Villanova Journal of Science, Technology and Management

Vol. 2. No. 1. 2020. ISSN: 2672-4995 (Online) 2672-4987 (Print)

HYBRID DATA SECURITY: A REVIEW OF CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

ASANBE M.O
Department of Computer Science
Villanova Polytechnic, Imesi-Ile,
Osun State, Nigeria
moasanbe@gmail.com

Abstract

As the use of computer networks and internet is ubiquitous, information security has become sizzling area of research in recent times. Data security is very crucial in exchange of information over computer networks because it secures the information from intruders. Although cryptography and steganography are two popular security mechanisms that could be used to provide data security, each of them has drawbacks. Cryptography encrypts the content of the message thereby making it difficult for intruders to fathom. Steganography on the other hand makes communication invisible, that is, message is embedded in a cover media in such a way that intruders cannot detect it existence. Cryptography problem is that, the cypher text looks meaningless, so the intruder can interrupt the transmission and use cryptanalysis to reveal the meaning of the message. Steganography problem is that once the presence of hidden information is revealed or even suspected, the message has become known. Therefore, effort in this paper was directed at reviewing various types of cryptography and steganography techniques. Also, a hybrid data security model was proposed by combining cryptography and steganography to improve information security leveraging on the strengths of the two techniques. In the proposed model, plain message was first encrypted using Data Encryption Standard (DES) making it cypher text. Secondly, the encrypted message (cypher text) was hidden in an image using Least Significant Bit (LSB) technique. The proposed model provided an enhanced data security scheme as attacker will not be able to detect the existence of the message hidden in the image and if per chance the message is discovered, the attacker will still not be able to make meaning of the content because the message was encrypted.

Keywords: Data Security, Encryption, Decryption, Cryptography, Steganography, Cryptanalysis, DES.

1. INTRODUCTION

During the last few decades there is a tremendous development in information and communication technology. Nowadays, information is rapidly available through the internet. Companies, individuals and businesses have the ability to communicate seamlessly with a worldwide audience through the internet and local networks. The transmission of information through internet may include sensitive personal data which may be intercepted by intruders, attackers or eavesdroppers. Also, there are many applications on the internet and many web sites which require the users to fill forms which may include sensitive and personal data. According to [1] Data security helps keep private data private. So, confidentiality and data integrity are required to protect the information against unauthorized access and use [2]. Data and Network security problem can be classified into four parts: Confidentiality, Authentication, Non-repudiation and Integrity Control. Confidentiality or secrecy is concerned with keeping information away from unauthorized users. That means unauthorized users should not be able to read and understand the information. Authentication means any party which may be sender or receiver can verify that the other party is who they claim to be. In other words, authentication is concerned with validating the identity of the other party. Non-repudiation means the sender cannot deny having sent a given message. If a transaction has occurred between two parties, the non-repudiation service can prove that for any party, they really perform the transaction themselves and not by any other person. Integrity means the receiver can confirm that a message has not been altered during transmission. In other words, integrity control protects the information from tampering [3]. The focus of this paper is on confidentiality which include cryptography and steganography. Cryptography and Steganography are cousins in the spy craft family: the former scrambles a message so it cannot be understood while the latter hides the message so it cannot be seen. This paper reviewed various cryptography and steganography techniques and since neither of the two methods can alone make data secure efficiently, so a proposed hybrid model is presented which integrate cryptography and steganography for enhanced data security.

2. SECURITY REQUIREMENTS FOR DATA TRANSMISSION

(a) **Confidentiality**: Information should be readable only by the intended receiver. Data in transit should be protected against eavesdropping. Confidentiality ensures secured transmission of data over public channels. In computer science, secure transmission refers to the transfer of data over a secure channel. Many secure transmission methods require a type of encryption. There are two main techniques to achieve this: Cryptography and Steganography. Cryptography is the science of secret writing of information. It has two components: Encryption and Decryption. Cryptography algorithms are of two types: symmetric (private) key and asymmetric (public) key. Steganography is a technique for covert communication in which the intruder cannot suspect the existence of communication [4].

(b) **Authentication**: Authentication is the process of verifying the identity of your communication partner. It ensures the communication partner is who they are supposed to be and not an intruder. Authentication is quite different from authorization. Authentication ascertains whether you are communicating with an intended party while authorization determines whether you are permitted to do so. Authentication ensures that an individual is who they claim to be, but says nothing about their right (authorization) [3]. The most well-known authentication techniques are: (i) authentication based on shared secret key, (ii) establishing a shared secret key: Diffie-hellman key exchange, (iii) authentication using a key distribution center, (iv) authentication using Kerberos, (v) authentication using public key cryptography [4].

(c) **Non-repudiation:** Non-repudiation in network security is the ability to prevent a denial in an electronic message or transaction. Non-repudiation requires that neither the sender nor the receiver of a message will be able to deny the transmission. Digital signatures (combined with other measures) can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place. In some transactions, non-repudiation is put into practice in one of the following ways:

- By sending mail through a *certified* option, which requires the recipient to acknowledge receipt through their physical presence and signature.
- Through the use of a witness or *notary public*, whose job is to verify identity and affix their name to the contract or transaction.
- By requesting a *read receipt* when sending an email, which shows you that the document was opened and read by the recipient.

(d) **Integrity Control:** Data integrity, in the context of networking, refers to the overall completeness, accuracy and consistency of data. Integrity control ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages. This can be achieved by using error checking and correction protocols [3].

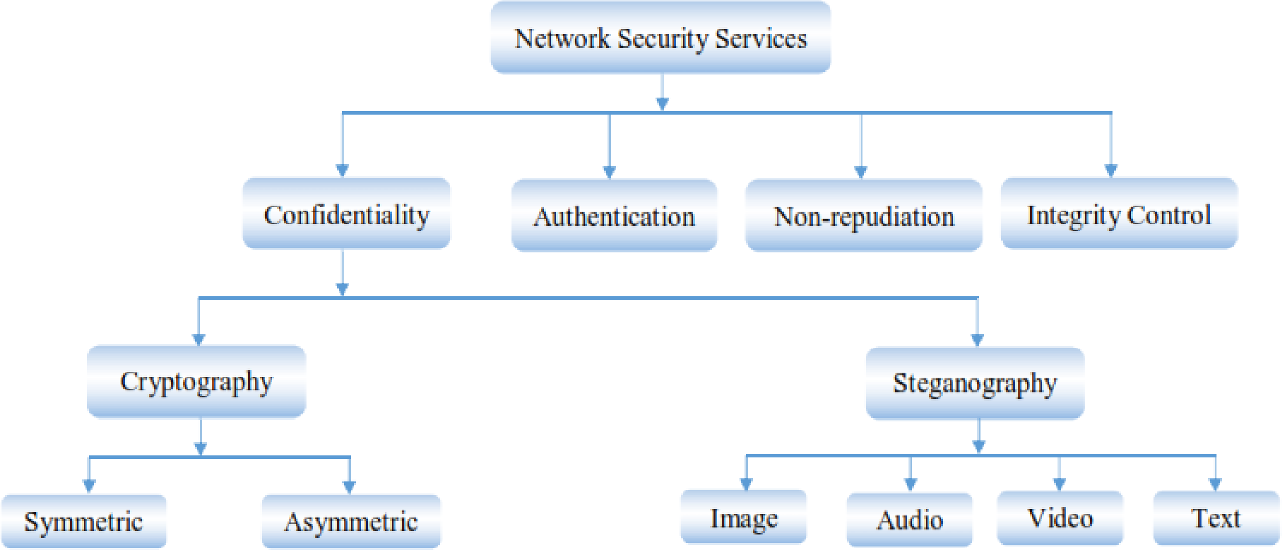

Figure 1: Classification of Network Security Techniques

3. CRYPTOGRAPHY

Cryptography is the art and science of transforming and transmitting confidential information securely against potential third-party adversaries [5]. In other words, cryptography is the art and science of achieving security by encoding messages to make them non-readable (unintelligible) [6]. It has its origin in Greek words "crypto" meaning hidden and "graphy" meaning writing. In cryptography the original message (plain text) is transformed into non-readable form (cipher text) by applying some mathematical operations. The cypher text is transmitted over the transmission medium and finally at receiver side, cipher text is converted back to the original message. Two basic terms used in cryptography are **encryption** and **decryption**.

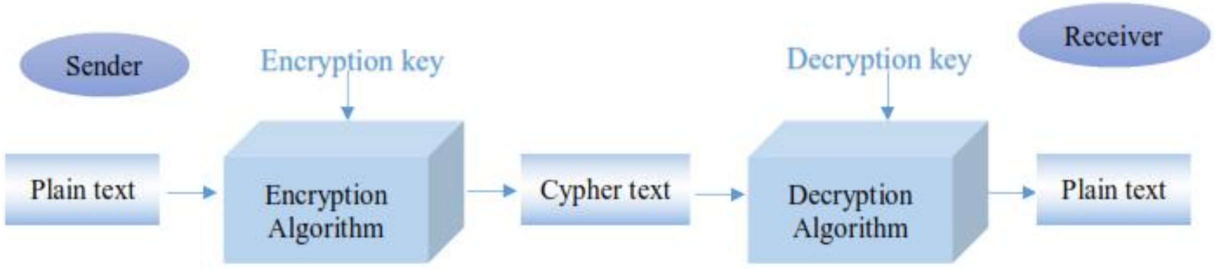

Figure 2: Cryptographic System

3.1 COMPONENTS OF CRYPTOGRAPHY

3.1.1 Plain Text: It is the confidential data to be transmitted over pubic transmission channels.

3.1.2 Cipher Text: It is an encoded (encrypted) resultant text after applying encryption algorithm with an encryption key to a plain text. It a transformed plain text which is not understandable to an intruder.

3.1.3 Encryption Algorithm: It is a mathematical process used for converting plain text into cypher text based on some encryption key. Different examples of such algorithms are DES (Data Encryption Standard), AES (Advanced Encryption Standard), Blowfish, RSA, Deffie-Hellman, DSA (Digital Signature Algorithm), ElGamal etc. It is used at sender's side.

3.1.4 Decryption Algorithm: It is exactly reverse mathematical process of encryption algorithm. It takes cipher text and produces the original plain text using decryption key. It is used at receiver's side.

3.1.5 Encryption Key: This key is a value that is applied within encryption algorithm to generate cypher text. It is very germane to cryptographic system. It may be known by both the sender and the receiver or only the sender. Safe guarding this key is of utmost important for making cryptographic system successful.

3.1.6 Decryption Key: This key is the value that is applied within the decryption algorithm to generate the plain text back from received cipher text. It may or may not be identical to encryption key depending on the type of encryption used.

3.1.7 Cryptanalysis: It is the process of defeating the work of cryptography. It is used to intrude and breach the cryptographic system with or without knowing the secret key of the process [6].

3.1.7 Cryptology: It is the study of cryptography and cryptanalysis together.

3.2 TYPES OF CRYPTOGRAPHY

Cryptographic systems can be divided into two basic types [6].

3.2.1 Symmetric Cryptography: It is also known as Secret Key Encryption. It is the type of encryption in which both sender and receiver use the same key (shared key) to encrypt and decrypt message. It could be implemented either using block cipher technique or stream cipher technique. Block cipher performs encryption block-by-block of plain text whereas stream cipher performs encoding character-by-character. Some examples of symmetric key encryption algorithms are DES, AES, Blowfish, IDEA.

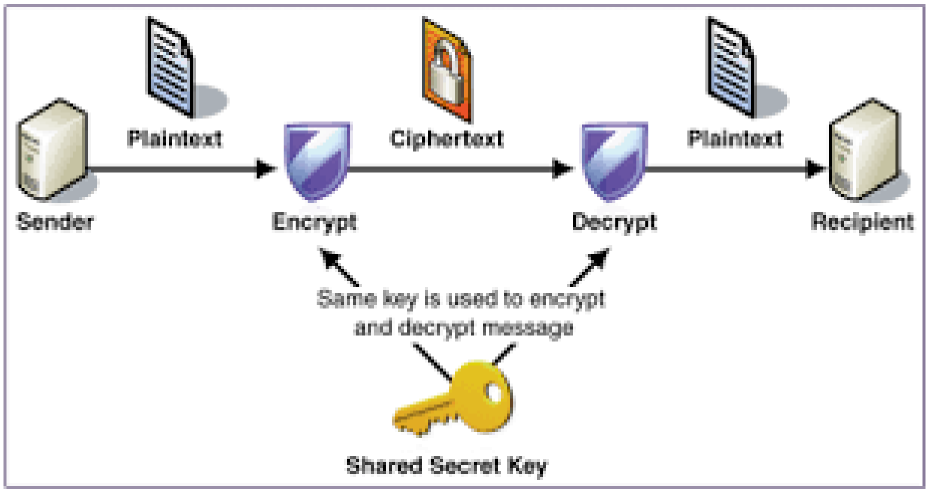

Figure 3: Symmetric Key Encryption

3.2.2 Asymmetric Cryptography: It is also known as Public Key Encryption, in which each user generates two keys. One is a Public Key used by anyone for encrypting messages to be sent to the user and a Private Key which the user needs to decrypt the message. The private is only known to the user while the Public Key is distributed to the general public. Figure 4 is the diagrammatical representation of Asymmetric cryptography. Examples of Public Key Encryption algorithms include Deffie-Hellman, RSA, DSA etc.

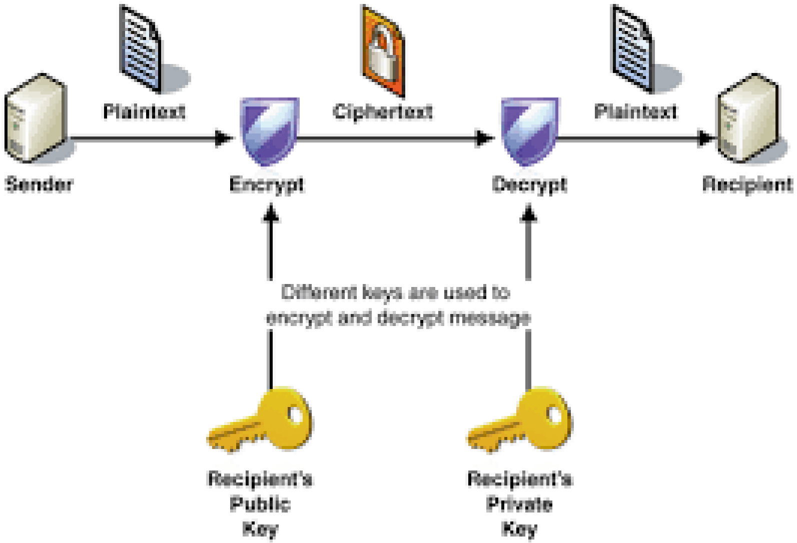

Figure 4: Asymmetric Key Encryption

4. STEGANOGRAPHY

Steganography is art and science of communicating in a way that hides the existence of the communication. Thus, it embeds hidden content in unremarkable cover media so not to arouse eavesdropper's suspicion [7]. In contrast to cryptography, which scramble the message and make it unreadable to an intruder, steganography on the other hand, exploit human awareness by hiding the existence of the message thereby an intruder will not be aware of the ongoing communication. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing". The idea and practice of hiding information has a long history. In Greece kings used to send information to their friends by writing the message on the head of a trusted soldier. During World War II steganography was used as a method of invisible communication. In modern steganography image, audio and video files are used as carriers [4].

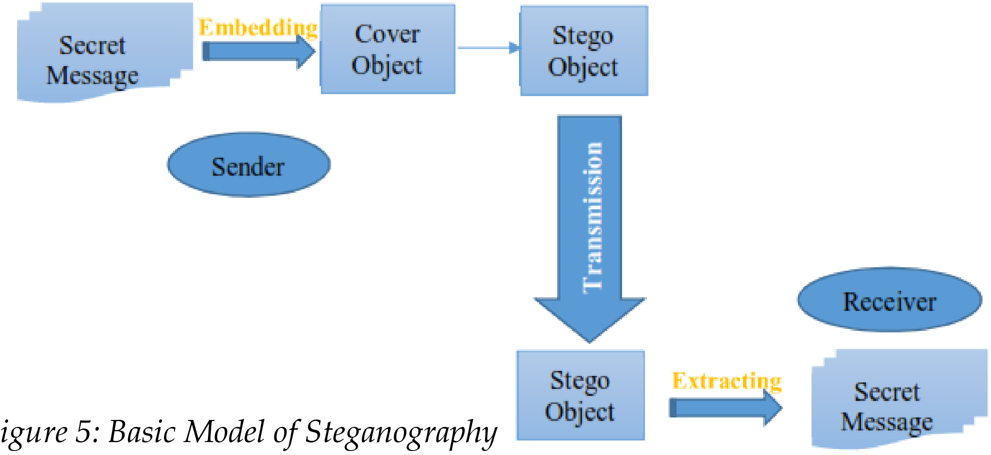

Figure 5: Basic Model of Steganography

4.1 COMPONENTS OF STEGANOGRAPHY

The carrier image: The carrier image is also called cover object that will carry the message/data which is used to be hidden.

The Message: A message can be anything like data, file or image etc.

The key: A key is sued to decode/decipher the hidden message

4.2 STEGANOGRAPHY TECHNIQUES

4.2.1 Image Steganography: In this method, images are used as cover object. Steganography is a two-step process: 1) create a stego image which is the combination of message and carrier. 2) extract the message image from the stego image [4]. Image steganography can be classified into four categories:

- Spatial domain
- Frequency domain
- Masking
- Filtering

4.2.2 Audio Steganography: When secret data is embedded into sound which act as cover media, the technique is known as audio steganography. This method embeds the secret message in WAV, AU and MP3 sound files [8]. Audio steganography employs different methods:

- Low Bit Encoding
- Phase Coding
- Spread Spectrum
- Echo hiding

4.2.3 Video Steganography: This technique is the combination of image and audio steganography. The great advantage of video is the large amount of data that can be hidden inside. There are different techniques of embedding secret data in video:

- Least Significant Bit
- Spread Spectrum
- Discrete Cosine Transform
- Non-uniform Rectangular Partition
- Masking and Filtering

4.2.4 Text Steganography: It uses text media to hide data. It hides the text behind other text file [9]. Since almost everyone can read, encoding text in neutral sentences is doubtfully effective. There are many techniques of embedding secret data in text:

- Format Based Method
- Random and Statistical Method
- Linguistics Method

5. CRYPTOGRAPHY VS STEGANOGRAPHY

The difference between steganography and cryptography is that in cryptography, one can tell that a message has been encrypted, but the message cannot be decoded without knowing the encryption key. In steganography, the message itself may not be difficult to decode, but most people would not detect the presence of the message [10].

6. THE PROPOSED MODEL

For better and efficient data security, either cryptography or steganography may not be enough, hence in the proposed model we combined steganography and cryptography to provide two levels of security. This type of hybrid technique is called crypto-stego technique, a model shown in figure 6. At the sender side the message is encrypted by using DES algorithm, the cipher text is embedded into a chosen image using LSB method and the stego file is generated which is sent to the receiver. The receiver extracts the cipher text, then decrypt it to get back the message. DES algorithm is used for the encryption because it is a symmetric key block cipher which takes 64-bit plaintext and 56-bit key as an input and produces 64-bit cipher text as output. A brute force attack on such key is impractical. The LSB method is a simple and flexible approach for embedding information in a cover image that results in very little changes in the stego image. These changes cannot be perceived by human eye.

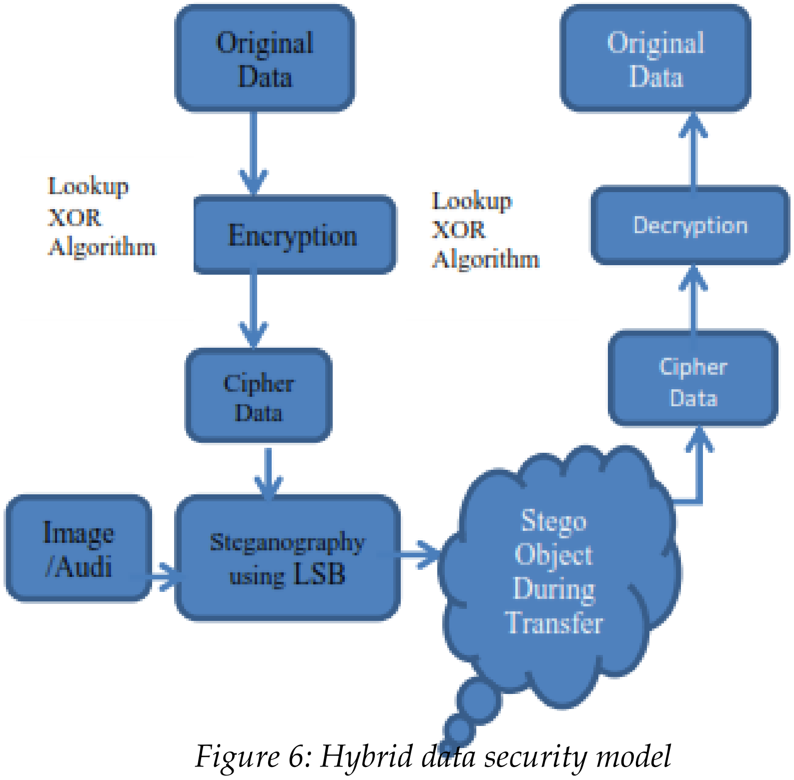

Figure 6: Hybrid data security model

7. CONCLUSION

Data security is an essential component of an organization in order to keep information safe from various competitors. It helps ensure the privacy of user's personal information from attackers. This paper reviewed various cryptography and steganography techniques. Steganography is the science that deals with how communication can be disguised while cryptography is the science of transforming the content of the communication and making it obscure. Both techniques on their own cannot guarantee absolute data security. Consequently, a hybrid data security model was proposed, which combine the two techniques thereby making data communication double secure. We can conclude that the proposed model is more effective for secret communication over the network channel.

REFERENCES

[1] Pallavi H. Dixit, Kamalesh B. Waskar, and Uttam L. Bombale (2015). Multilevel Network Security Combining Cryptography and Steganography on ARM Platform. *Journal of Embedded Systems, 3, 1, 11 – 15.* Doi: 10.12691/jes-3-1-2.

[2] Marwa E. Saleh, Abdelmgeid A. Aly, Egypt Fatma A. Omara (2016). Data Security Using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Applications (IJACSA). 7, 6.*

[3] Er. Babita and Er. Gurjeet Kaur (2017). A Review: Network Security Based on Cryptography & Steganography Techniques. *International Journal of Advanced Research in Computer Science. 8, 4.*

[4] Gandharba Swain and Saroj Kumar Lankar (2011). A Quick Review of Network Security and Steganography. *International Journal of Electronics and Computer Science Engineering"* ISBN:2277-1956.

[5] Arati Appaso Pujari and Sunita Sunil Shinde (2016). Data Security using Cryptography and Steganography. *IOSR Journal of Computer Engineering (IOSR-JCE). 18 (4), 130 - 139*

[6] Divya Shree and Seema Ahlawat (2017). A review on Cryptography, Attacks and Cyber Security. *International Journal of Advanced Research in Computer Science. 8,5.*

[7] Johnson, Neil F. and Sushil Jajodia (1998). Exploring steganography: seeing the unseen. *IEEE Computer, 32,2. 26-34*

[8] HilalAlmara'beh (2016). Steganography Techniques – Data Security Using Audio and Video, *International Journal of Advanced Research in Computer Science and Software Engineering. 6(2).*

[9] Rakhil, Suresh Gawande (2013). A Review on Steganography Methods. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*. 2(10)

[10]https://www.clear.rice.edu/elec301/Projects01/steganosaurus/background.html