Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Agbaje, M. O, Awodele O., & Ogbonna, A. C. (2015). Applications of digital watermarking to cyber security (Cyber watermarking). *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* (pp. 1-11). Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p001-011Agbaje1518.pdf

Applications of Digital Watermarking to Cyber Security (Cyber Watermarking)

Agbaje, M.O, Awodele O., and Ogbonna A.C
Babcock University, illisan- Remo, Ogun State,Nigeria.

agbajeolugbenga@gmail.com delealways@yahoo.com
acogbonna06@yahoo.com

Abstract

Cyber security is generally an extension of the traditional information technology (IT) security that is aimed at protecting systems, applications and data that exposed to a variety of forms of attack via the internet, ranging from data theft and espionage to corruption of data and denial of service attacks. There is a need for an increase in cyber security research due to losses from sabotage being experienced by nations, businesses and individuals from various cybercrime attacks. This paper takes a look at the applications digital watermarking to the process of protection in cyber space called cyber watermarking particularly focusing on theft of information (identity & credit card theft).The methodology of the research is through literature search and case study. The rest of the paper presents a brief overview of the digital watermarking and issues in cyber security.

Keywords: digital watermarking, cyber security

Introduction

Cyber security is generally an extension of the traditional information technology (IT) security that is aimed at protecting systems, applications and data that exposed to a variety of forms of attack via the internet, ranging from data theft and espionage to corruption of data and denial of service attacks. It can generally be summed up as "the protection of data and systems held and transferred in networks that are connected to the Internet". It is an extension of traditional IT security, and emphasizes protecting systems, applications and data that exposed to a variety of forms of attack via the internet, ranging from data theft and espionage to corruption of data and "denial of service" attacks (Accenture, 2010).

In today's information-age, an organization's dependence on cyberspace is becoming an increasingly important aspect of organizational security. As different organizations infrastructures are interconnected in cyberspace, the level of risk to national security has increased dramatically. The threat to cyber security is growing (More et al., 2014).

Countering the threat of attack on critical information assets and systems has emerged as a key priority for the US federal government and other governments worldwide. Similarly, private sector corporations are taking the risk of

Editor: Eli Cohen

cyber attacks with increasing seriousness, in part as a response to a series of high-profile attacks on organizations ranging from banks to online retailers to ISPs and also selling and stealing of intellectual works.

Cyber attack refers to the use of deliberate actions perhaps over an extended period of time to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and programs resident in or transiting these systems or networks. Washington post (2010) reported that least 34 companies including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical were attacked. Also Los Angeles Times (2010) reported that cyber attacks of Google facility in China prompting it to threaten shutting of its facility there.

In Nigeria, we moved from telephone enabled internet (dial-up) in the 90s to the latest mobile technology and emerged as one of African user's of mobile Internet without much attention being paid to cyber security early enough. The consequence is the resultant increase in cyber crimes and other fraudulent activities being perpetrated by criminals especially in the area of financial and identify theft.

Tonge, Kasture, and Chaudhari (2013) also observed that sudden jump from no telephone to the latest mobile technology without preparation for cyber security landed India today as the 5th in world ranking in the world of countries affected by cybercrime. These observations are not limited to the countries sited above.

The US government as a pioneer in cyber security has taken steps to improve federal IT infrastructure over the past decade. The 9/11 terrorist attacks on the US were certainly a wake-up call; legislation and reform was inevitable (Roman, 2011).

The annual Cyber Security Intelligence Index report by IBM reveals that after several years of continuing growth of the Internet, data breaches literally hit home in 2013. In 2013 alone more than half a billion records of personally identifiable information including names, emails, credit card numbers and passwords were stolen (IBM, 2014).

Information commissioner (2010) reported that fastest developing type of criminal activity in the last decade is known to be identity theft. This involves using someone else's name, address, unique personal identification number (e.g., SSN), bank account number or credit card number for criminally performing a financial transaction, hire a loan, buy merchandise for larger amounts of money, take a mortgage on the victim's house, buy property or gain certain rights.

Identity thieves may obtain information about a bank account number in numerous different ways; research shows that as many as 46 % of such thefts occur as a result of a forgotten credit card or some similar way of obtaining bank account information. Thieves can sift through garbage and obtain data from discarded bills. They can break into mailbox or redirect mail to their address with a demand for a temporary change address so that they can obtain victim's data needed for their bad intentions (Information commissioner, 2010).

Given society's increasing dependence on the internet for business and communications, cybercrime is a growing global problem that no company or country can tackle alone. At any given time, an estimated 150 000 viruses and other types of malicious code are circulating across the internet, infecting more than a million people every day.

Losses from sabotage, the theft of intellectual property, and cyber crime are counted in the billions of Euros. There are a growing number of individuals who use the Internet, and many of these new users are unfamiliar with risks in cyberspace. To illustrate, the number of Internet users around the world in 2000 was approximately 361 million; at the end of 2011, the figure had grown to 2.27 billion – more than a six-fold increase in a little over ten years.

Malicious cyber activities are becoming more sophisticated and easier to execute. Individuals interested in mounting a cyber attack do not need to have any advanced knowledge of computer programming, as they can purchase off the-shelf crime kit tool ware. An example of such programmes is the Zeus crime kit whose malicious code can be customized (Lindstrom, 2012).

This paper takes a look at the applications of digital watermarking to the process of protection in cyber space called cyber watermarking in the face of increased cyber attacks. The methodology of the research is through literature search and case study.

Literature Review

What is Identity Theft?

The term identity theft is defined as obtaining personal data or identity of another person in order to gain benefits or to incriminate another person. Identity theft is a special type of severe and irreversible infringement of informational privacy or personal data protection. By its intensity, the effects of identity theft can be compared to the consequences of violent criminal offences against life and limb or property.

Types of Identity Theft

The following are the various types of identity theft and percentages as reported in Figure 1: Credit card fraud, Phone and utilities fraud, Bank fraud, Employment fraud, Government document and benefits fraud, Loan fraud, attempted fraud and others.

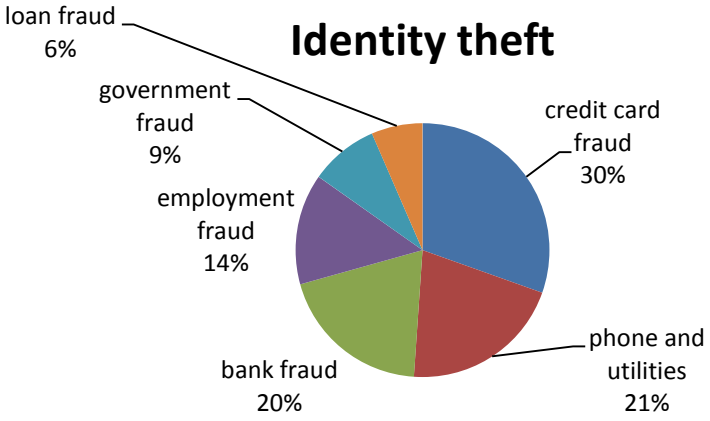

Figure1: Types of identity fraud.
Source: Alexander (2015)

Consequences of Identity Theft

A perpetrator can make use of many different methods of obtaining personal data so that he can start posing as someone else and enter in different legal relationships (e.g., employment, acquiring professional qualifications, obtain personal identity documents, etc.). The scope of identity theft is therefore not limited to the abuse of personal data, since it always includes the purpose of gaining certain benefits. Consequently, the protection of victims' rights is not limited only to data protection, but needs to focus on other rights as well, originating from broader aspects of the right to privacy

Identity thieves can also encroach upon the victim's right to personal dignity by damaging his or her honour and reputation, and causing constant emotional distress, mainly due to the fact that

theft of certain personal data can be irredeemable (e.g.. the theft of biometric personal data, unique identifier and alike).

Preparatory activities for this kind of criminal offences can include different types of both criminal and non-criminal activities; for example stealing a wallet containing personal documents, intercepting electronic messages, scanning and cloning RFID enabled cards, using computer viruses (i.e., with phishing and pharming attacks), using fraud to gain information or even searching for discarded papers containing personal data (an activity known as dumpster diving), etc.

The law also prohibits copying and storing of copies of documents in an electronic form. It is therefore forbidden to copy personal documents using scanners and other similar devices that record the copy in an electronic form and save it on an electronic medium. The law allows for the owner of an identity card to mark the copy of a document with his signature. It is recommended that the photocopy is signed in such a way that the signature is written over the copy of the picture and not in the blank space on the edges of the copy.

Since 1990, there have been already 33.4 million victims of identity theft in the United States, where this branch of criminal activity was born. It is estimated that this number grows by 50 % each year; however, the result of the police efforts to catch the "bad guys" is scarce. Nearly 88 % of the victims had no contact with the identity thief whatsoever. A modern criminal act swiftly, accomplishes his goal within a week or two, and disappears.

On the other hand, the victim discovers the scam only after some time, when, for example, he starts receiving immense bills at his address. It takes months, if not years before the victim manages to prove his or her innocence and gets rid of the consequences of the fraud. Experts estimate that the average costs of administrative, judicial, security or detective services for clearing one's good name are valued at approximately 740 USD.

Techniques for preventing identity thefts include Access control, Encryption, Digital Signatures. In this paper we explore the use of digital watermarking.

Methods of Identity Theft

There are different methods of identity theft, which can divide according to:

- The person, be performing the attack (the intrusion can be either authorized or unauthorized);
- Whether the data has been stolen from a database or during the information flow through a network (a direct attack on data storage or a medium for transmitting data; another possibility for theft of data is also when documents are being scanned from an analogue to a digital format);
- The motive (financial identity theft, criminal identity theft, assuming identity in daily life);
- The selected method (technical and non-technical methods). (Alexander, 2015).

The Internet

The Internet was first developed by the Defence Advanced Research Projects Agency (DARPA) in the late 1960s; its developers could not have fathomed the number of video, voice, and e-service applications that would be spawned in the future (Lindstrom, 2012). It is a massive network of networks - a networking infrastructure. It connects millions of computers and devices together globally, forming a network in which any computer or device can communicate with any other computer or device as long as they are both connected to the Internet. Information that travels over the Internet does so via a variety of languages known as protocols. Figure 2 shows a representation of the internet.

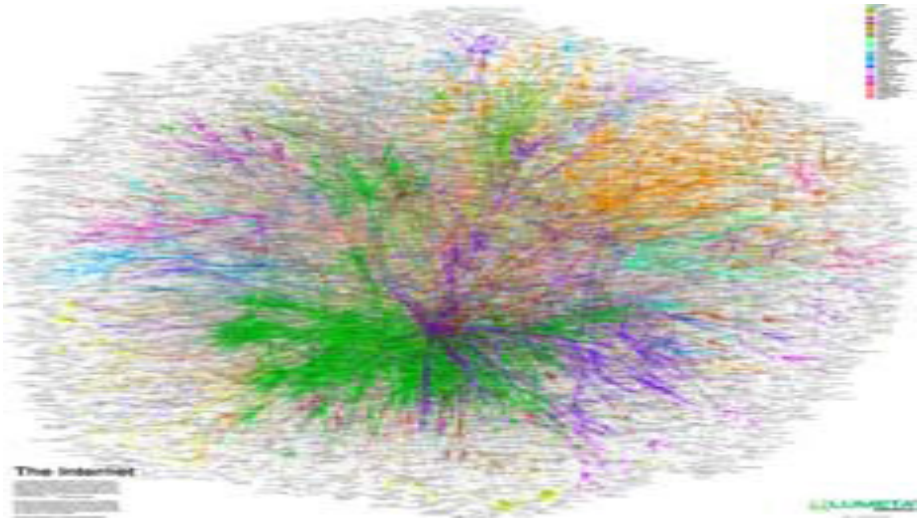

Figure 2: Make up of the Internet
Source: Huttenlocher (2014)

The Internet is one of the fastest-growing areas of technical infrastructure development (Sharma, 2012). As of now information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings, electricity supply, transportation infrastructure, military services, logistics and so on. At present virtually all modern services depend on the use of ICTs (ITU, 2012).

The rate at which ICTs is growing keeps bringing new opportunities for the society, but also new security challenges. Combined with a technical defect, human error or intentional damage, the increasing dependence on ICTs makes it difficult to minimize any consequences 59resulting from a break through a weak spot of the whole ICT system (CR, 2011). Safe, secure and reliable operation of ICTs is necessary for the functioning of government and public structures and is an indispensable prerequisite for prosperity and a sustainable 62economic growth (CR, 2011). The growing dependence on ICT increases the vulnerability of the country and its citizens to cyber attacks (CR, 2011).

Threats to essential services such as water and electricity supply, Cars traffic control, 65elevators, air conditioning and telephones also depend on the smooth functioning of ICTs. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Attacks against information infrastructure and Internet services have already taken place. Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. The financial damage caused by cybercrime is reported to be enormous (ITU, 2012).

These threats are not only local but global in nature (references). They are not restricted by geographical boundaries, and are targeted at all technologies, hardware/software/service providers and users – consumers, the private and the public sector alike. The threats are at an all-time high, in terms of sophistication and volume, and continue to trend upwards. If there was a simple answer or a solution to the cyber security challenge it would have been found by now, and it would have been adopted (Suffolk, 2013).

As long as a computer or other devices is connected to the Internet there is probability of exposure to cybercrime. Ponemon Institute presents the cyber crime study which is based on a sample

of 56 organizations in various industry sectors in United States. Table 1 shows the statistics of different types of cyber attacks occurred in year 2012 & 2013.

Table 1: Types of cyber attacks

Types of Cyber attacks	2012	2013
Viruses,worms,trojans	100%	100%
Malware	95%	97%
Botnets	71%	73%
Web-based attacks	64%	63%
Stolen devices	46%	50%
Malicious code	38%	48%
Malicious insider	38%	42%
Phishing & social engineering	38%	42%
Denial of service	32%	33%

Source: More et al., 2014

The result shows that attack with prominence include viruses, worm and trojan closely followed by malware and also botnets. Table 2 shows security methods commonly used in cyber attack prevention. It can be seen that 94% of organisation uses firewalls and 86% Role-based access and 83% by physical separation. Table 3 shows security technologies studied by More et al. (2014). Advanced perimeter and firewall tops the technologies used.

Table 2: Security Methods

Security Methods	Organisation
Firewalls	94%
Role-based Access	86%
Physical Separation	83%
Encrypt Data on HD	69%
Identity Management	69%
Encrypt Backup Data	63%
Monitor Use of Backup Media	36%

Source: Burd, 2006

Table 3: Security Technology

Security Technologies	2012	2013
Advanced perimeter controls and firewall technologies	58%	525
Encryption technologies	50%	48%
Security intelligence system	47%	45%
Access governance tools	42%	41%
Extensive use of data loss prevention tools	38%	41%
Enterprise deployment of GRC tools	37%	39%
Automated policy management tools	47%	45%

Source: More et al., 2014

Digital Watermarking

The art of paper manufacturing was discovered in China but paper watermarks did not appear until about 1282 in Italy. The marks were made by adding thin wire patterns to the paper moulds (Cox et al., 2008). Digital watermarking is the process of embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm (Megías, Serra-Ruiz, & Fallahpour, 2010). A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm (Katzenbeisser & Petitcolas, 2000). Digital watermarks are signals added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data.

Digital watermarking has to do with protecting digital file against illegal copy and manipulations without the knowledge of copyright owners. This review will focus on digital watermarking and to examine its possible application to cyber security.

Previous Works

Prakobphol and Zhan (2002) propose the design and prototype implementation of an image verification server that uses digital watermarking to prevent fraudsters from forging a legitimate user's profile in social networks using the image saved from the networks. The watermark algorithm is implemented in the Discrete Wavelet Transform, DWT. The watermark is a sequence of bit stream. The algorithm decomposed the image to obtain a low-frequency approximation representation. The watermark is embedded in low-frequency approximation representation (LL). Each time, the coefficient triple of a non-overlapping 3x1 sliding window is selected and manipulated. Sliding a non-overlapping 3x1 window over 3 coefficients, each time manipulating them, embeds the watermark. The median of the three coefficients are quantized to become a multiple of "space" to represent one bit of watermark data. In watermark extraction, the median of the sliding window is determined and quantized to obtain a reconstruction point. The bit value associated with that reconstructed point is assigned to extracted watermark sequence. The server also gives users better control over their privacy.

Topkara (2005) presents a watermarking based approach, and its implementation for mitigating against phishing attacks- a form of web based identity theft (ViWiD). ViWiD is an integrity check mechanism based on visible watermarking of logo images. It performs all of computation on the company's web server and does not require installation of any tool or storage of any data such as keys or history logs on users' machine. The watermark is designed to be unique for every user and carries a shared secret between the company and the user in order to thwart the "one size fits all" attacks. The main challenge in visible watermarking of logo images is to maintain the aesthetics of watermarked logo to avoid damage to its marketing purpose yet be able to insert a robust and readable watermark into it

Sztipanovits (2007) examines digital watermarking and recent developments in the field to survey possible parallels between digital image watermarking and data integrity or the broader data security. They discuss common architectural features and compare the two basic digital image watermarking methods. The architecture of digital watermarking consists of two main components: a watermark embedder and a watermark detector. The embedder combines some digital data and hidden information where the data is the carrier and the hidden information represents the watermark. The details of this architecture are heavily influenced by the application scenario. Roles of a watermark detector range from the recovery of watermarks in corrupted data to the identification of data integrity violations. Upon further reflection about the possible application of such a range of scenarios it becomes evident that they create conflicting requirements for the architecture.

Harjito (2013) presented copyright protection of scalar and multimedia sensor network data using digital watermarking. This research investigates different watermarking techniques to address the issue of copyright protection of the scalar data in wireless sensor networks (WSNs) and image data in wireless multimedia sensor network (WMSNs), in order to ensure that the proprietary information remains safe between the sensor nodes. They develop a Linear Feedback Shift Register (LFSR) and Kolmogorov Rule (LKR) watermarking technique for the copyright protection of scalar data in WSNs. The LKR watermarking technique developed can protect the copyright data from deletion, packet replication and multiple data identities (data Sybil attack), although it is ineffective against false data insertion, data modification and selective forwarding.

Braun (2014) presented a Forensic evidence of copyright infringement by Digital Audio Sampling Analysis - Identification. They presented methods for audio analysis including the use of watermarking in music copyright protection.

General Use of Digital Watermarking

Digital watermarking is being used in numerous applications. The various types of watermarks can be better described by going through some of the most common purposes such as these, mostly defined in:

- **Digital signatures** – The watermarks holds information identifying the owner of the content.
- **Fingerprinting** – The watermark hides information about the authorized user of the content.
- **Broadcast and publication monitoring** – The watermark is used to monitor the use of broadcasted or published information, as in the Philips Research initiative of creating VIVA (Visual Identity Verification Auditor) "to investigate and demonstrate a professional broadcast surveillance system. Broadcast material will be pre-encoded with an invisible unique watermark identifier."
- **Authentication** – The watermark (or in this case also called a vapormark) is used to guarantee that the content showed is precisely the one created.
- **Copy control** – This watermark records information regarding possibilities of reproduction of the data. It will store simple rules similar to "data cannot be copied" or "data can be copied once only, and never afterwards".
- **Filtering/Classification**– Classifies content so it is used appropriately; filters inappropriate content.
- **Linking/E-Commerce**– Enables access to information and purchase of related content
- **Remote Triggering**– Causes automatic action during Distribution.
- **ID Security:**ID is scanned to determine authenticity Digital watermarking of travel/identity documents protects against: Alteration, regeneration, photo swapping and counterfeiting, Can enable cross-jurisdictional authentication without standard ID desig,• Automates document authentication• Provides forensic analysis and tracking • Provides compatibility with both new and existing ID designs

Use of Digital Watermarking in Information Theft

(i) **Data integrity:** Data integrity plays fundamental role in ownership, attribution and reliability of digital records. The authors and users of digital records may not be aware of a whole host of potential problems that are associated with them. Examples may be, forging the time of the records, privacy considerations related to the record, or protected information in them. Such aspects are often not in the control of the author after the document is created.

(ii) **Privacy**: Privacy considerations related to the record, or protected information in them.

(iii) **Data security:** The purpose of digital watermarking in general is to place additional information into an existing content captured in files. With this information the author, the ownership or other maintained aspects of the document may be verified.

Proposed Watermarking Algorithm against Identity Theft

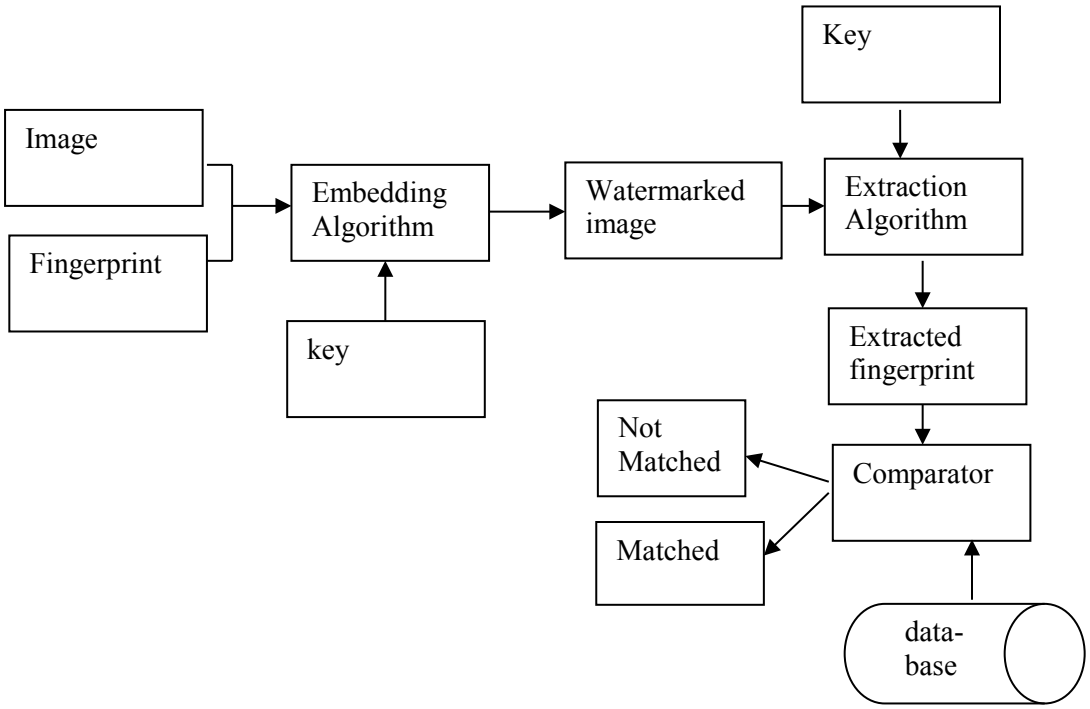

Figure 3: Image authentication watermarking using fingerprint.

Figure 3 shows the proposed algorithm for an identity management scheme. It consists of the embedding algorithm for combining an image with a sample of fingerprint of owner. They are combined to form a watermarked image. The embedding is done using a secret key. The same key is used in the extraction algorithm to extract the fingerprint. Using a comparator the database is searched to compare the two signals. The decision of matching and not matching is made for any transaction to proceed.

Applications: ID Security, ID Authentication and Piracy Deterrent

Digital watermarking of travel/identity documents protects against: Alteration, regeneration, photo swapping and counterfeiting.

- Can enable cross-jurisdictional authentication without standard ID design.
- Automates document authentication.
- Provides forensic analysis and tracking
- Provides compatibility with both new and existing ID designs

Conclusion

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. The proposed algorithm can be varied depending on the type of application for services being offered. Therefore it is hoped that the future digital watermarking will play a vital role in cyber security. Helps people to understand cyber watermarking and its importance. Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguard.

References

Accenture. (2010). *Cyber security: An escalating global challenge for all organizations*. pp. 1-12.

Alexander, A. (2015). *Protecting yourself from identity theft*. Retrieved from www.thewatermarkgrp.com

Baranwal, N., & Datta K. (2011). *Peak detection based spread spectrum audio watermarking using discrete wavelet transform.*

Braun, S. K. (2014). Forensic evidence of copyright infringement by digital audio sampling analysis - identification – marking. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 3*(3), 170-182.

Burd, S. A. (2006). *The impact of information security in academic institutions on public safety and security: Assessing the impact and developing solutions for policy and practice*, October 2006.

Cox, J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). *Digital watermarking and steganography.* Morgan Kaufmann Pub., Elsevier Inc.

CR. (2011). *Cyber security strategy of the Czech Republic for the 2011 – 2015 period*.

Huttenlocher, D. (2014). *NBA 600 Networks and the Internet Class 3*, Mon 10/22. The Johnson School, Cornell University. Retrieved from www.slidefinder.com

IBM. (2014). *IBM Security Services 2014 Cyber Security Intelligence Index Analysis of cyber attack and incident data from IBM's worldwide security operations.*

Information commissioner. (2010). *Guidelines for preventing identity theft* (pp 1-19). Retrieved from www.ip-rs.si

ITU. (2012). *Understanding cybercrime: Phenomena, challenges and legal response September 2012*. Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Katzenbeisser, S., & Petitcolas, F. A. P. (2000). Information hiding: Techniques for steganography and digital watermarking. *Information Hiding First International Workshop Proceedings*, 295–315.

Lindstrom, G. (2012). *Meeting the cyber security challenge. Geneva Centre for Security*. Los Angeles Times, January 15, 2010

Megías, D., Serra-Ruiz, J., & Fallahpour, M. (2010). Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification. *Signal Processing*, *90*(12), 3078-3092.

More, R. M., & Kumar, A. (2014). Study of Current Scenario of Cyber Security Practices and Measures: Literature Review. *International Journal of Engineering Research and General Science, 2*(5), August-September.

Prakobphol, K., & Zhan. (2002). *Alleviating identity theft in social networks*, pp. 1-4.

Perceptions about Network Security. (2011). Ponemon Institute, Research Report, June 2011.

Settipalli, N., & Manjula, R. (2011). Securing watermarked-relational data by using encryption and decryption. *ARPN Journal of Systems and Software, 1*(2).

Sztipanovits Mate, Hung Chih-Cheng and Qian Kai (2007), Watermarking Methods for Cyber Security.

Song, Y. (2005). *Digital watermarking-based authentication techniques for real time multimedia communication*. Phd thesis.

Suffolk, J. (2013). *Cyber security perspectives: Making cyber security a part of company's DNA*. Huawei Technologies.

Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: Challenges for society- literature review. *IOSR Journal of Computer Engineering, 12*(2), 67-75.

Topkara, M., Ashish, K., Mikhail, J. A., & Cristina, N. (2005). ViWiD: Visible watermarking based defence against phishing. Digital watermarking. *Lecture Notes in Computer Science, 3710*, 470-483.

Wang, W., & Lu, Z. (2013). *Cyber security in the Smart Grid: Survey and challenges.* Computer Networks, Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606, USA, pp 1344–1371.

Washington Post. (2010). January 14, 2010.

Yan, X., & Wu, Y. (2012). *The Digital Watermarking Techniques Applied to Smart Grid Security*. INTECH Open Access Publisher.

Biographies

Agbaje M.O. is a lecturer and currently working on his Ph.D at Babcock University, Nigeria. His research interests are Information security, Trusted Computing and Embedded systems.

Oludele Awodele has a Ph.D in Computer Science .He is currently the H.O.D of Computer Science department, Babcock University. His areas of interest are A.I and Computer Architecture. He has published scientific articles in several journals of international repute.

A.C. Ogbonna Ph.D is presently the dean of School of Computer Science and Engineering, Babcock University ilisan Remo Ogun State, Nigeria. He can be contacted at acogbonna06@yahoo.com