Amalgamation of Cryptography and Steganography on Global Security Systems

Article · April 2020

CITATION
1

READS
75

5 authors, including:

Joseph Okon Esin
Independent Researcher at the University of Calabar
7 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Agana Moses
University of Calabar
23 PUBLICATIONS **25** CITATIONS
SEE PROFILE

Bukie Paul Tawo
University of Calabar
14 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Prince Ana
Cross River University of Technology
20 PUBLICATIONS **23** CITATIONS
SEE PROFILE

Amalgamation of Cryptography and Steganography on Global Security Systems.

Joseph OkonEsin
Professor of Computing Information Systems/Cybersecurity
Jarvis Christian College, Hawkins, Texas USA

Moses AdahAgana
mosesagana@unical.edu.ng
Senior Lecturer& Head of Department
Computer Science Department, University of Calabar.

OfemAjahOfem
Senior Lecturer & Immediate-Past Head of Department
Computer Science Department, University of Calabar.

PaultuTawoBukie
Lecturer
Computer Science Department, University of Calabar

Prince OnebieniAna
Lecturer
Cross River State University of Technology, Calabar, Nigeria

Prelude

Cryptography is derived from the Greek "***KRYPTOS,"*** meaning hidden, andtheword "cryptography" originated from a Greek vernacular signifying "secret writing."The earliest knowledge of cryptography isdated in about 2000 BC, rooted in Egyptian practice of hieroglyphics,which consisted of complex pictograms known by only few elites.From 500-600 B.C., the Hebrew scribes used ATBASH, a reversed alphabet simple solution cipher and in 50-60 B.C. Julius Caesar adopted unassuming substitution with the normal alphabet as official means of communications(Manoj, 2010).The wisdom in the rear of Julius Caesar'sapproach was deep-seated on mistrust of his envoys when communicating withofficers. This distrust led to thecreation of a system in which each character during communications was replaced with Roman alphabet.During the European Renaissance, several Italian and Papal states adopted cryptographicmeasures entrenched with art of unveilingsecret data codes, and this eventually led to the discovery of alternative

conventional techniques known as Vigenere Coding in 15th century, anobtainable opportunity to move letters in the message to several alterable places away from the same locationin order to prevent hacking or the leaking of the message (Fitzgerald and Jessica, (2015).

Per Esin (2017), cryptography later became thestudy of science of secret writing that uses the mathematical techniques and most aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography algorithms is designed to make data unreadable by separating messages into symmetric (secret-key) and asymmetric (public-key) network security operations. Symmetric algorithms are used to cipher and decipher original messages (plaintext) by using the same key and asymmetric algorithms frompublic-key cryptosystemto ensure confidentiality of stream data. In Public-key encryption algorithms, there are two keys;private and public, where thepublic key is used to encrypt informationsent to a receiver who has access to the correspondence. Consequently, privateandpublic keys aredifferent, but equally needed for communication exchange.

As Rajyaguru (2012), Neetha (2015) and Ngwang (2016) noted, these days, cryptography has turned into a battleground for mathematicians and computer scientists with ability to securely store and transfer sensitive information. Nowadays, globalcommunities are trapped in the process of granting infinite access to receiving and/orsending hidden and threatening data and information across universallysecurednetwork systems. Cryptography is best understood when a sender sends a message which initially exists in the plaintext, but then, prior to transmittingthe messages over the secured network system, this message is encrypted and converted into the ciphertext, and received by the recipient in a decrypted and plaintext format (Judge 2014, and Kallam, Udaya & Vinaya, 2010). As Dipti and Neha (2010) in their studies on data hiding using cryptography and steganography asserted, data symmetric key cryptography, codenamed “Secret key” used to encrypt and decrypt plain text

and cipher text often share same key for encryption and decryption and tend to consume less execution time. Asymmetric key cryptography, also known as "Public key" is structuredto use two sources, privateand public keys. Public key is encrypted message from the receiver to the sender while the private key is amplified by the receiver to decrypt the message. In contrast, cryptography uses techniques named as trans positional, substitution, and stream to block cipher processes when necessary.

As Esin (2017), Bharti and Soni (2012), Sashhikala and Ajay (2009) asserted,hash function is an imperative component ofcryptography; a one-way encryption that is deeply engrained in generating hash codes which is faster than other algorithm by making the process more desired for authentication and integrity. Hash functions and associated codes areused for digital signature, message authentication and Internet security protocols. Per Huang, Ryota, Segawa and Abe (2006), authentication andintegrity are important components of original messages, and applying hash function to the message will play key roles in verifyingauthentication and integrity of sender'smessage to the receivers.

Framework of Cryptography

Cole (2003), Delforouz and Pooyan (2007) and Esin (2016) asserted that the evolution of human civilizations witnessed the reorganizing of most entities into tribes, villages, cities, states, kingdoms and nations and that the emergence of human redeployment invigorated the natural need for populace to establish secret codes of communication with selective inheritors, which, in turn, guaranteed the continuous evolution of cryptography. The myth of cryptography includes cryptosystems, outmoded and modern-day ciphers, public key encryption, data integration, message authentication, and digital signatures. Cryptography is one of the original cultures of Roman and Egyptian civilizations of 4000 years ago, where Egyptian traditional writing involved the use hieroglyph to transmit and communicate secret manages to each other. Hieroglyph is the oldest cryptographic secret code used by

transcribers to transmit messages on behalf of kings, modern-day suzerains and royals (Goljan, Fridrich and Holotyak 2006, &Rajyaguru, 2012). As Manoj (2010) noted, modern scholars adopted simple mono-alphabetic substitution ciphers during 500-600 BC to replace alphabets of message with alternative alphabets of secret language, rule and keys. The earlier Roman modus of cryptography, popularly known as the **Caesar Shift Cipher**, depended heavily on shifting the letters on a message by an agreed number with three as a common choice and the recipient of the message will then, shift letters back by the same number to obtain the original message. Cryptography is a thought-provoking chronicle distinguished as proven component of the history of human civilization leading to expansion of individuals' and organizations' opportunity to hide true intentions, gain competitive edge and reduce human vulnerabilities to hacking as a result of continued technology advancement. Cryptography algorithms are incorporatedinto streams of binary code that pass over network wires, Internet communication channels and airwaves(Cole 2003 &Delforouz and Pooyan, 2007).

Cryptography + Security + Encryption = Hexing

In about 400 B. C., the Spartans used a system of encrypting data and information to write messages on papyrus wrapped around wooden rod to communicate with recipients. These messages were readable only if they were properly wrapped with the correct and matching size of wooden rod. In about 100 B.C. in Rome, Julius Caesar developed an uncomplicated method of shifting letters of the alphabets like a bash scheme. He shifted the alphabets by three positions. The shifted alphabet is known as algorithm and the key is the number of locations shifted during the encryption and decryption operations.

Traditional Alphabet: ABCDEFGHIJK**L**MN**O**PQ**R**STUVWXYZ

Cryptographic Alphabet: DEFGHIJK**L**MN**O**PQ**R**STUVWXYZABC

As posed above, encryption algorithm process involves taking the first letter of the message, L and shifting it up three locations within the alphabet. The encryption algorithm will involvemoving letter O to match letter R that is shifted three places. Upon successful completion of encryption algorithm process, a carrier will take modern encryption version to the destination that will eventually lead to reversed process. Cryptography has increased and restored confidence in security operation for over three decades; it has also strengthened individuals and organizations of cryptography.

In the 19th century, cryptography evolved from the informal approaches to encryption to a sophisticated art of science of data and information security. It eventually led to the discovery of mechanical and electromechanical machines known as Enigma Rotor machine with advanced and efficient capability to code data and information in the early 20th century (McMillan and Abernathy, 2014).

During the second World War II, cryptographyemerged asa science for securing of digital data and mechanisms of mathematical algorithms to provide fundamental information about security services. It included the establishment of a large toolkit containing different techniques for security applications, which turned out to be a mathematical operation and was adopted by military units and government agencies to protect their secret operations (Judge (2014).

Per Goljan, Fridrich and Holotyak (2006), Rajyaguru, (2012), and Esin (2017) five fundamental data and information security services reinforcing projected objective of cryptography include Confidentiality, Data integrity, Authentication and Non-repudiation. **Confidentiality** is a security service provided by cryptography to protect data and information from unauthorized users, otherwise known as privacy or secrecy. Credible means involves the use of physical and mathematical algorithms and encryptions of data, information and languages. **Data integrity** cannot prevent the alteration of data but it

provides a means for detecting whether data has been manipulated by perpetrators; hence, it is designed to identify any alteration to the data such as abrupt changes and modification of data by an unauthorized user intentionally or accidently. Integrity service is designed to confirm or ascertain whether data is intact from the date of creation and transmitted by an authorized user. Per Wang and Moulin (2007), data integrity in the context of cryptography is concerned with verifying that data and information was not altered and modified prior to leaving the host system to the recipient system. **Authentication** often provides the identification of the originator to confirm to the recipient that data and information sent is legitimate, authentic and verified by the sender. Authentication service has two variants, message authentication identifying the originator of the message without regard to the sending router or the system and entity authentication assuring that data and information is received by the recipient. **Authorization**is a process of providing identity with username and password to access the system without authorization. Authorization is the function of specifying access rights to resources related to information security and computer security and direct access control into the system. An organization's fiscal affairs unit often authorizes payroll officer's access to records.Policy and formalized procedures are an integral part of the control of any organization's computer network system and regulates authorization to decide which employees should be granted or rejected authorization to the organization's payroll system. **Non-repudiation**is a security service ensuring that the original creator of the data and information cannot deny the ownership of the creation and transmission and ignore previous commitment of data and information sent to a recipient. In addition, non-repudiation is a service where the author of a statement or document cannot challenge the authorship. Such situation is often seen in a legal setting wherein the authenticity of a signature is being challenged; if so, authenticity is being repudiated.

Non-repudiation isoften used by an expert who has the knowledge of the signature key; the sender can create unique signature using the given data and the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.**Message authentication is** a process to validate the digital signature using a public key from a sender to be assured that the signature was created by an authorized sender in the possession of secret the private key. **Data Integrity**les with the expert who can identify if an attacker has access to the data and ability to verify if receiver end fails. By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely: Privacy, Authentication, Integrity, and Non-repudiation (McMillan and Abernathy, 2014 and Neetha, 2015).

Cryptography includes techniques such as microdots, merging words with images, to hide information in storage. Today in a computer-centric world, cryptography is most often associated with scrambling plaintext known as ordinary text, cleartext, ciphertext and encryption. Professionals who practice this field are known as cryptographers, while protocols that meet these criteria are known as cryptosystems. Cryptosystems are often related to mathematical procedures and computer programs; however, these procedures are involved in the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with strangers and interlopers. Cryptography is a set of primitive codes of data, information, messages and languages selectively used to protect security services including encryption, hash functions, message authentication codes (MAC) and digital signatures. Per Dipti, and Neha (2010), Rajyaguru (2012) and Neetha (2015), cryptographic is often integrated into a security service known as cryptosystem. A cryptosystem is a representation of cryptographic techniques designed to provide information security services and can be identified as a **cipher system**.

Cryptosystem provides confidentiality to data and information from the sender to the recipient.

Steganography

As Manoj (2010) and Judge (2014) asserted, steganography is rooted in Greek "Steganos," meaning protected and covered writing. The first allusion to steganography is credited to Herodotus in 440 B.C.and Demaratus, King of Sparta who cautioned Greece's authority about using a wooden tablet and beeswax to hide messages. Steganography and cryptography are onboth sides of the coin; steganography often hides traces of data transmission and communication while cryptography uses encryption to make messages incomprehensible. As Sashikala and Ajay (2009) asserted, steganographyis designed to transfer undisclosed messages to individuals and no interim person is expected to view and have access toactual real-life messages. Digital communications and computer system use the process to replace the unwanted data with plain text message and cipher text; then operate without any suspicion and misgiving and reduce the chance of data leakage.

Steganography algorithms restricts data transmission and communication access to public domain and equally protect against unauthorized access. Enhanced values of steganography are used in a wide-range of data systems in a global digital world such as bmp, .doc,.gif,. jpeg, mp3,. txt.wav and largely due to its popularity on the Internet operations (Sashikala and Ajay, 2009 &Neetha (2015). Steganography and cryptography are cousins in spy-craft operations, but stenography is deeply rooted with secret and protective measures. The remarkable three widely used types of steganography include pure, private key, and public key steganography (Goljan, Fridrich and Holotyak (2006), Rajyaguru, (2012) and Esin (2017):

- Pure steganographyis the least secure measure of communicate indicating sender and receiver can rely only on the presumption that no other parties are aware of secret messages.
- Private key steganography requires the exchange of a secret key co-name stego-key prior to sending message to the receiver, and should any message be intercepted, both sender and receiver who know the secret key can extract the secret message.
- Public key steganography uses a public and a private key to secure the communication between the parties wanting to communicate secretly. The sender will use the public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can be used by the receiver to read the message.

Steganography does not trigger changes in the structure of the message, while, cryptography often alters the standard of secret message prior to transferring along the network securesystem. As Judge (2014) noted, astuteness behind the steganography algorithm is to preventsuspiciousexistence of data and information, key source of access control such as username and password in order to prevent authorized users. Steganographic systems often hide secret messages within cover media and secret messages will go unnoticed regardless of perpetrators'attempts to intercept messages.Per Cole 2003, Delforouz and Pooyan, 2007, Manoj (2010) and Judge (2014), steganographic algorithm techniquesremained a remarkable advancementin ancient Greece in about 440 B.C. as Greek ruler,Histaeusretainedhis personal scheme involving shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, sending the slave on the way to deliver the messageto recipient. Unfortunately, he had to

have the slave's head uncovered in order toamplify hismessage to receivers.Steganography is an added component of cryptography used to protect the secrecy of transmitted messages. Steganography is the science of writing hidden messages guaranteeingdata and information embedded inside multimedia files, where image and host files should only be accessible to authorized parties. Objective of steganography algorithms techniques are to protect data and information and messages againstchallenges of digital forensic investigations.

Equal Contribution to Network Security system

Steganography and cryptography are cousins in spy-craft operations. In today's cybersecurity, investigation and forensics inquiry era, the internet is an essential component for data transmission, communication and information sharing processrequired to protect against unauthorized access to secured network systems.Cryptography and steganography are traditionally equally analogous in their protective defensive nature against sender and recipient of encrypted messages.

- Cryptography and steganography are interrelatedtechniques that share common goalsof protecting the confidentiality, authentication, integrity, and the availability of data much needed in network secured system.
- Cryptography and steganography are equally exceptional techniques to insulate and transmit messages through open secured network communicationsystems relative to transmitting messages to senders and recipients via common Internet.
- Cryptography is a science and sculpture of secret writing dated back to 1900 B.C.and involving three types of cryptographic algorithms such a secret key cryptography (SKC), public key cryptography (PKC), and hash functions.
- Steganography originated from Greek cultureand literally referred to shielded writing and the art of hiding existingdata and transmission of secret communication.

- Steganography algorithm involved the use of invisible ink and the use of second letter of each word in a large body of text to enable people to hide information in transmitting data and messages.

Recap

Steganography and cryptography algorithms are cousins in spy-craft relative to transmitting data, information and messages across secured network system.

Per Esin (2017) and McMillan and Abernathy (2014) strengthening of instructional and learning endeavors must be reinforced through professional engagement. As such, the following quiz is meant as a provocative reaction to the article above. **Circle the correct answer:**

1. Which of thefollowing is a set of mathematical rules used in cryptography?

a. Public key
b. Algorithms
c. Cybersecurity
d. Private key

2. Identify the process that converts plaintext into ciphertext.
    a. Hashing
    b. Decryption
    c. Encryption
    d. Digital signature

3. Which of thefollowing is a set of mathematical rules used in cryptography?
    a. Public key
    b. Algorithms
    c. Cybersecurity
    d. Private key
4. Identify the types of cipher classified as Caesar cipher.
    a. Polyalphabetic substitution
    b. Mono-alphabetic substitution

c. Polyalphabetic transposition
d. Trito-alphabetrictransportation

5. Which of the following is most accurate about the strength of a cryptosystem?
    a. The strength of the cryptosystem comes from the algorithm, secrecy of the key and length of the key.
    b. The strength of the cryptosystem determines integrity.
    c. The strength of the cryptosystem determines confidentiality
    d. The strength of the cryptosystem determines availability of secured data

6. Which of the following is the method of hiding data in another message and data format so that the very existence of the data is concealed?
    a. Substitution
    b. Transmission
    c. Communication
    d. Steganography

7. Which of thefollowing is a set of mathematical rules used in cryptography?
    a. Public key
    b. Algorithms
    c. Cybersecurity
    d. Private key

8. In cryptography, different steps and algorithms provide dissimilar types of security service. Which of the following provides only authentication, nonrepudiation, and integrity?
    a. Hash algorithm
    b. Encryption algorithm
    c. Digital signature
    d. Encryption paired with a digital signature
9. What is the name of the machine used by Germany in World War II to encrypt sensitive data?
    a. The Turing Machine
    b. The “Box”

c. The Enigma Machine
d. Verschlusseln

10. What is the purpose of a hash?
    a. A hash provides non-repudiation
    b. A hash provides integrity
    c. A hash provides confidentiality
    d. A hash provides instructions for an algorithm

11. Identify the encryption system that uses a private-secret key that must remain secret between sender and receivers**.**
    a. Master-symmetric algorithm
    b. Symmetric algorithm
    c. One-time algorithm
    d. Asymmetric algorithm

12. Identify the objective of cryptography**.**
    a. To determine the strength of algorithm
    b. To increase the substitution function in a cryptographic algorithm
    c. To decrease the transposition functions in cryptographic algorithm
    d. To deter the permutation

13. End-to-end encryption is used by users and link encryption is used by service providers. Which of the following correctly describes impact of cyber-technology**?**
    a. Link encryption does not encrypt headers and trailers
    b. Link encryption encrypts everything but data link message
    c. End-to-end encryption requires headers to be decrypted at each hop

14. What is the purpose of a key**?**
    a. A key provides the instructions to decrypt encrypted text
    b. A key provides the instructions to encrypt plain text
    c. A key provides math functions to provide encryption or decryption services

d. A key provides the instructions for an algorithm to encrypt and decrypt data.

15. Which function does a virtual private network provide?
    a. Create a tunnel through the internet
    b. Create a private WIFI signal
    c. Bypass security
    d. None of the above

16. Which of the following items best correctly describes a drawback of symmetric key system?
    a. Carry out mathematically intensive operations
    b. Computationally less intensive than asymmetric systems
    c. Key must be delivered through secure carrier
    d. Work much more slowly than asymmetric

17. Which key arrangement is required for symmetric key encryption?
    a. Two keys are involved
    b. One key is involved
    c. A and B
    d. None of the above

18. Which information should a sender use to ensure confidentiality for the recipient?
    a. The public key and a password
    b. Both the public and private keys
    c. The public key of the recipient
    d. The private key and a password

19. How are keys handled with asymmetric encryption?
    a. Two keys are involved
    b. Two identical keys are involved
    c. One odd key is used
    d. None of the above

20. Which type of data maintains confidentiality when using transport encryption?
    a. Blocks in motion
    b. Bits in motion
    c. Data in motion
    d. A and B

21. Which of the following correctly describes the differences between public key cryptography (PKC) and public key infrastructure (PKI)?
    a. The PKC is the act of using asymmetric algorithm, while PKI is the act of using a symmetric algorithm
    b. The PKC is used to create public and private keys pairs and PKI to perform key exchange and agreement
    c. The PKC provides authentication and nonrepudiation, while PKI provides confidentiality and integrity
    d. The PKC is alternative name for asymmetric cryptography, while PKI consists of public key cryptography mechanism

22. Which of the following United States Federal Government's algorithm was developed for creating secure message digest?
    a. Data encryption algorithm
    b. Digital signature standard
    c. Secure hash algorithm
    d. Data signature algorithm

23. Identify the encryption system that uses private or secret key that must remain secret between the two parties.
    a. Running key cipher
    b. Asymmetric algorithm
    c. Symmetric algorithm
    d. Concealment cypher

24. Identify the type of cipher classified as Caesar Cipher.
    a. Polyalphabetic substitution
    b. Mono-alphabetic transposition

c. Mono-alphabetic substitution
d. Polyalphabetic transposition

25. Which attack executed against a cryptographic algorithm uses all possible keys until a key is discovered that successfully decrypt the copytext?
    a. Frequency analysis
    b. Brute force
    c. Ciphertext-only attack
    d. Reverse engineering

26. Which of the following provides the preeminent definition of an encryption algorithm?
    a. Stream ciphers used for confidentiality
    b. Detection of encryption mathematics
    c. Mathematical functions used for encryption of an encryption algorithm
    d. Detection of encryption authentication

27. What is the primary purpose of using one-way hashing on user password**?**
    a. It minimizes the amount of primary and secondary users
    b. It prevents cybercriminals from reading passwords in plaintext
    c. It avoids excessive processing of asymmetric algorithm
    d. It decreases replay attacks.

28. Identify the most secure encryption scheme possible.
    a. Concealment cipher
    b. Symmetric algorithm
    c. Asymmetric algorithm
    d. One-time pad

29. The major component of IPsec must include two of the following.
    a. Integrity and user authentication
    b. Integrity and system authentication
    c. Confidentiality and authentication

d. Trust and availability

30. Identify significant differences between symmetric and asymmetric algorithm:
    a. Asymmetric algorithms are slower because they use substitution and transposition
    b. Symmetric algorithms are faster because they use substitution and transposition
    c. Asymmetric algorithms are vulnerable to cyber-attacks
    d. Asymmetric algorithms are easy to install and configure.

31. El Gamal is directly associated with which of the characteristics?
    a. A hash algorithm
    b. A symmetric algorithm
    c. A public key algorithm
    d. A message key algorithm

32. What key is used to create a digital signature?
    a. The receiver's private key
    b. The sender's private key
    c. The receiver's public key
    d. The sender's public key

Answers			
1	B	17	B
2	C	18	C
3	C	19	A
4	B	20	D
5	A	21	D
6	D	22	D
7	C	23	C
8	B	24	C
9	C	25	B
10	B	26	C
11	B	27	B
12	A	28	B
13	B	29	B
14	D	30	B
15	A	31	C
16	C	32	C

REFERENCES

Bharti, P. &Soni, R. (2012) “A New Approach of Data Hiding in Imagesusing Cryptography and Steganography.” *International*J*ournal of Computer Applications,* Vol.58, No.18. pp1-5.

Cole, E. (2003). *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. Wiley Publishing: Indianapolis.

Delforouz, A.&Pooyan, M. (2007). "Adaptive Digital Audio Steganography based on Integer wavelet transform." *International* J*ournal of Computer Applications* Vol. 8. (26-28).

Dipti, K. S. & Neha, B. (2010). “Proposed System for Data Hiding Using Cryptographyand Steganography.” *International Journal of Computer Applications* Volume 8 No. 9.

Esin, J. O. (2016). “Overview of Cyber Security: Endangerment of Cybercrime on vulnerable innocent global citizens” *International Journal of Engineeringand Science (IJES)* Volume 5, Issue 4: 2319-1805.

Esin, J. O. (2017). *System Overview of Cyber-Technology in a Digitally Connected Society.* Bloomington, Indiana: Author House.

Fitzgerald, A.& Schneider, J. (2015). “Keep it Secret, Keep it Safe: Nine Stepsto Maintaining Data Security.” *The United States Cyber Security Magazine*, 3 (7) 74-75.

Goljan, M., Fridrich, J. &Holotyak, T. (2006). “New blind Steganalysis and its implications. *IST/SPIE Electronic Imaging: Security,Steganography of Multimedia Contents*.” Vol. 8, (pp. 1-13).

Judge, J.C. (2014) “Steganography: past, present, future. SANS Institutepublication.” *International Journal of Innovative Research in Computer andCommunication Engineering*, Vol. 2, Issue 6.

Kallam, R. B., Udaya, K, & Vinaya, B. (2010). “A Survey on Cryptography and Steganography Methods for Information Security.” *International Journal of Computer Applications*. Volume 12 No. 2.

Manoj, I. V. S. (2010) "Cryptography and Steganography." *International Journal of Computer Applications*." Vol.1, No.12, pp 63-68.

McMillan, T. & Abernathy, R. (2014).*Certification Guide, Learn, Prepare and Practice for Examination Success CISSP*. Indianapolis, IN: Indiana University Press.

Neetha, F. (2015). "Information Security using Cryptography and Steganography."*International Journal of Engineering Research& Technology* (*IJERT) NSRCL* – 2015 (3) 28.

Ngwang, E. N. (2016). Individual Freedom, Cyber Security and Nuclear Proliferation in a Borderless Land: Innovations and the Trade-offs in Scientific Progress." *The Journal of Educational Research and Technology (JERT).* Vol. 5. No. 5, 33-72.

Huang, X., Ryota, K., Norihisa, S.& Abe, Y. (2006). "The Real-Time Steganography Based on Audio-o-Audio Data Bit Stream." *International Journal of Computer Applications*. Vol.106 (pp.15-22).

Kallam, R. B., Udaya, K, & Vinaya, B. (2010). "A Survey on Cryptography and Steganography Methods for Information Security." *International Journal of Computer Applications*. Volume 12 No. 2.

Rajyaguru, M. H. (2012). "Combination of Cryptography and Steganographywith Rapidly Changing Keys*." International Journal of Emerging Technology and Advanced Engineering,* Vol.2, No.10.

Sashikala, C. &Ajay, J. (2009) "Steganography an Art of Hiding Data." *International Journal on Computer Science and Engineering* Vol.1(3), 137-141.

Wang, Y. & Moulin, P. (2007)."Optimized feature extraction for learning-based image Steganalysis." *International Journal on Computer Science and Engineering*Vol. 2, No 1 (pp. 31-45).