THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Data Security Using Cryptography and Steganography

Ekuma, James Nkorabon
Principal Lecturer, Department of Computer Science,
Federal Polytechnic Idah, Idah, Kogi State, Nigeria
Asaju, Bukola Christine
Senior Lecturer, Department of Computer Science,
Federal Polytechnic Idah, Idah, Kogi State, Nigeria
Akilakpa, Babatunde Olaniyi
Assistant Chief Technologist, Department of Computer Science,
Federal Polytechnic Idah, Idah, Kogi State, Nigeria

Abstract:
Communication between and among individual/devices across networks, nations and around the world has become seamless as a result of the super gateway communication system; the Internet. Internet has made the world a global hamlet, thus has the ability to give every individual in the world open access to every part of the world. This open access of the Internet has made it one of the most vulnerable technologies of our time. Though policies and regulations on privacy of information ,intellectual property right, theft of information, etc have been promulgated by word communication bodies, and agencies concern in various countries, violators such as hackers, sniffers, and their other collaborators have continually been on the increase not only their number, but by the number of their attacks, ways/methods in which they attack. Different security methods have been developed to secure data from every form of attach, which ranged from transposition of text, through cryptography, to steganography. This paper discusses the design of a combination of cryptography and steganography with the aim of providing more security to data on transmission on the super-highway; the Internet.

Keywords: *Secret-key, public key, cipher text, plaintext, cryptography, steganography. encryption, decryption*

1. Introduction

Communication of data and the desire to maintain confidentiality, integrity and privacy of information to avoid copyright violation and its likes gave way to the need for data security and protection. The growing possibilities of modern communications need a special means of security especially on computer network. The network security has become more important as the number of data being exchanged via the Internet increases. Therefore, confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. In addition, rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. This is achieved through steganography or cryptography. The word 'Steganography' originated from Greek, meaning 'covered or hidden writing' (Shulmin and Krylova, 2017). Steganography is a security mechanism of hiding sensitive information among the bits of a cover file such as an image, text, an audio or a video file in such a way that only sender and receiver knows about the hidden message inside the cover file. Cryptography also comes from a Greek word meaning hidden or secret writing for secure Communication in the presence of an unauthorized person. Cryptography includes encryption and decryption process of a message. Cryptography allows data to be sent in disguise so that an intruder who taps the information make no meaning from it, (Kurose and Ross, 2013). Cryptography is the art of protecting sensitive information by encrypting it into an unreadable format called cipher text. The main aim in steganography is to hide the very existence of a message in a cover medium while the goal of cryptography is to make data unreadable by a third party.

The cryptography and steganography are two widely techniques used for confidentiality of data exchange. Cryptography is used to cipher information and steganography is used to hide the existence of data communication. Cryptography scrambles the information by using a key so that a third person cannot access the information without the key. Steganography hides the information by using a cover medium so that a third person cannot identify the communication. Cryptography algorithms are divided into symmetric (secret-key) and asymmetric (public-key) network security protocols. Symmetric algorithms are used to encrypt and decrypt original messages (plaintext) by using the same key. While Asymmetric algorithms uses public-key cryptosystem to exchange key and then use faster secret key algorithms to ensure confidentiality of stream data. In Public-key encryption algorithms, there is a pair of keys, one key is known to the public, and is used to encrypt information to be sent to a receiver who owns the corresponding private key. The private and public keys are both different and need for key exchange.

Steganography is the art and science of writing hidden messages in such a way that no one, except the sender and intended recipient, suspects the existence of the message, a form of security through hiding the message. That is, Steganography is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. Like cryptography different type of steganography techniques are available based on the hiding techniques, cover medium used etc.

1.1. Overview of Steganography

Secret information is encoded in amanner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information only, but also to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed. The basic model of steganography consists of carrier, message and password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are included as below:

- Least significant bit insertion (LSB)
- Masking and filtering
- Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. This technique embeds the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least significant bit does not result in human perceptibledifference because the amplitude of the change is small.

1.2. Overview of Cryptography

Basically, the purpose of cryptography is to provide secret communication. Cryptography hides the contents of a message from malicious people. In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something. In cryptography, the system is broken when the attacker can read the secret message.

If separately used, the aforementioned algorithms (steganography and cryptography) provide confidentiality to the data but have some loop holes. So as an alternative we can go for a combination of cryptography and steganography.
It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting *stego-image* can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the *stego-object*, he would still require the cryptographic decoding key to decipher the encrypted message.

There are different kinds of cryptographic and steganographic techniques available, ranged from Caesar's mono-alphabetic and poly-alphabetic symmetric key cryptography, Block cipher, public key encryption, cipher block chaining, RSA, each with it challenges (Kurose and Ross, 2013) so we can have different combinations of cryptography and steganography, this paper combines both algorithms based on their security, using LSB and AES algorithms. We are focused on image based steganography i.e. the cover medium is image.

2. Problem Statement

While there have been numerous techniques for securing data including the individual use of both cryptography and steganography, there have also been counter techniques for exposing such data which pose a challenge to their actual goal i.e., securing data. Although encrypted data appears to be difficult to decipher, it is relatively easy to detect. Encryption only obscures the messages, meaning, not its existence. Using cryptography alone will attract suspicion from the attacker and at such expose the secrecy of the file to threat

3. Motivation

This proposed work is motivated by the problem statement above i.e., to control unauthorized access to confidential and secret messages through creating complexity in the process of unraveling or hacking secret data by making such secret message unsuspicious.

4. Aim/Objectives

The aim of this paper is to design a method of achieving high data security through multi layers system

- Design system that can encrypt data, hide the data in an image such that it does not attract suspicions from unauthorized persons

5. Literature Review

Usha (2011), proposed an encrypting system, combining cryptography and steganography techniques with data hiding. Instead of using a single layer security system scholars have been proposing multi layer security systems that combines both cryptography and steganography techniques.

L. S. Ahmed et al., (2012), proposed amethod of encrypting a message by a substitution cipher then it will be embedded using LSB insertion. Saja and Aser, (2016), proposed a higher level security approach for data communication system based on AES cryptography and DWT steganography, Deepak (2016), also presented a dual image steganography technique: countermeasure and analysis which combines LSB embedding based image steganographic technique and AES algorithm to secure the image data from outside intruders and attackers. Also Manisha and Deepkiran, (2016), presented a Dual Steganography Technique Using Status LSB and DWT Algorithms one that combines two steganography algorithms.
Bharti and Soni (2012) proposed a novel scheme based on steganography and cryptography to embed data in color images. Umamaheswari(2010) proposed a system that compresses the secret message, encrypts it by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm.

A study by Pandey and Shrivastava (2012) proposed combined approach of Secure Medical Image, by using encryption and steganography; the image is embedded using lossless LSB data hiding method with patient information and then embedded image is encrypted using two share method. Song *et al*. (2011) demonstrated that a new secure communication protocol can be conducted by combining steganography and cryptography techniques based on the LSB matching method. Nandakumar *et al*. (2011) used examples of combining steganography and visual cryptography techniques as evidence. In the proposed method, secret data are embedded using a Matrix embedding technique using Hamming codes and shares are generated from this stego image using the Random Grids method.

Sarmah and Bajpai (2010) presented a new system for the combination of cryptography and Steganography using four keys which as at then was provedto be a highly secured method for data communication in near future.
Prema and Natarajan (2013) designed and implemented secured algorithm using genetic algorithm along with visual cryptography to ensure improved security and reliability. Bansod *et al*. (2012) suggested algorithm based on hybrid cryptographic techniques built on DES (Date Encryption Standard) and RSA (Rivest Shamir Adleman) algorithms; the combination of both techniques provides superior security control. The suggested algorithm is modified BPCS (Bit Plane Complexity Segmentation) steganography technique that can replace all the 'noise-like' regions in all the bit-planes of the cover image with secret data without deteriorating the image quality.

In this paper a combined technique of AES cryptography with LSB Steganography is proposed, reason is that of achieving a highly secured multi layer system with high PSNR value, low MSE value, good imperceptibility and robustness. Here the secret message is encrypted using AES algorithm which results to a cipher text. The cipher text is then embedded in a cover image using LSB embedding algorithm to give a stego image. Many works have been reviewed exposing us to the advantages of combining both cryptography and steganography together. The main advantage of this Crypto/Stegno System is that the method used for encryption, AES (Advanced Encryption Standard), is very secure and the LSB (Least Significant Bit) substitution Steganography techniques are hard to detect. The essence of cryptography is to make obscure the intended message whereas creating awareness to the fact that a message is intended to be communicated thereby causing attacks inevitable. But the introduction of steganography is to hide the existence of a message. That is, creating a camouflage of the intended message. The attacker is deceived and cannot know what to look for. Let's take for instance, a case of Jack and Betty.

Jack is a prisoner who is planning an escape and wishes to inform his wife of his plans and assistance he would require from her. If Jack should send an encrypted message, the prison security would suspect the content of his messages as encrypted messages are ones that are alarming in the sense that they tell the unauthorized persons that I contain a secret I don't want you know thereby causing curiosity and suspicions and Bobs plans may fail. But if Jack decides to send a beautiful picture of his wife Betty that have a secret encrypted message, this definitely would throw the prison securities of their guard as they would not suspect any hidden agenda behind such a beautiful picture but rather see it as a man who is trying to let his wife know he misses her.(Kurose and Ross, 2013)
The above illustration is the idea behind this proposed work, hiding the existence of a message behind a cover image.

6. Methodology

Cryptography and steganography have their own vulnerabilities so combining them creates a stronger secured systemrather than using them individually. Using cryptography can hide the information from the user but it cannot hide the existence of a communication which steganography does.In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. According to Vivek J., et al (2012), steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded.
However, it is a good practice to use Cryptography and Steganography together for adding multiple layers of security. To do this, the data is encrypted using a cryptographic algorithm producing a cipher text that is further embedded in an image or any other media with the help of steganographic algorithm. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.
This proposed technique uses AES cryptography combined with LSB steganography techniques in java programming language. A pictorial representation of the concept is given below.

The figure below depicts the combination of cryptography and steganography:

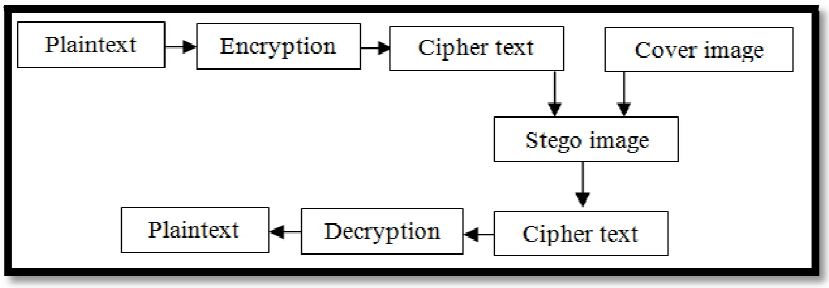

Figure 1: Flow Diagram of the Proposed Concept

7. Encryption

During encryption, the plain text is converted into a cipher text using AES encryption algorithm. AES is a symmetric block cipher that has been analyzed extensively and is used widely today. AES symmetric key encryption algorithm is used with key length of 128-bits for this purpose. High security, mathematical soundness, resistance to all known attacks, high encryption speed, suitability across wide range of hardware and software are the characteristics of AES algorithm. The basic structure of AES is shown in the Figure below.

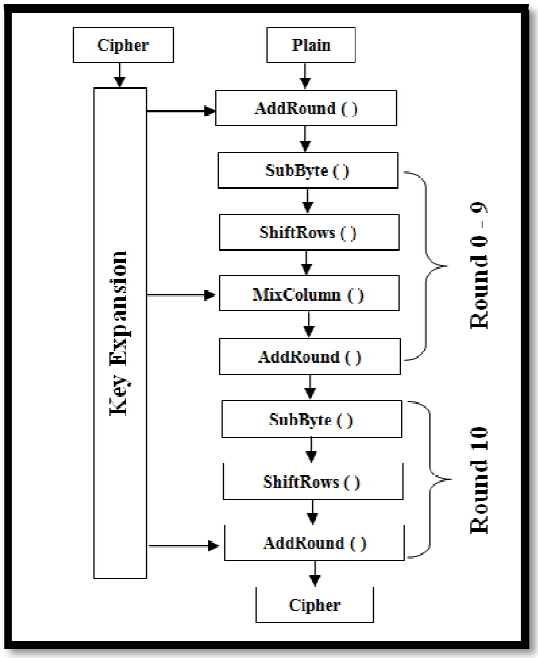

Figure 2: The Basic Structure of AES

8. Decryption

A cipher key (the same as the one used for encryption) is supplied to decrypt the encrypted message in order to get the original message. The processes of encryption and decryption are handled by AES (Advance Encryption Standard) algorithm.

9. Encoding

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. LSB coding is the simplest way to embed information in an image file by substituting the least significant bit of each sampling points with a binary message. The following steps were used during the encoding stage:

- Encrypt the message using AES encryption algorithm.
- Convert the image file into bit stream.
- Convert each character in the message into bit stream.
- Replace the LSB bit of the image file with the LSB bit of character in the message to hide.

10. Decoding

In this stage, the encoded file is decoded to get the hidden ciphered text. The cipher text is decoded first and then decrypted by the public key that is known only by the authorized receivers or users of the proposed system.

11. Conclusion and Recommendation

In this paper, a design of a combine security approach communication model is presented that combines cryptography and steganography techniques to provide two layer of security, so that a stegoanalyst or an intruder does not suspect the existence of secret message and when he finally does, finds it hard to reach the plaintext without knowing the secret key to decrypt the cipher text. Firstly the secret message is encrypted using the AES cryptographic technique, and then the encrypted data is hidden or embedded in cover image using LSB steganography. With this combination, the secret message can be transmitted over an open channel because not only does the cipher text look meaningless but its presence will be concealed by using steganography to hide its existence in an image.

12. Reference/Bibliography

i. Abikoye O. C, Awesome K.S, Oladipupo A. J (2012). Efficient Data Hiding Using Cryptography and Steganography, *In International Journal Applied Information Systems (IJAIS) 4*(11). ISSN: 2249-0868

ii. Ashwini B. and Komal B. (2016). Review and comparative study of dual steganography techniques for embedding text in cover images. *International Journal of Scientific & Engineering Research, 7*(2), 138-141.

iii. Bharti P. and Soni R. (2012). ANew Approach Data ofHiding in Images using Cryptography and Steganography.*International Journal of Computer Applications*, *58*(18): 1-5.

iv. Bansod S P,Mane V.M and L.R. Ragha, 2012. Modified BPCS Steganography Using Hybrid Cryptography for Improving Data Embedding Capacity. *In Communication, information & computing technology (ICCICT), international conference, IEEE*, pp: 1-6.

v. Deepak, K. P., Srinivasa, D. R. and Sriram, G. (2016). Dual image steganography technique: countermeasure and analysis. *IOSR Journal of Computer Engineering (IOSR-JCE), 18*(6), 92-100.

vi. Essam H., Mona A. and Aboul E. (2016). An image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System. *Proceedings of the Federated Conference on Computer Science and Information Systems,* Vol. 8 pp. 641-644.

vii. Kurose, J. F and Ross, K. W. (2013). Computer Network: A Top-Down Approach. Sixth Edition. Pearson Education Inc. New Jersey

viii. Manisha and Deepkiran M. (2016). Dual Steganography Techniques using Status LSB and DWT Algorithms. *International Journal of Innovative Research in Computer and Communication Engineering,4*(6).

ix. Nandakumar, A., P. Harmya, N. Jagadeesh and S.S. Anju, 2011. A Secure Data Hiding Scheme Based on Combined Steganography and Visual Cryptography Methods.*In Advances in Computing and Communication, Springer Berlin Heidelberg, pp: 498-505*.

x. Nivedhitha R. and Meyyappan T. (2012). Image security using steganography and cryptographic techniques. *International Journal of Engineering Trends and Technology, 3*(3).

xi. Pandey and Shrivastava, 2012. Secure Medical Image Transmission using Combined Approach of Datahiding, Encryption and Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 2(12): 54-57.

xii. Prema, G. and S. Natarajan, 2013. Steganography Using Genetic Algorithm along with Visual Cryptography for Wireless Network Application. *In Information Communication and Embedded Systems (ICICES), International Conference, IEEE*, pp: 727-730.

xiii. Roszaiti I. and YeahS. K. (2011), Steganography Algorithm to Hide Secret Message Inside an Image. *In Computer Technology and Application. Vol. 2 pp* 102-108.

xiv. Saja M. and Aser M. (2016). Higher level security approach for data communication system based on AES cryptography and DWT steganography. *Jordanian Journal of Computers and Information Technology, Vol. 2,* No. 3, pp.179-191.

xv. Sarmah, D.K. and N.P. Bajpai, 2010. Proposed System for Data Hiding using Cryptography and Steganography. *In International Journal of Computer Applications*, 8(9): 7-10.

xvi. Satwinder S. and Varinder K. (2015). Dual layer security of data using LSB image steganography method and AES encryption algorithm. *International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8,* No. 5, pp. 259-266.

xvii. Sherekar, S. S., Thekare, V. M. and Jain, S. (2009). Critical review of perceptual models for data authentication. *In Emerging Trends in Engineering and Technology (ICETET) 2nd international conference, Nagpur, IEEE, 323-329.*

xviii. Shulmin, A. and Krylova, E. (2017). Steganography in Contemporary Cyberattacks. https://securelist.com/steganography-in-contemporary-cyberattacks/79276/. Retrieved 20/03/2020

xix. Song, S.,Zhang J., Liao X., Du J. and Wen Q., 2011. A Novel Secure Communication Protocol Combining Steganography and Cryptography. *In Proceed Engineering* 15: 2767-2772.

xx. Umamaheswari, M., S. Sivasubramanian and S. Pandiarajan, 2010. Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS International Journal of Computer Science and Network Security, 10(8): 154-160.

xxi. Usha, S., Kumar G. A. S and Boopathybagan, (2011). A Secure Triple Level Encryption Method using Cryptography and Steganography. *International Conference in Computer Science and Network Technology (ICCSNT) IEEE, 2*(11), 1017-1020.

xxii. Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and Kshitiz Rastogi 2012. Public-Key Steganography Based on Modified LSB Method. *Journal of Global Research in Computer Science*, 3(4). ISSN: 2229-371X, pp. 26-29.