, and will ensure services constantly without any interruption to Internet users to access all type of services including text, databases, and multimedia. This feature makes to have incorporated infrastructure of all current networks and consequently will be easier to have access services and applications regarding the environment in South Asian. Accessing 4G networks will be possible virtually by using any wireless device such as PDAs, cell phones, and laptops.

K. Grand Challenges of Security and Privacy

The heterogeneity of these 4G wireless networks exchanging different types of complicated data to blanket very wide geographic area (considering in South Asia) with seamless service with the core addresses mobility, security, and QoS through reuse of existing mechanisms while still trying to work on some mobility and handover issues is to be safety [3]. Therefore, it is necessary for the organization to develop an effective series of tools that support maximum 4G security measures as a means of protecting data that is transmitted across the network from hackers and other security violations.

Furthermore, the encryption and decryption methods being used for 3G networks are not appropriate for 4G networks as new devices and services are introduced for the first time in 4G networks. To overcome these security and privacy issues, two approaches can be followed. The first is to modify the existing security and privacy methods so that they will be applicable to heterogeneous 4G networks. Another approach is to develop new dynamic reconfigurable, adaptive, and lightweight mechanisms whenever the currently utilized methods cannot be adapted to 4G networks.

L. Grand Challenges of Quality of Service (QoS)

With respect to network quality, many telecommunications providers are promising there will be enhanced connectivity, and the quality of data that is transmitted across the network will be of the highest possible quality, as in the case of Ericsson's 4G Network for TeliaSonera. The main challenges to 4G networks are integrating non-IP-based and IP-based devices. It is known that devices that are not IP address based are generally used for services such as VoIP. On the other hand, devices that are IP address based are used for data delivery. 4G networks will serve both types of devices. Consequently, integrating the mechanisms of providing services to both non-IP-based as well as IP-based devices is one of key challenges 4G networks have to address.

M. BWA Market in South Asia

South Asia is not only the largest and the fastest growing broadband wireless market globally but also encompasses the broadest array of new technologies. Of all the current 337 HSPA (High Speed Packet Access) networks tracked by the GSM association (GSMA), 21 percent are in South Asia; of all the 592 WiMAX networks tracked by the WiMAX Forum, nearly 20 percent are in South Asia [9].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE I

CLASSIFICATION OF THE ASIAN BWA MARKETS

Classification	Market definition	Markets
The leaders	100% + mobile penetration and advanced 3G/HSPA networks	Australia, Japan, Korea, Hong Kong, Singapore, Taiwan and New Zealand
The giants	Large population countries with room for increasing mobile penetration, nascent 3G/HSPA networks, and potential for WiMAX adoption	China, India and Indonesia
The emerging markets	Room for increasing mobile penetration and nascent 3G/HSPA networks with extensive promise for WiMAX adoption	Philippines, Malaysia, Thailand, Vietnam and Bangladesh

Pursuant to this, clarified issues are proper Spectrum Management will make more opportunities like employment, revenue, GDP in South Asian countries with a cooperative pattern.

N. Recommendation

To develop and apply a harmonized policy framework for the management of the radio spectrum to include allocation, assignment and licensing and would take into consideration the consumer demands for new services, technological developments, the various stages of telecommunications developments and the peculiar circumstances [10]. The core principles of spectrum management would be achieved in order to:

- Maximize the efficient use of radio spectrum
- Ensure that spectrum is made available for new technologies and services, and flexibility is preserved to adapt to new market needs
- Develop a fair, efficient and transparent process for awarding licenses
- Make allocation and licensing assignments based on marketplace demands and other appropriate means
- Promote competition
- Ensure that spectrum is available for important public benefits (i.e. safety and health).
- New spectrum requirements should be met through the market in all but exceptional circumstances.
- Pricing mechanisms should be used to ensure that the value of spectrum is reflected in the fees paid by public sector users.
- Band-sharing should be pursued as far as possible, with fee reductions available to reflect the value of sharing permitted.

South Asia's market size geographical diversity and divergent market dynamism are creating test beds for the technical standards and business cases for BWA. The developments in South Asia will likely provide key indicators and, in some cases, the necessary volume, or carrier innovation, for global adoption. One sixth of the world's mobile phones are in China and India alone. If China continues to favour its own 3G (and future 4G) standard over WiMAX this could tip the balance for the future of BWA while India's stance on 3G technology adoption also has great potential to impact market dynamics.

Industry estimates also show that Asia will soon be the top region for BWA video consumption and, by 2017, this region is predicated to generate over half (53%) of all traffic, followed by Europe (26%) and North America (14%). These estimates can be explained by the fact that wireless broadband has been the widely chosen option for broadband connectivity across many of the South Asian countries.

III. BUSINESS ALIGNMENT IN SOUTH ASIA TO SUPPORT BWA BUSINESS MODELS

BWA can be used to support the delivery of data services such as SMS, IM and email which typically have been maintained as discrete VAS products managed at the marketing level with little interaction across other business departments. Operators may now start the business model in response both to their desire to achieve revenue growth from BWA services and to respond to the increasingly competitive and margin-stressed industry for their traditional services. The following are some of key considerations when transforming business operations to support the BWA business models in South Asia [11].

- Simplification and rationalization of the legacy product portfolio can be accomplished as part of the business transformation program to support BWA operations. A robust product profitability review and retirement of legacy products should be examined. In conjunction with the overall business transformation such product rationalization can serve to improve the overall customer experience and lower costs to serve.
- Customer-centric management of BWA resources, including the horizontal mobilization of technical and business personnel for planning, marketing, operations and customer relationship management.
- Achieving procurement and supply chain excellence is of utmost importance for a multi-channel approach to the procurement of services, including the management of content Intellectual Property Rights (IPRs) and Digital Rights Management (DRM).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Effective vendor management and partner selection become key components of an enhanced Supply Chain function.

- Shifting sales and marketing focus from discrete and bundled services to converged multi-channel services.
- Implementing pricing structures and billing systems those offer both mult-channel options and third party OTT access pricing and revenue sharing.
- Management of data warehousing, customer profiling, real time data integration and analysis for location-based services.

IV. Conclusion And Future Works

The size of 3G market in Latin America will grow to $112.97 billion in 2017 from $79.56 billion in 2011. Growing importance of mobile broadband and bundled services will propel the market to ensure 6 percent annual growth during the period, and the coverage and quality of mobile broadband services combined with the high penetration of mobile devices have driven the telecom operators in South Asian to offer services of high added value [10]. A report from Beijing-based research company Analysys International, the penetration rate of 3G in China could be more than 20 percent by the end of the year. With the emergence of WiFi, WiMax 3G and 4G, broadband wireless telecommunications have been spreading all over the world at an exponential rate. The extensive use of radio spectrum everywhere created challenges for the reduction of interference through smart spectrum management practice. New challenges evolve for the harmonization of new standards and technologies introduced by different operators and organizations. The new challenges of addressing the cross-border issues between neighboring countries in South Asia demand strong international cooperation. Unbounded opportunities have been opened up through the applications of broadband wireless communications for realizing Wireless World Wide Web (WWWW) or Internet connectivity for the rural people. This will bring unprecedented changes in the socio-economic conditions of rural populace. At this moment, the telecom regulators all over the world are puzzled with the WiMAX, 3G, and 4G and beyond licensing policies and implications. The BTRC of Bangladesh is also planning to develop a good 3G and 4G licensing policy to open up unbounded opportunities for its people through appropriate use of the Wireless Internet. In future work, it will be necessary to propose a spectrum-sharing method that considers QoS issues for network traffic.

References

[1] International Telecommunication Union- http://www.itu.int
[2] W. Song and W. Zhuang, “Resource Allocation for Conversational, Streaming, and Interactive Services in Cellular/WLAN Interworking,” IEEE GLOBECOM ’07, pp. 4785–4789, (Nov. 2007).
[3] W. Song, W. Zhuang, and Y. Cheng, “Load Balancing for Cellular/WLAN Integrated Networks,” IEEE Network, vol. 21, no. 1, pp.27–33, (Jan.-Feb. 2007).
[4] L. Berlemann, C. Hoymann, G. R. Hiertz, S. Mangold, “Coexistence and Interworking of IEEE 802.16 and IEEE 802.11(e),” Vehicular Technology Conference, vol. 1, pp. 27–31, (May 2006).
[5] D. Niyato, E. Hossain, “Intergration of WiMAX and WiFi: Optimal Princing for Bandwidth Sharing,” IEEE Communications Magazine, vol. 45, no. 5, pp. 140–146, (May 2007).
[6] Infocomm Development Authority of Singapore (IDA) - http://www.ida.gov.sg
[7] M. Nekovee, “Dynamic spectrum access - concepts and future architectures,” BT Technology Journal, vol.24, no.2, pp. 111–116, (Apr. 2006).
[8] Federal Communications Commission (USA) -http://www.fcc.gov/
[9] KPMG International, Broadband Wireless in Asia Pacific, 2010
[10] CIA World Factbook: http://www.cia.gov/library/publications/the-world-factbook/geos/bg.html
[11] SKT and StarHub Analysis: http://www.kpmg.de/docs/Broadband-Wireless-Access-in-Asia-Pacific-O-201009.pdf, visited date June 6, 2013

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

On the Implications of Current Radio Spectrum Management Issues in Bangladesh

Md. Kabir Uddin[1] and M Abdus Sobhan[2]

School of Engineering and Computer Science

Independent University, Bangladesh, Bashundhara, Dhaka

[1]kabiruddin@gmail.com

[2]sobhan30@gmail.com

***Abstract*— The brisk and mammoth yield of wireless mobile community, coupled with their demands for high speed, wideband, multimedia services, stands in clear contrast to the limited radio spectrum allocated in international agreements. Advanced mobile services combine the innovation potential of reckoning, data communications, and the wireless industry. So, Current Radio Spectrum Management (CRSM) [1] remains as a key challenge to the efficient engineering of mobile wireless networks. Different types of innovation scenarios can be distinguished, depending on the constellation of sunk cost and the cost of coordination between suppliers along the value chain. No single spectrum management framework supports all equally well, although spectrum use markets seem to be most broadly compatible. A mixed approach is possibly superior to any given individual class of spectrum management. Broadening the literature on spectrum policy, the author of this Paper focuses on implications and issues of Current Radio Spectrum Management regimes for rolling out in mobile services in Bangladesh with the current status of Radio Spectrum Management (RSM) polices and outline the key issues in RSM for next generation mobile wireless networks although the development of 3G in many countries new directions are being researched.**

***Keywords*— CRSM, RSM, QoS, ISM, Spectrum**

I. INTRODUCTION

In the contemporary world, Bangladesh emerging 3G, 4G mobile data services and mobile computing will enhance the existing services by blending the extraordinary innovation potentials of the wireless, reckoning and digital information industries. In Bangladesh, 97% of the householdes have mobile device, 65% people use mobile phone [2] alongside within 2014, financial value of mobile applications will be more than 30 billion in the global market [3]. Visions as to the unlimited opportunities of new wireless platforms (e.g., meshed networks), intelligent devices (e.g., agile radio), and ubiquitous wireless applications, captured in the notion of pervasive computing, abound. The author anticipates that by 2030 mobile data communications will generate more than twenty percent of the revenues of wireless service providers. In Bangladesh mobile devices rather than PCs or laptops may become the primary internet access tool. Despite the limitations of the present wireless platforms, most importantly fairly limited bandwidth, the number of mobile internet users is growing rapidly. Network operators are currently upgrading their networks to platforms that provide higher bandwidth and will support more advanced multi-media applications. Evolutions of the present "second generation" (2G) of mobile services, often termed "2.5G" services, can provide up to 171.2 kbps and are better suited to deliver mobile data applications, including basic internet access. A few network operators have begun to offer "third generation" (3G) services, which are designed to provide 384 kbps in a fully mobile and up to 2 Mbps in a stationary environment, which is sufficient to allow video streaming and other multimedia applications. Wireless local area networks (e.g., WiFi or Hiperlan) which in most countries even Bangladesh are operated in unlicensed spectrum bands and can provide up to 54 Mbps, are deployed to provide local connectivity. Mobile network operators were only lightly or not at all regulated. One of the crucial issues in the wireless industry is the framework put into place to govern spectrum access and use. The proliferation of wireless applications and services has put great strain on the traditional system of administrative licensing and revealed its shortcomings. Many countries have introduced spectrum auctions to accelerate the assignment of licenses. However, these limited reforms have created new problems and more fundamental changes in spectrum management are being considered. It also reduces barriers to new operators and new services as it makes a better use of available spectrum, which is especially important for limited spectrum suitable for mobile applications. To improve end-user affordability, especially for broadband services because the cost of service delivery is directly reflected in service pricing, and the cost of delivering broadband services is higher than cost to deliver voice only. As we are moving towards the next generation (WiMAX, 3G, 4G) of mobile systems, the need for improving coverage, systems capacity and service quality becomes more and more important.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. Current Radio Spectrum Management Issues and Implications

A. Approaches of Spectrum Management

With the remarkable growth in applications for licenses, the weaknesses of the administrative approach, including long delays, the impossibility for the government to pick the most promising proposals, and the lack of economic incentives to use spectrum efficiently, became evident. In response, many nations began to experiment with more flexible forms of licensing. Some countries have started to fundamentally overhaul the system of spectrum management and to search for more adequate alternative frameworks. Of the range of options, the author reviews five categories, of which all other variants are subsets: administrative licensing, flexible licensing, ownership, spectrum commons, and open access. These regimes differ with regard to the nature of rights they bestow and other important dimensions of spectrum management (Table 1).

TABLE I
ELEMENTARY FEATURES OF SPECTRUM MANAGEMENT REGIMES [4]

	Administrative licensing	Flexible licensing	Ownership	Commons	Open access
Rights	Exclusive	Exclusive	Exclusive	Quasi-exclusive	Non-exclusive
Allocation	Government planning	Government planning	Endogenous (owners), government	Endogenous (users), government	Endogenous (users)
Assignment	Administrative process	Auction	Auction, market transactions	Auction of usage rights, users	None
Dynamic adjustment	Government planning	Government planning, licensees	Market transactions	Auction of usage rights, users	Users
Interference protection	Government planning, queuing	Government planning	Ownership rights	User-defined rules	Protocols, etiquette rules
Congestion management	Government planning, queuing	Government planning, queuing	Owner-defined protocols, queuing	User-defined protocols, queuing	Protocols, etiquette rules, real-time auctions
Selection in case of competing uses	Government planning	Government planning	Market transactions	Government, users, technology	Technology, voluntary standards

Three of the five regimes (administrative licensing, flexible licensing, and ownership) grant exclusive rights to the licensee, although they are structured differently. Pro forma, a license only grants temporary usage rights but not ownership. In a spectrum ownership model, full property rights would be established, granting owners not only a right to use but also a right to leave spectrum unused, to lease it to third parties, to sell it, or to give it away. These three models continue to be based in the paradigm that exclusive control of a communications channel is a necessary prerequisite for interference avoidance. In contrast, spectrum commons would grant usage rights to a well-defined group. They establish exclusive rights with regard to the external environment but shared use within the commons. Open access models allow anybody meeting certain minimal conditions, which are established to avoid interference and reduce congestion, use of spectrum.

B. Comparative Properties of Spectrum Management Regimes

Although under ideal conditions, administration could yield an efficient outcome, the practice of spectrum management is far from it. For example, large swaths of licensed spectrum remain underutilized ("white spectrum") while other bands are crowded. The administrating agency often lacks the information to judge alternative proposals and licensing is therefore often politicized, slow and plagued by inefficiencies. The proliferation of potential wireless applications has led to an explosion of license applications and has multiplied these problems. In response, agencies have introduced more flexible approaches to spectrum allocation and replaced the traditional, time consuming "beauty contests" with auctions. Spectrum auctions can be considered the major innovation in spectrum policy during the past decade. They allow the placing of a market value on spectrum, are transparent and not easily prone to political manipulation. In our context it is most important that auctions result in upfront spectrum fees that constitute entry cost into the mobile market. These upfront fees may increase the incentive of the licensee to pursue a "walled garden" strategy to enhance the chances of cost recovery. Poorly designed auctions can also increase the pressure towards industry consolidation and further reduce the number of gateways between application and service providers and users. One approach is used in the three unlicensed bands that are currently available in the Bangladesh 100 MHz of spectrum in the 2.4 GHz range, known as the Industrial Scientific and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Medical (ISM) band, is designated as unlicensed in the Bangladesh and in many other countries. Several MHz spectrums are in the 5 GHz band as the unlicensed national information infrastructure. Proposed another 255 MHz spectrum is in the 5.470-5.725 GHz band [5]. Users of these unlicensed bands have to comply with "etiquette rules", technical specifications, such as power limits or communication protocols intended to eliminate interference.

C. Spectrum Management and Market Organization

An unresolved issue is the transaction cost associated with the untested regimes. The different spectrum management regimes constitute particular sets of ownership and disposition rights whose implications for the evolution of mobile communications can be subjected to systematic analysis. Spectrum management directly affects the organization or the network platform and indirectly the opportunity set of vertically related industries. However, spectrum management does not fully determine industry performance but interacts with other factors. Among these are business strategy (e.g., the extent to which suppliers create modular technology), the cost and demand conditions of services, and public policies other than spectrum management (e.g., third party access rules, standardization). The most visible effect of the spectrum management regime is on the number of gateways to subscribers. In exclusively licensed services, this number is fixed by the government. Spectrum management also affects the cost of entering the market, a second determinant of the horizontal and vertical industry structure. Entry costs, in particular if they are sunk have an effect on market structure as higher sunk entry costs typically lead to a higher market concentration. With rival uses for spectrum, at least in some bands, it is widely seen as desirable to reflect the opportunity cost of spectrum. An increasing number of countries have therefore introduced spectrum fees, either determined administratively or in a spectrum auction. It is the latter, one-time fees that have raised concern as the present model of exclusive rights may create distortions that contribute to deviations between the opportunity cost of spectrum and the sunk price paid for a license. These potentially undesirable effects can be mitigated if a secondary market for spectrum is established, which would allow reducing the sunk portion of the one-time fee.

D. The Spectrum, Pricing and Analysis

The 700 Megahertz (MHz) spectrum – considered the most valuable at present – for mobile operators and will enable service providers to deploy higher-performance mobile broadband services over greater distances than the services they offer today. As a result, the operators will be able to roll out their service network with less equipment or investment for more people. In line with the suggestion of the International Telecommunication Union (ITU), Bangladesh can allocate 700 MHz band for fourth generation (4G) mobile technology – Long Term Evolution (LTE) – which provides far more speed data transfer than 3G technology. Its broadband attractive physics – like its ability to penetrate walls – the spectrum has become desirable yet again for broadband communications, particularly mobile broadband.

TABLE II

3G AUCTION PRICES IN ASIAN COUNTRIES 2001-2013 [6]

Countries	Number of Licences	Band MHz	Year of Licence	Spectrum Price (USD, Million)	Duration of licence in Year	Spectrum Price per licence per year (USD, Mill)
Indonesia	3	800, 900, 1800, 1900, 2100	2006	120	10	4
Singapore	3		2001	218.4	20	3.64
Hong Kong	2		2011	243	15	8.1
	4		2001	671	15	11.183
Pakistan	5+		2013	873 (target)	15	11.64
Bangladesh	5		2013	525	15	7
India	7		2010	11751	20	83.93
Taiwan	5		2002	1397	16	17.46

3G is not just the access to mobile broadband, it has a cascading role in the economy through e-health, e-agriculture, e-education and employment. At present the mobile operators of Bangladesh have 11 percent 3G handset users. The 3G and BWA spectrum auctions held in 2013 and 2008 consecutively and added approximately USD 621 million to the exchequer. Globally, wireless spectrum auction prices are measured using "$/MHz/Pop" benchmark. This is defined as "price paid in US Dollars ($) per Megahertz (MHz) of spectrum for providing wireless service to one person (Pop) in the license area". This auction pricing benchmark is determined by four key parameters:

- Spectrum Characteristics
- Spectrum Regulation
- License Area Characteristics and
- Auction Structure

While the $/MHz/Pop for 3G spectrum auction in India was one of the lowest in the world (at $0.32), the price for BWA spectrum was one of the highest (at $0.12), closely followed by Switzerland's (3.4 GHz & 2.6 GHz) auction price. As the government is in the process of drawing up guidelines and structure of 2G spectrum auction, carriers have given their recommendations regarding the auction structure to the regulator. How auction will be structured and the various strategies adopted by both incumbent and new carriers in acquiring the spectrum, and most importantly, the manner in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

which (if at all) the premium will be passed on to the end consumers.

E. Spectrum Management and Innovation

It is now possible to analyze the nexus between spectrum management regimes and innovation processes. This means that there is a link between spectrum policy and innovation in mobile services but it is mediated by other intervening factors. As a result, a particular spectrum management regime is neither sufficient nor necessary to achieve a certain outcome. If technology were exogenous to the spectrum management regime, there would be a "correspondence" between the types of innovation and investment processes and the most conducive spectrum policy. The task for policy-makers would be to find the regime most conducive to the prevailing technology. However, if technology is endogenous to spectrum management, this relation becomes recursive and spectrum management also shapes the path of innovation. Nevertheless, spectrum management influences the relations between the layers in the value chain and thus potentially the locus of innovation. A first understanding of the relations can be developed under the (strict and unrealistic) assumption that technology is exogenous to the spectrum management regime. The level of investment and the rate of innovation will be influenced by the appropriately conditions. Among the factors influencing appropriately of a risk premium is the ability of a supplier to achieve competitive advantages, for example based on the value generated for users, service functionality and design, or patents. Nonetheless, it will influenced by the ability of a service provider (e.g., network operator or device manufacturer) to ascertain access to sufficient spectrum to maintain the promised quality of service. This is essentially a demand for the use of spectrum space. Open access regimes are based on the promise that technology will assure sufficient spectrum availability [7]. As this proposition is afflicted with uncertainty, investors and innovators will demand a higher return compared to a situation in which they can assure spectrum use.

If technology is flexible, the prevailing spectrum management framework will shape its path. A system of exclusive rights will strengthen the position of the rights holder in the value chain. This does not necessarily have to be the network operator but could also be another player in the value chain, such as an equipment manufacturer or a mobile portal. Past experience reflects this fact, with investment and innovation organized by network operators in licensed and by equipment manufacturers in the unlicensed bands. The establishment of upfront license fees, as is typical for the present auction model and some visions of the ownership model that would use auctions as an initial assignment mechanism, has further implications. Notwithstanding, the entry cost aspect of license fees will strengthen the incentive of the rights holder to limit the number of participants in vertically related markets to enhance revenue and profit opportunities. The spectrum management approach also affects the overall dynamics in vertically related markets. A widely shared view is that open access models will increase the number of gateways to users and thus stimulate innovation in vertically related applications and services markets.

The empirical experience with alternative spectrum management regimes is fairly limited but it is interesting to take a look at recent cases of major innovations in mobile communications. The hitherto most successful examples of mobile internet services – imode in Japan and Nate in Korea – are "innovation systems" based on close cooperation between networks service providers, manufacturers, and service providers. This business model is characterized by high sunk costs and relatively high coordination needs and it seems that the combination of exclusive control of spectrum, a proprietary technology platform to organized the business processes, and a modular interface with the network that enabled content creation, have facilitated its growth. The proprietary network platform seems to have facilitated the appropriation of innovation rents. This does not imply that exclusive control over spectrum is a sufficient condition for success as the example of the European UMTS platform indicates.

One of the key questions is the relation between these emerging applications and services that are characterized by higher sunk and coordination cost. To a certain degree, applications in these bands, such as WiFi or Bluetooth, are complementary to solutions offered by licensed service providers but to a certain degree they are also substitutes. First, WiFi has a much lower range and especially the 5 GHz services are susceptible to obstacles. So far, WiFi does not provide mobility and there are serious security issues. Moreover, the different unlicensed technologies do not co-exist in a benign fashion and interference problems persist (e.g., between Bluetooth and 802.11b). If use increases, interference protection and coordination of uses may become a serious challenge. However, it is possible that these issues can be addressed by means of innovative technology. Possible options include voluntary standardization, appropriate network topologies (e.g., standardized IP access points that could serve as traffic controllers in case of congestion), or etiquette rules developed by the users.

F. Recommendation and Grand Challenges for Bangladesh

Their data business will take a few more years to turn viable as some related factors—such as 3G-ready handsets, local contents and awareness of internet – are still not widespread in the market. 3G licence in an auction on September 8, 2013, and the regulator handed over the licenses to the all (5 operators).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The data business will take time to pick up in Bangladesh though voice will always remain very important and Internet is not just a way of communication or an entertainment tool, rather it has to be a part of the business process. It is about connecting institutions and making the business process more efficient and upgrading productivity.

TABLE III

SELECTED REGION 3G USERS AND PENETRATION [6]

Area	2009	2014 (Projections)
Western Europe	39%	92%
Eastern Europe	9%	40%
North America	38%	74%
Asia Pac (without Japan)	7%	37%
Japan	91%	100%
Middle East & Africa	7%	35%
South & Central America	4%	17%
Global	15%	43%

There is a huge opportunities, particularly in the sectors such as education, health and agriculture, and a lot of contents will have to be developed in these sectors to make the 3G and 4G technology a hit, In contest of Bangladesh perspective it will not only drastically increase internet speed, but with it the number of internet users in the country, which is currently at only eight million, most of whom use narrowband mobile internet. The service in particular and digitisation of the nation in general will contribute significantly to socio-economic development not to mention the opening up of a wide, brighter world of infotainment for users. The operators should keep their tariffs affordable so everybody can use high-speed internet and another significant issue is training – to access certain mobile services. This diversity of the Bangladesh gives rise to a number of constraints and points to some critical needs as regards spectrum management. The following constraints currently exist:

1. Limited financial and human resources for effective national spectrum management
2. Insufficient experienced persons trained in such areas as international conventions and regulations
3. Inadequate institutional arrangements to deal with the evolving spectrum issues resulting from the proliferation of wireless technologies
4. Insufficient information on spectrum management best practices
5. Lack of central coordination of spectrum management in Bangladesh
7. Independently evolving regulatory practices
8. Varied legal and regulatory Frameworks
9. Lack of coordination and resources to analyze and solve problems of interference between neighboring countries
10. Diversity and difficulties in pricing regimes
11. Dissimilar spectrum allotment/assignment in several bands

III. CONCLUSION

We have increased the tele-density from 30% to 64% and internet density from 3% to 27% [3]. Data business will become viable in Bangladesh faster than that in its neighbours. Different institutions, both private and public, have already shown interest in internet. Educational institutes are developing contents for their students, while other sectors such as health and agriculture are also getting ready. Bangladesh Bank has tightened the policy on mobile financial services. The number of mobile banking accounts in Bangladesh has nearly double since March 2013 to 7.21 million [8] over 100 million mobile phones are now in use in Bangladesh, a country of 152 million. Launched in 2011 by the two private sector banks, mobile phone-based financial services in Bangladesh have well outpaced Pakistan within two years, where it was introduced in 2009. State-run Teletalk is a limited private mobile company like the other mobile companies but by the prejudice of government has been offering 3G services on a trial basis since October 2012 but failed to create enthusiasm among users due to inconsistent service. Although there is a strong push towards privatization, spectrum policy can pick from a much broader range of options. The alternative approaches define characteristic sets of property and disposition rights and influence investment and innovation processes in the wireless industry in complex but tractable ways [9]. Market-based, commons, and open access models have unique advantages and disadvantages and are compatible with different types of innovation processes. The author indicates that a framework of spectrum use markets is fitting most broadly with the various innovation scenarios. Nevertheless, too little is known about the relations. The insights suggest that a mix of approaches would be the superior overall framework. This goal could be realized in two principal ways, by dividing spectrum space vertically or horizontally. The alternative is to create different regimes in designated bands. This raises the complicated and as yet unresolved question as to how the bands should be allocated. One of the central problems of spectrum management then is to find an institutional mechanism to determine this mix. The past administrative planning approach has not worked well. Ideally, an efficient meta-mechanism should be used to determine the mix of spectrum regimes. To do this effectively, one would need a metric to compare the different regimes. At least in principle, spectrum markets could solve these issues, although such an approach would be incompatible with open access even in the event that a market price would be zero. However, there are important differences between a market for spectrum ownership rights and a market for spectrum use rights. Another method would be to assess the value generated in each regime and to adjust its domain accordingly.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

[1] Antonelli, C (1992) The economic theory of information networks. In: Antonelli, C (ed), The Economics of Information Networks, pp. 5-27 Elsevier Science, Amsterdam
[2] www.btrc.gov.bd
[3] The Daily Star, February 3, 2013, Bangladesh
[4] Antonelli, C (2001) The Microeconomics of Technological Systems. Oxford University Press, Oxford
[5] Antonelli, C (2003) The aEconomics of Innovation, New Technologies and Structural Change. Routledge, London, New York
[6] Md. Kabir Uddin, "A Comparative Study of Spectrum Pricing for 3G and WiMAX", 2013
[7] Bar F, et.al. (2000) Access and innovation policy for third-generation Internet. Telecommunications Policy, 24:489-518
[8] The Daily Star, September 13, 2013, Bangladesh
[9] Md. Kabir Uddin and M Abdus Sobhan, "A Study on the Radio Spectrum Management in South Asian Countries: Challenges and Opportunities.", 2013

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cortex simulation system proposal using distributed computer network environments

Boris Tomaš [#1]

[#] *University of Zagreb, Faculty of Organization and Informatics, Pavlinska 2, Varaždin, Croatia*
[1] boris.tomas@foi.hr

***Abstract*—In the dawn of computer science and the eve of neuroscience we participate in rebirth of neuroscience due to new technology that allows us to deeply and precisely explore whole new world that dwells in our brains. This review paper is merely insight to what is currently ongoing research in the interdisciplinary field of neuroscience, computer science, and cognitive science.**

***Index Terms*—Artificial neuron, artificial neural networks, neuron simulation**

I. Introduction

There are many new and different approaches to the understanding of human brain, some use neuroscience/neurobiology to investigate biological characteristic of working brain. Those characteristics are well researched up to the level of molecules that form neurons and inter neuron connections synapses like described in [1]

Other approach for understanding human brain is creating simulations or even emulations of human brain using current achievements in the field of computer science. Those simulations use tremendous amount resources to simulate elements of human brain; simulations even go up to the level of simulating movement of single molecule. By this day there has not been successful simulation of entire human brain.[2] However, there are simulations of single columns of a human brains and full neural system simulation of lesser life forms like worm *Caenorhabditis elegans* that is a part of Open worm project[3]. Currently there has been some advances in simulating rat's brain.[4]

Important approach for this review is artificial intelligence (AI) which uses several techniques to implement some sort of artificial intelligence. These systems are used for decision making in financial institutions, they are being used in computer games for simulating opponents, and many more applications. AI uses many different approaches, one of it is neural networks of artificial neurons[5]. Others are complex expert systems that are capable of learning. However, AI research outputs agents that are specialized for resolving only specific problem for example AI using neural network for ballistic interception movement[6].

By this day there is no know AI agent that is being self-aware and intelligent enough to confront human intelligence[7]. However, there are intelligent systems, for example Watson that is miraculous piece of software that is beyond of human species regarding data processing, data mining, language recognition, processing and finally conclusion making[8]. This system only possess huge amount of data, and it relays on the data. In elementary school we are taught that intelligence is not equal to knowledge but this is ability of an entity how well it manages in new and unknown situations.[9] If you cut power electricity of Watson machine "he" will do nothing about it, next time he will simply reboot and will not complain or regret about being plugged out thus cease to exist.

II. State of the art

A. Computer science

The most relevant field of science for this research is computer science, especially areas of software development, software architecture, networking, AI, computing, grid computing, distributed computing, parallel computing. It is known that neural networks are used in decision making, for example in stock markets[10]. Current advancements in this field are very oriented towards better computing capabilities of neural networks, to provide better and faster results for decision makers. As being invented in late 1960[11] when computer power and our knowledge of working brain was not know enough, it can be easy assumed that this approach should be altered by incorporating more important concepts of human brain and it should be implemented using more advanced computer technologies as previously mentioned e.g. parallel computing, distributed or grid computing.

B. Neuroscience

Advancements in brain architecture, neuron architecture, neuroplasticity, connectome concepts[12], motoric related formation of neural networks, emphatic related formation of consciousness and many more are relevant areas of neuroscience. Although, many advancements in neuroscience have been made, there still are many unsolved problems relevant to this work[2]:

- How is consciousness formed?
- Where is memory stored and how it is retrieved?
- How does the brain transfer sensory information into coherent, private percepts?
- How are the senses integrated?
- How does previous experience alter perception and behaviour?

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C. Cognitive and other sciences

Swarm theory[13] uses examples from nature (ants, termites, birds,) to enhance computing techniques in computer science, again, to solve problems for e.g. decision makers., cognitive models, consciousness tests, consciousness models. Latest neural networks achievements thrive to understand how neuron can be simulated in order to provide better understanding of neuron and more importantly to improve computing and decision making. There is also hardware approach[14] that tries to implement concept of biological neuron on a microscopic level of integrated circuits. By this day, there are electronic chips that can communicate with real and living neurons in brain, this is one direction - human computer interfacing[15]; other is to create computer chips that process information the same way this information is processed in real biological neural networks

III. Relevant projects

There are several project that are relevant to this work:

A. Blue Brain Project[20]

The Blue Brain project represents an essential first step toward achieving a complete virtual human brain. The researchers have demonstrated the validity of their method by developing a realistic model of a rat cortical column, consisting of about 10,000 neurons. Blue Brain Project is collaboration between several universities in the world and industrial partners like IBM. Project goal is the simulation of human brain, not achieving an artificial intelligence in machines, however scientist do expect that some form of consciousness or intelligence might emerge. This project uses huge amount of resources from IBM supercomputers. Resources for each neuron are equal to single everyday laptop. This demand for resources come from fact that this project simulates every chemical characteristic of neuron.
In this paper () such use of resources is not necessary because not all neuron features are required for achieving intelligence, some features are required for biological achievability and sustainability.

B. Cajal Blue Brain Project[21]

This project is run by several Spanish institutions, it is a part of Blue Brain Project but has taken a different path. As Blue Brain Project it also thrives to simulate portions of human brain using software development on powerful supercomputers.

C. Nengo[22][23]

This project is carried out by Canadian scientists. Nengo is a software for simulating large-scale neural network systems. Largest simulation is carried out on super computers and is called Spaun. In Nengo, network architecture is designed in really nice and easy GUI. Positive thing is that Nengo project provides the visual input for the simulated brain: 28 x 28 pixels. Also they provide output for the simulated brain in the form of robotic arm. Real problem is that this hand is nothing less than a read only output, it could easily be a computer screen. There still does not exit correlation between input and output, like any dependence, something that enables Spaun to change the outside environment and that way influence its own state and conditions. Spaun neuron model, and network model has to be, in beginning set to solve specific problem. This means that when simulation starts it reads predefined values. This shows large intrusion in self determination of the network. In this work it is intended to simplify the model as much as possible, and let the neuron model organize its connections and in indirectly the network architecture.

D. Would digital brain have a mind?[24]

Nevile Holmes analyses reason why digital brain still does not have mind of its own or consciousness. Those reasons are:

- The activation of a classical neuron is not an arithmetic sum of the synaptic effects. Rather, a complex process involving the intervals between action potentials at individual synapses and their relative timings between synapses deter- mines the activation. The more neurons are studied the more such complexity is revealed.
- The human nervous system contains many different kinds of neurons and many kinds of glial cells. The glial cells provide more than support because they signal and have synapses just as neurons do.
- Action potentials alone do not control nervous signalling. Graded potentials and hormonal signalling also play a part, as does the great variety of different neurotransmitters and hormones. It is noticeable that author recognizes lack of biological importance to existing artificial neuron model.

IV. Research questions

Research has found that there is no artificial intelligence agent that is comparable to human intelligence[16]. Also, it is possible that some concepts from swarm theory can be used to explain formation of intelligence and consciousness in our brains. It is assumed, by some authors, that consciousness is a by-product of evolution process[17]. This knowledge can be used to create similar concepts in software. Swarm theory simply determines properties and functions, it does not explain why swarm intelligence emerges. This is hard to prove but not impossible.
There is common feature found in every swarm theory example it is the purpose there has to be a reason why entities form a swarm, and because of this reason swarm thrives to fulfil this reason more efficiently than the single swarm entity. The same principle can be applied to human brain and biological neural networks where our neurons form swarms with its functions (e.g. transferring action potential between neurons), but they need a reason to achieve swarm intelligence: that may be overall human intelligence with purpose to live and to survive. This is relatively philosophical issue that has been very well elaborated. Existing AI, neural networks, brain simulations do have a purpose: computing data, data mining, simulating intelligence in computer games,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

simulating brain activity etc. but none has the purpose to live, to survive or to become better. As by this date not AI agents or software in general has passed the Turing test, one of the famous tests is being held by Loebner test each year. Most "human like" AI agent receives an award, no agent has received maximum grade in this competition.[18] It believed that it is possible to implement such simple software nodes that have ability to communicate together (inside single computer node and over the networks like Internet). This single node will resemble to single artificial neuron in artificial neural networks, but it would not be the same, it will resemble more to biological neuron. That is, it will implement some newly discovered concepts from biological brains (neuroplasticity, temporal computing). On the other hand, purpose would not be to make simulation of living brain because simulating whole brain and its concepts require huge amount of resource. To minimize eventual use of large amount of resources intention is to include only significant features of living brain, for example not all brain features are required for forming of consciousness and intelligence, precisely, they are required in biological and chemical sense: for example synapses are one important biological feature but one of its main purposes is to make directional path between two neural cells to isolate action potential propagation. This is not required in software because directions can be created differently like using linked lists or other pointer usages. Network architecture is not relevant for artificial networks, but it is for biological neural networks. Only important feature in neural networks is that they can encode information as unique sequence of neurons, something very similar to hash functions. To prevent overload of data, thus lack of space to store data some processing should be done to purge irrelevant data, in biological sense this is called forgetting, we forget simply to purge our brain of not necessary information, along with forgetting some scientist find dreams ways of purging irrelevant data and confirming data that is important.[19] Interesting questions is why does interaction between encoded information (in node sequences) emerges intelligence and/or consciousness? There is apparently huge gap between neuroscience and artificial intelligence because in 1960s that gap did not existed, researchers created artificial neuron based on current knowledge of biological neuron. As the years have passed by, more neuroscience discoveries were made and we now know much more than 50 years ago, on the other hand artificial neurons and artificial neural networks (ANN) went in directions of computing and data processing. Over time this gap became significant. However, there are attempts to create simulations/emulations, later in further sections. General purpose of this work is to try to fill this gap by designing new artificial neuron model with selective characteristic (of biological neuron) that can coexist in modern computer systems and is capable of communicating in computer networks like Internet.

1) Is it possible to create model of artificial neuron (node) that is capable of network communication (using custom protocol)?
2) Is it possible to create such system and network architecture that can sustainably host artificial network of nodes?
3) Is it possible to create such system that shows self-consciousness and intelligence that can satisfy relevant tests?
4) Is it possible to create a form of swarm intelligence artificially using network of simple nodes?

V. Approach

Using extensive literature research from all fields, it is intend to find out needed characteristics and features that are necessary to be incorporated in a new neural model. After designing the model it is planned to start experiment phase:

A. Development stage

During this stage new model will become implemented as a single piece of software. Also, it is planned to take such approach that will not be as much model oriented but some form of wrapping technology around the model. This is necessary because eventual easier model change in real case scenarios during real-time.

B. Development of new networking protocol

Design of necessary network protocol that can support communications between nodes. This protocol should be as light as possible, and even as low level implementation as possible on the ISO/OSI network stack.

C. Development of system's input and output

Input/output is technology that allows system to interact with its surroundings and environment.
During experimental phase it is intend to analyse and explain all behaviour that may arrive correlating it to related existing discoveries in neuroscience and cognitive science. After experimental stage there is testing stage, it is planned to use existing tests to prove or disapprove existence of any form of intelligence and consciousness.

VI. Research design & methodology

Plan is to partially follow *constructive research method*:

- Fuzzy information sources
  In proposed fields there are sources like science paper, conference articles, books, book chapters. However, there are also popular articles that cannot be taken as reliable. As the nature of this work is highly experimental, those sources may provide fuzzy guidelines for research and next steps.
- Theoretical body of knowledge
  Using gathered sources it is planned to determine a strong body of knowledge.
- Relevant problem definition
  Relevant problem is initially described in previous sections, during definition of theoretical body there might be changes in definition of relevant problem definition.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Solution design
  One of results of this research is a system that uses software and network infrastructure to prove or disapprove hypothesises.
- Practical and theoretical relevance
  Finally there is extensive analysis of experimental solution. In concluding sections there should be recognized relevant influence on theoretical fields as well as new practical uses of designed experimental system.

VII. Significance

Success of this research would be that it can prove that life as we know it can exist even in software environments (although, in 2011 scientists from NASA made a breakthrough and found life form that is not phosphorous based as the life we know it). If successful it can explain how and why consciousness forms in living brain, it can certainly help dealing with many neural diseases. If unsuccessful research can pinpoint potential pitfalls in research for true artificial intelligence.

VIII. Possible pitfalls

- Complexity
  System complexity might become pitfall if it implements too much characteristics from biological examples.
- Resources
  System is very resources dependent and use of European research computing grids would be required. To achieve distributed network topology it would be necessary to deploy system nodes on remote locations over the Internet, population can help in this research by assigning certain amount of resources to this research (similar approach as SETI@Home)
- Related work and literature
  There are significant resources in each field, as this research is in several fields there is substantial literature. However, in interdisciplinary field there is not much resources but few really significant projects that deal with the similar issue.

IX. Conclusion

This work is highly experimental and includes cutting edge of different science fields. There is also a great risk that it would not be possible to prove hypothesis. Exploring our mind is something humankind is trying to do since ancient times. Today technology to scan and monitor non invasive, is present and can be used to monitor activity inside brain. Neuroscience has gained giant leap towards understanding biology of our brains. However, brain is data/signal processing device that behaves more as computer, this interdisciplinary nature of this work is something currently being on the cutting edge of science. Countries, philanthropists, and many more invest great amounts of resources into this field, because it is recognized that brain is one universe we yet need to explore.

December 12, 2013

References

[1] M. Rossmann and B. Hesse, "Implementation of a biologically inspired neuron-model in FPGA," *...for Neural Networks, ...*, 1996.
[2] J. van Hemmen and T. Sejnowski, *23 problems in systems neuroscience*. 2006.
[3] G. W. Williams, P. A. Davis, A. S. Rogers, T. Bieri, P. Ozersky, and J. Spieth, "Methods and strategies for gene structure curation in WormBase.," *Database : the journal of biological databases and curation*, vol. 2011, p. baq039, 2011.
[4] H. Mao, P. Skelton, and K. Yang, "Computational simulation of controlled cortical impact on C57Bl/6 mouse brain," *Journal of Neurotrauma*, vol. 28, p. A124, 2011.
[5] P. Braspenning, F. Thuijsman, and A. Weijters, *Artificial neural networks: an introduction to ANN theory and practice*, vol. 931. 1995.
[6] M. Roisenberg, J. Barreto, and F. Azevedo, "Specialization versus generalization in neural network learning for ballistic interception movement," *Proceedings of 8th Mediterranean Electrotechnical Conference on Industrial Applications in Power Systems, Computer Science and Telecommunications (MELECON 96)*, vol. 2, 1996.
[7] P. Andras and B. Charlton, "Self-Aware Software Will It Become a Reality?," in *Self-star Properties in Complex Information Systems*, vol. 3460, pp. 229–259, 2005.
[8] D. A. Ferrucci, "Introduction to “This is Watson”," *IBM Journal of Research and Development*, vol. 56, pp. 1:1–1:15, 2012.
[9] R. J. Sternberg and E. L. Grigorenko, "Practical intelligence and its development," in *The handbook of emotional intelligence Theory development assessment and application at home school and in the workplace*, pp. 215–243, 2000.
[10] R. K. Dase and D. D. Pawar, "Application of Artificial Neural Network for Stock Market Predictions: A Review of Literature ," *International Journal of Machine Intelligence*, vol. 2, pp. 14–17, 2010.
[11] R. Solomonoff, "Some recent work in artificial intelligence," *Proceedings of the IEEE*, vol. 54, 1966.
[12] O. Sporns, G. Tononi, and R. Kötter, "The human connectome: A structural description of the human brain.," *PLoS computational biology*, vol. 1, p. e42, 2005.
[13] Y.-f. Z. Y.-f. Zhu and X.-m. T. X.-m. Tang, "Overview of swarm intelligence," *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, vol. 9, 2010.
[14] G. Bo, D. Caviglia, and M. Valle, "An on-chip learning neural network," *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium*, vol. 4, 2000.
[15] A. Bahari, "Study on interfacing of a nano-chip with brain tissue," *International Journal of Physical Sciences*, vol. 5, pp. 1622–1625, 2010.
[16] J. Hendler, "Introduction to the Special Issue: AI, Agents, and the Web," *IEEE Intelligent Systems*, vol. 21, 2006.
[17] R. C. Berwick, A. D. Friederici, N. Chomsky, and J. J. Bolhuis, "Evolution, brain, and the nature of language.," *Trends in cognitive sciences*, vol. 17, pp. 89–98, 2013.
[18] A. P. Saygin, I. Cicekli, and V. Akman, "Turing Test: 50 Years Later," *Minds and Machines*, vol. 10, pp. 463–518, 2001.
[19] J. Lindsley, "Why we sleep: The functions of sleep in humans and other mammals," 1989.
[20] H. Markram, "The blue brain project.," *Nature reviews. Neuroscience*, vol. 7, pp. 153–160, 2006.
[21] Universidad Politécnica de Madrid, "Cajal Blue Brain," 2010.
[22] J. Sarangapani, "Neural Engineering: Computation, Representation, and Dynamics in Neurobiological Systems [Book Review]," *Control Systems, IEEE*, vol. 25, 2005.
[23] U. o. W. Centre for Theoretical Neuroscience, "Nengo."
[24] N. Holmes, "Would a digital brain have a mind?," *Computer*, vol. 35, 2002.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Chaotic Scheme for Image Encryption Based on Arnold Cat's Map

Ansam Osama Abdul-Majeed
Department of Software Engineering
College of Computer Science and Mathematics / University of Mosul
Mosul, Iraq

Abstract— **Digital images are widely used media over the Internet for different purpose. Therefore, security becomes important in the transmission. This paper presents spatial domain multilevel image encryption algorithm based on Arnold cat's map. The algorithm divides the image into different size overlapping blocks along the levels of encryption. The block at level 1 begins at the center of the image and this block is iteratively enlarged in the next levels. In each level of the proposed algorithm, Arnold cat's map is implemented in each level on the block's pixels. Also, zigzag scan is applied on the whole image to further reducing the correlation between adjacent pixels. In order to achieve the diffusion, the pixel values are xored with different xor values begin at a value, which is generated randomly, beside control parameters and iteration number of Arnold cat's map, by using mid-product algorithm with the secret key as an initial seed. The results of experiments indicated that the proposed algorithm is highly decorrelated the adjacent pixels and it resists the statistical attacks. The values of ciphered image entropy are close to the ideal value. Furthermore, the proposed algorithm is very sensitive to key. It was concluded that the use of zigzag scan beside Arnold cat's map in spatial domain was very efficient to hide the statistical characteristics of the image.**

Keywords-Image encryption; Arnold cat's map; Zigzag scan; mid-product.

I. INTRODUCTION

Today, huge amount of different information has been transmitted over Internet. Thus, information security become very important issue in order to preserve the transmission of private and critical information[1]. Cryptography is the process of transforming original media from significative to ambiguous form to protect it from unauthorized persons. In recent years, the chaotic encryption played an important role in image encryption because one of the most important properties of chaotic is the sensitiveness to the initial condition and control parameters that makes it resists the statistical attacks [2].

Compared with the traditional algorithms; the chaotic algorithms are susceptible to the control parameters, while traditional algorithms are susceptible to key. In addition, diffusion and confusion are performed in traditional encryption by rounds, while they are performed by iteration in chaotic encryption [3]. Anyway, the higher security image encryption algorithm needs to fulfill the concepts of confusion and diffusion. Confusion and diffusion mean shuffling the pixels, as well as modifying the values to hide the statistical properties of the image [4].

In the past few years, many image encryption schemes using Arnold cat's map has been proposed. G. Chen, Y. Mao, and C. K. Chui, (2004), extend the 2D Arnold cat's map to 3D map. In between the adjacent round, the algorithm applied "xor plus mod" operation on each pixel to achieve the diffusion.The key is schemed by using Chen's chaotic system [3].

M. Ahmad, O. Farooq, and J. Blackledge, (2010), proposed a novel scheme that divided the image into 8×8 macroblock, computed the DCT coefficients for that block, and partitioned the block into non-overlapping blocks of coefficients. At each level, the block size reduced into the half, iteratively. The scheme shuffled the coefficients by using Arnold cat's map, and the Logistic map used to produce the control parameters and to mask the value of image pixels [1].

S. Keshari, and S. G. Modani, (2011), suggested method uses chaotic map to convert image pixels to corresponding map variable that used as initial condition to iterate other map. The algorithm then scrambled the position of pixel using Arnold cat's map [2]. S. Kashyap, and K. Karthik, (2011), divided the image into blocks, applied DCT, and then applied Arnold transform individually on each block using control parameters and number of iterations as a key. The algorithm generated a hash function by using the mean and variance of the blocks [4].

Z. Tang, and X. Zhang, (2011), proposed an image encryption algorithm by dividing the image into number of overlapping squared blocks. For each block, the algorithm generated a pseudo-random number as iterative number of Arnold transform for that block. After that, the Arnold cat's map applied in random order on each of these blocks [5].

This paper was aimed to propose multilevel image encryption algorithm in the spatial domain based on chaotic Arnold cat's map which is implemented on the pixels of overlapping blocks. In the proposed algorithm, the first block begins at the center of the image, and it is enlarged iteratively in hierarchical manner along the levels of encryption. The proposed algorithm used zigzag scan beside the Arnold cat's map to further reducing the correlation between adjacent pixels. In order to fulfill the concept of diffusion, the pixels values are xored with incremented values, depending on another random generated xor value. The control parameters and the iteration number of Arnold cat's map as well as the xor

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

value are randomly generated by using mid-product algorithm with 20 digits secret key number.

The rest of the paper is organized as follows: section II presents a brief overview of used methods. Section III discuses the popular measures used to evaluate the encryption quality. The proposed algorithm and its stages are presented in Section IV. Section V evaluates the experimental results and discussed them. Finally the conclusion drawn in section VI.

II. Overview of Methods that Used

The methods that used in this proposed algorithm were the following:

A. Arnold Cat's Map Transform

One of the chaotic maps, which is appropriate for squared images encryption, is the Arnold cat's map [5]. The mathematical representation for Arnold Transform is as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \qquad (1)$$

where x_n, and y_n are the coordinate of pixel in image which its dimension is N×N, while p and q are two positive integer numbers act as control parameters [4]. From (1), it is clear that the Arnold cat's map shuffles the pixel's position by shearing the image in both directions, and then flexing it by using modulo operation. Furthermore, applying Arnold cat's map K times on the image will cause restoring the image to its origin, where K depends on p, q and N [3].

The inverse Arnold cat's map can be represented as follows:[4].

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod N \qquad (2)$$

Because of the periodicity property of Arnold cat's map, it is important to add another processing to the algorithm in order to increase its security [2].

B. Zigzag Scan

Zigzag scan is a famous scanning algorithm which is used to turn an image, (2D matrix), into 1D vector in such manner that decreases the correlation between adjacent pixels [6]. Fig.1 illustrates the scanning approach of zigzag scan.

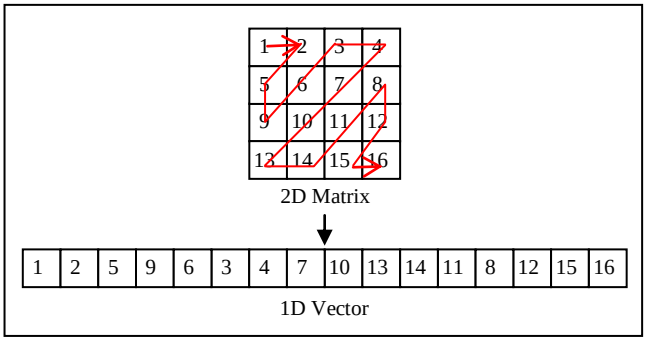


Figure 1. Zigzag scan

C. Mid- Product Random Number Generation

This method starts by multiplying two numbers (initial seeds) x and y of n digits to generate another number. The middle digits of the resulting number represent the random number z. This procedure is repeated to generate the rest random numbers [7]. The method uses y instead of x, and z instead of y.

III. Measurements of Encryption Quality

The most popular measures that use to ensure the security and efficiency of the image encryption algorithm are as follows:

A. Histogram Analysis

In order to make the encryption algorithm resists the statistical attacks, the histogram of the cipher image must be uniform, so the opponent could not be able to obtain any information about the grayscale distribution [1].

B. Corrolation Coefficients

The correlation between two variables is how these variables related to each other. If the correlation coefficient equals to 1, this means that the two variables are highly correlated. On the other hand, if correlation coefficient closes to 0, this means that the two variable are decorrelated. Furthermore, if the correlation coefficient equals to -1, this means that one of these variables is the negative of the other [8].

Because the correlation among the adjacent pixels in the plain image is strong, the good encryption algorithm must reduces this correlation as much as possible in the cipher image. The correlation coefficient between adjacent pixels x and y can be computed according to (3) [1]:

$$corr(x,y) = \frac{\sum_{i=1}^{N} \left[\left(x_i - mean(x)\right) \quad \left(y_i - mean(y)\right) \right]}{\sqrt{\sum_{i=1}^{N} \left(x_i - mean(x)\right)^2 \sum_{i=1}^{N} \left(y_i - mean(y)\right)^2}} \qquad (3)$$

C. Entropy

The randomness of variables is measured by entropy, which is computed by (4):

$$E(v) = -\sum_{i=0}^{255} p(m_i) \log_2 p(m_i) \qquad (4)$$

The entropy of a variable of 28 symbols $v = \{m_0, m_1, \ldots m_{255}\}$ with equal probability, p(mi), equals 8, which is the perfect value. The entropy of cipher image must be close to the perfect value as much as possible[1].

D. Maximum Deviation

Maximum Deviation measures how the cipher image deviated from the plain image. It can be founded as follows:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Find the number of every grayscale pixel value (0-255) for both plain and cipher image, which is p_count and c_count, respectively.
- Find absolute difference between p_count and c_count.
- Find the sum of deviation D, where D is

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i , \quad (5)$$

Where h_i is i^{th} absolute difference. A good encryption algorithm must maximize the Deviation as much as possible[8].

E. Irregular Deviation

Irregular deviation measures the irregularity of the changes in the cipher image that is caused by the encryption algorithm. The irregular deviation can be founded as following:

- Find the absolute difference, D, between plain and cipher images.
- Find the histogram H of D, where h_i is the number of value of absolute difference Di.
- Find the average value, DC, of pixels that deviated at every deviation value.

$$DC = \frac{1}{255} + \sum_{i=0}^{255} h_i , \quad (6)$$

- Find the sum of the absolute difference values between DC and H. the result of summation is the irregular deviation.

The good encryption algorithm try to minimize the irregular deviation value as much as possible [8].

IV. The Proposed Algorithm

This paper propose multilevel image encryption algorithm in the spatial domain consisted from the following stages (see Fig. 2):

A. Zigzag Scanning Stage

In order to make further reducing in the correlation between the adjacent pixels, zigzag scan applied to the original plain image and to each intermediate cipher image resulted from each level.

The zigzag scan stage converted the image to one-dimensional vector which is converted back to two-dimensional matrix before enter to the next stage.(see Fig. 3).

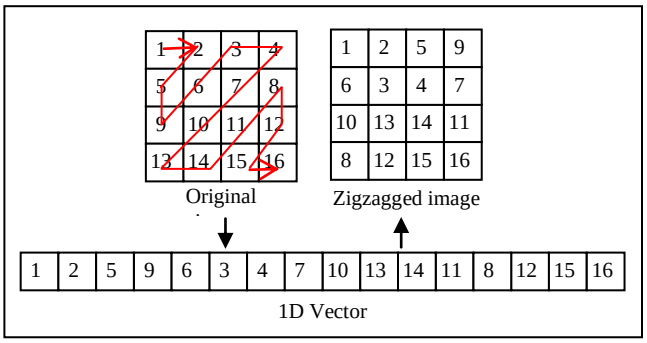


Figure 3. Zigzag scanning stage of the proposed algorithm

B. Blocking Stage

The proposed algorithm divided the image, along the levels of encryption, into overlapping squared blocks at the center of the zigzagged image. In the first level, the block begins at (row/2, column/2) position, and ends at (row/2+1, column/2+1). At each level of encryption, the size of the block increased by one row in both top and bottom, and one column in both right and left of the block in the previous level. At the last level, the block size occupied the whole image size.

The number of blocks depended on the number of levels which depended on the size of image. For instance, 256×256 image was encrypted by 128 levels and 128 squared blocks. Fig. 4 illustrates the manner in which the proposed algorithm got a block at each level.

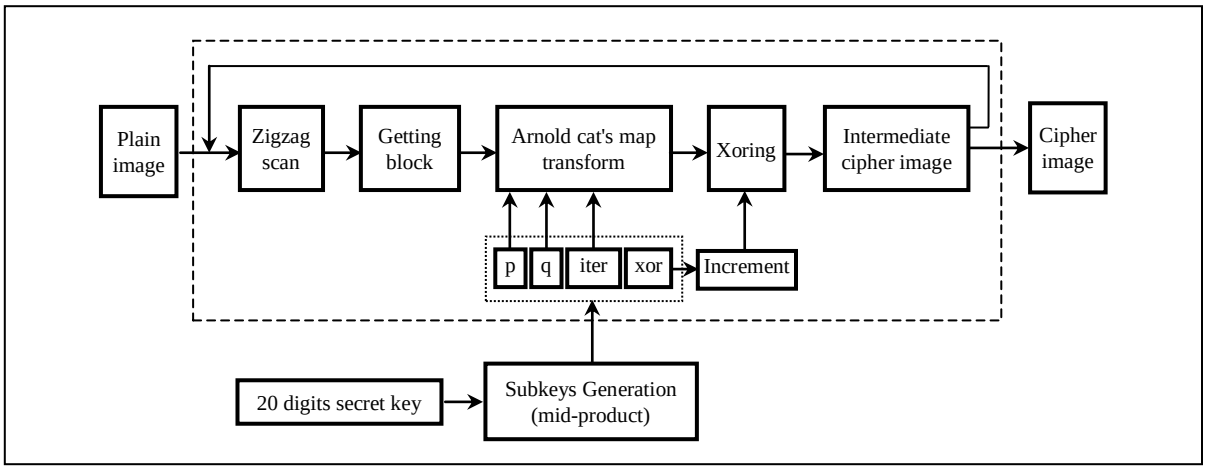


Figure 2. Block diagram of the proposed algorithm

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

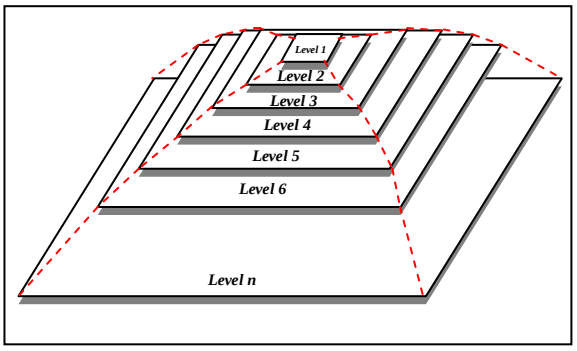


Figure 4. Blocking scheme of the proposed algorithm

C. *Arnold Cat's Map Transform Stage*

The proposed algorithm applied Arnold cat's map transform on the pixels of block at the current level using the random generated p, q, and iteration number for that level. These pixels were transformed again within the larger blocks in the next levels.

D. *Xoring Stage*

The generated random number of xor used, at each level, as a seed to generate further values of xor by incrementing the previous value by 1. Each pixel in the transformed block was xored with different values. If the value of incremented xor reached 255, it reset to the xor seed value. The xored pixels were xored again within the larger blocks in the next levels using another different values depending on the value of xor seed. This was important in order to increase the diffusion.

The transformed xored block reloaded to its original position in the plain image to produce the intermediate cipher image which was used as input to the next level. The operation from (A.-D) was repeated in the next level, with increasing block size including the pixels of the previously processed block.

E. *Generating Subkeys Sequence*

The proposed algorithm implemented the mid-product random number generation algorithm to generate a sequence of different keys for each level. The length of this sequence was equal to level×4. Each level required four subkeys which are the iteration number and the control parameters (p and q) for the Arnold cat's map. The fourth subkey was the xor value which is a seed for further xor values that were used to modify the image pixels to achieve the diffusion.

The secret key, which was shared between sender and receiver, is a number of 20 digits whose digits are from 1 to 9. This number was split into two 10 digits numbers and used as the initial seeds for mid-product algorithm. The proposed algorithm selected the first two digits from the generated random number and saved it in the subkeys sequence. To avoid producing number 0, the algorithm removed the '0' digit from any producing number.

The following pseudo-code illustrate the proposed algorithm:

- Read a grayscale squared image.
- Set d to the first dimension of the image.
- Set the variable begin_row to d/2.
- Set the variable end_row to d/2.
- Set the variable begin_column to d/2 +1.
- Set the variable end_column to d/2 +1.
- Set the variable level to d/2.
- Input a secret key of 20 digits number.
- Generate a sequence of level×4 subkeys using secret key as a seed.
- Set round to 1.
- Repeat
- Apply zigzag scan to the image.
- Get a block from the zigzagged image starting at position (begin_row, begin_column) and ending at position (end_row, end_column).
- Apply Arnold cat's map transform on the block using roundth p, q, and iteration subkeys.
- Set xor value to random generated xor value (Rnd_xor).
- FOR each transformed pixel in the block
    - Xored the pixel with xor value
    - IF xor < 255
      Increment xor by 1.
      ELSE
      Set xor to Rnd_xor.
      END IF

  END FOR
- Reload the transformed-xored block to the zigzagged plain image to get the intermediate cipher image.
- Decrement begin_row by 1.
- Increment end_row by 1.
- Decrement begin_column by 1.
- Increment end_column by 1.
- Increment round by 1.
- Until round = level.

The Decryption process required the opposite process of encryption using inverse Arnold cat's map, inverse zigzag scan, opposite block generation scheme, and the same secret key with opposite subkeys sequence.

V. EXPERIMENT'S RESULT AND DISCUSSION

The proposed algorithm was experimented using different grayscale images of 256×256 and 512×512 size, and the efficiency of the encryption was tested using different quality measurements. The result showed that the histogram of the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

cipher image was distributed uniformly, this is because the proposed algorithm used xor many times on the same pixel with different values along the levels of encryption process. Fig. 5 shows the histogram for both plain 'Fruit' image and its corresponding cipher image.

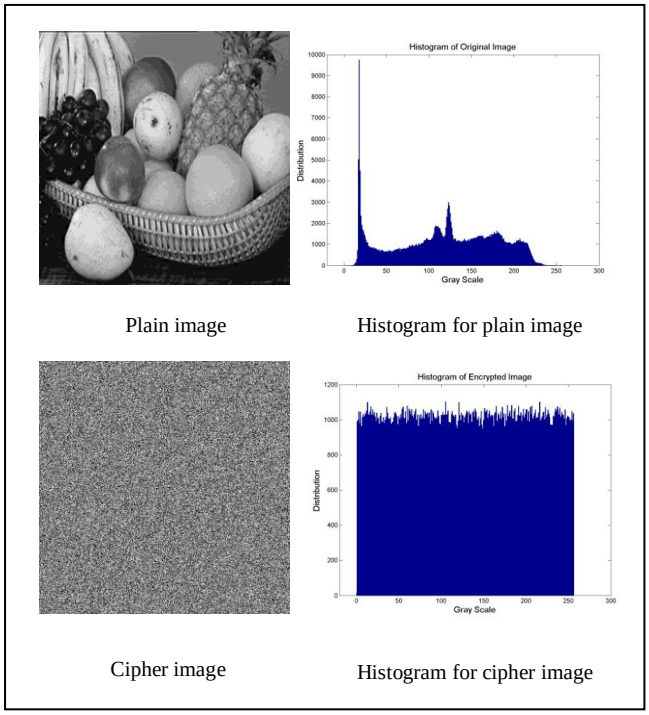


Figure 5. Plain and cipher image of 'fruit' and their histograms

The mean values of all tested images (listed in table I) are about 127, making it hard to get information about pixel values distribution.

TABLE I. THE MEAN OF GRAYSCALE VALUES FOR BOTH PLAIN AND CIPHER IMAGES

Image	Mean Value	
	Plain Image	***Cipher Image***
Sailboat	124.6570	127.2948
Airplane	178.6740	127.5098
Barb	112.4516	127.4581
Boat	158.9199	127.5426
Cameraman	118.7245	127.2090
Fruit	116.7825	127.6463
Goldenhill	111.9491	127.3763
Seaside	118.0883	127.5022
Pepper	120.2198	127.4593
Retina	123.9967	127.5288

In order to compute the cipher image pixels correlation coefficients, 2000 adjacent pixels were randomly selected for horizontal, vertical, and diagonal directions. The correlation coefficients of the plain and cipher tested images are listed in table II.

TABLE II. CORRELATION COEFFICIENTS OF THE PLAIN AND CIPHER IMAGES

Image	Correlation Coefficient					
	H^a	V^b	D^c	H^a	V^b	D^c
Sailboat	0.9825	0.9796	0.9701	0.0067	-0.0071	-0.0016
Airplane	0.9135	0.9185	0.8712	0.0033	-0.0082	-0.0072
Barb	0.9388	0.9605	0.9149	0.0053	-0.0113	0.0031
Boat	0.9590	0.9487	0.9243	0.0083	0.0059	-0.0011
Cameraman	0.9351	0.9640	0.9217	-0.0054	0.0003	0.003
Fruit	0.9792	0.9910	0.9743	0.0006	-0.0215	0.0016
Goldenhill	0.9359	0.9486	0.9026	-0.0017	0.0004	0.0069
Seaside	0.9876	0.9651	0.9611	0.0007	0.0013	0.0303
Pepper	0.9767	0.9787	0.9661	0.0030	-0.01	0.0092
Retina	0.9971	0.9976	0.9966	0.0023	0.0033	0.0028

a. Horizontal correlation coefficient
b. Vertical correlation coefficient
c. Diagonal correlation coefficient

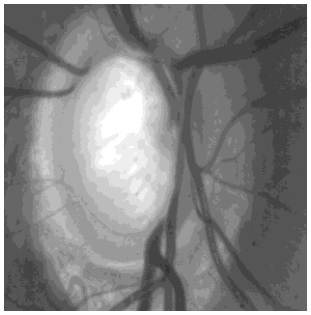
The values of correlation coefficient of cipher images indicated that the proposed algorithm decorrelated the adjacent pixels of cipher image strongly, this is because the proposed algorithm implemented zigzag scan, to further reducing the correlation, beside the Arnold cat's map which implemented on hierarchical manner, on block pixels, along the levels of encryption. Fig. 6 shows the distribution of adjacent pixels for both 'retina' plain and cipher images.

The entropy for cipher images also tested and it was close to 8. Table III lists the entropies of both plain and cipher tested images.

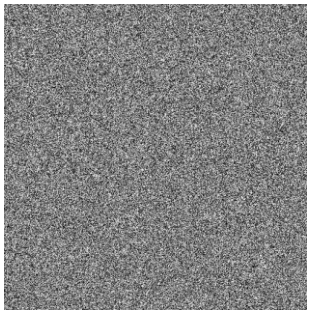
TABLE III. ENTROPIES OF BOTH PLAIN AND CIPHER IMAGES

Image	Entropy Value	
	Plain Image	***Cipher Image***
Sailboat	7.4409	7.9993
Airplane	6.7678	7.9973
Barb	7.3924	7.9971
Boat	6.6491	7.9992
Cameraman	7.0097	7.9970
Fruit	7.5696	7.9994
Goldenhill	7.4761	7.9974
Seaside	6.1605	7.9971
Pepper	7.5936	7.9993
Retina	7.1535	7.9992

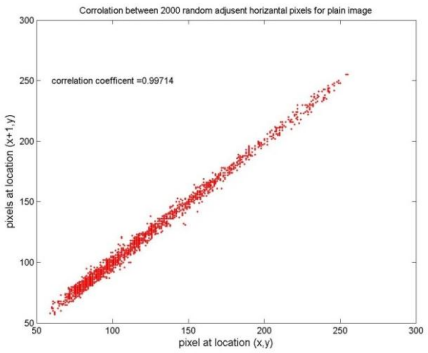
http://sites.google.com/site/ijcsis/
ISSN 1947-5500



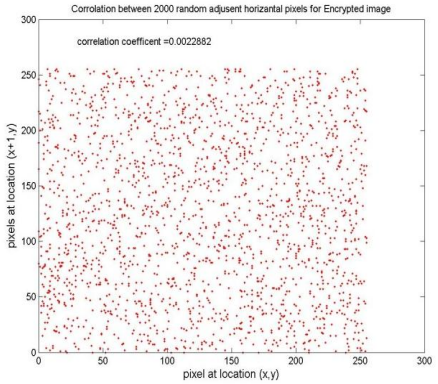
Plain image



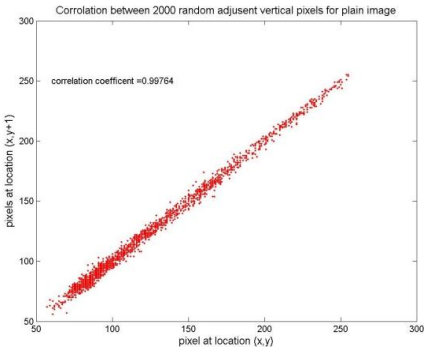
Cipher image



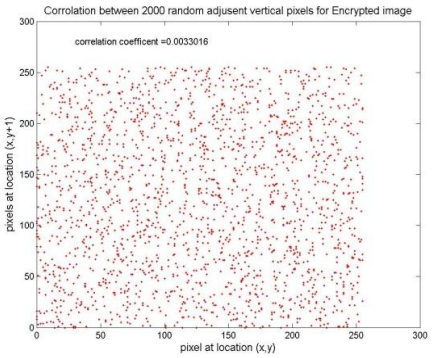
Horizontal distribution of plain image pixels



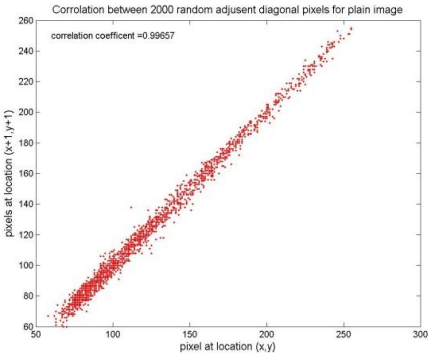
Horizontal distribution of cipher image pixels



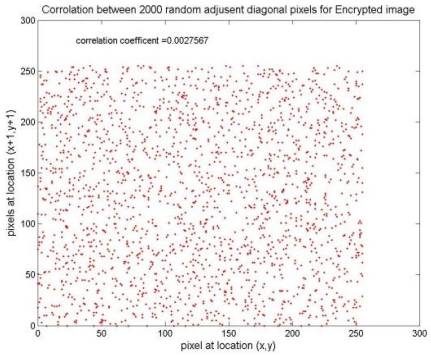
Vertical distribution of plain image pixels



Vertical distribution of cipher image pixels



Diagonal distribution of plain image pixels



Diagonal distribution of cipher image pixels

Figure 6. The horizontal, vertical, and diagonal pixels distributions of both 'retina' plain and cipher image

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The maximum and irregular deviations of ciphered image are listed in table IV. The proposed algorithm deviated the cipher image strongly from its corresponding plain image and this deviation was irregular.

TABLE IV. MAXIMUM AND IRREGULAR DEVIATIONS OF CIPHER IMAGES

Image	*Maximum Deviation*	*Irregular Deviation*
Sailboat	175464.0	267188.0
Airplane	66758.0	39972.0
Barb	45470.5	73342.0
Boat	269668.0	198462.0
Cameraman	64277.0	69546.0
Fruit	126478.5	283856.0
Goldenhill	45617.0	73742.0
Seaside	92340.5	70572.0
Pepper	144680.5	276122.0
Retina	227350.5	270380.0

The testing also included decryption of an image with just one digit different secret key. The results of decryption are shown in Fig. 7. Changing one digit from the secret key caused complete changes of the random generated sequence subkeys. For instance, the sequence subkeys for four encryption levels using secret key "64892312456718452795" was 75, 55, 86, 82, 13, 69, 36, 21, 68, 97, 96, 78, 35, 33, 86, 38. The subkeys sequence generated from one digit different secret key "64892312456718452794" was 75, 51, 91, 97, 68, 94, 72, 74, 67, 97, 19, 42, 31, 44, 87,72. Changing the middle digit of the secret key "64892312466718452795" produces the subkeys sequence 97, 79, 64, 75, 58, 52, 96, 68, 35, 63, 29, 86, 39, 12, 55, 64.

The key space of the proposed algorithm was large enough to defeat the brute-force attack because the number of different secret keys that can shared by sender and receiver is 9^{20}.

The number of levels in 512× 512 images was double of the number of levels in 256×256 image, which is interpreting the better results of 512×512 images.

VI. CONCLUSION

This paper proposed an image encryption algorithm based on Arnold cat's map and zigzag scan with xor operation applied on pixels values. The experimental results show that proposed algorithm able to resist the statistical attacks due to the uniformly distribution of cipher image histogram and the strong decorrelation between the adjacent pixels that achieved by the algorithm. Furthermore, the entropy of cipher image is very close to the ideal value. The results show that the cipher image is strongly deviated from its corresponding plain image and this deviation was irregular. It was concluded that the use of zigzag scan with Arnold cat map which is implemented in spatial domain in overlapped manner was very efficient to hide the statistical characteristics of the image.

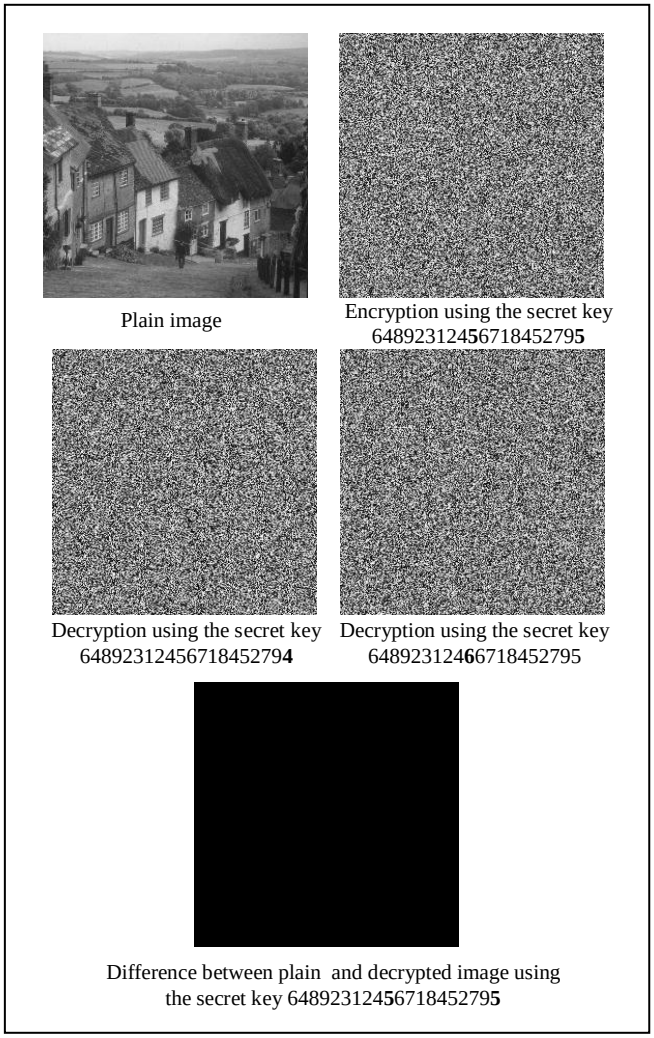


Figure 7. Result of decryption cipher images with one digit different secret key

REFERENCES

[1] M. Ahmad, O. Farooq, and J. Blackledge, "Chaotic image encryption algorithm based on frequency domain scrambling," Dublin Institute of Technology, (2010), .available in:" http://www.dit.ie/media/electricalengineering/documents/jonathanblackledge/186.pdf

[2] S. Keshari, and S. G. Modani, "Image encryption algorithm based on chaotic map Lattice and Arnold cat map for secure transmission," IJCST, vol. 2, issue 1, 2011, pp. 132-135.

[3] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons and Fractals, vol. 21, issue. 3, 2004, pp. 749–761.

[4] S. Kashyap, and K. Karthik, "Authenticating encrypted data,", 2011 National Conference on Communication (NCC), Bangolore, 2011, pp. 1-5.

[5] Z. Tang, and X. Zhang, "Secure image encryption without size limitation using Arnold transform and random strategies," Journal of multimedia, vol. 6, no. 2, 2011, pp.202-206.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[6] S. S. Hegde, and B. N. Rao, "Visual cryptography (vc) using zigzag scan approach," IJCSET, vol. 1, issue. 8, 2011, pp.456-461.

[7] A. Aghaie, "Random numbers in computer simulation and development of a newly combined algorithm generating random numbers," in the fifth Asia pacific industrial engineering and management systems confrence, 2004, pp. 12:3:1-12:3:10.

[8] N. El-Fishawy, and O. M. Abu Zaid, "Quality of encryption measurement of bitmap image with RC6, MRC6, and Rijndael block cipher algorithms," International Journal of Network Security, vol. 5, no. 3, 2007, pp.241-251.

AUTHORS PROFILE

Ansam Osama received her B. Sc. degree in Computer Sceince from the University of Mosul in 2005, and M. Sc. degree from the University of Mosul in 2011. She is currently an assistant lecturer at department of Software Engneering / College of Computer Science and Mathematics / University of Mousl. Her research interests are in data security and information hiding.

An Overview of an Advanced Vehicle Security System

Tariq Alwada'n[1], Adel Hamdan Mohammad[1], Nidhal El-Omari[1], Hamza Aldabbas[2]
[1]Computer Science Department, The world Islamic Sciences and Education University, Amman-Jordan
[2]Prince Abdullah bin Ghazi Faculty of Information and Technology, Al-Balqa' Applied University, Salt-Jordan

***Abstract*—In the past few decades wireless networks have become increasingly popular, due to the wide availability and rapid introduction of wireless transceivers into a variety of computing devices such as PDAs, laptop and desktop computers. Global Positioning System (GPS) is used to determine position and speed of objects by using the satellite technology. Furthermore, Radio Frequency is another technology which is used to determine the objects' locations. In this paper we have presented an overview for using the previous technologies to track a stolen vehicle by using a system that is resulted from mixing all of those technologies in addition to proposed an enhancement idea that could help the resulted system to determine the cars' thieves by sending their photos to the security agency base to be recognized.**

Index: WiMAX, Wi-Fi, GPS, Mobile Cell Phone, Radio Frequency.

I. INTRODUCTION

Wireless communication brings essential changes to telecommunications and data networking. Air is used as the transmission medium, allowing great flexibility; networks can be deployed quickly where cablings difficult. Good performance and low prices encourage progressively more home users and companies to choose these new kinds of networks. Wireless communications could replace wired communications in many situations. Travelling users today have access to the internet at many places like their offices, homes, and even at public places like air-ports, conferences, shopping centers, hotels, and libraries. Also wireless technologies plays a critical important role in developing countries. In remote areas with no infrastructure, connecting using wireless technology is almost the solution for ease of access and cost savings which will take any developing country to a new level of information economy and wealth creation. Well educated and skilled staff and as a result intellectual capital is becoming the keystone for organizations to get and stay competitive in dynamic markets [1].

A. Wireless Communication Technologies

In recent years various wireless network technologies have been developed to offer different services, increased coverage area and data rates. In this introduction we will describe in overview:

1) Wi-Fi: (Abbreviation of Wireless Fidelity) is a class of wireless Local Area Network (LAN) devices; the technology is based on the IEEE 802.11 standards [2]. Today, Wi-Fi devices can be found in many desktop computers, smart phones, printers, and indeed all modern laptops and (PDAs) are equipped with Wi-Fi technology. Wi-Fi's original purpose was mobile computing devices (for example laptops in LANs), but is now progressively more used for more purposes, including VoIP phones, games, and televisions and DVD players. The above functions require the device to be within range of an access point. The most common Wi-Fi standard IEEE 802.11g has a data transfer rate of around 54Mbps; the range indoors is a maximum 150 feet (approximately 45 meters) and double that outdoors though, this depends on the conditions, like obstacles, power and weather. In Wi-Fi both 802.11b and 802.11g are using 2.4 GHz under the speed of 11 Mbps and 54Mbps respectively, while 802.11n operates in both 2.4 and 5 GHz with theoretical speed600 Mbps [3].
In Wi-Fi MAC (Media Access Controller) users are competing when they are connected to Wi-Fi access point, and users therefore have different levels of bandwidth. Wi-Fi however is short range (tens of meters) can be encrypted with WEP (Wired Equivalent Privacy) or WPA and WPA2 (Wi-Fi Protected Access encryption).

2) WiMAX: (Worldwide Interoperability of Microwave Access) is based on the IEEE 802.16 standard (also called Broadband Wireless Access). WiMAX was formed in 2001 by the WiMAX Forum, in order to endorse WiMAX as a standard [4]. WiMAX was described as a standard based technology for use as "last mile" broad band delivery rather than using wires. This technology is originally designed for the communication of multimedia services (Internet, voice, email, games and others) at high data rates (of the order of Mb/s per user) [5]. "WiMAX is the emerging BWA (Broadband Wireless Access) technology of next generation because of its mobility, coverage and high transmission speed" [6]. WiMAX is a wireless WAN technology with great data transmission rate and is a candidate for the 4G network trying to support users with mobile service [7].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

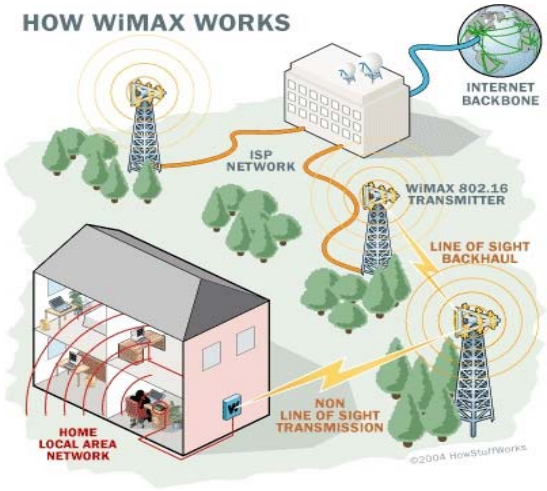


Fig.1. WiMax vs WiFi [9]

This technology was planned to be used to link Wi-Fi hot spots together. WiMAX 802.16 operates at range of 10-66 GHz and is classified as fixed wireless broadband; later, in 2004 802.16a was updated and operates at lower frequency range2-11 GHz and is classified as fixed wireless broadband as well. Finally in 2005 mobile wireless broadband was created under 802.16e which operates at frequency range of 2-6GHz [8].

WiMAX technology has an advantage which is not affected by obstacles like buildings. This makes WiMAX especially useful and cost-effective for countryside homes where setting a traditional wire would be more difficult and very expensive. For the meantime, its security is becoming a serious issue with the proliferation of wireless threats [10]. Mobile WiMAX carries the promise of ubiquitous broadband wireless access enabling real-time and multimedia applications [11]. Mobile WiMAX supports a full range of multiple input multiple-output (MIMO) methods including spatial multiplexing (SM), space time block coding (STBC), and eigen-beamforming (EB) [12]. WiMAX speed in theory delivers up to 70 Mbps, and range coverage 112 Km. These numbers changes depends on the conditions, like obstacles, power and weather, expected values is 10 Mbps in 2 Km coverage area [13]. One of the most significant features of WiMAX is support of applications with distinctive QoS conditions in terms of delay, jitter and bandwidth [14]. WiMAX can support two forms of wireless service: Non-Line of Sight (Non-LOS) and Line Of Sight (LOS). Non-LOS works in the same manner as WiFi systems where an antenna on a computer connects to the WiMAX tower. It uses a lower frequency range (2 to 11 GHz).

LOS uses a fixed, high antenna that must point straight at the WiMAX tower and align with its antenna. LOS has a better and robust performance. It uses higher frequencies - up to 66 GHz with coverage area of up to 30 miles in ideal conditions. Figure(1) shows the differences between the Wi-Fi technology and the WiMax technology. Also it shows the Non-LOS and LOS WiMAX forms [13], [15]. Table(I) also describes a comparison between WiMAX standards in terms of completion date, spectrum usage, operation (LOS, Non LOS), bit rate, and cell radius.

TABLE I
WIMAX STANDARDS [13]

	WiMAX Standards			
	(802.16)	**(802.16a)**	**(802.16-2004)**	**802.16-2005**
Date Complete	Dec 2001	Jun 2003	Jun 2004	Dec 2005
Spectrum	10-66GHz	< 11GHz	< 11GHz	< 60GHz
Operation	LOS	Non-LOS	Non-LOS	Non-LOS and Mobile
Bit Rate	32-134 Mbps	Up to 75 Mbps	Up to 75 Mbps	Up to 15 Mbps
Cell Radius	1-3 miles	3-5 miles	3-5 miles	1-3 miles

B. Mobile Cell Phone

Each city is divided by the network providers into small cells. Each cell usually has a size of about 26 km2. These cells are designed as six sided figures or hexagons. Hexagons fit together properly, contain a base station in the middle [16]. Each base station compromised of one tower and one small building holding some radio devices. Figure(2) shows this design. Now every cell in analog system used 1/7th of voice channels, that is a cell in addition to 6 cells surrounding the hexagonal arrangement and each used 1/7th of the offered channels, so every cell own a different group of frequencies and no collisions with one another. A cellular network provider obtained (832) radio frequencies to be used in one city [17].

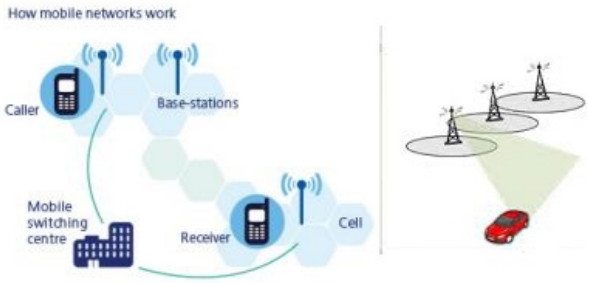


Fig.2. How Cell phone works [17], [18]

The rest of the paper is organized as follows: The next section introduces an overview of the existing security system including the Global Positioning System (GPS) and Radio Frequency (RF) Tracking Technology. The third section presented our suggested security system in details. The last section we discuss future possibilities and conclude the paper.

II. OVERVIEW OF THE EXISTING SECURITY SYSTEM

A. Global Positioning System

One of the greatest inventions in the twentieth century is the Global Positioning System (GPS) technology. This technology is used to determine position and time of an item using the GPS. It is a set of satellites which accept signals from the GPS senders (transmitters) and sends out data to the receivers [19]. There are many forms of vehicle tracking systems; some of these systems are [20]:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- **Passive**

In this system a GPS device is used to record the position of a vehicle over time. When the tracker is detached, the information can be upload to a computer and examined.

- **Active**

This system has the ability to send the location of a vehicle in real time and this data is normally checked from a central location. This form of system can be used for recovering stolen vehicle. A small number of transmitters can perform both types; if the cellular network is available, they work as active way, but if it's not available they work as a passive way [19].

B. Radio Frequency Tracking Technology

In such a system, a radio transceiver, generally called a VLU (Vehicle Locator Unit), is set up in the car and stays inactive till the car required being located. As soon as this happened, the VLU is activated. This might be done by using a remote radio activation signal that is sent from local radio towers. As soon as the VLU is activated, it sends a radio signal that can then be tracked by using tracking receivers set up in security vehicles or police cars. This way is very useful especially if the car is hidden in a cargo container, garage or any place that is not covered by cell network. One of the disadvantages of this system is that it does not support instant location data to the control-center therefore the tracking and recovery procedures can possibly take more time than the GPS technology [21].

III. OUR SUGGESTED SYSTEM

In this system we employed a hybrid vehicle tracker from Pegasus Technologies incorporates. This tracker has the ability to use both GPS and RF tracking technologies to track the stolen vehicle. Pegasus uses a very strong GPS receiver onto the RF based Vehicle Locator Unit, This gives the ability for the system to use both GPS and RF tracking at the same time [21]. The transmitter is fitted in the vehicle as in Figure(3) where it is difficult to be detected by the thief. As a consequence, it is not easily to be deactivated.

Fig 3. Hybrid Tracking Device

The GPS transmitter transmits signals constantly to the monitoring base. Then the GPS server analyses the signal /data coming from the vehicle, saves it securely and supplies the information when requested. The unit that is responsible for triggers the alarm when the vehicle is stolen is the control system or the GPS interface which will make possible to track the vehicle. This interface can be activated via cell phone technologies such as an alert call or SMS. When the vehicle is stolen, instantly call or SMS the necessary code to a predetermined number. As consequences the alarm in vehicle is activated and that will allow the security agencies to trace the car and determine its location [19].

Fig. 4. Tracking Process [22]

Figure(4) shows the whole process. Finally we added a new device to the whole system. We added a camera inside the car as in Figure (5). As soon as the GPS interface triggers the alarm inside the vehicle, the camera gets activated by the same signal. This camera can be a real time device to transfer a real time picture inside the car to the base station. In this case the security agency will have the thieves' pictures. The camera will get its power from the car battery, and has its own hard disk to store data to be retrieved later after recovering the car if the place is not covered by cell network.

Fig. 5. Real Time Camera

IV. CONCLUSIONS AND FUTURE WORK

In remote areas with no infrastructure, connecting using wireless technology is almost the solution for ease of access

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

and cost savings, also it is the best technology to track objects. Such an example of this technology is WiMAX. WiMAX is a wireless WAN technology with great data transmission rate and it is a candidate for the 4G network trying to support users with mobile service. One of the greatest inventions in the twentieth century is the Global Positioning System (GPS) system technology. This technology is used to determine position and time of a vehicle using the GPS satellites and WiMAX towers. Radio Frequency Tracking Technology is another technology that is useful if the vehicles or objects are hidden in a cargo container, garage or any place that is not covered by cell network. We have suggested a security system that uses a hybrid vehicle tracker. This tracker has the ability to use both GPS and RF tracking technologies to track the stolen vehicle. Finally we added a camera to our system to be located inside the car to determine the cars' thieves by sending their photos to the security agency base to be recognized. Our future work is concerned with applying and conducting more experiments on our system.

REFERENCES

[1] M. Alzaghal N.El-Omari. Shifting towards city-wide wireless Jordanian cities. The Proc. of the Second Conference on Innovations in Computing and Engineering Machinery (CICEM 2012), 11:59–63, April 2011.
[2] William Lehr A and Lee W. Mcknight B. Wireless Internet access: 3G vs. WiFi. Telecommu-nications Policy, Research Program on Internet and Telecoms Convergence, Mas-sachusetts Institute of Technology (MIT).
[3] Matthew S Gast. 802.11 Wireless Networks: The Definitive Guide, Second Edition. O'Reilly Media, Inc., 2005.
[4] Jeffrey Andrews, Arunabha Ghosh, and Rias Muhamed. Fundamentals of WiMAX: Understanding Broadband Wireless Networking. Prentice Hall Press, Upper Saddle River, NJ, USA, 2011.
[5] Loutfi Nuaymi. WiMAX: Technology for Broadband Wireless Access. Wiley Publishing, 2007.
[6] Hsing-Shao Liu, Chia-Hui Wang, Ray-I Chang, and Ching-Chia Hsieh. A cost-effective wimax deployment for high-quality video streaming of live news reporting. In Proceedings of the 2009 IEEE conference on Mobile WiMAX, MWS'09, pages 151–156, Piscataway, NJ, USA, 2009. IEEE Press.
[7] Po-Wen Chi, Ching-Lun Lin, and Wei-Chih Lin. Fast uncontrolled handover scheme for wimax infrastructure networks. In Proceedings of the International Conference on Mobile Technology, Applications, and Systems, Mobility '08, pages 109:1–109:6, New York, NY, USA, 2008. ACM.
[8] A. Ghosh, D. R. Wolter, J. G. Andrews, and R. Chen. Broadband wireless access with wimax/802.16: current performance benchmarks and future potential. Comm. Mag., 43(2):129–136, February 2005.
[9] Eric Meyer. Wimax vs wifi. Website, January 2006. http://www. techwarelabs.com/articles/other/wimax wifi/.
[10] Frank A. Ibikunle. Security issues in mobile wimax (ieee 802.16e). In Proceedings of the 2009 IEEE conference on Mobile WiMAX, MWS'09, pages 117–122, Piscataway, NJ, USA, 2009. IEEE Press.
[11] Yazan A. Alqudah and Huiqin Yan. On handover performance analysis in mobile wimax networks. In Proceedings of the 2009 IEEE conference on Mobile WiMAX, MWS'09, pages 20–23, Piscataway, NJ, USA, 2009. IEEE Press.
[12] Mai Tran, David Halls, Andrew Nix, Angela Doufexi, and Mark Beach. Mobile wimax: downlink performance analysis with adaptive mimo switching. In Proceedings of the 2009 IEEE conference on Mobile WiMAX, MWS'09, pages 135–139, Piscataway, NJ, USA, 2009. IEEE Press.
[13] M.H. Alzaghal. Emergency Communications Interoperability for Disaster Management: Case Study: Jordan. Lambert Academic Publishing, 2010.
[14] Bruno Sousa, Kostas Pentikousis, and Marilia Curado. Evaluation of multimedia services in mobile wimax. In Proceedings of the 7th International Conference on Mobile and Ubiquitous Multimedia, MUM '08, pages 64–70, New York, NY, USA, 2008. ACM.
[15] Nidhal Kamel Taha El-Omari and Mohamad H. Alzaghal. Utilizing wimax as a public safety network in jordan. In AINA, pages 350–355. IEEE Computer Society, 2010.
[16] Andre Wemms. Designing mobile networks ii: What do they look like? Website, April 2011.
[17] Raj Soni. Benefits of mobile phones, how cell phones work, where to buy them. Website, April 2010.
[18] Rick Nigol. Trim the text. Website, December 2007.
[19] Rajesh Namase. How to trace a stolen car using mobile phone technologies? Website, May 2011.
[20] Jeremy Laukkonen. What is vehicle tracking? Website.
[21] Inc. Pegasus Technologies. Rf vs. gps tracking. Website.
[22] Sai Digital Magazine. Micro vbb advanced car security system review. Website, November 2009.

Tariq Alwada'n received the PhD Degree in Computer Science from De Montfort University, Leicester-United Kingdom, 2012. MS in Computer and Information Networks from Essex University, Colchester, United Kingdom (2007) and BS in Computer Engineering (2006) from Al-Balqa'a Applied University, Jordan.
He is professor assistance at the World Islamic Sciences and Education University, Jordan. Research Interests include: Cloud Computing, Grid Computing, Human Computer Interaction and Software Engineering.

Dr. Adel Hamdan Mohammad, got his B.S in Computer Science and information System from Philadelphia University in 1998. M.Sc and. PhD degrees in computer Information System in 2005 and 2009 respectively.
He was an Assistant Professor at Computer Science Department, Faculty of Information Technology, in the Applied Science University from 2009 up to 2013. Now he is a Professor Assistant and head of Computer Science Department in world Islamic sciences and education university (WISE) Amman, Jordan.
Dr. Mohammad research interests include Artificial intelligence, software engineering (agile methodologies) , Intelligent Systems and expert systems.

Hamzah Aldabbas received the PhD Degree in Computer Science and Software Engineering from De Montfort University, Leicester-United Kingdom, 2012. MS in Computer Science (2009) and BS in Computer Information Systems (2006) from Al-Balqa'a Applied University, Jordan.
He is professor assistance at Al-Balqa'a Applied University, Jordan. Research Interests include: Grid Computing, Human Computer Interaction and E Government Adoption.

Nidhal Kamel El-Omari recived his PhD in Computer Information Systems in Image Processing from Arab Academy for Banking and Financial Science (AABFS), Amman, Jordan in 2008. He received his BS in Computer Science and M.Eng in Computer Engineering in 1986 and 2005, respectively from University of Jordan. He is professor assistance at the World Islamic Sciences and Education University, Jordan. Research Interests include: Cloud Computing, Artificial intelligence, software engineering.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Computational Intelligence Techniques Used In Iris Recognition: A Survey

Shraddha Sharma
UIT, RGPV, Bhopal, India
.

Shikha Agrawal
UIT, RGPV, Bhopal, India
.

Sanjay Silakari
UIT, RGPV, Bhopal, India
.

Abstract: Authentication is a very crucial issue for all security protocols. Biometric based authentication is widely used for security issues such as iris, face, fingerprints etc. Iris Recognition takes into account together of the simplest biometric technique used for human identification and verification, owing to its distinctive feature that disagree from one person to a different, and its importance within the security field. Now-a-days various researchers used many soft computing techniques in the iris recognition system. This paper gives a brief survey of these techniques used for feature extraction such as neural network, genetic algorithm, fuzzy logic and particle swarm optimization.

Keywords: Authentication, iris recognition, Feature Extraction, Neural Network, Genetic Algorithm, particle swarm optimization, Fuzzy Logic.

1. Introduction:

The internet is one of the most suitable and widely used techniques in computing system. But, now-a-days, it is facing many challenging problems like data integrity, confidentiality, authentication and availability of information in all forms. Among them, authentication is an important and complex issue for any trustworthy systems. It determines that the person who is using the system resources should have the rights associated with its identity. In addition, for many security functions like key management, secure cluster communication, it is the first step to perform. There are many authentication techniques like passwords or smart cards which have been used for authentication. There are some drawbacks with these systems like multiple passwords/smartcards for various systems etc. To reduce the cons of traditional security systems, new technology called biometric is introduced which associates an individual with his identity.

The biometric is a promising field of technology that uses physiological or behavioral characteristics to mark or verify someone[1]. Physiological characteristics used for

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

authentication uses fingerprint, face and iris. A traditional biometric identification system consists of following two phases: -enrollment and identification. During the enrollment section, biometric feature set is extracted from user's biometric information and a sample is captured and stored. In identification phase, the same feature extraction algorithm is used to extract the features of an individual and then compared with the stored samples, extracted in the previous phase. For identification if both samples are matched then that person is considered as authenticated otherwise not.

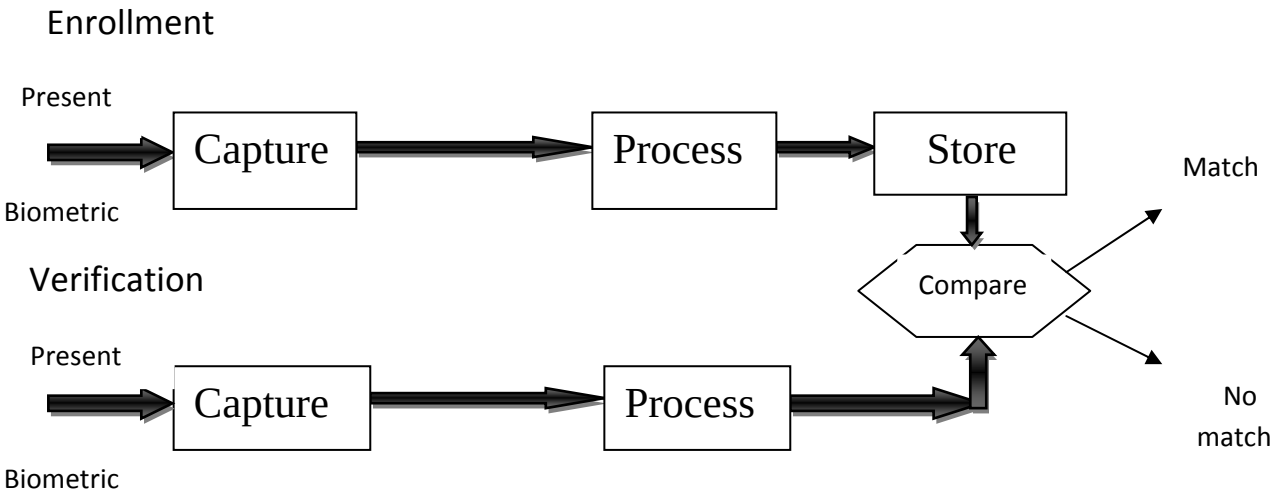


Fig1: Phases of biometric based authentication system

Now-a-days, many biometric strategies have been developed like fingerprint, iris, face, signature, retina, hand-geometry and speaker. Among them, iris authentication system is the primary existing technique for identification because of the singularity and long-run stability. The chance of two people having a constant Iris pattern is one in 1078 and even twins has totally different Iris pattern[2]. The process of Iris recognition consists of four steps: iris image acquisition, preprocessing, feature extraction, and matching and recognition.

1. Iris image acquisition: The first step of iris recognition is image acquisition. Special cameras have been used to capture the images of iris. First the smaller size image of the iris is combined with the possibility of varying colors of iris. The user has to stand in front of special device with eyes widely open in a range of 10-50 cm so that a clear image can be extracted.

2. Iris pre-processing: Images captured in above phase are then preprocessed to remove the noise and blurring effect. Preprocessing is subdivided into 2 parts:

a. Positioning: First the image is considered so that the inner and outer boundaries of the iris in images should be determined and then ensures that the iris data should be reliable which estimates for every scan. It evaluates the circular and non-circular boundaries of an iris.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

b. Normalization: images captured from the devices may be of different sizes for the same person. It is due to deviation in illumination or other factors. This process produces the same iris regions so the two images of the same iris capture from different devices or conditions posses same characteristic feature.

3. Iris feature extraction: in the feature extraction process, the feature of the iris is extracted and a template is generated which is stored in the database and further used in matching step. The generated template consists of an ordered sequence of data from the images extracted from the above steps.

4. Matching and recognition: In matching phase, the feature extracted in verification step is compared with the stored image in the database. If the distance or difference (calculated using hamming distance and Euclidean distance) between these templates is less than the threshold value than these two images belongs to same person otherwise or not.

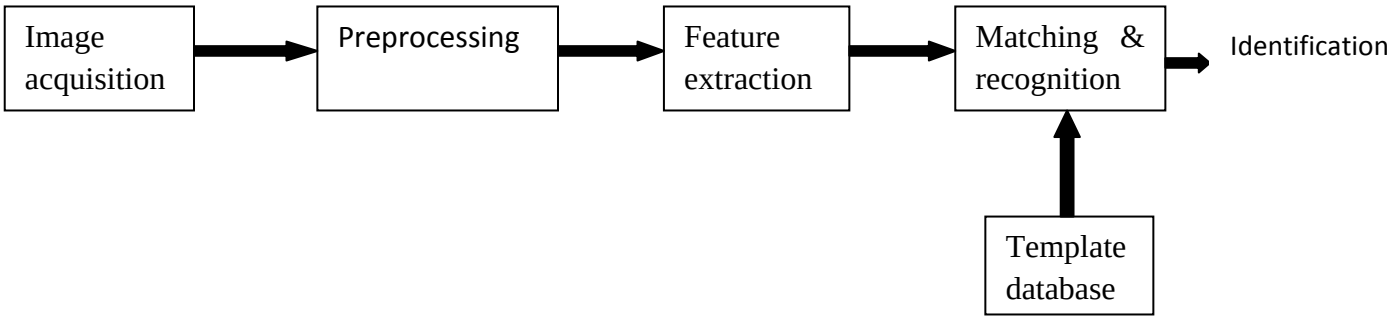


Fig2: Steps of iris recognition

Soft computing is an important branch of computational intelligent and knowledge-based systems. It is applied on those problems in computer science whose solutions are not easy to calculate, uncertain and between 0 and 1 Its goal is to exploit the robustness, good relationship with reality, low cost solution, uncertainty and partial truth to obtain tractability and tolerance of imprecision.. There are many soft computing techniques used in a feature extraction process like a neural network, genetic algorithm, fuzzy logic and particle swarm optimization. The aim of this paper is to provide a brief survey on application of these soft computing techniques in iris recognition system. The organization of this paper is as follows: section 2 presents the brief introduction of neural network used by various researchers in iris recognition system. Section 3 provides the brief overview of genetic algorithm in iris system. in section 4 some researchers describes the uses of fuzzy logic to handle uncertainties in iris recognition system. Section 5 contains the PSO algorithm used for classification of features from images and finally section 6 concludes the paper.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

2. Neural Network:

The neural network is simplified form of the biological network system and working of neural network is inspired by a human brain. Generally, neural network is a highly interconnected network of processing element in architecture similar to brain. The processing elements ate called neurons. The characteristics of neural network are mapping capabilities or pattern association, generalization, robustness, fault tolerance and parallel and high speed information processing. Actually neural network learns with the help of known example. These networks are then trained with known examples. Once they get trained, it can be used to solve the unknown cases of the problems. Neural network have been successfully applied to problem in the fields of pattern recognition, image preprocessing, data compression, forecasting and optimization to quote a few, in feature extraction techniques and so on. Neural network is used to classify the patterns extracted from feature extraction process.

In year 2005 Ching-Han Chen et al [3] proposed a new technique called wavelet probabilistic neural network to classify the pattern extracted from feature extraction process. WPNN combines two networks: Wavelet Neural Network and Probabilistic Neural Network. Authors use Sobel Transform and vertical projection to extract the feature extraction & to adjust the weights of WPNN. The authors applied PSO technique to train the WPNN. This system is applied to CASIA dataset and experimental results shows that recognition time/per image is less than 1ms and Equal error rate (EER) parameter of iris recognition is 3.32% that shows the superiority of the proposed method.

In year 2007 Rahib H. Abiyev et al [4] introduced a new iris recognition system for identification of persons. Instead of using Haugh Transform for recognition, they detect a rectangular area of iris for fast localization of the image. Finally Neural Network is used to classify the images for recognition. Experimental result when applied to CASIA dataset shows accuracy rate of 98.25% and thus shows superior performance when compared to Dyadic wavelet transform.

In year 2010 Fernando Gaxiola et al [5] presents a new architecture of a neural network to recognize the people. With the help of image processing method, the database is enhanced & the iris boundaries are calculated to cut the unwanted areas of the iris, then the iris images are processed and trained by modular neural network. The modular neural network is made up of three simple neural networks and each networks works like functional modules. To integrate all results of the three modules, gating network is used. Author reports 96.80% identification rate for person identification when applied to CASIA dataset.

In year 2010 Leila Fallah et al [6] proposed iris recognition method in which learning vector quantization (LVQ) is used. LVQ is a special case of the artificial comparative neural network. This paper uses convenience matrix for iris recognition. This matrix takes an iris image as input & produced edges of iris images. This edge has been used as input in probabilistic neural

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

network. This method can easily classify noisy & non noisy images and shows very promising simulation results.

In year 2011 A. Murugod et al [7] uses back propagation neural network (BPNN) for classification of iris template generated by a feature extracted method. The number of nodes in input layer is equal to the dimension in feature vector & output is equal to number of subjects in the dataset. By using BPNN, the system reliability gets improved by selecting half region of the iris. When it is applied to MMU dataset then experimental result shows 100% success rate and shows better performance when compared with traditional techniques (like GW, LBP& HOG).

In year 2012 Omaima et al [8] gives an iris recognition system on five different Artificial Neural Networks (ANN) models. These are feed forward (FFBPNN), cascade forward (CFBPNN), perform fitting (Fit Net), pattern recognition (Pattern Net) and learning vector division (LVQ Net). To train these models individually ten different ANN coaching algorithms (LM, BFG, BR, CGF, GD, GDM, GDA, GDX, OSS and RP) were used. Author reported that among the five ANN models, performance of Pattern Net model is superior. This model is then trained with ten coaching algorithms and found that Train LM is the best coaching algorithm for iris recognition system.

In year 2012 Vivek Srivastava et al [9] proposed the combination of functional modular neural network & fuzzy logic to classify the images. The authors use Minkowski distance which trains the pattern with less no. of clusters. Fuzzy clustering is used to find the best numbers of clusters which is used to decode the parameter of network for functional modular network. The functional modular neural network is designed to classify the input data based on survey distribution. It has single hidden layer. The experimental results prove that the novel approach is more flexible & provides recognition rate 98.12% than the LPQ techniques.

3. Genetic Algorithm:

Genetic algorithms (GA) are derivative-free optimization techniques, which can through procedures analogous to biological evolution. Genetic algorithms belong to the area of evolutionary computing. They represent an optimization approach where a search is made to “evolve” a solution algorithm, which will retain the “fit” components in a procedure that is analogous to biological evolution through natural selection, crossover, and mutation.

A genetic algorithm works with a population of individuals, each representing a possible solution to a given problem. Each individual is assigned a fitness score according to how good its solution to the problem is. The highly fit individuals are given opportunities to reproduce by crossbreeding with another individual in the population. This produces new individuals as offspring, who share some features taken from the parent. The unfit members in the population are finally died out. An entirely new population of possible solutions is produced in this manner, by mating the best individuals from the current generation. In this way, over many generations, desirable characteristics are spread throughout the population. Recently, GAs is finding widespread applications in solving problems requiring efficient and effective search, in business, scientific and engineering circles like a synthesis of neural network architecture, travelling salesman problem, graph coloring, scheduling, numerical optimization, and pattern recognition,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

feature extraction and image processing. In feature extraction process, genetic algorithm is used for better selection of feature subsets based on different feature selection methods to obtain the classifier.

In year 2008 Kaushik Roy et al [10] proposed a new method for feature selection and enhanced the system security. The proposed system uses genetic algorithm for better selection of feature subsets based on different feature selection methods to obtain the classifier. This system is more efficient compared with traditional feature selection system like principal component analysis & gives an identification rate of 97.90% for ICE dataset & 96.30% for WVU dataset.

A new biometric approach is exciting in which the individuals are identified by their skin texture of the edges of the iris. In the year 2010 Jashua Adams[11] uses this application. He extracts the image by using Local Binary Patterns Then he applied a new technique called genetic & evolutionary feature extraction to optimize these feature sets up to 50% with high identification rate. WMNE helps of GEC; the numbers of features get minimized with minimum number of recognition rate. An experimental result proves that it is a superior system with high success rate when it is applied to the FRGC data set.

Some researcher used GABOR filter to extract features & preventing for information losses but it generates very large features which required extra space for storage. In year 2011 Hamed Ghodrati et al [12] uses multi objective GA to reduce the limitations of Gabor Filters & to increase the accuracy of the system. Due to Gabor filter, parameters are not optimized because of randomness of new images. Therefore GA is used to optimize the Gabor filter parameter & to decrease the filter size. Further the extracted image is encoded by using amplitude variation quantization. Experimental result when this applied on CASIA- IRIS V INTERNAL database shows very promising results with CRR=99.68% & EER=0.26% for 2125 iris images.

In year 2012 Hamed et al [13] gives another paper that uses two GA based novel approaches. In The first approach genetic algorithm is used to optimize the parameter of Gabor filter to so as extract the optimized features and in the second approach GA is used to select most prominent templates from these optimized features. Experiments were performed on CASIA dataset and results were compared with traditional GABOR filter, it has been reported that the value of CCR parameter is 1.09% and recognition rate is 98.63%.

In year 2013 V. Saishanmuga Raja et al [14] proposed a hybrid technique of neural network & genetic algorithm for classification of images to optimize the low recognition rate & increase recovery time. First the neural network is used for localization of iris & generates images. Then genetic algorithm is used to reduce the parameter of neural network. The genetic algorithm is an optimization process, which requires a group of initial solution in each generation. In every generation one best solution is selected according to fitness process. Here genetic algorithm is used to optimize training time of neural network. A simulation result gives a recognition rate 98.48% & reduces the training time of neural network up to 20s with the existing neural network without GA.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

4. Fuzzy Logic:

Although the probability theory has been an age old and effective tool to handle uncertainty, it can be applied only to situations whose characteristics are based on random processes, that is, processes in which the occurrence of events is strictly determined by chance. However, in reality, there turn out to be problems, a large class of them whose uncertainty is characterized by a nonrandom process. Here, the uncertainty may arise due to partial information about the problem, or due to information which is not fully reliable, or due to inherit imprecision in the language with which the problem is defined, or due to receipt of information from more than one source about the problem which is conflicting. Fuzzy set theory enhances huge potential for effective solving of the ambiguity in the problem. Fuzziness means 'ambiguity'. Fuzzy set theory is used to handle the uncertainty which is raised due to ambiguity in any system. The common instances of the fuzziness manifests are understanding human speech and recognizing the features.

Fuzzy logic is useful in representing human knowledge in a specific domain of application and in reasoning with that knowledge to make useful inferences or actions. The conventional binary logic is crisp and allows for only two states. This logic cannot handle fuzzy descriptors, examples of which are "fast" which is a fuzzy quantifier and "weak" which is a fuzzy predicate. They are generally qualitative, descriptive, and subjective and may contain some overlapping degree of a neighboring quantity, for example, some degree of "slowness" in the case of the fuzzy quantity "fast". Fuzzy logic allows for a realistic extension of binary, crisp logic to quantitative, subjective, and approximate situations, which often exist in problems of intelligent machines where techniques of artificial intelligence are appropriate.

In the feature extraction process fuzzy logic handles uncertain & imprecise data during classification. The pupil is the dark circular area of human iris. Sometimes pupil is partially influenced by the certain noises such as eyelids, eyelashes etc., and it create uncertainties in the extracted feature. Therefore to deals with these uncertainties fuzzy logic is used.

.

In year 2010 C.C. Teo et al [15] proposed fuzzy logic based new segmented iris method. The pupil is the dark circular area of human iris. Sometimes pupil is partially influenced by the certain noises such as eyelids, eyelashes etc., it creates uncertainties in the extracted feature. Therefore to deals with these uncertainties fuzzy logic is used. This new scheme is tested in MMU2 database with 18414 iris images & concluded that this scheme 97.30% correctly segmented the images.

After considering all visible properties of iris S R Kodituwakku et al [2010] [16] attempt to use fuzzy logic in an iris recognition system. Proposed system consists of enrollment & verification phase. In enrollment phase, with the help of image processing methods, first the features of iris are extracted & then converted into numeric form called as iris codes. In verification phase fuzzy logic was used that takes above iris codes as crisp set. Then comparison of codes from both is phases are made to determine match or mismatch. Authors concluded that the proposed system when applied to CASIA dataset has success rate of 98.6%, FAR of 0.23% & FRR of 1.16% for 432 eye images

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Naresh Babu et al [2011] [17]proposed a new method in iris recognition system and named it as fuzzy iris recognition system to reduce the problem of existing recognition systems like noise, in consistency & illumination. They use Haugh Transform for detecting lines in feature extraction & for classification fuzzy logic is used. Fuzzy logic handles uncertain & imprecise data during classification. A simulation result shows that this proposed system outperforms compared to existing techniques.

In year 2011 Fernando Gaxiola et al [18]presents a new architecture of neural networks with type -2fuzzy integration for iris recognition combined system. With the help of this architecture, the system's performance gets improved & reduced the noise in the iris. The modular neural network made up three modules. All these modules consist of the one input layer, two hidden layers and are output layer and uses scaled gradient algorithm for learning. For integration of the two sub module type - 2 fuzzy integration is used. This architecture is tested on CASIA dataset for 594 images & achieves 97.98% of recognition rate.

Chung-Chih Tsai et al [19] proposed a new approach with fuzzy matching process for effective matching of images in year 2012. For iris segmentation they proposed an effective method to detect the boundaries of the iris images & after that they used a Gabor filter to extract local feature from the segmented eye. Then fuzzy matching algorithm is used to calculate the similarity between a pair of images of iris. A simulation result proves that this system is much better than original PCM when applied to an UBIRIS dataset with recognition rate 97.115% and EER=0. 1482.

5. Particle Swarm Optimization:

Particle swarm optimization (PSO) is SI based one of the optimization techniques in computer science. It measures the quality of candidate solution. It represents the best solution like a point in space of n- dimensional.. SI systems are the population of simple agent interacts with each other in an environment. This inspiration came from nature like behavior of ant in a colony, fish schooling, movements of particles in space etc. PSO is used in the feature extraction process as it is easy to understand. It takes every solution of search space and in every iteration, solution updates them and one of them is the optimal solution PSO is a global search strategy and avoids complex operations of genetic. With the help of PSO, the system not only achieves a higher recognition rate but also less computing time. Actually PSO is used as classifier to classify the correct features from images.

In the year 2010 Fuyou Han et al [20] proposed a new method in which he uses PSO for selection of features. First wavelet maximum is used for localization of image & then extraction of the image with the help of Gabor Filter is done. To select the key features of images GA is hybridized with PSO. Due to this, training time gets decreased and recognition rate gets improved. To check the validity of this proposed method, it is applied at CASIA database and compared with GA shows recognition rate of 96%.

In year 2012 Logannathan et al [21] first uses the combination of wavelet neural network & probabilistic NN to classify the biometric images. WPNN is used as pattern classifiers in the proposed system. Since the dimension of inputs in WPNN is very large therefore PSO is used to train it so that the architecture of WPNN gets optimized and system capabilities get improved.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The system when tested on CASIA database shows high accuracy & feasibility than other system.

In year 2012 Jin Liu et al [22] introduced the novel approach for iris recognition systems. In this system, Gabor Filter & wavelet maxima components are used to extract the images. Since, both the methods required lots of memory and time to save the extracted features. In this paper, the combination of radial basis function neural network (RBFNN) and PSO is used to classify the extracted images. The experimental result proves that the proposed system is much superior from another system in terms of performance.

Table1: Summary of various soft computing techniques used for feature extraction in iris recognition

S.No	Computational techniques used in iris system	Dataset Used	Recognition Rate (%)	Year	Other parameters	Compared With
	Neural Network					
1.	[3]	CASIA		2005	Best EER=3.32% Recognition time/image=<1ms	WPNN
2.	[4]	CASIA	99.25%	2007	Avg time = 0.4s	Dyadic Wavelet Transform
3.	[5]	CASIA	97.13%	2010		Multichannel Gabor Filtering
4.	[7]	MMU	98.33%	2011		Histogram of oriented gradient
5.	[8]	CASIA		2012		Fit net, FFBPNN,CFBPNN & LVQ Net
6.	[9]	CASIA	98.12%	2012		Local phase quantization
	Genetic Algorithm					
7.	[10]	1CE	97.90%	2008		Entropy Based, K-NNR, T-Statistics
8.	[11]	FRGC	92.16%	2010		Periocular Skin Texture
9.	[12]	CASIA IRIS V-3 Internal	99.68%	2011	EER=0.26%	GABOR wavelet filter
10.	[13]	CASIA	98.63%	2012	EER=1.09	2D-LDA+2D-PCA

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

11.	[14]	CASIA	98.48%	2013	Average time=20s	Neural network without GA
	Fuzzy Logic					
12.	[15]	MMU2	97.30%	2010		Hough Transform
13.	[16]	CASIA		2010	FAR=0.23% FRR=1.16%	
14.	[17]	CASIA	97%	2011		Wavelet+PCA+ NN
15.	[18]	CASIA	97.98%	2011		Modular neural network using contour segmentation
16.	[19]	UBIRIS	97.115%	2012	EER=0.1482	Original PCM
	PSO					
17.	[20]	CASIA	96%	2010		Feature selection using GA

6. Conclusion:

Iris recognition is one of the best biometric systems to secure the visual identification of a person. It has four phases: image acquisition, preprocessing, feature extraction and matching. Among them, feature extraction is the most important step in which several features of the iris are extracted and stored in a database for further used. Inconsistency between these features should be clearly discriminating and exact so that system can recognize the person with maximum efficiency.

Now-a-days various soft computing techniques are used by several researchers in the iris recognition system. This paper includes some of soft computing techniques like neural network, genetic algorithm, PSO and fuzzy logic. Different types of neural networks like WPNN, BPNN and RBFNN are used as a feature classifier in the feature selection process of iris recognition system. Each of these techniques have their own advantages like RBFNN doesn't require any mathematical description of how input and output features are co-related, WPNN is a very simple recognition classifier model used for reducing the low recognition rate in the iris recognition system and BPNN provides a good balance between input and output features that are similar. Also these neural networks have higher training time so researchers hybridized these networks with the PSO and genetic algorithms to reduce it.

Researchers used a genetic algorithm in an iris recognition system to optimize the parameters of Gabor filter used for feature extraction and to reduce the generated features so that extra storage space is not required. PSO is used to select the correct features in the feature selection process for obtaining high recognition rate while fuzzy logic is used to reduce the uncertainties of features present in preprocessing step so that correct images can be classified in further steps. This paper concludes the survey that how the recognition rate of iris system gets improved and training time gets reduced by using these techniques. In future, it provides a proposal for the growth of new techniques in this area.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

References:

[1] Yan Sui, Xukai Zou and Yingzi Du," Biometrics-based Authentication: a New Approach" ICCCN, VOL. 77, NO.5, pp. 1-6, 2011.

[2] Mohamad Ramli, Nurul Akmar, Kamarudin, Muhammad Saufi, Ariffuddinin,"Iris Recognition for Personal Identification",The International Conference on Electrical Engineering (ICEE), NO. 099, pp. 1-5, 2008.

[3] Ching-Han CHEN,Chia-Te CHU, "Low Complexity Iris Recognition Based on Wavelet Probabilistic Neural Networks" published in IEEE transactions, pp. 1930-1935, 2005.

[4] Rahib H. Abiyev and Koray Altunkaya, "Iris Recognition for Biometric Person Identification Using Neural Networks", Springer, pp. 554–563, 2007.

[5] Fernando Gaxiola, Patricia Melin, , and Miguel López, "Modular neural networks for person recognition using segmentation and the iris biometric measurement with image pre-processing ", IEEE transaction, pp. 1-7, 2010.

[6] Leila Fallah Araghi, Hamed Shahhosseini, Farbod Setoudeh, "IRIS Recognition Using Neural Network", IMESC, Vol. 1, pp.1-3, 2010.

[7] A. Murugan G. Savithiri, "Fragmented Iris Recognition System using BPNN", International Journal of Computer Applications, Vol 36– No.4, pp.28-33, 2011.

[8] Omaima N. Ahmad AL-Allaf, Abdelfatah Aref Tamimi, Shahlla A. AbdAlKader, "Artificial Neural Networks for Iris Recognition System: Comparisons between Different Models, Architectures and Algorithms", International Journal of Information and Communication Technology Research, Vol. 2,No. 11, pp. 795-803, 2012

[9] Vivek Srivastava, Bipin Kumar Tripathi,Vinay Kumar Pathak, "Biometric Recognition By Hybridization Of Evolutionary Fuzzy Clustering With Functional Neural Networks", Springer, pp. 13, 2012.

[10] Kaushik Roy and Prabir Bhattacharya, "Optimal Features Subset Selection Using Genetic Algorithms for Iris Recognition", Springer Concordia Institute for Information Systems Engineering (CIISE), pp. 894–904, 2008.

[11] Joshua Adams, Damon Woodard, Gerry Biometric Recognition", ACMSE, pp.1-4, 2010. Dozier, Philip Miller, George Glenn, Kelvin Bryant, "GEFE: Genetic & Evolutionary Feature Extraction for Periocular Based

[12] Hamed Ghodrati, Mohammad Javad Dehghani, Habibolah Danyali,, "Iris Feature Extraction Using Optimized Gabor Wavelet Based on Multi Objective Genetic Algorithm", IEEE, Department of Telecommunication Engineering, pp. 159-163, 2011.

[13] Hamed Ghodrati, Mohammad Javad Dehghani, Habibolah Danyali, "Two Approaches Based on Genetic Algorithm to Generate Short Iris Codes" ,I.J. Intelligent Systems and Applications, , pp.62-79,2012.

[14] V. Saishanmuga Raja ,S.P. Rajagopalan, "IRIS Recognition System using Neural Network and Genetic Algorithm", International Journal of Computer Applications, Vol. 68, No.20, pp. 49-53, 2013.

[15] C.C. Teo, H.F. Neo, G.K.O. Michael, C. Tee, and K.S. Sim , "A Robust Iris Segmentation with Fuzzy Supports", ICONIP, Springer, pp. 532–539, 2010.

[16] S. R. Kodituwakku and M. I. M. Fazeen, "An Offline Fuzzy Based Approach for Iris Recognition with Enhanced Feature Detection", Advanced Techniques in Computing Sciences and Software Engineering, Springer, pp. 41-44, 2010.

[17] Naresh Babu N T, Vaidehi V, “Fuzzy Based IRIS Recognition System (FIRS) For Person Identification”, IEEE- ICRTIT, pp.1005-1010, 2011.
[18] Fernando Gaxiola, Patricia Melin, Fevrier Valdez, and Oscar Castillo, “Modular Neural Networks with Type-2 Fuzzy Integration for Pattern Recognition of Iris Biometric Measure”, Springer, pp. 363–373, 2011.
[19] Chung-Chih Tsai, Heng-Yi Lin, Jinshiuh Taur, and Chin-Wang Tao, “Iris Recognition Using Possibilistic Fuzzy Matching on Local Features” IEEE Transactions On Systems, Man, And Cybernetics, Vol. 42, No. 1, pp.150-162,2012.
[20] Fuyou Han, Jinsong Li, Miao Qi, Ming Sheng, “An approach of Iris Recognition Based on Particle Swarm Optimization”IEEE transaction, Frontier of Computer Science and Technology, pp.541-545, 2010.
[21] Mr. Logannathan.B, Dr. Marimuthu.A, “Iris Authentication Using PSO” International Journal of Computer& Organization Trends, Vol. 2, pp. 10-15. -2012.
[22] Jin Liu, Xiao Fu, Xingbin Yao, “PSO-RBFNN Based Optimized PNN Classifier Model “, IEEE transaction Computer Science and Network Technology, pp. 456-459 2012.

.

SIGNIFICANT FACTORS AFFECTING THE USE AND INTEGRATION OF INFORMATION TECHNOLOGY (IT) TOOLS IN TEACHING IN SOUTH WESTERN NIGERIAN POLYTECHNICS

[1]Aladesote, O. Isaiah
Computer Science Department
Rufus Giwa Polytechnic, Owo, Ondo State.

[2]Agbelusi Olutola
Computer Science Department
Rufus Giwa Polytechnic, Owo, Ondo State.

[3]Ojajuni O. James
Computer Science Department
Rufus Giwa Polytechnic, Owo, Ondo State.

ABSTRACT

Information Technology (IT) also referred to as Information and Communication Technology (ICT) can be described as electronic technologies used for information storage and retrieval (Adomi & Kpangban, 2010). This paper examined various factors hindering the use of IT tools in teaching in South Western Nigerian Polytechnics and also extract the most significant factors that pose serious challenges to the use and integration of IT in teaching using Gain Ratio extraction technique. Questionnaires were distributed to Lecturers and seasoned administrators in the Polytechnic sector to access their knowledge and belief on the stated factors. The responses from the respondents were used to form a dataset. C# Programming was used for the implementation. Also, Microsoft Excel was used for the analysis of the data collected. The result of the analysis shows that seven (7) factors were highly hindering the use and integration of IT tools into teaching.

Keywords: ICT, Gain Ratio, Microsoft Excel, Extraction Technique.

INTRODUCTION

Information and Communication Technology (ICT) used as an extended synonym for Information Technology (IT), is usually a more general term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers, middleware as well as necessary software, storage- and audio-visual systems which enable users to create, access, store, transmit, and manipulate information (Adomi & Kpanghan, 2010). Integration of Information and Communication Technology (ICT) tools in teaching has been at the forefront of the education sector for recent years (Mee & Zaitun, 2006).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Information and communication technologies (ICT) are electronic technologies used for information storage and retrieval. Development is partly determined by the ability to establish a synergistic interaction between technological innovation and human values. The rapid rate at which ICTs have evolved since the mid 20th century, the convergence and pervasiveness of ICTs, give them a strong role in development and globalization (Nwagwu, 2006). ICTs have a significant impact on all areas of human activity (Brakel and Chisenga, 2003). The field of education has been affected by ICTs which have undoubtedly affected teaching, learning and research (Yusuf, 2005). A great deal of research has proven the benefits to the quality of education (Al-Ansari, 2006). ICTs have the potential to accelerate, enrich and deepen skills to motivate and engage students to integrate school experience to work practices, create economic viability for tomorrow's workers as well as strengthening teaching. (Davis and Tearle, 1999; Lemke and Coughlin, 1998; cited by Yusuf, 2005).

In a rapidly changing world, basic education is essential for an individual to be able to access and apply information with the use of ICT. The Economic Commission for Africa has indicated that the ability to access and use information is no longer a luxury, but a necessity for development. Unfortunately, many developing countries especially in Africa, are still low in ICT application and use (Aduwa-Ogiegbean and Iyamu, 2005). According to the Online Oxford Dictionary, Information and Communications Technology usually abbreviated as ICT, is often used as an extended synonym for information technology (IT), but is usually a more general term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers, middleware as well as necessary software, storage- and audio-visual systems which enable users to create, access, store, transmit and manipulate information. In other words, ICT consists of IT as well as telecommunication, broadcast media, all types of audio and video processing and transmission and network based control and monitoring functions.

PROBLEM STATEMENT

The forces that have driven institution of higher learning to adopt and incorporate ICT in teaching include greater information access, greater communication, increased cooperation, collaboration and cost-effectiveness (Surry and Ely, 2001). Much as investment in ICT continues to increase, information communication technologies such as computers, video players and projectors have not been effectively used in lecture rooms in institutions of higher learning in Nigeria (Farrell, 2007). Most lecturers do not use ICTs in lecture rooms while few that use the ICT tools in teaching

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

do not use them as expected. Despite the keenness of some institutions of higher learning to establish effective ICT education programs, they are confronted with enormous problems that may impede the proper implementation of these programs (Nwachukwu et al, 2009). Some of these problems are epilepsy power supply, fast changing of ICT tools, no enough ICT tools, Management attitude and poor network infrastructure, etc.

AIM AND OBJECTIVES

The aim of this research work is to investigate the factors that serve as challenges to the use of ICT tools in teaching in South Western Nigerian Polytechnics.

Objectives of the study

The specific objectives of this study are to:

(a) identify the variables responsible to challenges in the use of IT tools in teaching.

(b) extract variables that are highly challenging to the use and integration of IT tools in teaching in Nigerian Polytechnic.

METHODOLOGY

The existing works of the authorities in the field of IT in Education were reviewed. The first method employed was the use of questionnaire which consists of three parts. The first part of the questionnaire gathered the respondent's personal data or background such as their age group, gender, marital status and their educational attainment. The second part focused on the collection of data on factors affecting or preventing the integration of IT tools in teaching while the respondents were asked about their views on the research topic in the third part. Respondents provided information about their views through close-ended and open – ended questions on this topic.

Two hundred (200) questionnaires were distributed to three (3) Polytechnics in the South West region of Nigeria and 131 were returned by the respondents. Thus, a response rate of 65.5% was achieved. The responses from educational attainment in the first part and the second part of the questionnaires were used to generate a dataset in which the listed factors in the second part were used as the variables of the dataset and column heading. The response from each respondent formed a record in row of the dataset while the educational attainment serves as class in the last column of the dataset (See Appendix 1). The educational attainment was rated 1 for PhD, 2 for Masters, 3 for First Degree / Postgraduate Diploma, 4 for Higher National Diploma and 5 for Nigeria Certificate of Education and 6 for National Diploma. The degree of agreement on the item as a factor affecting the use of ICT was rated using Agree (A), Strongly Agree (SA), Disagree (D),

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Strongly Disagree (SD) and No Comment (NC), if the respondent never encountered the situation mentioned. Gain Ratio technique using C# Programming language was used to extract significant variables after which a threshold was set to actually determine factors that pose serious challenge to the integration of IT tools in teaching in Nigerian Polytechnics. Microsoft Excel was adopted to depict the data presentation of the data collected.

The dataset has twenty four (24) discrete variables. Let D be set consisting of d data samples with n distinct classes. The expected information needed to classify a given sample is given by (Asha Gowda Karegowda et al, 2010)

$$I(D) = -\sum_{i=1}^{n} pi \log_2(p_i) \quad \ldots\ldots\ldots\ldots \quad (1.0)$$

where pi is the probability that an arbitrary sample belongs to class C_i and is estimated by d_i/d. Let attribute A has v distinct values. Let d_{ik} be number of samples of class C_i in a subset D_j. D_j contains those samples in D that have value a_j of A. The expected information or entropy based on the partitioning into subsets by A, is given by

$$E(A) = -\sum_{i=1}^{n} I(D) \frac{d1j + d2j + \cdots dnj}{d} \quad \ldots\ldots\ldots\ldots \quad (1.1)$$

The information gained is given by

$$\text{Gain } (A) = I(D) - E(A) \quad \ldots\ldots\ldots\ldots \quad (1.2)$$

where E(A) is the entropy of the A and I(D) is the expected information.

$$\text{The splitInfo}_A(D) = -\sum_{i=1}^{v} (|Di|/|D|) log_2(|Di|/|D|) \quad \ldots\ldots\ldots\ldots \quad (1.3)$$

Equation (1.3) represents the information generated by splitting the training data set D into v partitions corresponding to v outcomes of a test on the attribute A.

$$\text{The Gain Ratio (a)} = \text{Gain (A)} / \text{SplitInfo}_A \text{ (D)} \quad \ldots\ldots\ldots\ldots \quad (1.4)$$

$$\text{The threshold Y1} > \frac{1}{d-1}\left(\sum a_i^2 - \frac{1}{d}\left(\left(\sum ai\right)^2\right) + \frac{1}{d-1}\left(\sum a_i^2\right)\right) \quad \ldots\ldots\ldots\ldots \quad (1.5)$$

FACTORS AFFECTING THE USE AND INTEGRATION OF IT TOOLS IN TEACHING WITH THEIR SYMBOLS

A1 = ICT tools are changing too fast to keep current trend

B1 = I have to spend extra time and effort after integrating ICT tools in teaching

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C1 = The Management does not provide any incentive for lecturers to integrate ICT tools in their teaching.

D1 = The network connectivity is poor

E1 = There is no network coverage in teaching environment

F1 = The Management does not have any evaluation on integration of ICT tools in teaching

G1 = The ICT tools are always reliable

H1 = I have had difficulty getting quality training programme towards the use of ICT tools

I1 = I have had difficulty getting support from technical staff

J1 = The hardware available is not sufficient to accommodate ICT supported teaching

K1 = The hardware available is already outdated to accommodate ICT supported teaching

L1 = The software available is not sufficient to accommodate ICT supported teaching

M1 = The software available had already outdated to accommodated ICT supported teaching

N1 = Certain software is difficult to learn and use

O1 = The Management do not provide any instruction on how to integrate ICT tools in my teaching

P1 = The Management do not initiate any program (such as seminar & workshop) to encourage ICT supported teaching.

Q1 = The Management does not have any vision on integration of ICT tools in teaching

R1 = My peers have giving negative comments about using ICT tools in teaching

S1 = Students have negative attitude towards ICT supported teaching

T1 = Students have negative feedbacks on ICT supported teaching

U1 = Most students are not computer literate

V1 = I found myself difficult to change from my current teaching practice to integrate ICT tools in teaching

W1 = There is no space to accommodate ICT tools

X1 = Epilepsy power supply does not encourage integrating ICT into teaching

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

RESULT AND DISCUSSION

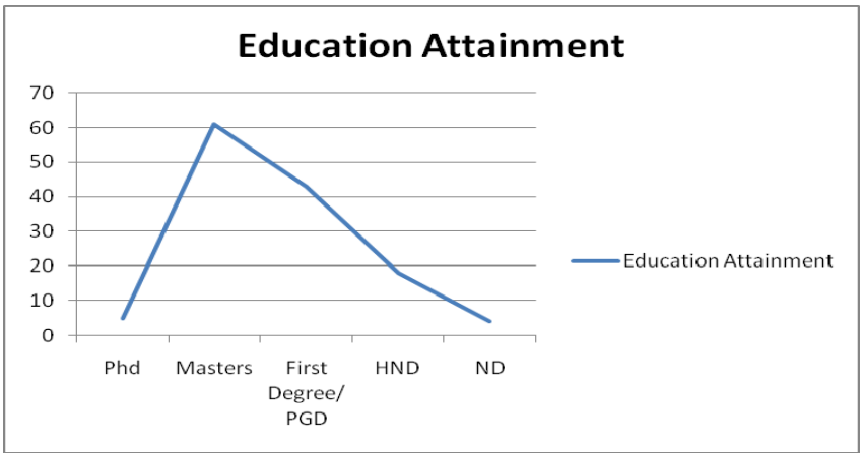


Figure 1.1: A graph showing the Education Attainment of the respondents.

From the Figure 1.1 above, it can be deduced that Masters Holders are more involved in administering the questionnaire than those with other higher qualifications. Meaning that Lecturers in Nigerian Polytechnics are mostly Masters Holders.

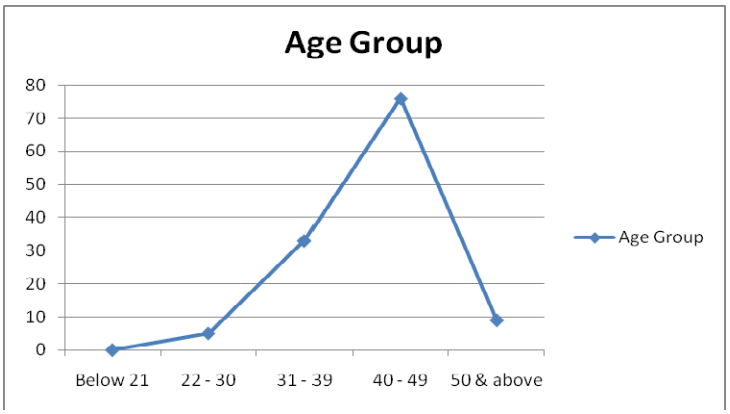


Figure 1.2: A Graph showing the Age group of the Respondents

From Figure 1.2 above, it can also be deduced that the age group between 40 – 49 has the highest knowledge of ICT in South Western Nigerian Polytechnic.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Questionair Output

	I(S):	E(A):	I(S) - E(A):	Split	Gain Ratio:
A1	2.0441	4.9597	-2.9156	1.4771	-1.9739
B1	2.0441	6.3321	-4.288	1.7674	-2.4262
C1	2.0441	5.7976	-3.7535	1.6282	-2.3053
D1	2.0441	6.8379	-4.7938	1.5834	-3.0275
E1	2.0441	6.1941	-4.15	1.8867	-2.1996
F1	2.0441	6.6387	-4.5946	1.6691	-2.7527
G1	2.0441	6.165	-4.1209	1.7601	-2.3413
H1	2.0441	7.5591	-5.515	1.9075	-2.8912
I1	2.0441	6.495	-4.4509	1.7232	-2.5829
J1	2.0441	8.0721	-6.028	1.9245	-3.1322
K1	2.0441	5.9036	-3.8595	1.8499	-2.0863
L1	2.0441	6.1867	-4.1426	1.7214	-2.4065
M1	2.0441	7.6914	-5.6473	1.8366	-3.0749
N1	2.0441	5.5041	-3.46	1.8541	-1.8661
O1	2.0441	7.4862	-5.4421	1.8257	-2.9808
P1	2.0441	7.2135	-5.1694	1.9521	-2.6481
Q1	2.0441	7.7165	-5.6724	1.8576	-3.0536
R1	2.0441	5.6341	-3.59	1.7757	-2.0217
S1	2.0441	6.8898	-4.8457	1.8627	-2.6014
T1	2.0441	6.0021	-3.958	1.7124	-2.3114
U1	2.0441	6.7531	-4.709	1.8007	-2.6151
V1	2.0441	6.7371	-4.693	1.8886	-2.4849
W1	2.0441	4.9743	-2.9302	1.5796	-1.8550
X1	2.0441	3.7794	-1.7353	1.0495	-1.6535

Table 1: Gain Ratio technique result for the variables

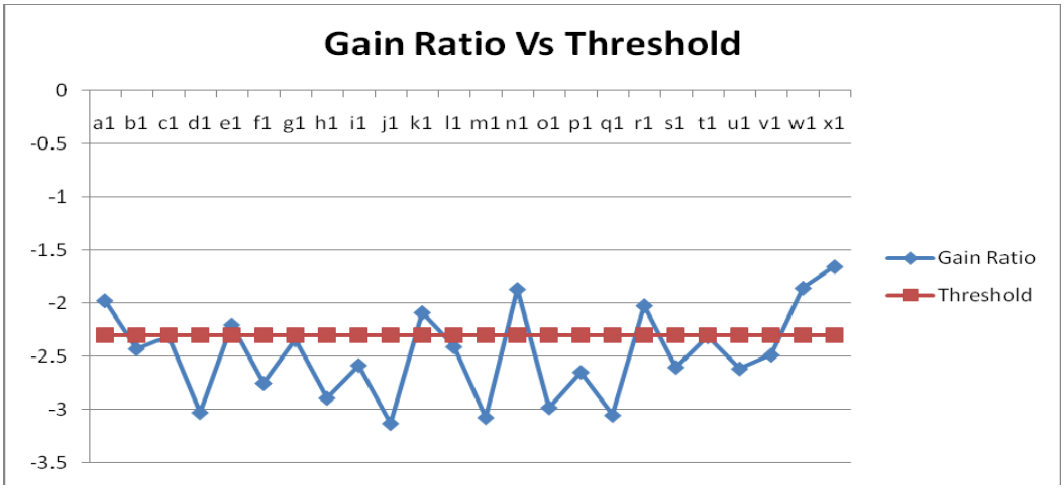


Fig 1.3: the Graphical Representation of Gain ratio Result and Threshold

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

From Table 1 shows the Gain Ratio results of factors under consideration while Figure 1.3 above shows the graphical representation of Gain Ratio result of each factor and the threshold value, which is -2.29513. Figure 1.3 reveals that out of the twenty four (24) factors considered, seventeen (17) factors (B1, C1, D1, F1, G1, H1, I1, J1, M1, N1, O1, P1, Q1, S1, T1, U1 & V1) are below the threshold, meaning that these factors are not significant; that is, they do not pose serious challenge to the use and integration of IT tools in teaching in Nigerian Polytechnics while the remaining seven (7) factors (A1, E1, K1, L1, R1, W1 & X1) that are above the threshold are significant, that is they pose serious challenge to the use and integration of IT tools in teaching (see Appendix 1).

CONCLUSION

The findings of this research work have showed that there are no similarities with other findings on the use of ICT tools in teaching in higher education in the developed nations like Malaysia. Epilepsy power supply, inadequate space to accommodate IT tools, negative comments about IT tools in teaching, insufficient hardware and software availability and that few available ones are outdated, no network connectivity and dynamism on the part of IT tools making it difficult to keep current trend are factors hindering the integration of IT tools in teaching in Nigerian Polytechnics and this has led to the low level of research in the South Western Nigerian Polytechnic.

RECOMMENDATION

In the view of the above conclusion, it is worth noting that successful integration of IT tools in teaching in Nigerian Polytechnics will not only lead to quality teaching but also produce quality and competent graduates that would favourably compete with its counterpart anywhere in the world. Proper funding of Polytechnic Education in order to meet the purpose of its establishment and incorporate the use of IT in teaching should of higher priority of all stakeholders.

The Federal Government should formulate a policy through the Federal Ministry of Communication Technology (FMCT) on how to integrate ICT tools in teaching in Nigerian Polytechnics in order to bridge the digital divide between Nigeria and the rest of the world. Moreover, the issue of epilepsy power supply that is a major factor hindering the integration of ICT tools in teaching should be properly addressed.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

REFERENCES

Adomi, E. E. & Kpangban, E. (2010): "Application of ICTs in Nigerian Secondary Schools". Library Philosophy and Practice.

Aduwa-Ogiegbaen, S. E. and Lyamu, E. S. (2005): "Using Information and Communication Technology in Secondary Schools in Nigeria: Problems and prospects". Educational Technology and Society, 8 (1), 104-112.

Asha Gowda Karegowda, A. S. Manjunati & M. A. Jayaram (2010): " Comparative Study of Attributes Selection using Gain Ratio and Correlation Based Feature Selection", International Journal of Information Technology and Knowledge Management. Volume 2, No. 2, pp. 271 – 277, July – December 2010.

Brakel, P.A., & Chisenga, J. (2003): "Impact of ICT Based Distance Learning, the African story". *The* Electronic *Library 21* (5), 476-486.

Davis, N. E. & Tearle, P. (1999): "A Core Curriculum for Telematics in Teacher Training". Tele-teaching 98 Conference; Vienna http://www.ex.ac.uk/telematics/T3/corecurr.

Farrell, G. (2007): "Survey of ICT and Education in Africa" Uganda country report. http:// www.infodev.org 5/11/2008

Lemke, C. & Coughlin, E. C. (1998): "Technology in American Schools". Seven dimensions for gauging progress. Milken Exchange Commission on Educational Technology. http://www.mff.org/pubs/ME158.pdf.

Nwagwu, W.E. (2006): "Integrating ICTs into the Globalization of the poor Developing Countries" *Information* Development *22* (3): 167-179.

Surry, D. W. and Ely, D. P. (2001): "Adoption, Diffusion, Implementation, and Institutionalization of Educational Innovations". In R. Reiser and J. V. Dempsey (Eds.), Trends and Issues in Instructional Design and Technology (pp. 183-193), Upper Saddle River, NJ: Prentice-Hall.

Yusuf, M.O. (2005): "Information and Communication Education: Analyzing the Nigerian National Policy for Information Technology". International *Education Journal 6* (3), 316-321.

Yusuf, M.O. (2005): "Integrating Information and Communication Technologies in Nigeria Tertiary Education". An Online Journal of Africa Education Research Network, 43 -50.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Appendix 1: Dataset used

A1	B1	C1	D1	E1	F1	G1	H1	I1	J1	K1	L1	M1	N1	O1	P1	Q1	R1	S1	T1	U1	V1	W1	X1	CLASS
A	A	D	A	A	SA	A	SA	D	SA	A	A	D	A	D	D	D	D	D	A	D	A	D	SA	3
A	D	SA	SA	SA	SA	SA	SD	SA	SD	SD	SD	SD	SD	SA	SA	A	SD	SD	SD	A	SD	SD	SA	2
D	A	A	SA	SA	A	SD	A	NC	NC	A	A	A	D	A	A	NC	SA	SA	D	SA	SD	D	SA	2
A	SA	SA	SA	SA	SA	SA	SA	A	SA	D	D	D	SA	SA	SA	SA	D	A	A	A	SD	SD	SA	2
SA	A	A	A	A	NC	A	D	D	A	D	A	D	A	NC	NC	D	D	A	A	A	D	A	A	2
A	D	A	NC	A	A	A	A	D	D	D	D	D	A	A	D	D	D	D	D	D	D	D	A	2
A	D	A	SA	SA	SA	SA	SA	A	SA	SA	SA	SA	SA	SA	SA	A	D	D	SD	SA	DS	D	SA	3
SA	D	SD	D	D	D	A	D	D	D	SA	D	D	D	SD	SD	SD	SD	SD	SD	A	SD	SD	SD	3
A	A	A	A	SA	SA	D	A	SA	SA	SA	SA	SA	NC	AA	NC	NC	A	A	A	SA	D	D	SA	4
D	A	A	SA	SA	A	D	A	D	A	A	A	A	A	D	SA	A	A	D	A	SA	D	D	SA	3
SA	NC	SA	SA	SD	NC	D	NC	NC	NC	SD	SA	NC	SD	D	SD	SD	SD	D	NC	D	NC	D	NC	3
D	SD	A	SA	SA	A	SA	SA	D	SA	SA	SA	SA	SD	SA	SA	NC	SD	SD	SD	SA	SD	SD	SD	3
C	D	NC	A	A	NC	D	D	D	A	D	A	D	D	NC	D	D	D	D	D	A	SD	D	A	3
SA	A	D	D	D	D	SA	D	D	SD	D	D	D	SD	D	SD	SD	SD	SD	SD	SD	SD	D	D	3
SA	A	A	A	SA	SA	SA	A	A	A	D	A	D	D	A	A	A	SD	SD	SD	A	SD	A	SA	3
SA	SD	SA	SA	SA	SA	SA	D	A	D	D	D	D	D	D	D	D	D	D	D	SD	D	D	SA	2
A	A	SA	SA	SA	SA	D	SD	A	A	A	A	SA	D	A	D	D	A	SA	A	SA	SD	SD	SA	2
A	A	A	SA	A	A	A	A	A	A	A	A	SA	D	A	A	A	D	D	D	A	A	D	SA	2
D	A	A	A	A	A	A	A	D	A	D	A	D	A	NC	D	NC	A	A	A	A	D	D	A	3
SA	SA	SA	SA	A	SA	D	D	D	SA	SA	SA	SA	D	SA	A	A	A	A	A	A	SD	D	SA	2
SA	A	A	A	A	D	SA	A	A	D	A	A	A	SA	SA	SA	D	A	D	D	SD	D	D	SA	5
A	A	D	SA	D	D	D	A	D	D	A	SA	A	A	D	A	D	D	SD	SD	A	D	SD	SA	3
D	A	A	D	D	D	SA	SA	SA	A	A	D	D	SA	D	SA	SD	D	SA	D	D	SA	D	SA	5
SA	SA	A	SA	SA	D	SA	A	A	SA	SA	SA	SA	SA	SA	SA	SA	SA	SA	SA	D	SA	A	SA	2
SA	SA	SA	A	SA	A	A	A	SA	SA	SA	SA	SA	SA	SA	A	A	SA	A	A	D	SA	A	SA	2
A	A	SA	SA	SA	SA	D	SA	SA	SA	SA	SA	SA	D	SA	SA	SA	SA	SD	D	A	D	D	A	4
D	SD	SA	SA	D	D	D	SA	A	A	A	SA	A	D	A	A	D	D	D	D	A	D	SD	SA	3
D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	A	A	1
A	A	A	SA	SA	SA	SA	D	D	D	D	D	D	D	D	D	D	D	SA	D	D	D	A	SA	3
SA	D	SA	SA	SD	SA	D	D	D	SA	D	SA	D	D	SA	D	D	D	D	D	D	SD	SD	SA	2
SA	SA	D	SD	D	A	SA	SD	SD	SD	SD	SD	D	SD	SD	SD	SD	D	D	D	SD	SD	D	SA	2
SA	SA	A	SA	SA	SA	D	NC	A	SA	D	SA	NC	D	SA	D	D	A	SA	SA	A	SA	D	SA	2
A	D	D	A	SD	A	A	A	D	A	A	A	A	A	A	D	D	A	D	D	D	A	SD	SA	3
A	D	A	SA	A	A	SA	A	D	D	D	SA	SA	SA	SA	SA	D	D	D	D	A	SD	D	SA	1
A	D	D	SA	A	SA	A	D	D	SA	SA	SA	SA	SA	SA	SA	D	D	D	SA	D	SA	D	SA	2
A	A	D	A	A	A	D	SA	SA	SA	SA	SA	SA	SA	SA	A	A	A	SA	A	D	A	A	A	2
A	A	A	SA	SD	D	SA	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	SD	SA	2
SA	SA	SA	SA	SD	D	SA	A	D	SA	D	A	D	D	D	D	D	A	A	D	D	D	D	SA	2
SA	A	A	SA	A	SA	SD	SD	SA	SD	D	D	D	D	A	A	A	SD	D	D	SD	D	D	SA	4
SA	D	D	SA	D	A	D	D	A	SA	D	A	A	A	A	D	D	A	NC	D	D	SD	A	SA	3
A	SA	SA	SA	D	A	D	A	SA	A	SA	SA	D	D	A	SA	SA	D	A	D	D	D	SD	SA	3
A	SA	SA	A	D	A	SA	SA	A	A	SA	A	A	D	A	D	D	D	D	D	A	SA	A	SA	4
A	NC	NC	NC	NC	NC	A	NC	NC	NC	NC	NC	NC	D	NC	NC	NC	A	NC	NC	`A	A	NC	A	4
A	A	D	A	D	A	D	A	A	A	A	A	A	A	D	D	D	D	A	D	D	D	D	A	2
SA	A	A	SA	A	SA	SA	SD	D	A	D	D	D	D	A	D	SD	SD	SD	SD	D	SD	SD	SA	2

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

SA	A	A	SA	A	A	A	D	D	A	D	A	A	SA	A	A	NC	A	A	A	D	A	D	A	2
A	D	A	SA	D	D	SA	D	D	SA	A	SA	SA	D	SA	D	D	D	D	D	A	SD	D	D	2
SA	SD	SD	A	D	D	A	SA	D	D	D	D	D	A	D	SD	D	D	D	D	A	D	D	A	2
A	A	A	A	A	A	D	A	A	A	A	A	A	NC	A	A	NC	A	A	A	A	D	D	A	2
A	D	A	SA	A	A	A	D	D	SA	A	D	D	D	A	A	D	D	D	D	A	D	D	SA	3
A	A	D	A	A	D	D	A	D	A	A	A	A	D	D	D	D	D	D	D	A	D	D	A	4
A	NC	A	SA	D	NC	NC	SA	NC	A	D	A	NC	D	NC	NC	NC	NC	SA	SA	D	NC	SD	NC	4
SA	A	A	A	A	A	NC	D	D	D	SA	D	D	A	D	D	A	A	D	SA	SA	A	D	SA	4
A	D	A	SA	D	D	SD	SD	D	A	D	D	A	D	A	D	A	D	A	D	A	SD	SD	SA	2
A	A	D	A	A	SA	A	SA	D	SA	A	A	D	A	D	D	D	D	D	A	D	A	D	SA	3
A	D	SA	SA	SA	SA	SA	SD	SA	SD	SD	SD	SD	SD	SA	SA	A	SD	SD	SD	A	SD	SD	SA	2
D	A	A	SA	SA	A	SD	A	NC	NC	A	A	A	D	A	A	NC	SA	SA	D	SA	SD	D	SA	2
A	SA	SA	SA	SA	SA	SA	SA	A	SA	D	D	D	SA	SA	SA	SA	D	A	A	A	SD	SD	SA	2
SA	A	A	A	A	NC	A	D	D	A	D	A	D	A	NC	NC	D	D	A	A	A	D	A	A	2
A	D	A	NC	A	A	A	A	D	D	D	D	D	A	A	D	D	D	D	D	D	D	D	A	2
A	D	A	SA	SA	SA	SA	SA	A	SA	SA	SA	SA	SA	SA	SA	A	D	D	SD	SA	DS	D	SA	3
SA	D	SD	D	D	D	A	D	D	D	SA	D	D	D	SD	SD	SD	SD	SD	SD	A	SD	SD	SD	3
A	A	A	A	SA	SA	D	A	SA	SA	SA	SA	SA	NC	AA	NC	NC	A	A	A	SA	D	D	SA	4
D	A	A	SA	SA	A	D	A	D	A	A	A	A	A	D	SA	A	A	D	A	SA	D	D	SA	3
SA	NC	SA	SA	SD	NC	D	NC	NC	NC	SD	SA	NC	SD	D	SD	SD	SD	D	NC	D	NC	D	NC	3
D	SD	A	SA	SA	A	SA	SA	D	SA	SA	SA	SA	SD	SA	SA	NC	SD	SD	SD	SA	SD	SD	SD	3
C	D	NC	A	A	NC	D	D	D	A	D	A	D	D	NC	D	D	D	D	D	A	SD	D	A	3
SA	A	D	D	D	D	SA	D	D	SD	D	D	D	SD	D	SD	SD	SD	SD	SD	SD	SD	D	D	3
SA	A	A	A	SA	SA	SA	A	A	A	D	A	D	D	A	A	A	SD	SD	SD	A	SD	A	SA	3
SA	SD	SA	SA	SA	SA	SA	D	A	D	D	D	D	D	D	D	D	D	D	D	SD	D	D	SA	2
A	A	SA	SA	SA	SA	D	SD	A	A	A	A	SA	D	A	D	D	A	SA	A	SA	SD	SD	SA	2
A	A	A	SA	A	A	A	A	A	A	A	A	SA	D	A	A	A	D	D	D	A	A	D	SA	2
D	A	A	A	A	A	A	A	D	A	D	A	D	A	NC	D	NC	A	A	A	A	D	D	A	3
SA	SA	SA	SA	A	SA	D	D	D	SA	SA	SA	SA	D	SA	A	A	A	A	A	A	SD	D	SA	2
SA	A	A	A	A	D	SA	A	A	D	A	A	A	SA	SA	SA	D	A	D	D	SD	D	D	SA	5
A	A	D	SA	D	D	D	A	D	D	A	SA	A	A	D	A	D	D	SD	SD	A	D	SD	SA	3
D	A	A	D	D	D	SA	SA	SA	A	A	D	D	SA	D	SA	SD	D	SA	D	D	SA	D	SA	5
SA	SA	A	SA	SA	D	SA	A	A	SA	SA	SA	SA	SA	SA	SA	SA	SA	SA	SA	D	SA	A	SA	2
SA	SA	SA	A	SA	A	A	A	SA	SA	SA	SA	SA	SA	SA	A	A	SA	A	A	D	SA	A	SA	2
A	A	SA	SA	SA	SA	D	SA	SA	SA	SA	SA	SA	D	SA	SA	SA	SA	SD	D	A	D	D	A	4
D	SD	SA	SA	D	D	D	SA	A	A	A	SA	A	D	A	A	D	D	D	D	A	D	SD	SA	3
D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	A	A	1
A	A	A	SA	SA	SA	SA	D	D	D	D	D	D	D	D	D	D	D	SA	D	D	D	A	SA	3
SA	D	SA	SA	SD	SA	D	D	D	SA	D	SA	D	D	SA	D	D	D	D	D	D	SD	SD	SA	2
SA	SA	D	SD	D	A	SA	SD	SD	SD	SD	SD	D	SD	SD	SD	SD	D	D	D	SD	SD	D	SA	2
SA	SA	A	SA	SA	SA	D	NC	A	SA	D	SA	NC	D	SA	D	D	A	SA	SA	A	SA	D	SA	2
A	D	D	A	SD	A	A	A	D	A	A	A	A	A	A	D	D	A	D	D	D	A	SD	SA	3
A	D	A	SA	A	A	SA	A	D	D	D	SA	SA	SA	SA	SA	D	D	D	D	A	SD	D	SA	1
A	D	D	SA	A	SA	A	D	D	SA	SA	SA	SA	SA	SA	SA	D	D	D	SA	D	SA	D	SA	2
A	A	D	A	A	A	D	SA	SA	SA	SA	SA	SA	SA	SA	A	A	A	SA	A	D	A	A	A	2
A	A	A	SA	SD	D	SA	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	SD	SA	2
SA	SA	SA	SA	SD	D	SA	A	D	SA	D	A	D	D	D	D	D	A	A	D	D	D	D	SA	2
SA	A	A	SA	A	SA	SD	SD	SA	SD	D	D	D	D	A	A	A	SD	D	D	SD	D	D	SA	4

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

SA	D	D	SA	D	A	D	D	A	SA	D	A	A	A	A	D	D	A	NC	D	D	SD	A	SA	3
A	SA	SA	SA	D	A	D	A	SA	A	SA	SA	D	D	A	SA	SA	D	A	D	D	D	SD	SA	3
A	SA	SA	A	D	A	SA	SA	A	A	SA	A	A	D	A	D	D	D	D	D	A	SA	A	SA	4
A	NC	NC	NC	NC	NC	A	NC	NC	NC	NC	NC	NC	D	NC	NC	NC	A	NC	NC	`A	A	NC	A	4
A	A	D	A	D	A	D	A	A	A	A	A	A	A	D	D	D	D	A	D	D	D	D	A	2
SA	A	A	SA	A	SA	SA	SD	D	A	D	D	D	D	A	D	SD	SD	SD	SD	D	SD	SD	SA	2
SA	A	A	SA	A	A	A	D	D	A	D	A	A	SA	A	A	NC	A	A	A	D	A	D	A	2
A	D	A	SA	D	D	SA	D	D	SA	A	SA	SA	D	SA	D	D	D	D	D	A	SD	D	D	2
SA	SD	SD	A	D	D	A	SA	D	D	D	D	D	A	D	SD	D	D	D	D	A	D	D	A	2
A	A	A	A	A	A	D	A	A	A	A	A	A	NC	A	A	NC	A	A	A	A	D	D	A	2
A	D	A	SA	A	A	A	D	D	SA	A	D	D	D	A	A	D	D	D	D	A	D	D	SA	3
A	A	D	A	A	D	D	A	D	A	A	A	A	D	D	D	D	D	D	D	A	D	D	A	4
A	NC	A	SA	D	NC	NC	SA	NC	A	D	A	NC	D	NC	NC	NC	NC	SA	SA	D	NC	SD	NC	4
SA	A	A	A	A	A	NC	D	D	D	SA	D	D	A	D	D	A	A	D	SA	SA	A	D	SA	4
D	D	D	A	D	D	SA	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	A	A	1
SA	SA	A	SA	SA	D	SA	A	A	SA	SA	SA	SA	SA	SA	SA	SA	SA	SA	SA	D	SA	A	SA	2
SA	SA	SA	A	SA	A	A	A	SA	SA	SA	SA	SA	SA	SA	A	A	SA	A	A	D	SA	A	SA	2
A	A	D	A	A	SA	A	SA	D	SA	A	A	D	A	D	D	D	D	D	A	D	A	D	SA	3
A	D	SA	SA	SA	SA	SA	SD	SA	SD	SD	SD	SD	SD	SA	SA	A	SD	SD	SD	A	SD	SD	SA	2
D	A	A	SA	SA	A	SD	A	NC	NC	A	A	A	D	A	A	NC	SA	SA	D	SA	SD	D	SA	2
A	SA	SA	SA	SA	SA	SA	SA	A	SA	D	D	D	SA	SA	SA	SA	D	A	A	A	SD	SD	SA	2
SA	A	A	A	A	NC	A	D	D	A	D	A	D	A	NC	NC	D	D	A	A	A	D	A	A	2
A	D	A	NC	A	A	A	A	D	D	D	D	D	A	A	D	D	D	D	D	D	D	D	A	2
A	D	A	SA	SA	SA	SA	SA	A	SA	SA	SA	SA	SA	SA	SA	A	D	D	SD	SA	DS	D	SA	3
SA	D	SD	D	D	D	A	D	D	D	SA	D	D	D	SD	SD	SD	SD	SD	SD	A	SD	SD	SD	3
A	A	A	A	SA	SA	D	A	SA	SA	SA	SA	SA	NC	AA	D	NC	A	A	A	SA	D	D	SA	2
D	A	A	SA	SA	A	D	A	D	A	A	A	A	A	D	SA	A	A	D	A	SA	D	D	SA	3
SA	D	SA	SA	SD	NC	D	NC	NC	NC	SD	SA	D	SD	D	SD	SD	SD	D	NC	D	NC	D	NC	3
D	SD	A	SA	SA	A	SA	SA	D	SA	SA	SA	SA	SD	SA	SA	NC	SD	SD	SD	SA	SD	SD	SA	3
A	D	A	SA	A	A	A	D	D	SA	A	D	D	D	A	A	D	D	D	D	A	D	D	SA	2
A	A	D	A	A	D	D	A	D	A	A	A	A	D	D	D	SD	D	D	D	A	D	D	A	3
A	NC	A	SA	D	NC	NC	SA	NC	A	D	A	NC	D	NC	NC	D	NC	SA	SA	D	NC	SD	A	4
SA	SD	SA	SA	SA	SA	SA	D	A	D	D	D	D	D	D	D	D	D	D	D	SD	D	D	SA	2
A	A	SA	SA	SA	SA	D	SD	A	A	A	A	SA	D	A	D	D	A	SA	A	SA	SD	SD	SA	2
A	A	A	SA	A	A	A	A	A	A	A	A	SA	D	A	A	A	D	D	D	A	A	D	SA	2
D	A	A	A	A	A	A	A	D	A	D	A	D	A	NC	D	NC	A	A	A	A	D	D	A	3
A	A	SA	SA	SA	SA	D	SA	SA	SA	SA	SA	SA	D	SA	SA	SA	SA	SD	D	A	D	D	A	4
D	SD	SA	SA	D	D	D	SA	A	A	A	SA	A	D	A	A	D	D	D	D	A	D	SD	SA	3

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

An Overview of Contemporary Cyberspace Activities and the Challenging Cyberspace Crimes/Threats

By

Samson Olasunkanmi Oluga*

Dr Azizah Bt Haji Ahmad

Ahmad Jamah Ahmad Alnagrat

Haroon Shakirat Oluwatosin

Maryam Omar Abdullah Sawad

Nur Adlya Bt Muktar

Of

School of Computing (SOC)

College of Arts and Sciences (CAS)

Universiti Utara Malaysia

06010 Sintok, Kedah

Malaysia

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Abstract

One thing that has emanated from the development of the internet technology and popular embrace of social networking is the emergence of a second digital world which is a virtual reality world called the cyberspace. The cyberspace users who can be described as the *Cyberians* are attracted to the cyberspace from time to time especially because of the various opportunities/activities available via the cyberspace cutting across many spheres of human endeavor. There are however many threats or challenges which may be inimical to the safety of the cyberspace, the cyberspace assets/resources and the interest of the *Cyberians,* the regular cyberspace users or cyber citizens. This paper, based on extensive examination of contemporary literature on the cyberspace, explores fundamental activities of the cyberspace and explicates various forms of cybercrimes orchestrated by cyber criminals posing great threats to the cyberspace. The basic ideas of the paper are equally captured in vivid illustrative models.

Keywords: Cyberspace, Cyber activities, Cybercrimes/Threats

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Introduction/Background

It is axiomatic that the present age of humankind is a computer technology age where virtually all aspect of human activities are computerized or computer-based and basic tasks in most spheres of human endeavor are enhanced or better executed via the instrumentality of modern or state of the art computer technology. It is also crystal clear that the whole wide world is presently in a state of constant transformation courtesy of the advent of advanced computer technology breakthroughs that are systematically revolutionizing the human society. The interesting thing about today's computer technology advancement orchestrated by competitive wizards, working rigorously, independently or collaboratively, all over the globe but driven by the positive goal of making the world a better place, is the quick succession of contemporary computer-based innovations.

Today, it will be highly unimaginable to think of life without computers or reverting to the pre-computer technology age characterized basically by manual execution of human activities and expending a lot of time, energy, efforts or resources on given tasks only to attract minimal results or outcomes. On the other hand, the minimum input with maximal output that is characteristic of computer technology application makes it exceptionally rewarding and simply preferred especially by those who have chosen to be computer technology compliant and always abreast development. The computer/ICT based internet technologies presently afford numerous end users myriads of opportunities online which are improved replicas or computerized versions of the traditional offline activities. It is in the light of the various online social, political, economic and educational activities as well as many others that computer technology/ICT has provided humankind a second world now described as the cyberspace.

The word/term cyberspace has attracted a number of definitions or semantic interpretations especially by experts and lexicographers trying to shed more light on the meaning of the concept. This is characteristic of topical concepts or contemporary phenomena coming to limelight or arousing research interest. Cyberspace according to Adnan (2010) is an unreal world where information is constantly transmitted through or between computers. It is a web of private cum public computer networks. It is a geographical milieu of online conversations, email exchanges, flame wars, spam attacks and information dissemination or exchange. The cyberspace according to Pfaffenberger (2000) simply refers to the virtual space that computer systems have aided its creation, that is, the computer technology invented world. In a similar

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

vein, McGraw Dictionary of Computing and Communications (2003) briefly describes the cyberspace as the digital realms which include websites and virtual worlds.

It is clear from the above definitions/descriptions of cyberspace that the cyberspace is a computer-technology invented /aid world. It is important to point out the fact that the first definition or description of cyberspace as an unreal world may not be as appropriate as the virtual space and digital realm/virtual world of the second and third definitions or descriptions respectively. This is simply because the cyberspace involves a lot of real happenings and activities similar to those of the physical world, so called the real world, hence there is a close relationship. It is against this background that the second world of the cyberspace is also described as the virtual reality world based on the fact that the lexeme 'virtual' semantically depicts something very close to reality.

This paper presents the outcome of an extensive examination of contemporary literature on the topical concept of cyberspace activities and the challenging cyberspace crimes/threats. The paper articulates fifteen (15) fundamental cyberspace activities that are attracting the attention/interest of several millions of cyber-navigators of different ages, genders, professions or status to the cyberspace, from time to time, day to day and place to place. The paper equally sheds light on some eighteen (18) prevalent cybercrimes/cyber threats that now constitute great challenge to the cyberspace as they can be inimical to the safety of the cyber assets/resources and the interest of the *Cyberians*. It fashions illustrative models to capture the ideas or concepts discussed to aid comprehension.

An Exploration of Fundamental Cyberspace Activities

The cyberspace has been constantly growing in terms of the numerical strength of its various users across nations as well as in relation to the various cyberspace activities attracting the numerous users to the cyberspace the world over. Korchmaros, Ybarra, Langhinrichsen-Rolling, Boyd and Lenhart (2013) corroborate the numerical growth of cyberspace users by pointing out the fact that 95% of United States adolescents aged 12-17 use the internet while 54% of the group text messages on daily basis. This is based on the outcome of their study of some 615 adolescents. Kumar (2013) equally puts the total number of internet users in India at 14.2 million by March 2013 with a total of 164.8 million net connections apart from apart from the numerous users of the popular cybercafés. The situation in other Asian countries like Malaysia, Indonesia, Singapore, Japan, Pakistan and China is not different.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The cyberspace is equally growing in terms of the existing cyber activities which have some similitude with those of the physical world and which tend to be more convenient and with less constraint as they can be done usually anywhere there are required facilities and cyber connection. The most fundamental of the cyberspace activities focused are cyber commerce, cyber learning, cyber socialization, cyber gaming, cyber entertainment, cyber journalism, cyber broadcasting, cyber advertising, cyber politics, cyber tourism, cyber medicine, cyber governance, cyber evangelism and cyber mobilization. These are captured in the diagram below and are discussed one after the other in the light of the views of contemporary cyberspace researchers.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Commerce in the Cyberspace

Cyber commerce, otherwise called electronic commerce i.e. e-commerce, covers all forms of electronic, online or internet business transactions. Vakharia, Mishra and Kumar (2013) describe electronic commerce as that which involves selling and buying of goods and services over the World Wide Web i.e. the internet-based business transactions which are fast becoming the order of the day especially because of their cost, choice, and time advantage among other benefits. They identify four main type of electronic commerce namely Business to Business Electronic Commerce,(B2BEC), Business to consumer Electronic Business(B2CEC), Consumer to Consumer Electronic Commerce (C2CEC) and consumer to Business Electronic Commerce(C2BEC). Specifically, in relation to electronic banking, Usman and Shar (2013) identify some basic electronic/banking services viz electronic fund transfer, electronic cheque version and WEB/ATM services. Rahman and Lacey (2013) observe that the development as well as the popularity of the internet has necessitated the transformation of some aspect in traditional commerce into electronic commerce which many have embraced and successfully implemented. This is simply because it has been realised that to compete in today's business/market, especially in a digital age, key business processes/transactions must have online or internet representation i.e. cyber-representation.

Cyber Learning/Education in the Cyberspace

Online learning and electronic learning are some of the terms used to depict the concept of cyber learning/education. Online learning according to Chiu, Chiu and Chang (2007) cited by Yee (2013) refers to learning done via the internet, intranet or extranet. It is regarded as one of the digital tools for the enhancement of teaching and learning the effectiveness or efficacy of which can be a function of how it is utilized. Yee (2013) identifies and examines the various online learning difficulties of some international students in Australian online learning setting or environment. Adeoluwa, Aboderin and Omodara(2013) equally identify computers and internet as essential media of educational technology that have been successfully utilized in teaching and learning. The study conducted by Zhuhadir,Yang and Lytras (2013) on the impact of the social media systems on cyber learners shows that they can facilitate the dissemination of knowledge and engagement of students in the course of teaching more effectively than the traditional face to face teaching approach.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The cyberspace is therefore providing various means of knowledge acquisition and dissemination for virtually all categories of people at all levels. There are electronic-based learning aids for students at various educational levels, pre-school, primary, secondary and tertiary. Permvattana, Amstrong and Murray (2013) discuss how e-learning can be designed to benefit the vision impaired. There are many courses now available online just as there are many exams now conducted online. Many learning materials are made available online just as there are lecture notes/lectures that can accessed online. Electronic versions of books, journals and magazines are now available online and library materials can be accessed without getting to the library. In fact, cyber learning/education has made the acquisition of knowledge interesting and relatively easy for all and sundry especially students, teachers and researchers. There are cyber fora for people to ask members of the cyber communities what they do not know or what they want to know the more, and those who know usually guide those who want to know or want to know the more.

Cyber Socialization/Relationship via the cyberspace

Naturally, humans are social beings hence socialization is more or less a distinctive human characteristic. The development of the internet–aided social networking and emergence of the cyber community now enhance human socialization potentials beyond expectations. Shahid (2013) observe that the importance of the internet technology is evident in virtually all spheres of human life and many now prefer the use of the internet and the new media for social communication than other traditional communication media. In a similar vein, Misra and Stokols (2012) confirm that cyber-oriented individuals have preference for the social virtual environments especially the chart rooms and there is the possibility that many of their real life/world relationships/marriage partners emanated from the cyberspace virtual world. Cyberspace-enhanced social communication has really revolutionized the seeking/initiation of romantic relationships/partnership as can be seen in growing rate of today's online dating. Finkey, Eastwick, Karney, Rels and Sprecher (2012:49) therefore assert that "it is fundamentally altering the dating landscape, restructuring the romantic acquaintance process and changing the nature of compatibility matching". However, it has been observed that some social Cybarians do abuse cyberspace via excessive cyberspace social communication and therefore end up with cyber-relationship addiction. This results from the addiction to the social relationship networking chart room and messaging to the extent that they now find online relationship/acquaintances more important than the existing real life/world

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

relationships/acquaintances. De Fife (2012) adds that excessive social networking or social network addiction can have negative impact as this can lead to social isolation/disengagement from real life activities/societies which ultimately may degenerate to affect social-psychological health by resulting in depression.

Cyber Entertainment in the Cyberspace

Cyber entertainment (cyber-tainment) can overlap with some other cyberspace activities especially those that can equally serve as good instruments of relaxation, amusement and warding off stress. However, cyber entertainment in this context is specifically in respect of how the internet functions as the mechanism or instrument for the provision of online songs, films, video games etc. for the entertainment or enjoyment of today's more than 1.5millions internet users (Jaff & Chen, 2010). O'Keeffe and Clark-Pearson (2011) identify the YouTube as a key entertainment and communication website that happens to be the favourite of many, especially the youth and the young at heart, as well as some blog, gaming and virtual world sites. They further strongly caution that the use of the internet or cyberspace by children needs to be monitored to prevent any abuse or misuse that could negatively impact on them. Lopez-Fernadez, Freixa-Blanxast and Honrubia-Serrano (2013) also buttress the need for a controlled adolescent online/cyber entertainment use by stressing the fact that researches have reported/established non-substance addition to online entertainment among adolescents. However, the fact still remains that cyber entertainment can be to the benefit of users especially when used to ward off stress or ease tension like playing music while working on the system.

Cyber Gaming in the cyberspace

Cyber gaming happens to be one key cyber activity that is attracting the vast majority of the youths to the cyberspace these days. It is basically supposed to be another means of relaxation for the gamers both contemporary trends show that it is now being abused and misused making it attract attention. An International Conference on Cyber Games (CG2008) held in Beijing, China from 27-30 October, 2008 which is a pointer to the topicality of cyber gaming as a key component of the cyber space or key cyberspace activity. Yee (2007) points out that there is an enhancement of cyber gaming with the Massive-Multiplayer Online Role-Playing Games (MMORPGs) online environment that facilitates the interaction of millions of people on daily basis. Cole and Griffith (2007) point out the uniqueness of the MMORPGs in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

that they are used as traditional games and for the initiation of relation and for the exploration of places basically because they have both visual and auditory components for players' use. However, Kapahi, Ling, Ramadass and Abdullah (2013) discuss the issue of excessive gaming identified as a sub type of addictive online/internet behaviour emanating from the creation of interactive environment for games platforms. This provokes a sense of wonder, amazement and awe of the fantasy world making cyber gaming an activity that gives gamers the room for imagination. Massive Multiplayer Online Role-Playing Game (MMORPG) is one of the appealing forms of gaming addiction for problematic internet users.

Cyber Journalism of the Cyberspace

Traditional journalism basically involves news gathering and dissemination by the press via the print media like newspapers and magazines hence to Meier (2007:13) "journalism researches, selects and presents issues that are new, factually correct and relevant. It creates public spheres by observing the society, delivering these observations to the mass audience through the periodic mass media and thus constructing a common reality". The development of the digital/internet technology has brought significant changes to the practice of journalism as the traditional mass media control of news transmission or information dissemination to the public has been neutralised or modified by the advent of the digital media (Kaul, 2013).The public now have the option of reading either the traditional hard copy/printed newspapers /magazines sold at the newsstands or the electronic soft copies/versions which many newspapers now make available online.

Sherwood and Nicholson (2013) in their study of newspaper sport journalists discovered that Twitter, Facebook and Fan Forum are web 2.0 platforms commonly used by Australian newspaper sport journalists in the course of news sourcing/researching, news reporting and interacting with their readings. It is important to point out the fact that the development of digital/cyber journalism has attracted divergent views/opinions as some believe it negatively impact on journalism as the way many opt for the online newspapers /magazines will have sales implication while some believed that the traditional print journalism is enhanced by the digital journalism. Potter (2012) points out that some have therefore jumped to the conclusion that the advent of digital journalism will mark the end of the century of print journalism while some are of the opinion that the advent of digital journalism only marks end the of the 20th century journalism and the rise of the new era of journalism that continues to achieve its fundamental goals in dynamic ways.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Broadcasting in the today's Cyberspace

Cyber broadcasting is the otherwise regarded as webcasting and it is usually in respect of two main forms of online/internet broadcasting, namely, online or internet radio broadcasting and online/internet television broadcasting which involves online/internet audio and audio-visual stations or news transmission or information dissemination respectively. The internet radio is otherwise called web radio, net radio, e-radio or streaming radio simply because it involves the use of streaming technology that employs streaming audio format like Window Media Audio and Read Audio. The good thing is that the internet radio stations/services can equally be accessed and enjoyed from any part of the world where there is a good internet service just as the case of CBS Radio and Citadel Broadcasting. Cover It Live, Blog Talk Radio and U Stream are contemporary web-based news broadcasting media.

Somu and Rengarajan (2012:350) observe that the Internet Protocol Television (IPTV)is becoming more and more important especially because of its live TV broadcast as well as a hordes of other interesting services like Video on Demand (VOD) and Personal Video Recorder (PVR).The IPTV according to them refers to "a system that offers digital TV services through internet protocol over the computer network infrastructure which is now an area of research interest because of the increasing desire of TV consumers for interactivity and personalisation". Hartung, Horn, Huschke, Kampmam, Lohmar and Lundevall (2007) however, argue in support of the hybrid broadcast unicast delivery especially because unicast technology is believed to be sufficient based on resource utilization and users experience in many situations . For example, it can enable users to access content on demand without following any fixed schedule among others.

Cyber Advertisement via the Cyberspace

This can also be morphologically regarded as 'cybertisement' though it is now a registered trade mark just as 'cybertising'. Online advertising according to Ha (2008:31)means "deliberate messages placed on third party websites including search engines and directories available through internet access". According to her, they are not unsolicited listing on third party sites and do not include marketers website for promotional and non-promotional

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

purposes, e-mails and other forms of marketing communications and shopping sites such as Amazon.com. Similarly, Haghirian and Madlberger (2005:) define mobile advertising as "the usage of interactive wireless media such as cellular phones and pagers, cordless telephones, personal digital assistants, two-way radios, baby crib monitors, wireless networking system, GPS-based locators and maps to transmit advertising messages to consumers in form of time and locations, sensitive, personalised information with the overall goal to promote goods and services". Cyber advertisement becomes pertinent now that there is dwindling readership of newspapers, a fundamental medium of traditional advertisement, with many now reading newspapers online just as they opt for the online TVs (Salman, Ibrahim, Abdullah, Mustaffa & Mahhob, 2011). However, the need to properly reward or monetize news media online efforts has been identified to complement the new media development and encourage the internet-facilitated new communication/media technology revolution (Yap, 2009).

Cyber Politics/Politicking in the Cyberspace

This, as the name suggests, simply refers to online/internet politics/politicking or political activities as opposed to the age long traditional face to face, print or broadcast media politics/politicking or political activities. Raves (2013) observes that ICT/internet affords citizens of different nations more opportunities to engage in political discourses/discussions thereby making the people to become politically informed and engaged. She, however, points out the fact that some people abuse this medium of cyber politics by being uncivil and derogatory in their political discussion simply because such online political communication gives room for relative animosity. Aronson (2012) in her study of cyber politics examines the role/impact of the new media on the political activities and electoral process in the United States and discovered that they do influence the electoral process vis-a-vis provision of vital political information, increasing political involvement and participation, setting political agenda and influencing election outcome among others.

The concept of cyber politics has become so germane that some institution of higher learning like Villanova University had to incorporate cyber politics components into their political science/communication studies programmes. Also, the political parties of different countries now seize the opportunities of the new media to reach out to the electorate. The incumbent seeking re-election tries to showcase their score cards to the people via the new media to justify their campaign/ quest for re-election just as the opposition uses the new media as well to present their views on why the incumbent should not be considered by the electorate with

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

reasons and promises. Elections before election even come up via online opinion polls which in many cases reflect political trends and realities. Cyber politics/politicking was quietly but extensively utilized during the recent Malaysian elections as instrument of underground political mobilization just as used in many contemporary elections too. It is therefore not surprising that there have been a number of online opinion polls conducted in respect to the next United States presidential election that is still about a thousand days away. This was presumed to be between the Democrat's former Secretary of State, Hillary Clinton and Chris Chistie the present Republican Governor of New Jersey who secured a land slide second term victory.

Cyber Medicine/Cyber Medical Practices in the cyberspace

Cyber medicine otherwise described as internet health by Segal (2009) refers to the act of "accessing electronic health records, consulting physicians emails, shopping online for pharmaceuticals and blogging about illness experience" among others. The author adds that health information is not only transmitted but equally transformed via the web just as internet health users are not just informed but equally transformed via the web. There is therefore an emerging area/concept of medical practice which involves the use of the internet for certain aspects of medical service delivery especially online medical consultation and online drug prescription by qualified physicians. Cyber medicine, however, is not exactly the same as telemedicine though they are over lapping. The former represents an improvement over the latter. The former is said to be usually applied to diagnostic and curative health delivery with limited participants' involvement while the latter relates to preventive and public health. The latter has to do medical consultation or remote treatment of patients usually through telephone conversation or fax communication. The former has to do with studying application of the internet and global networking technologies to medicine and public health, examining the impact and implication of the internet and evaluating opportunities and challenges for health care (Eysebach, Ryoung & Drepgen 1999).

It is important to point out that cyber medicine is not just limited to medical expert's/practitioner's unseen/unknown patients or virtual treatment of patients via the internet. Rather, it equally incorporates the process of medical training. Cowan, Sabari, Kaprales, Porte, Blackstein, Christancho and Dubrowski (2010) in their work or orthopaedic surgey training present a 3-D serious game that was designed using an iterative test and design method for the purpose of training orthopaedic surgery residents the series of steps

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

comprising the total kneel arthroplasty (replacement) procedure using a problem-based learning approach .The usability test of this is a pointer to the fact that the serious game is simplistic, intuitive and stimulating. There is also the cyber knife VSI (Versatile, Simple and Intelligent) system by Accuracy Incorporated designed to enable unprecedented precision of the system and benefiting patients a great deal.

Cyber Governance/Government via the cyberspace

E-government according to Haque, Memon and Shak (2013) refers to online digital government or internet based government involving the use of ICT for the exchange of information and delivery of services with the citizens, business or other arms of government. This, therefore, can be in form of government to citizen (G2C), Government to Business (G2B) or Government to Government (G2G).They identify efficiency, convenience and accessibility to/of public services as key benefits of e-government. Banday and Mattoo (2013) however, add collaboration, empowerment, timelessness and cost effectiveness as the benefits of social media use in e-government. This, to them, requires good social media policy and security measures due to the susceptibility of the social media/government information system to cyber threats/attacks.

The governments of many developed/developing nations now depend a lot on cyber system of/for governmental administration. Cyber journal (2013) expressly declares that the government of Canada (GC) depends on its wired and wireless network for communications and day to day operations hence any threat to their information assets could be very serious and which usually should be prevented. The same goes for the United State that uses the NSA and other security agencies to guard against national cyber information threats/insecurity that may negatively impact on cyber governmental administration. The website challenge of the Obama health care policy is considered by many as a great challenge of the president Barak Obama administration even though many believe it is doing well in some other areas simply because of the role of cyber governance in the present day American governmental administration. Singapore is another country known for a highly cyber-dependent governmental system of administration which was a major reason why some opponents of the government opted for a cyber-attack against the government recently to drive home some point (The Star, 2013). It is important to point out that even the government of North Korea that restricts the use of the internet /cyberspace by citizens has a government website.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Still on the issue of the social media use in e-government, Banday and mattoo (2013) also explicate this with specific reference to the situation in India. They point out that apart from individuals, business organisations and academic institutions that have been using the social media for information dissemination, social interactions, business promotion etc., government have been opting for the social media tools to revolutionize governmental administration for effective government–citizens communication. They further stress the fact that the United Kingdom, the United States, Australia, and Sweden among many other nations do use social media for digital diplomacy.

Cyber Tourism/Online Tourism via the Cyberspace

Cyber tourism, otherwise regarded as online tourism or E-tourism, according to Singh (2003) cited by Dixit, Belwal and Singh (2006) is "a new form of travel product distribution where a supplier/ service provider offers products/services mainly through the medium of internet to a group of customers irrespective of their physical location". Online tourism according to them is fast becoming a concept of research interest hence its semantic interpretation has gone beyond the utilization of the instrumentality of ICT for the enhancement of the marketing of the business of traditional tourism. Rather, it now involves virtual tourism that brings tourist attraction to virtual tourists where ever they are as opposed to the traditional idea of tourists going to the tourist attraction locations.

One of the recent technologies that have facilitated the actualization of the concept of cyber tourism is the three dimension technology simply called the 3D Tech. This technology is the brain behind the 3Dimension virtual tourism which involved the realistic 3D navigation of virtual reality tourist destinations so as to virtually explore physical places without physically travelling to those places. This is made pretty close to reality with the aid of multimedia support features like sound effects and incorporation of narration mainly with the aid of the 3DVT and usually on the internet. Buhalis and Deimezi (2003) confirm the fact that ICT applications have been positively imparting on global tourism especially in relatively tourism-dependent Greek economic System. They add that some innovative tourism organizations are enthusiastically embracing e-tourism and internet tools to enhance business communication with their clients and other stakeholders. He, however, stresses the fact that there is still the need for better utilization, understanding and maximization of the potentials of e-tourism so as to enjoy its competitive advantages vis-a-vis other tourist destinations.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Evangelism via the cyberspace

This is otherwise regarded as internet evangelism or cyber mission. Edmiston **(**2007) identifies the vital role of information technology as one key means for the fulfilment of the great evangelical mission to mark the beginning of his elaborate discussion of internet evangelism and Cyber mission. He observes that the internet has become a spiritual counsellor where many people now channel their spiritual questions and where they now obtain vital information on personal spiritual matters. This according to Chiluwa (2012c) explains why some religious organisations/institutions, that strongly believe that the internet is a fulfilment of prophecy or last day evangelical instrument, have been maximizing the benefits of the new media for the propagation of religious activities. Chiluwa (2013) adds that some offline worships and practices like healing ministration, anointing/communion services, feet worshiping, tithe and offering are also done online. He points out that the online Christian worship in Africa has become so popular thereby leading to the emergence of the Internet Church.

Edmiston (2007) further observes that the mission agencies need to have good understanding of the cyberspace based on the fact that contemporary trends in ICT have shown that the internet and related tools/devices will soon emerge as the dominant instruments of human religious communication. Some of the key benefits of cyber evangelism/internet mission identified include its low cost, low risk, wide geographical reach, possibility of one to many and many to one communication, media multiplicity, multilingualism, its being always on (unterrupted), preservation of messages, not being location dependent/constrained, not requiring many operation licences, bypass of demotivational restrictions etc. He however, rounds off his discussion by stressing the fact that there will be the need for the development of well-established internet evangelism and cyber mission units by 21st century mission agencies so as to reach the unreachable, access the inaccessible and follow up the young believers.

Cyber Mobilization/Activism and Fund raising on the Cyberspace

This can equally be described as online, digital or electronic mobilization/activism/fund raising which simply involves the uses of electronic communication technologies or tools like Twitter, Facebook, YouTube and email to appeal to some people or canvass for their support in respect of a given cause basically to influence their action in favour of the said

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

cause. The Tunisians and Egyptians would quickly come to mind at the mention of cyber mobilisation. Kuebler (2011) discusses the role of the internet as a relatively free space in the political mobilization of Egypt and Tunisia irrespective of all sorts of censorship in place. He points out that Egypt's blogosphere is one of the best documented in the Middle East which has impacted on the Egyptian politics. Kamis and Vaughan (2012) also confirm how the use of the social media especially Facebook, including Twitter, YouTube and text messages, were instrumental to Egyptian revolution. These were said to have been actively and effectively utilized to mobilize and coordinate the protesters towards supporting the common political goal.

However, Stork (2010) adds that cyber mobilization predates even the Tunisian and Egyptian uprisings or the Arab spring uproar by pointing out that the revolutions of Iran and Moldova which were described as "Twitter Revolutions" preceded even the popular Arab spring. Equally important is the fact that the Arab woman are said to be quietly utilizing the instrumentality of the social media underground to advance their causes now described as cyber feminism. She therefore also stresses the role of social media/networking as a tool for the political mobilization of citizens and the actualization of the cause of pro-democracy movements. Cyber mobilization, however, is not limited to political activism or human mobilization only as this can also be in the form of financial mobilisation which entails mobilization of funds required for the execution of given projects especially a philanthropic projects. Corson-Finnerty and Blanchard (1998) therefore describe cyber fundraising as the utilization of internet tools for the enhancement of fund raising and not as a replacement for the traditional method, in such a way that incorporates/accommodates the socially active/ engaged generation of new internet users.

An Explication of Challenging Cyberspace Crimes/Threats

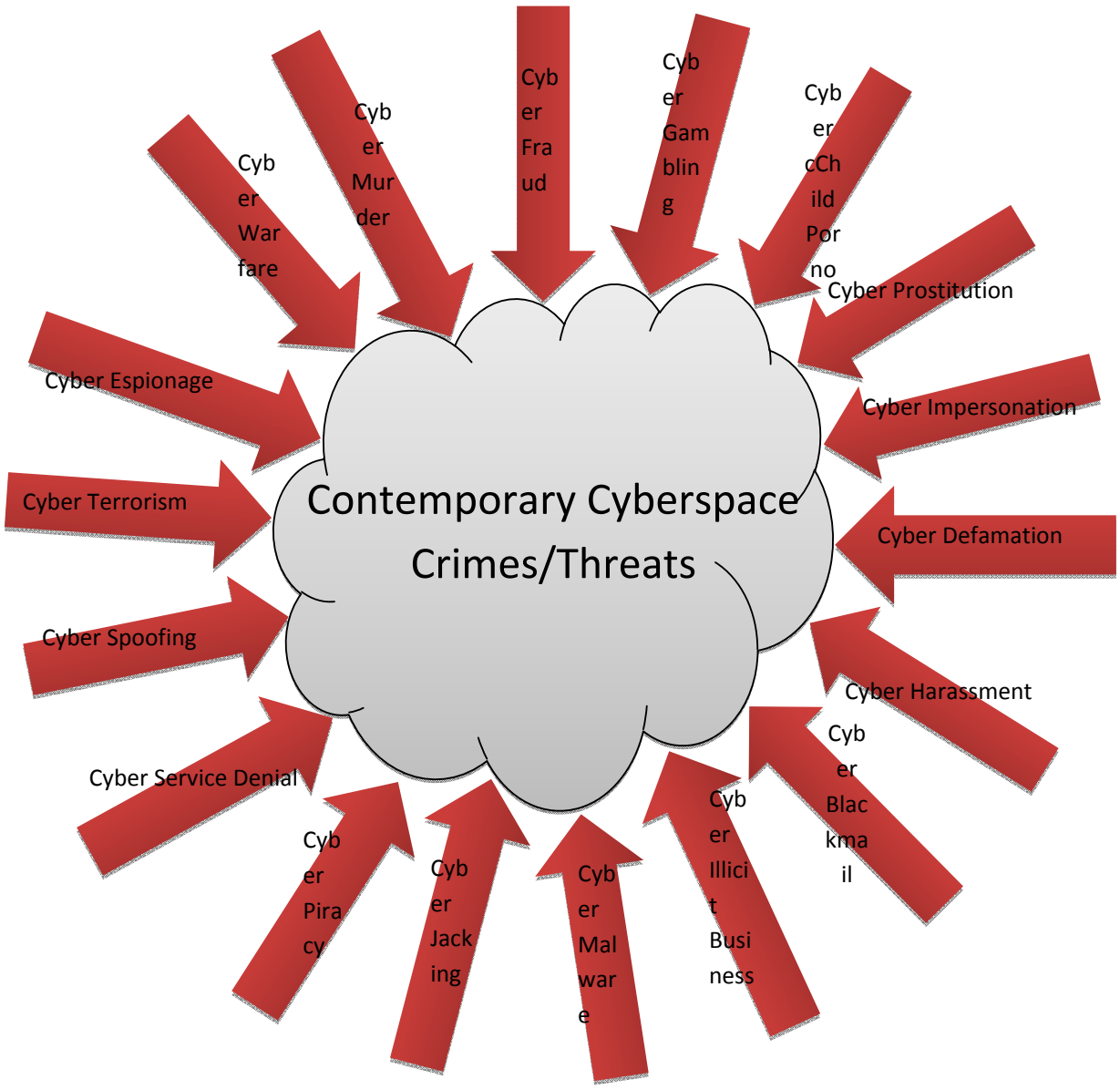
It is disturbing that the cyberspace that is serving multi-dimensional purposes and which is benefitting various people in different ways is now confronted by the preponderance of cyber crimes perpetrated by some, usually unknown, cyber criminals. This unfortunate development has the potential to negatively impact on the life-touching/changing cyberspace activities if not properly and promptly addressed. This means just as we the infiltration of numerous criminal acts or activities in the human society in the physical world, the same is equally happening or experienced in the digital or internet world of the cyberspace. More

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

unfortunately, various types of the cybercrimes keep emerging as existing ones are detected as many innocent and uninformed Cyberians continue to fall victims.

The term cybercrime is otherwise regarded as computer crime, internet crime or web crime and it has attracted various definitions or interpretations by those who have shown interest in this area of study. Nosrati, Hariri and Shakarbeygi (2013:104) first simply describe computer crime as "any crime that involves a computer and a network" and net crime as "the criminal exploitation of the internet". They further comprehensively defines cyber crime in line with Halder and Jaishankar (2011) as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet (chat room, email, notice boards and groups) and mobile phones (SMS/MMS)". Kshetri (2013:118) equally defines cybercrime as "a criminal activity in which computers or computer networks are used as the principal means of committing an offence or violating laws, rules and regulations. To McGee and Byington (2013) cybercrime simply refers to the use of computer in conjunction with the internet for the perpetration of what they describe as White Collar Crime (WCC). There are various cybercrimes presently constituting threats to the cyberspace like cyber fraud, cyber gambling, cyber (child) pornography, cyber prostitution, cyber impersonation, cyber blackmail/extortion, cyber harassment, cyber defamation, cyber malware, cyber illicit business/transaction, cyberjacking, cyber piracy/copyright infringement, cyber denial of service, cyber spoofing, cyber spying and espionage, cyber terrorism, cyber warfare and cyber murder. These are captured in the model below and then discussed one after the other in the light of relevant literature.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500



Cyber Fraud of the Cyberspace

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

There is prevalence of fraud of various types perpetrated by cyber criminals via the cyberspace just as there are prevalent fraudulent activities in the physical world. Many innocent cyberspace users have fallen victims of the traps of the cyber fraudsters and there is the possibility of many falling victims except precautionary security measures are put in place. Various types of cyber frauds can be identified, namely, financial fraud, email/text message fraud, electoral fraud, airtime fraud, online publication fraud etc. One of the major cybercrimes identified by Nagpal (2008) is financial crime which basically aims at extorting money from targets or victims and which is identified as the key motive behind most crimes. This, according to him includes credit card frauds, money laundering and bank account manipulation. He specifically identifies the "Salami fraud" as an example which involves the insertion of a program into a bank's server to be deducting a token amount from every customer's account which over a period becomes a huge amount of money.

The email/text message fraud is a kind of cyber fraud where the recipient/victim is given a piece of deceptive information aimed at defrauding him or her like saying he/she has been left an unknown inheritance, has won a computer generated lottery or should allow the use of his/her account to lodge a huge amount stolen from some foreign organizations or nations. The cyber electoral fraud relates to the kind of voting fraud or manipulation of results/information where the electronic or online voting system is employed. Cyber fraudsters also advertise and sell some fake products online like those for weight loss and fast money making ventures aimed at siphoning innocent victims' hard earned money. Airtime fraud occurs when somebody's airtime is programmed to be transferred to another person when the victim recharges. On the online publication fraud, Jalahan and Mahboobi (2013) point out how some cyber criminals now create fake websites for journal publications with bogus impact factors just to attract authors who want their work published as quickly as possible and who are ready to pay the exorbitant publication fee charged for the papers that are not usually properly reviewed if reviewed at all.

Cyber Gambling on the Cyberspace

This simply refers to the internet based gambling otherwise regarded as online gambling which according to Wood and Williams (2011) presents the traditional form of gambling in an electronic format on the internet thereby making it accessible to those with internet connection and electronic means of money transfer to participate. They point out that there were 2243 internet gambling websites as of August 2009 with virtual slot machines, pokers,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

horse betting , skill games and casino table games, among others, available online and the number keeps increasing. Although cyber gambling is legalized and regulated in some places especially where traditional gambling is not illegal, it is prohibited in many other places especially where traditional gambling is a crime. Even states like Nevada and New Jersey in the United States only passed laws that allow some forms of online gambling. However, cyber gambling makes it possible for people from all walks of life to gamble freely including those from places where it is prohibited thereby making the cyberspace a free gambling zone.

Griffith and Parke (2002) identify some factors that are likely to be responsible for growth of the internet gambling business like existence of sophisticated gambling software, integrated e-cash system, multilingual sites, increased realism (via web cam gambling) remote wagering and improved customer care systems. They further point out that cyber gambling may not make it easy to control or curb adolescent gambling as those of them who have the credit card information of parents or older siblings can still gamble online. Also, those under the influence of alcohol or drug can gamble away fortune online when they not in the right frame of mind whereas they may be restrained in a non-online gambling setting especially where there are reasonable gamblers or in the company of close friends. The possibility of internet gambling being doubly addictive is however identified based on the fact that internet use and gambling could be addictive. It is in the light of this that Kuss and Griffith (2011) are of the opinion that excessive gaming can result in some of the common symptoms of substance addiction.

Cyber (Child) Pornography of the Cyberspace

Pornography traditionally depicts obscenity and sexually explicit materials. Cyber pornography usually abbreviated as cyber porn and sometimes called web or net porno, according to Desai and Patel (2013) refers to the stimulation of sexual or erotic activities on the internet. They point out that there are free and commercial pornographic sites that offer variety of sexually explicit materials like photos, videos as well as live web cam access that enable those interested to access pornography of all kinds. Cyber pornography happens to be one of the fastest growing online businesses and this is evident in the thousands of pornographic sites in existence. It is important to note that while pornography or cyber pornography is not illegal or prohibited in some countries or societies the case is not the same in many other countries or societies. However, child pornography which involves sexual exploitation of children or involvement/exposure of children to the act of pornography,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

whether online or offline is prohibited in virtually all nations of the world. It is unfortunate that those in the cyber pornography business still engage in this to the satisfaction of pedophiles. This must have informed the recent arrest of 43 men members of an international child porn network with about 140 identified as their victims and several thousands of images discovered in their systems.

There have been a number of researches on the consequences of consumption or excessive exposure to pornographic materials. Owen, Behun, Manning and Reid (2012: 116) observe that "Youth who consume pornography develop unrealistic sexual values and beliefs. Permissive sexual attitudes, sexual occupation and early experimentation have been correlated with more frequent consumption of pornography". They equally point out how researches have linked adolescent use of pornography with increased degrees or levels of sexual aggression just as researches have suggested that those who consume online pornographic materials are prone to low degree of integration/emotional bonding but high level of delinquent/problematic behavior and incidence of depression. In a similar vein, Seigfried-Spellar and Rogers' study (2013) of the effect of consumption of adult-only bestiality and pornography shows that those who started earlier are more likely to be involved in deviant pornography (bestial or child) compared to those who started later.

Cyber Harassment (Bullying and Stalking) on the Cyberspace

Cyber harassment, cyber bullying and cyber stalking are closely related concepts though some have ascribed them slightly different interpretations and classifications. Cyber harassment according to Willard (2007) refers to the act of using telecommunication services to repeatedly communicate unwanted, unpleasant and demeaning messages that are intened to cause emotional distress to the target victims. The two main types of cyber harassment are cyber bullying and cyber stalking. Cyber bullying according to Fraser, Bond-Fraser, Buyting, Korotkov and Noonan (2013:26) involves the use of the internet to denigrate, demean or harass a person with a degree of anonymity and possibly 24 hours a day and 7 days a week. To Belsey (2004) cyber bullying involves the use of electronic communication devices to intimidate, harass and threaten somebody thereby achieving an effect similar to the traditional direct bullying. It is in the light of this that Smith, Mahdavi, Carvalho, Fisher, Russell and Tippett (2008) also define cyber bullying as aggressive behavior of some individual or group executed via modern electronic communication means over a period of time against some defenseless target victim.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber stalking according to Hazelwood and Koon-Magnin (2013) involves repeated pursuit of target individuals by using unwanted electronic communication and by threatening, coercing or intimidating them. Nagpal (2008) also stresses the fact that cyber stalking involves repeatedly harassing or threatening target individuals using the internet, emails or other electronic communication devices. This shows that the basic element of cyber bullying and cyber stalking is harassment or threat hence the classification of both as forms of cyber harassment. The slight distinction lies in the fact that cyber bullying, just as the traditional bullying relates to children and teenagers while cyber stalking is in respect of cyber harassment of adults. This is in line with the position of Chiong (2009) who identifies the case of Megan Meier, who killed herself after being deceived and cyber bullied by a neighbour's mother, as that which popularized cyber harassment .This however, is unlike the categorization of Willard (2006) of online harassment and cyber bullying as two of the identified seven forms of cyber crime similar to Fraser, Bond-Fraser, Buyting, Korotkov, and Noonan (2013) identification of cyber harassment and cyber stalking as methods of cyber bullying. One important point by Notar, Padgett and Roden (2013) in respect of cyber bullying is the fact that the perpetrator need not be strong or swift as all that is needed is access to cellphone or computer with the desire to terrorize target victims.

Cyber Impersonation of the Cyberspace

There is an increase in the rate of cyber impersonation and identity theft of the cyberspace in recent times to which many innocent victims continue to fall victims. Cyber impersonation and identity theft according to T & M Protection Resources (2004) involves using of the internet to post unauthorized, incorrect and/or malicious content that relates to a given individual or fraudulent establishment of an entire personal profile carefully designed and maintained to give the semblance of a real or an existing account. This act can be perpetrated without the knowledge of the affected/target victims as effort is usually made to make such an activity difficult to discover. Ensour (2013) identify two main types of online impersonation as individual impersonation and website impersonation hence these can be in form of impersonation in online commerce, impersonation targeting children, online friendship impersonation, personal identity information theft etc.

Impersonation and deception according to Banerjee, Barman, Faloutsus and Bhuyan (2014) are now very rampant on the internet and they constitute fundamental mechanics usually employed in the perpetration of serious scams especially by pharmers, phishers and DNS

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

squatters. Reznik (2013) corroborates this point and adds that internet or online impersonators usually access the target victims' accounts simply by stealing their passwords using all possible tricks at their disposal and they can equally create a fake profile with which they continue to impersonate their target victim. This is also buttressed with the case of a New Jersey woman who created a fake Facebook profile to discredit her detective ex-boyfriend by portraying him as a drug addict cum sex deviant before she was eventually discovered and accordingly prosecuted. The cyber bullying case of Megan Meier also has element of impersonation as the woman who cyber bullied her first impersonated a 16 year old male friend before eventually resorting to cyber bullying.

Cyber Prostitution on the Cyberspace

Prostitution is an age long illicit act often described as the oldest business or profession which has been revolutionized by computer/internet technology evident in the new concept of cyber prostitution as there is now cyber or online sex. According to Nunez, Medalle, Penaflor and Ranario (2012) cyber prostitution is an online or internet based/aided sexual activity involving the performance of lewd shows before the computer which are paid for accordingly and as agreed. Now, there are online advertisements of brothels sometimes with photographs those offering the services made available, known or unknown to them, so that those interested in their services can contact them online, by email or via text message to book appointment. There are cases of those who pay to watch the private or nude activities of housed prostitutes while dressing, undressing or bathing via cameras strategically installed usually without their knowledge.

Beckham and Prohaska (2012) equally observe that many sex workers now operate on the internet which reduces the number of those now on the streets and makes their activities less obvious. To them, the internet therefore now offers myriads of opportunities for the sexually deviant people to constantly whet their appetite but add that some unfortunate prostitutes usually fall victims of their acts of sexual violence. In a similar vein, Farley (2011) cited in Beckham and Prohaska (2012: 637) also points out that "men who purchase sex often dehumanize women, view them with anger and contempt, and lack empathy for their suffering, hence they separate sex from emotions and they therefore objectify women". However, the cruelty of cyber prostitution is not taken lightly when discovered. Green (2014) reports the arrest of one Aaron Prater charged with felony count of promoting prostitution as one of the ninety people arrested in a six-month five-state investigation into online or cyber

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

prostitution by the Fort Wayne Police Department. This was done in collaboration with members of a federal project leading to several arrests in Ohio, Illinois, Kentucky, Michigan and Texas.

Cyber Defamation (Libel and Slander) on the Cyberspace

Defamation according to Desai and Patel (2013) is otherwise regarded as cyber smearing as it involves the use of a computer/ICT aided message to smudge somebody's image, damage someone's reputation or dent the victim's personality hence its description as character assassination. Such defamation according to Potter (2013) is of two main types namely libel or libelous defamation and slander or slanderous defamation. The former involves defamation in written/printed form or any other form that is permanent while the latter involves defamation in spoken/speech form requiring some additional proofs. Angelotti (2013) looks at the libelous defamation of a form of social media networking, Twitter, with an audience of over 140 million people, described as Twibel and points out the fact that the United States courts are yet to rule on a few Twibel suits that have come up. She further points out the historical position of defamation law to maintain a balance between freedom of speech and protection of people's reputation. She is therefore of the opinion that Twibel should be a legal means of preventing defamation on Twitter without inhibiting civil discourse thereby making the defamation law a legal instrument and not a legal hindrance.

Cyber Malware (Virus, Worm & Trojan) Attack of the Cyberspace

Cyber malware simply refers to malicious code/software which Nosrati, Hariri and Shakarbeygi (2013) identify as one of the three main cybercrimes/attacks that basically target computer devices or networks. To Maitanmi, Ogunlere, Ayinde and Adekunle (2013) malware comprises viruses, worms, Trojans as well as other software that access/attack people's computer systems without their knowledge or pretentiously and which could destroy vital or valuable information if not quickly detected and halted or remedied.

Viruses according to them are computer programs which spread to other computers usually just as biological viruses do but which must be attached to some documents or programs before they can spread and do the havoc or corrupting or deleting data or disrupting an entire system. File virus, boot sector virus, macro virus and hoax(er) virus are forms of computer virus identified by Obi and Okpor (2013). Worms, on the other hand according to them, can automatically replicate themselves and capitalize on some loopholes or weaknesses to attack

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

target systems or essential computer resources like memory space or processing time. Trojans or Trojan horses are unauthorized malicious programs that usually pretend to be authorized and on the basis of which target systems that erroneously accept are attacked (Ibikunle & Eweniyi, 2013). Some of the forms of Trojans identified by experts are hand on theft Trojan, remote access Trojan, data sending Trojan, destructive Trojan, denial of service Trojan and security disabler Trojan.

Cyber Jacking on the Cyberspace

Cyber jacking is somehow closely related to traditional hijacking because just as hijacking involves forcefully or violently seizing and taking control of an aircraft or other related means of transportation, cyber jacking involves forcefully breaking into other people's or organisations' secure or protected systems with the intension of accessing vital information. Nagpal (2008) discusses the concept of web jacking which according to him involves forcefully taking over people's or organisations' websites by web jackers who crack their passwords and may eventually change them. This will ultimately block the access of the original or rightful owners of the hijacked websites thereby depriving them of the sole control of the websites vis-a-vis what is placed on or done via the sites. Recently, the websites of some online/electronic journals have been reportedly hijacked by some cyber criminals who are now operating them with some bogus impact factors to attract authors and make them pay the publication fees, the ultimate goal of hijacking and controlling the journals websites. La Barge and McGuire (2012:47) also discuss the concept of session hijacking which according to them is all about "the exploitation of a valid session key to gain unauthorized access to a computer system or a computer network" They identify four main forms of session hijacking namely session fixation, session side jacking, session key theft and cross site scripting.

Cyber Illicit Business Transactions (Drugs and Fire Arms) of the Cyberspace

The cyberspace is now being used as a cyber haven/rendezvous or safe avenue to initiate, execute or finalize some illegal or illicit business transactions especially the sales of hard drugs and fire arms transactions thereby making the perpetrators activities somehow more hidden. Maitanmi, Ogunlere, Ayinde and Adekunle (2013) therefore identify cyber drug trafficking as a prominent form of cyber crime which is aided by internet technology making the sale and purchase of illegal substances possible online especially through encrypted

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

emails. Nosrati, Hariri and Shakarbeygi (2013) also corroborate the prevalence of cyber drug business and stress the fact that the illicit online business is thriving because it does not involve physical contact or face to face communication hence, many who ordinarily would not have been bold enough to engage in such a transaction conveniently engage in the illicit online business transaction. Another form of cyber illicit business that is thriving online is the sales of guns or fire arms especially those who would have passed background check test like children and those who are non-compos mentis i.e. who are not of sound minds. It is therefore not surprising that the United States alone records about 31,000 gun deaths every year which includes about 19,000 suicides (Bloomberg, 2013).

Cyber Service Denial of the Cyberspace

This is another way of perpetrating cybercrime aimed at depriving given individuals or organizations the opportunity of enjoying desired/required cyber facilities. Denial of Service (DoS) attack is executed basically by flooding a given computer or server with overwhelming requests far more than what can be handled which prevents incoming of expected legitimate requests and which may result in the crash of the system or server and eventual deprivation of authorized users' access. One main type of cyber service denial is Distributed Denial of Service (DDoS) which usually involves a number of perpetrators from different locations or when malware infected computer systems are remotely controlled (as botnet/zombie network) simply to overwhelm the target system or computer.

Gupta, Joshi and Misra (2010) identify Trinoo, TFN, TFN2K, Stachel Draft, Shaft, MStream, Knight and Trinity as some attack tools. According to them a Distributed Denial of Service (DDoS) attack is a situation where a legitimate user or an organization is deprived of some basic cyber services like web, email or network connectivity, that they would normally expect to have". Singleton (2014) however, points out that DDoS attack may not be to attract financial or monetary benefit but to attract some high level attention or recognition. Another form of DoS is email bombing which in a similar vein entails spamming or flooding of an email address or a server with emails so as to block legitimate or authorized emails.

Cyber Piracy/Copy Right Infringement on the Cyberspace

Piracy simply refers to the act of making or producing illegal or unauthorized copies of products or materials considered as the intellectual property of others like books, computer programs or software, films/videos musical CDs or DVDs etc. This is usually prohibited

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

because such items or materials are protected by the copy right law. The copy right law therefore usually prohibits infringement on people's copy righted materials or intellectual property by any person or organization without the copy right owner's permission or appropriate authority's approval. Hommige (2013) observes that with the unique use of the internet as means of information sourcing, gathering and transmission comes the rampant problem of intellectual property infringement due to the unlawful online uploading, downloading or reproduction of other people's copy righted products or materials. Singleton (2013) points out that in February 2013, 178 million Americans watched 33 million online videos which show the value of the intellectual property on the internet just for movies only. Rampant piracy of software according to Hommige (2013) also results in a global loss of about $47 billion annually. Many countries have therefore taken the bold steps of making cyber piracy laws but there are some reservations and challenges in relation to effective implementation of the laws especially due to the ubiquitous nature of the of the cyberspace and the perpetrators of cyber piracy.

Cyber Blackmail and Extortion on the Cyberspace

Cyber blackmail is the online version of the traditional blackmail as it involves using information or secret got about the victim to demand or be demanding for some incredible amount of money backed with the threat to release the said information or secret in case the victim fails to meet the blackmailer's demand. One common secret used in cyber blackmailing or online blackmailing is the nude or seminude pictures of people copied or intercepted by the blackmailer in the course cyber sexual relationship or sexually explicit text messages sent in the course of sexting secret lovers. A lot of money is usually extorted from victims of cyber blackmail especially the wealthy public figures who have names to protect and who do not want to be exposed and there are some ransom ware developed for easy remission of cyber blackmailer's requested ransom. Unfortunately, many blackmailers will usually resurface after collecting and squandering an earlier requested ransom once the victim and the secret are still alive.

Closely related to cyber blackmail is 'sextortion' or sexual blackmail. Sextortion, coined by experts from a combination of 'sex' and 'extortion', involves requesting sexual favour with threat to reveal a secret or release information about somebody's sexual affairs, images or messages. It is therefore a form of sexual blackmail which involves using sexual secret or information to exploit sexually. Frost (2013) gives an account of how some men called

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

'cappers' chat online with teens they call 'camwhores' flatter and manipulate the teens to flash or bare sensitive parts of their body which they secretly capture/snap and use to further blackmail them to do worse things like striping, masturbating or performing other sexual acts that are equally recorded. Many victims of cyber blackmail and sexual blackmail end up killing themselves when they can no longer cope with the incessant demands of the anonymous cyber blackmailers just as in the reported case of Amanda Todd who committed suicide in 2011. Gharibi and Shaabi (2012) therefore caution on sending or posting sensitive personal information on the social networking sites as this may expose people the more to the risk of physical and sexual extortion.

Cyber Spying/Espionage of the Cyberspace

Spying is generally an activity aimed at getting secret information about the target individual, organization or nation while cyber spying involves the use of computers, computer networks or software to get private information which can also be at the individual, organizational, national or international level. Cyber spying is therefore similar to traditional spying except for the fact that it is online or internet based and computer networks or systems aided making it possible for cyber spies to intercept or download valuable documents or information of others by hacking their systems and compromising the security put in place or simply by installing spyware or tracking programs on target systems.

Cyber spying is however described as cyber espionage when there is a large scale case of spying especially which involves nations. China is believed to be one of the perpetrators of cyber espionage done to enhance China's economic competitiveness especially in science and technology hence China is usually alleged of economic espionage (Bryan-Krekel, 2002). However, Pandey and Kusum (2013) believe that on China's economic espionage mechanism, those affected need to put their houses in order, maintain their edge and capitalize on this since reengineering cannot take the place of innovation or originality. The United States National Security Agency (NSA) is also recently accused of large scale spying on Germany, Brazil and others following the spying revelation of Edward Swoden the cyber fugitive now in Russia. The United States however, has been emphasizing the need to employ cyber security surveillance and related measures to protect the interest of America and Americans especially by keeping eyes on the perceived and potential terrorists the world over so as to nip any plans against the US in the bud.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Cyber Spoofing on the Cyberspace

Spoofing is all about deception in cyber communication and impersonation aimed at making the targets believe what they would not have believed or do what they would not have done normally. It therefore involves deceptive attempts of some intruders to access the systems/information of some target users by pretending to be who they are not. Different types of cyber spoofing have been identified by Khan (2013) and also by Dalla and Geeta (2013) hence we have SMS spoofing, call spoofing, email spoofing and website spoofing. SMS spoofing involves mobile phone information theft/access and the use of the mobile phone number to send and receive text messages usually through the internet pretending to be the rightful owner of the mobile phone number. Email spoofing similarly involves sending email messages that appear to emanate from the rightful owner of the email address with a similar header but which actually originated from another source. This is done with the aim of sending misinformation or getting vital information like passwords in response. Call spoofing otherwise regarded as caller ID spoofing involves making deceptive telecommunication where telephone network is made or manipulated to show a given number on the receiver's caller ID display quite different that of the real or actual caller. Website spoofing is a situation where a cyber criminal deceives victims with web information and tries to obtain vital information with which they can further scam or defraud e.g. account numbers or passwords. Cyber spoofing however requires or involves some other cyber crimes for its actualization like phishing, key logging, spyware and hacking.

Cyber Murder on the Cyberspace

Cyber murder simply refers to computer or internet technology aided killing which becomes possible because the computer/internet technology is now part and parcel of virtually every human activity which also accounts for why it is embraced by nearly all and sundry. It is in the light of this that Fortinash and Holoday-Worret (2012) describe cyber murder as internet homicide which, according to them, refers to a kind of killing aided by the internet which facilitates the online meeting of the victim and the perpetrator. Ibikunle and Eweniyi (2013) identify as the first example of cyber murder the case in the United States of an hospitalized patient about to be operated but against who some cyber criminal was engaged to murder by remotely altering his prescribed drugs by hacking the hospital computer system. The patient was eventually given a wrong combination of drugs by the nurse and the patient died. In a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

similar vein, there are cases of serial killers who operate via the cyberspace to link, hook and kill their victims or targets hence their activities are equally facilitated by the internet.

Cyber Terrorism of the Cyberspace

Cyber terrorism simply put refers to online or internet based act of terrorism. Embar-Seddon (2002) defines cyber terrorism as "premeditated use of disruptive activities or the threat thereof, in cyberspace, with the intention to further social, ideological religious, political or similar objectives, or to intimidate any person in the furtherance of such objective". In a similar vein, Nosrati, Hariri and Shakarbeygi (2013) describes cyber terrorism as deliberate or intentional use of computers, networks, the internet or other computer tools/devices to perpetrate terrorist activities or to achieve terrorist objectives which could be political or ideological. Cassim (2012) also adds that cyber terrorists now see the cyber space as a digital-age battleground and use computer based high technology to execute their violent or destructive plans making these difficult to detect. Cyber terrorists therefore could target the computer networks controlling power or water supply; road, rail, sea or air transport system; telecommunications, financial/economic or defense system with the ultimate goal of crippling the systems and causing unprecedented havoc. Ahmad, Yunos, Sahib and Yussof (2012) however, present a cyber terrorism conceptual framework that captures the motivation (social, political or ideological), tools (network warfare), method (unlawful means), domain (cyberspace), target (computer/information systems) and impact (economic loss, systemic disruption, and injury/death) of cyber terrorism.

Cyber War/Warfare of the Cyberspace

Cyber warfare is otherwise described as digital war or computer warfare. Cyber warfare according to Dipert (2010) simply refers to an attack of a nation's governmental or civilian information systems via cyber attack instruments like malware and denial of service which unlike in conventional warfare does not cause a physical damage, injure or kill people but which can be inimical to the affected nation's key interests. To Adnan (2010) cyber warfare involves the use of computers and the internet to conduct a cyberspace warfare which may include electronically blinding, jamming, deceiving, overloading or intruding into the target's information and communication circuits/systems. The Star, a Malaysian newspaper, of 9th November, 2013 edition has a story about the recent cyber attack of an Anonymous network of hackers who had threatened war on the government of Singapore and its infrastructure

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

because of the decision to license online news. They actually attacked and made all official websites inaccessible for days which affected the websites of the Police, Internal Security, Ministries of Finance, Home Affairs, National Development, Office of the Prime Minister, the Parliament and the Cabinet. The Estonia's botnet attack of 2007 and 1998 hacking of Serbia's defense system are previous cases that are fresh in the memories of many people. It is important to point out the difference between cyber warfare and cyber terrorism as stressed by Applegate (2014). The former is used to advance the cause or agenda of a given nation while the latter is used to advance the ideology, cause or agenda of a terrorist group or organization.

Conclusion

This paper therefore presents in a nutshell the pros and cons of the virtual world of the cyberspace via the exploration of the fundamental beneficial cyberspace activities and the explication of the prevalent cyber crimes posing great threats or dangers to the cyberspace in the light of relevant contemporary literature. It is therefore paradoxical that just as there are myriads of cyberspace activities positively impacting on individual, organizational, societal, national and international activities or efforts, there are also emergent and challenging cyberspace criminal acts or activities being perpetrated that could negatively impact on individual, organizational, societal, national or international activities or efforts. There is therefore the dire need for all cyberspace stakeholders to sustain or maximize the benefits of the cyberspace, ensure the safety of the cyberspace, protect the cyberspace assets and the interests of the cyberspace users the world over using all logical means and possible strategies.

Good knowledge and application of the basic information and computer security measures are imperative for cyberspace users to be on the safe side while utilizing computer, computer network or cyberspace resources. Contemporary cyber security guidelines and research findings of experts should be widely circulated to enlighten cyberspace users so as to keep them abreast of developments and equip them with the knowledge of contemporary cyber security/safety measures. Such security awareness or consciousness becomes pertinent as a way of exposing reigning or emerging cyberspace crimes/threats, to continually protect innocent cyberspace users and to safeguard their interests. Since cyber criminals now form networks and work in collaboration to rain some cyber havocs, the war against cyber crime should be reinforced with collaborative strategies at the individual, organizational, societal,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

national and international levels. With all cyberspace stakeholders' hands on deck, cyber crimes/threats can be reduced to the barest minimum and the cyberspace made a better and healthier haven for all and sundry.

References

Adnan, M.H. (2010). A dictionary for communication and public relations practice. Shah Alam, Selangor: University Publication Centre (UPENA).

Pfaffenberger, B. (2000). Dictionary of computer terms. (8th ed). Chicago, Il: Webster's New World Book.

Korchmaros, J.D., Ybarra, M.L., Langhinrichsen-Rolling, J., Boyd, D. & Lenhart, A. (2013). Perpetration of teen dating violence in a networked society. *Cyberpsychology, Behavior and Social Networking*, 16(8), 561-567.

McGraw-Hill Dictionary of Computing and Communications (2003). New York: McGraw-Hill Co. Inc.

Vakharia, A.B., Mishra, V. & Kumar, S. (2013). Security glitches related to e-commerce and their solutions. *International Journal of Computer Application,* 2(3), 85-94.

Usman, A.K. & Shah, M.H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, 18(2), 1-15.

Rahman, S.M. & Lackey, R. (2013). E-commerce system security for small businesses. *International Journal of Network Security and Its Applications*, 5(2), 193-210.

Permvattana, R., Armstrong, H. & Murray, I. (2013). E-learning for the vision impaired : A holistic perspective. *International Journal of Cyber Society and Education*. 6(1), 15-30.

Yee, R.C.S. (2013). Perception of online learning in an Australian university: An international students' perspective – support for learning. International *Journal of Cyber Society and Education,* 6(1), 45-50.

Adeoluwa, O.V., Aboderin, O.S & Omodara, O.D. (2013). An appraisal of educational technology usage in secondary schools in Ondo State, Nigeria. *International Journal of Innovational and Applied Studies,* 2(3), 265-271.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Zhuhadar, L., Yang, R. & Lytras, M.D. (2013). The impact of social multimedia system on cyber learners. *Computer in Human Behaviour*, 29(1), 378-385.

Sahid, M. (2013). Role of media in political socialization of young generation. *American Based Research Journal*, 2(1), 56-61.

Misra, S. & Stokols, D. (2012). A typology of people-environment relationshipin the digital age. *Technology in Society*, 34(1), 311-325.

Finkel, E.J., Eastwick, P.W., Karney, B.R., Rels, H.T. & Sprecher, S. (2012). Online dating: A critical analysis from the perspective of psychological science. *Psychological Science in the Public Interest*, 13(1), 3-66.

Yee, N. (2007). Motivation of play in online gamers. *Cyber Psychology and Behaviour*, 9(6), 772-775.

Kapahi, A., Ling, C.S., Ramadass, S. & Abdullah, N. (2013). Internet addiction in Malaysia: Causes and Effects, *iBusiness*, 5(2), 72-76.

Cole, H. & Griffiths, M.D. (2007). Social interactions in massively multiplayer online role-playing gamers. *Cyber Psychology and Behaviour*, 10(4), 575-583.

Kaul, V. (2013). Journalism in the age of digital technology. *Online Journal of Communication and Media Technology*, 3(1), 125-143.

Meier, K. (2007). Journalistik. Konstanz: UVK

Sherwood, M. & Nicholson, M. (2012). Web 2.0. platforms and work of newspaper sport journalists. *Journalism*, 14(7), 942-959.

Pottker, H. (2012). Fort mit kommuni kations barrieren. Erwagungen zur rolle des journalismus in der digital mendienwelt. Neue Zuricher Zeitung. Retrieved December 10, 2013 from http://www.nzz.ch/aktwell/startseite/fort-mit-kommunikations-barrieren.

Somu, M. & Rengarajan, (2012), A review on the performance of caching algorithms for video streaming services in IPTV. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(5), 350-355.

Lopez-Fernadez, O., Freixa-Blanxast,& Honrubia-Serrano, M.L. (2013). The problematic internet entertainment use scale for adolescents : Prevalence of problematic internet use

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

among Spanish high school students. *Cyber Psychology, Behaviour and Social Networking*, 16(2), 108-118.

O' Keeffe, G.N. & Clark-Person, K. (2011). Clinical report-The impact of social media on children, adolescents and families. *Pediatrics – Official Journal of the American Academy of Pediatrics.* Retrieved on 5th December, 2013 from pediatrics @ publications.org/content.

Hartung, F., Horn, U., Huschke, J., Lomar, T., Kampmann, M. & Lundevall, M. (2007). Delivery of broadcast services in 3G networks. *IEEE Transactions on Broadcasting*, 5(3), 188-199.

Ha, L. (2008). Online advertising research in advertising journals: A review. *Journal of Current Issues and Researches in Advertising*, 30(1), 31-48.

Haghirian, P. & Madlberger, M. (2005). Consumer attitude toward advertising via mobile devices - An empirical investigation among Austrian users. ECIS, 447-458.

Aronson, E.D. (2012). Cyber-politics: How new media has revolutionized 3rd electoral politics in the United States. *Colgate Academic Review*, 9(1), 148-196.

Cowan, B. Sabri, H. Kapralos, B., Porte, M., Backstein, D., Christancho, S. & Dubrowski, A. (2010). A serious game for total kneel arthroplasty procedure, education and training. *Journal of Cyber therapy and Rehabilitation*, 3(3), 285-298.

Eysenbach, G., Ryoung, S.E. & Diepgen, T.L. (1999). The impact of informatics. Shopping around the internet today and tomorrow: Towards the millennium of cybermedicine. BMJ, 319:1294.

Segal, J.Z. (2009). Internet health and the 21st century patient: A rhetorical view. *Written Communication*, 26 (1), 351-369.

Cyberjournal (July, 2013). Network security: Protecting our information assets. Communication Security Establishment Canada, 3, 1-8. www.csec.st.gc.ca.

Banday, M.T. & Mattoo, M.M. (2013). Social media in e-governance: A study with special reference to China. *Social Networking*, 2, 47-56.

Haque, M., Memon, R.A. & Shaikh, A. (2013). E-government using grid technology: Developing a grid framework for G2G e-communication and collaboration system. *International Journal of Independent Research and Studies*, 2(1), 8-15.

Dixit, M., Belwal, R. & Singh, G. (2006). Online tourism and travel – Analysing trends from marketing perspective. *Skyline Business School Journal*, 3(1), 89-99.

Buhalis, D. & Deimezi, O. (2003). E-tourism development in Greece.: Information communication technologies adoption for the strategic management of the Greek tourism industry. *Tourism and Hospitality Research*, 5(2), 103-130.

Edmiston, J. (2007). Internet evangelism and cyber missions and their impact upon how we do mission in the 21st century. Accessed 13th December, 2013 from www.cybermissions.org/article / 21stc-missions.pdf.

Chiluwa, I. (2012c). Online religion in Nigeria: The internet church and cyber miracles. *Journal of Asian and African Studies*, 47(6), 734-749.

Chiluwa, I. (2013). Communiuty and social interaction in digital religious discourse in Nigeria, Ghana, and Cameroon. Journal of Religion, Media and Digital Culture, 2(1), 1-37.

Kuebler, J. (2011). Overcoming the digital divide: The internet and political mobilization in Egypt and Tunisia. *Cyber Orient*, 5(1). Retrieved from www.cyberorient.net/article. Do?articleid=6212.

Kamis, S. & Vaughan, K. (2012). "We are all Khalid Said": The potentials and limitations of cyberactivism in triggering public mobilization and political change. *Journal of Arab and Muslim Research*, 4(2) DOI: 10.1386/jammr.4.2-3.145-1.

Stork, M. (2011). The roles of social media in political mobilization: A case study of the 2011 Egyptian uprising. Unpublished M.A. Dissertation of University of Andrew, Scotland.

Corson-Finnerty, A. & Blanchard, L. (1998). *Fundraising and friendship raising on the web*. Chicago: American Library Association.

Jalahan, M. & Mahboobi, H. (2013). New corruption detected: Bogus impact factors compiled by fake organisations. *Electronic Physician*, 5(3), 685-686.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Wood, R.J. & Williams, R.J. (2011). A comparative profile of the internet gambler: Demographic characteristics, game play patterns, and problem gambling status. *New Media Society*, 13(7), 1123-1141.

Griffiths, M.D. & Parke, J. (2002). The social impact of internet gambling. *Social Science Computer Review*, 20(3), 312-320.

Kuss, D.J. & Griffiths, M.D. (2011). Online gaming addiction in children and adolescents: A Review of Empirical Research. *Journal of Behavioural Addiction*, 1(1), 1-20.

Desai, P.N. & Patel, A.N. (2013). Cyber crime against person. *International Journal of Innovations in Engineering and Technology*, 2(3), 198-201.

Owens, E.W., Behun, R.J., Manning, J.C., & Reid, R.C. (2012). The impact of internet pornography on Adolescents: A review of the research. *Sexual Addiction and Compulsivity*, 19(2), 99-122.

Seigfried-Spellar, K.C & Rogers, M.K. (2013). Does deviant pornographic use follow a guttman-like progression? *Computer in Human Behaviour*, 29(5), 1997-2003.

Willard, N. (2006). *Cyber bullying and cyber threats*. Eugene, OR: Centre for Safe and Responsible Internet Use.

Willard, N. (2007). *Cyber bullying and cyber threats: Responding to the challenge of online social aggression, threats and distress*. Champaign, Il: Research Press.

Fraser, I., Bond-Fraser, L., Buyting, M., Korotkov, D. & Noonan, S. (2013). Cyber bullying and the law: Are we doing enough? *The American Association of Behavioral and Social Science Journal*, 17(1), 26-39.

Notar, C.E., Padgett, S. & Roden, J. (2013). Cyber bullying: A review of literature. *Universal Journal of Education Research*, 1(1), 1-9.

Belsey, B. (2004). Cyber bullying: An emerging threat to the 'always on' generation. Retrieved January 10, 2014 from www.cyberbullying.ca/pdf/cyberbullying_article_by_Bill - Belsey.pdf.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Hazelwood, S.D. & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminlogy*, 7(2), 155-168.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S. Russel, S. & Tippett, N. (2008). Cyber bullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4), 376-385.

T&M Protection Resources (2014). Cyber identity theft and impersonation. Retrieved 6th January, 2014 from www.tmprotection.com

Reznik, M. (2013). Identity theft on social networking sites: Developing issues of internet impersonation. *Touro Law Review* 29(2).Retrieved from http://digital/commas.tourolaw.edu /lawreview/vol29/1552/12.

Chiong, P. (2009). Cyber bullying and cyber stalking: The verdict. Retrieved January 10, 2014 from www.watoday.com.au/theverdict/2009/cyberbullying.html.

Ensour, H.S. (2013). Online impersonation: A case study in Hashemite Kingdom of Jordan. *International Journal of Engineering and Computer Science*, 5(3), 20-25.

Banerjee, A., Barman, D., Faloutsos, M. & Bhuyan, L.N. (2014). Cyber fraud is one type away. Retrieved January 6, 2014 from http://www.cs.ucr.edu/anirban/anir-infocom.

Numez, V.C., Medalle, M.E., Penaflor, M.V. & Renario, R.J. (2012). Cyber dating determinant factor to cyber prostitution: Basis for the creation of local ordinance. A Research Proposal Presented to the Faculty of Graduate School, Cebu Normal University, Cebu City.

Farley, M. (2011). Comparing sex buyers with men who don't buy sex. A study released exclusively to Newsweek Magazine, 158(4), 637.

Beckham, K. & Prohaska, A. (2012). Deviant man, prostitution and the internet: A qualitative analysis of men who killed prostitute who they met online. **International Journal of Criminal Justice Science**, 7(2), 635-648.

Nosrati, M., Hariri, M. & Shakarbeygi, A. (2013). Computers and internet: From a criminological view. *International Journal of Economy, Management and Social Sciences*, 2(4), 104-107.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Angelotti, E.M. (2003). Twibel law: What defamation and its remedies look like in the age of twitter . *Journal of High Technology Law*, 13(2), 430-507.

Maitanmi, O., Ogunlere, S., Ayinde, S. & Adekunle, Y. (2013). *The International Journal of Engineering and Sciences,* 2(4), 19-25.

Obi, J.C. & Okpor, D.M. (2013). Soft computing virus identification system. *International Journal of Fuzzy Logic System*, 3(2), 63-72.

Ibikunle, F. & Eweniyi, O. (2013). Approaches to cyber security issues in Nigeria: Challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education,* 1(1), 1-11.

Singleton, T. (2014). Understanding the cybercrime waves. *ISACA Journal*, 1(1), 1-5.

Gupta, B.B., Joshi, R.C. & Misra, M. (2010). Distributed denial of service prevention techniques. *International Journal of Computer and Electrical Engineering*, 2(2), 268-276.

Hemmige, N. (2013). Piracy in the internet age. *Journal of Intellectual Property Rights*, 18(1), 457-464.

Bloomberg, M.R. (2013). Forward in Daniel W. Webster and Jon S. Vernick (eds).*Reducing gun violence in America*. Baltimore: John Hopkins University Press.

LaBarge, R. & McGuire, T. (2012), Cloud penetration testing. *International Journal on Cloud Computing Services and Architecture*, 2(6), 43-62.

Bryan-Krekel, P.A. (2012). Occupying the information high ground: Chinese capabilities for computer network operators and cyber espionage. Retrieved from US-China Economic and Security Review Commission at http://www.uscc.gov/rfp/2012/uscc/020report.

Pandey, S.N. & Kusum, H. (2013). China's economic miracle and the statecraft. *Global Research Journal of Business Management*, 1(1), 1-4.

Khan, A.A. (2005). Preventing phishing attacks using one time password and user machine identification. *International Journal of Computer Application*, 68?(3), 7-11.

Dalla, H.S. & Geeta, M.S. (2013). Cyber crime-A threat to persons, property, government and societies. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), 997-1002.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Frost , R. (2013). Kids online: What are the risks? Centre Arizona Centre against Sexual Assault. http://www. Pewinternet.org/media/files/reports/2013/pip_teenandtechnology.pdf.

Dipert, R.R. (2010). The Ethics of Cyber Warfare. *Journal of Military Ethics,* 9(4), 384-410.

Applegate, S.D. (2014). Cyber Warfare- Addressing new threats in the information age. Retrieved January 26, 2014 from www.academia.edu/cyber_warfare.

Fortinash, K. & Holoday-Worret (2012). *Psychiatric mental health nursing* (5th ed.). Louis: Elsevier.

Green, R.S. (2014).Cyber pimp admits running escort service. *The Journal Gazette*. Retrieved January 4, 2014 from www.journalgazette.net/apps/pbcs.dll/article?

Cassim, F. (2012). Addressing the spectre of cyberterrorism: A comparative perspective. *Potchefstroom Electronic Law Journal,* 15(2), 381-415.

Ahmad, R., Yunos, Z., Sahib, S. & Yusoff, M. (2012). Perception on cyber terrorism: A focus group discussion approach. *Journal of Information Security*, 3(1), 231-237.

Salman, A., Ibrahim, F., Abdullah, M.Y., Mustaffa,N. & Mahhob, M.H. (2011). The impact of new media on traditional mainstream mass media. *The Innovation Journal: The Public Sector Innovation Journal*, 16(3), 1-11.

Nagpal, R. (2008). Evolution of cyber crimes. *Asian School of Cyber Laws Publications*. www.cyberlawdb.co/gcld/wp.

Kumar, V.D. (2013). Cyber crime prevention and role of libraries. *International Journal of Information Dissemination and Technology,* 3(3), 222-224.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IJCSIS AUTHORS' & REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2014
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500
http://sites.google.com/site/ijcsis/