Study on Cryptography, Steganography and Combination of both for Data Security

Meher Afroj

Department of Computer Science and Engineering, Bangladesh University of Business and Technology

DOI: **https://doi.org/10.51584/IJRIAS.2023.8602**

Received: 17 May 2023; Accepted: 31 May 2023; Published: 30 June 2023

Abstract- Secure data communication is a key factor today while communicating through the unreliable network. Nowadays almost all applications are internet-based and it is important that communication made confidential and secure. But network of so many people is always unreliable. Cryptography and steganography are two important techniques which is used for secret and reliable communication over the network. Cryptography is the process of protecting information using different cryptographic algorithms so that only the intended person can read and process it. Steganography is the process of protecting information by hiding it inside another file such as image, audio, video and so on. But in recent years cryptanalysis study becomes so strong that only cryptography or only steganography alone may not enough for securing data. So the combination of cryptography and steganography produce stronger method than previous. In recent years many works has done or proposed about combining different types of cryptography and steganography schemes to make the transmission of data more secure through unreliable medium efficiently. This paper will help to understand some recent works related to combining cryptography and steganography within a short period of time and also will help to precede further study.

Keywords- Cryptography, Steganography, Ciphertext, Plaintext, Encryption, Decryption

I. Introduction

Internet users are increasing day by day. The rise of the Internet is one of the most important factors of information technology. As the internet is rising and the users are increasing, an enormous amount of data is being exchanged over the Internet. Security has been the major aspect for communication due to tremendous growth of networking technologies. The most important motive for the intruder is to obtain the value of the confidential data by attacking the system. Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks [1]. So we need a secured system which gives the assured security of data to us [2]. To maintain the privacy and security of confidential and sensitive information there is a need of approaches which enhances the level of information security. Information hiding is one of the many available approaches which increase the level of information security. The most powerful and widely used approaches of information hiding used to contravene the threats to information security are Cryptography and Steganography. We can make more secure system by using the combination of both approaches.

Cryptography was created as a technique for securing the secrecy of communication by making transmitted data apprehensible for the intended users and incomprehensible for others. Cryptography provides security by manipulating the original confidential information so that it becomes unintelligible for the intruders. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret [3]. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography[4].It is the art that conceals the existence of communication by hiding the confidential information in some other cover medium such as text, image, audio and video. Text steganography have a very small amount of redundant data, therefore they are very often used, audio and video steganography are very complex in use, image steganography is the most widely used hiding process of data that provides a secure and simple way to transfer the information over the internet [4].

Cryptography is used nowadays in almost all applications that use Internet as means of communication. Real time applications of cryptography include ATM machines; password protection of email passwords, social account (Facebook, twitter, etc.) passwords; E-commerce; Defense forces; intelligent agencies [5]. As cryptography cannot keep the existence of the message secret, steganography is used to overcome this shortcomings of cryptography and support the cryptography techniques to provide better and more efficient information security[6], [7]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Areas where steganography is used include bank and commercial organizations, digital watermarking, Ecommerce, military, and the areas where cryptography is used [1], [7]. Steganography differs from cryptography in the sense that where cryptography focuses on keeps in the contents of a message secret, steganography focuses on keeping the existence of a message secret[5].

II. Background

The need to conceal messages has been with us since we moved out of caves, started living in groups and decided to take this civilization idea seriously. 19th century supposed to be the golden era of modern civilization. Invention of computer have blessed us with different knowledge and ideas and also advanced the speed of civilization. Commencements of Internet have made the network among people stronger and larger. Today we can imagine the whole world inside a small smartphone or tab or pc or in any other device that can run internet. We can share any kind of knowledge or message by the blessings of networking. But people still need their privacy while using uncovered network. So researchers find that the concept of cryptography will work in this case. Different types of cryptographic schemes are introduced to hide the original message. The process of converting the original message into some unreadable format is known as Encryption and the process of converting the encrypted message into original message format is known as Decryption. A fixed length key along with different cryptographic algorithm is used to encrypt the message. In symmetric key encryption only one secret key is used to both encrypt and decrypt the original message (e.g. AES, DES, Blowfish, RC4, RC5, RC6 etc.) [5]. In asymmetric key encryption two keys are needed, one for encrypting the message which is known as private key and another for decrypting the encrypted message known as public key (e.g. RSA, DSA, ElGamal, Knapsack algorithms etc.) . In this way, the receiver knows who the message had to come from. This method makes up the backbone of the Digital Signature. Problems arise when communications between multiple organizations require the use of many public keys and knowing when to use which one. No matter which method is used, a combination of methods applied one after the other becomes give the best result.

But there is another term known as cryptanalysis where an intruder tries to find the confidential message without knowing the key (e.g. Ciphertext only attack, Known plaintext attack, Chosen plaintext attack, Man-in-the-Middle attack, Side channel attack etc.). For example some symmetric cryptographic algorithm such as DES is Bruteforce attackable, double DES is vulnerable to Meet-in-the-Middle attack, AES is vulnerable to Side channel attack and so on. Some asymmetric algorithm such as RSA is vulnerable to Robot attack, Knapsack algorithm is vulnerable to lattic attack etc. Many well-known cryptographic schemes are breakable against different cryptanalytic attack. Although some of those schemes are obsolete now but this cryptanalytic attacks are still thread to the existing network security.

There is another term known as Steganography. It is the practice of concealing a file inside another file (mostly an image). Most communication channels like telephone lines and radio broadcasts transmits signals which are always accompanied by some kind of noise. This noise can be replaced by a secret signal that has been transformed into a form that is indistinguishable from noise without knowledge of a secret key and this way, the secret signal can be transmitted undetectable. Digital steganography is a form of security through obscurity which is very easy to accomplish and harder to detect and decrypt and use BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, TGA, DLL, EXE etc. [8].

Another term known as Steganalysis is the art of detecting, decoding and altering messages hidden via Steganography. It becomes very easy when before and after Steganography copies are present. Steganalysis can make the hidden data work against the creator. Any malicious interceptor could alter as the carrier file without the knowledge of sender or the intended receiver. Hence inaccurate and wrong data could be passed under identity of the original sender.

To make these cryptanalytic and Steganalysis attacks more difficult only hiding the content of the message or only hiding the whole message is not enough. If we hide the whole encrypted message so that the intruder cannot find it then it may reduce the chance of the attacks. Hence the idea of combining cryptography and Steganography is introduced. Many Research paper has already been proposed different systems that have bind different cryptographic and steganographic algorithms to increase security. Proposal has been given on online payment system by using steganography and visual cryptography to secure the identity and the personal information of client and organization [9]. To increase data security over cloud researchers had proposed a method so that the individuals can upload to and download from the cloud in secure manner [5]. To make an stego image(that hold any secret information) more similar to the original image so that it become less susceptible to the intruder a method combining LSB steganography and chaos cryptography was introduced in [6]. A new technique called multi-level secret data hiding which integrates two different methods of encryption, namely: visual cryptography and steganography was presented to provide more security over internet [10]. Another image steganography method using DES (with 16 rounds and 64 bit block size) and K-means cluster with LSB steganography was introduced to hide data more securely [11]. The combination of cryptography and steganography is also used to propose method for assured data through the network, in the banking sector, to secure payment system etc. [2], [3], [7].

III. Discussion

Working procedure or methodology of five papers are simply discussed in this chapter which may useful for further study related to using Cryptography and Steganography for information security.

A. Critical Analysis of Cryptography and Steganography

This paper gives an overview about the concepts of cryptography and steganography and comparative analysis between various selected encryption algorithms of cryptography and steganography.

Cryptography: It is the science of producing scrambled message from the original one to secure it from intruder while passing through the untrustworthy communication medium.

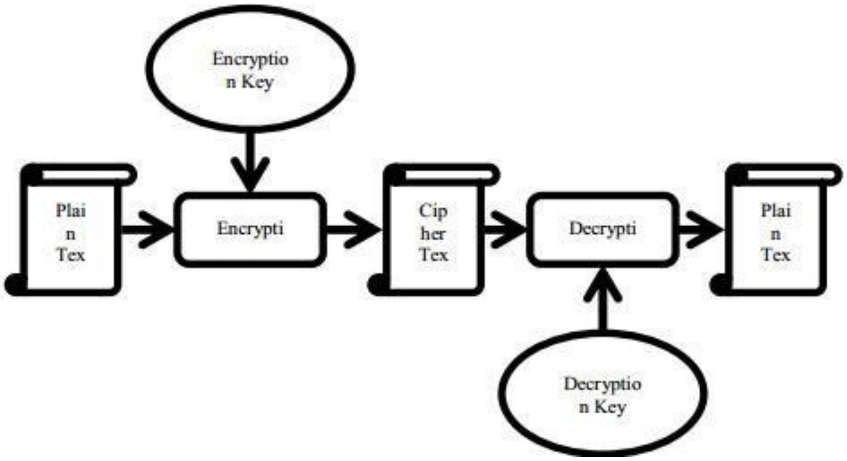

Figure 1: Process of Cryptography

Cryptographic encryption algorithms are classified into two categories depending on the number of keys operate on the plaintext. Symmetric key cipher and Asymmetric key cipher. Some symmetric algorithms are 3DES, AES, Blowfish, Twofish, RC5 etc.

By comparing these symmetric algorithms the paper indicate that AES ensure higher level of confidentiality with block size 128bits, key size 128/192/256bits, number of rounds 10/12/14 and also provide very fast encryption speed at low memory space.

Steganography: It is the science of hiding information into different files using different algorithms.

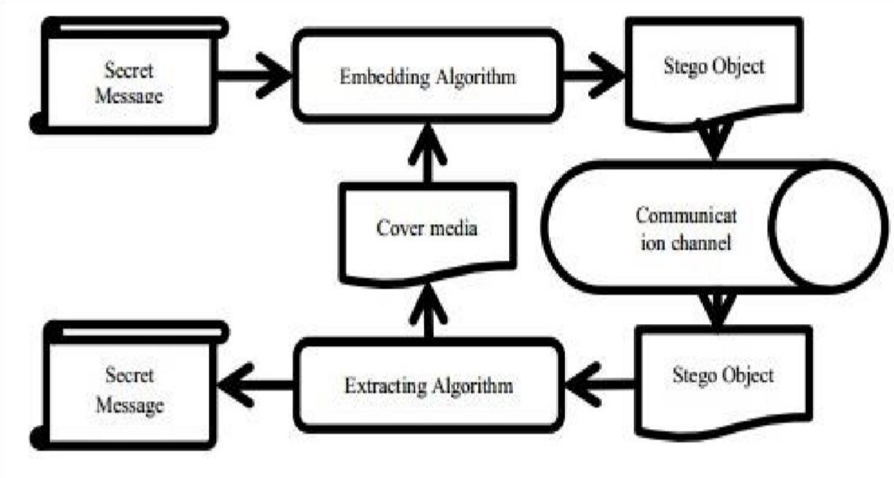

Figure 2: Process of Steganography

Steganography methods are classified into two types. Traditional methods (uses binary code) and Hex symbol method (uses hex code). Traditional methods use text, image, audio and video file as cover medium. Hex symbol method is more robust and provide higher level of security than the Traditional methods. As Hex symbol method uses hex code rather than binary code, it is capable of embed more secret information than Traditional methods.

Following flow chart will help to understand the Hex symbol algorithm.

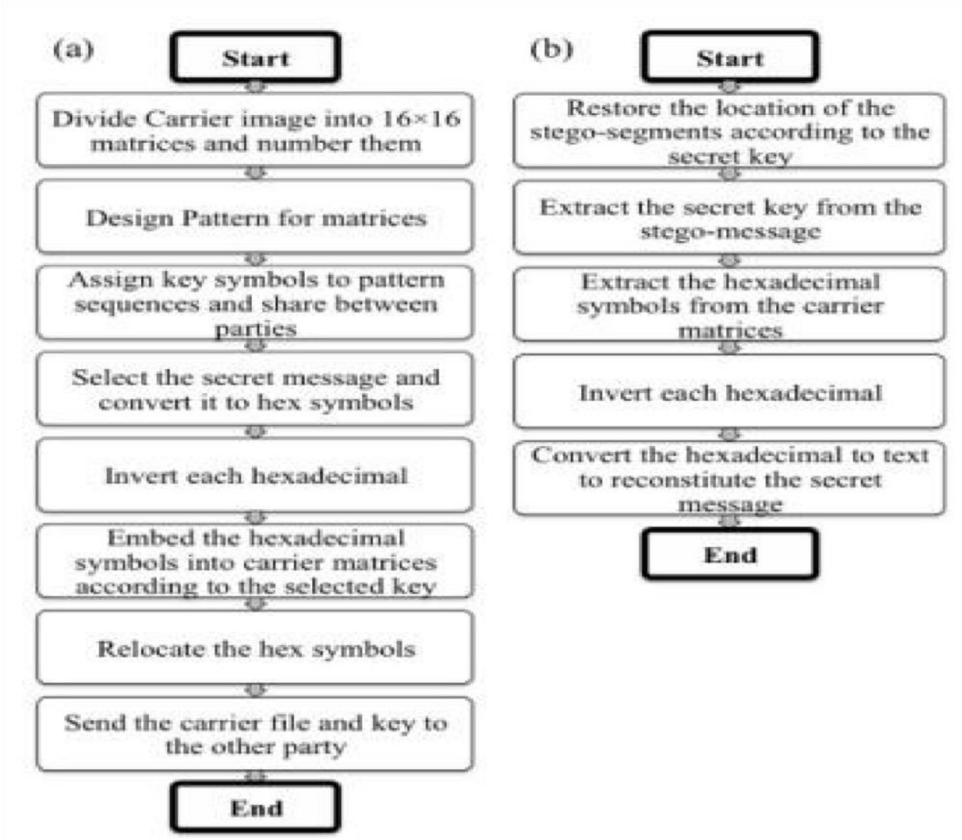
(a)
Start
Divide Carrier image into 16×16 matrices and number them
Design Pattern for matrices
Assign key symbols to pattern sequences and share between parties
Select the secret message and convert it to hex symbols
Invert each hexadecimal
Embed the hexadecimal symbols into carrier matrices according to the selected key
Relocate the hex symbols
Send the carrier file and key to the other party
End
(b)
Start
Restore the location of the stego-segments according to the secret key
Extract the secret key from the stego-message
Extract the hexadecimal symbols from the carrier matrices
Invert each hexadecimal
Convert the hexadecimal to text to reconstitute the secret message
End

Figure 3: (a) Embedding of the secret message in carrier file by the sender

(b) Extracting of the secret message from stego file by the receiver

B. A Survey on Recent Approaches Combining Cryptography and Steganography

This paper conducts a comparative study of steganography and cryptography and surveyed a number of methods combining cryptography and steganography in one system.

In the following the basic differences between the cryptography and steganography tabulated.

TABLE 1
Cryptography vs. Steganography

SL. No	**Criteria/Method**	**Steganography**	**Cryptography**
1.	Definition	Cover writing	Secret writing
2.	Input file	At least two	One
3.	Carrier	Any digital media	Usually text based
4.	Resultant Output	Stego file	Ciphertext
5.	Key	Optional	Necessary
6.	Security services offered	Authentication, Confidentiality, Identification	Confidentiality, Identification, Data Integrity and authentication Nonrepudiation
7.	Type of Attack	Steganalysis	Cryptanalysis

Different systems are developed before by combining both techniques to make a system more secure. There are two ways of combination named as Class A and Class B.

Class A method: In this method first encryption is performed on the secret message using any symmetric or asymmetric algorithm (AES, DES, Twofish, Blowfish, RSA) and then this encrypted data is hidden in another file producing stego object. The methods have higher security levels and less risk of expose since ciphertext is hidden by the steganography technique.

Class B method: In this method first secret message is embed into another cover medium, produce stego object and then the whole stego object is encrypted via different encryption algorithms. Class-B usually provides larger space for hiding information inside the cover object, because the encryption process is applied to all data inside the cover object. But it provides less security than Class A.

Both Class A structure and Class B structures are shows in Fig3 and Fig4 respectively.

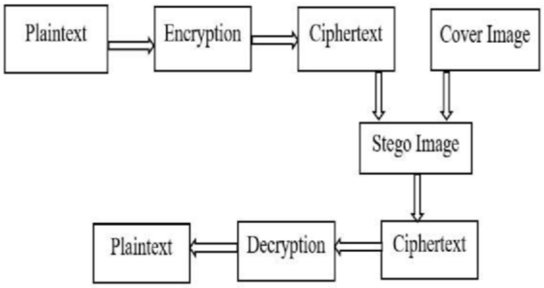

Figure 4: Class A

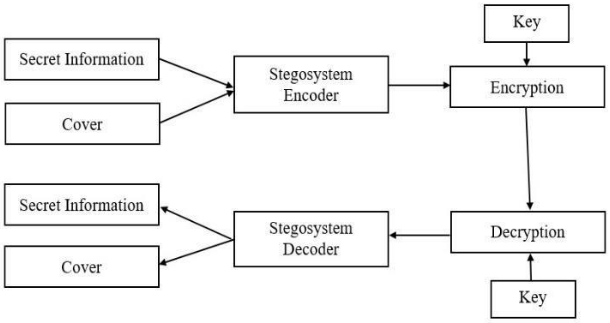

Figure 5: Class B

The Comparative Analysis of surveyed methods came to a conclusion that Class A methods are more popular in research than the one of Class B as Class B is vulnerable to suspect of the existence of a secret data inside it.

C. Assured Data Communication Using Cryptography and Steganography

This paper proposed Assured Data Communication by Using Cryptography and Steganography together in which a cipher text of text message is created using cryptography techniques and then this cipher text is hidden into Multimedia using steganography techniques. SDES is used as encryption and decryption algorithm and LSB method is used as steganographic algorithm.

In SDES Algorithm

- Input(plain text) is 10bits long and Output(cipher text) is also 10bits long.
- Requires 2 rounds and Round keys are generated using permutations and left shifts.
- Encryption: initial permutation, round function, switch halves.
- Decryption: same as encryption, except round keys used in opposite direction.

$$\text{Ciphertext} = \text{IP}^{-1}(f_{k2}\ (SW\ (f_{k1}\ (IP\ (plaintext)))))$$

$$K_1 = P8(Shift(P10(key)))$$

$$K_2 = P8(Shift(Shift(P10(key))))$$

$$Plaintext = IP^{-1}(f_{k1}(SW(f_{k2}(IP(ciphertext)))))$$

In above algorithm, IP stands for Initial permutation, fk1 and fk2 are Round functions with keys k1 and k2, SW means Shift operation, K1 and K2 are Secret keys.

Algorithm of Proposed System

Begin

1. Message.
2. Encrypting message.
3. Implementing LSB Method steganography

4. Embedding data.

5. Stego image.

6. Extraction of embedded message.

7. Encrypted message generation.

8. Decryption.

9. Original Message. End

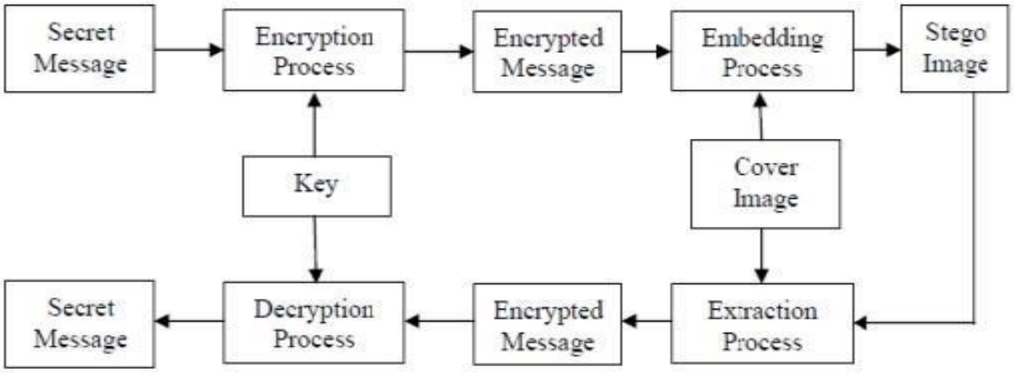

Figure 6: Block Diagram of Proposed System

This paper claims to achieve a higher similarity between cover and stego image that performs a better imperceptibility which is very necessary for assured data communication.

D. Enhanced Blend of Image Steganography and Cryptography

In this paper, a method is proposed by integrating Steganography and Cryptography to provide security to 24 bit color images. In this case, LSB based method (use least significant bit to hide secret information) is used to hide an image (color image) in another image, resulting stego image is then encrypted using chaotic theory (use several mathematical equations to produce randomness in the encryption).

The proposed system has following six modules (first three at the sender and last three at the receiver): 1. Splitting

2. Stegano Encoding
3. Chaotic Encryption
4. Chaotic Decryption
5. Stegano Decoding
6. Merging

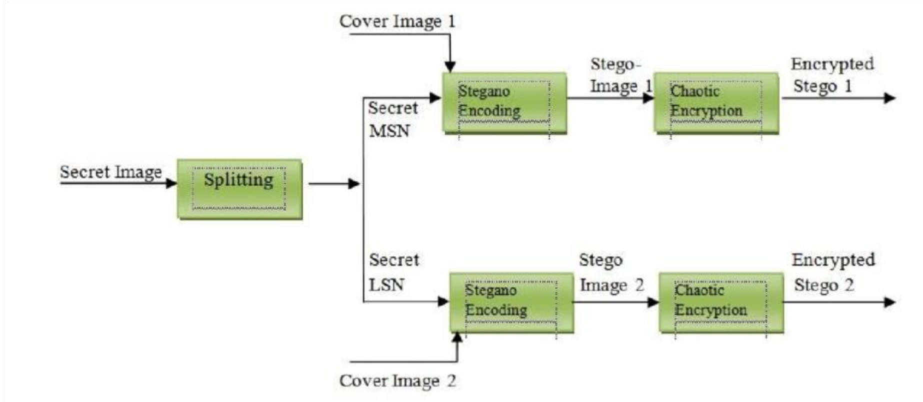

Figure 7: Block Diagram of Proposed Method at Sender

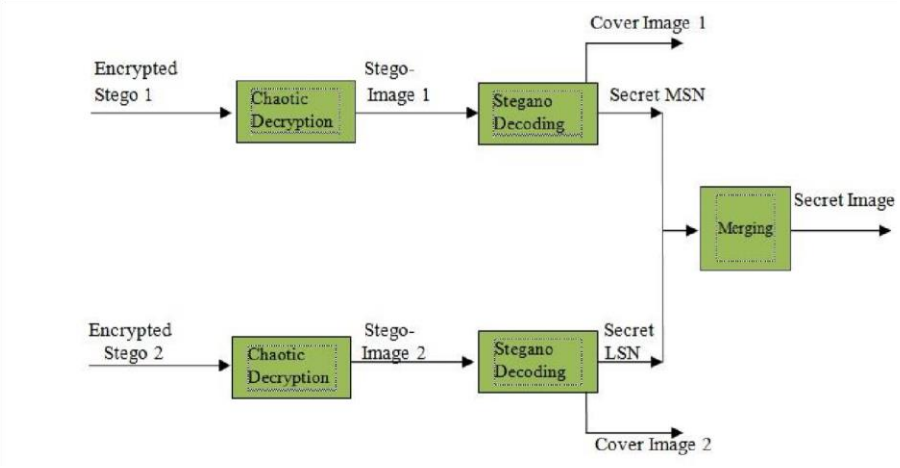

Figure 8: Block Diagram of Proposed Method at Receiver

Algorithm

1) Splitting the image: Split the secret image into two secret images by splitting each pixel of Red, Green and Blue planes of the image into two sub-pixels called MSN Secret and LSN Secret. Here MSN is Most Significant Nibble and LSN is Least Significant Nibble. Following steps are applied on both images (Secret MSN and Secret LSN).

2) Stegano Encoding: Secret image is embedded in randomized order in the cover image using 4-4-4 hiding Technique. For Example,

Cover Image Pixel: [1101**1100** 1100**0110** 1000**0111**]

Secret image Pixel: [1100 1001 1010]

Stego image Pixel: [1101**1100** 1100**1001** 1000**1010**]

3) Chaotic Encryption: Consists of two main steps named 2D Chaotic Confusion (Three encryption key known as confusion key performed on three red, green and blue pixels to produce confusion of the image, created by column wise shuffle and row wise shuffle which is applied to shuffle the pixel positions of the stego images) and 1-D chaotic Diffusion (which is applied to change the intensity values of pixels of Confused stego images).

This paper claims that the proposed algorithm is very sensitive to the change in the secret key, which makes it impossible to recover the original data through cryptanalysis attack.

E. Enhanced Cloud Data Security using Combined Encryption and Steganography

Cloud computing is Internet-based on demand service that has appeal in corporate data centers. Modern civilization is depending on cloud platform for security and storage but even it is vulnerable to various threats. This paper propose an enhance security to data using cryptography and steganography. The process use RSA algorithm for encryption and DWT method for steganography.

Key Generation in RSA

1. Two large distinct prime numbers p and q are chosen randomly. This makes factoring harder.
2. Calculate n = pq and then find $\varphi(n) = (p-1)(q-1)$
3. Choose the public key (say ’e’) such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$ as the public key exponent.
4. For the private key exponent, find d such that $d = e -1 \bmod \varphi(n)$.
5. Thus we have: The public key consisting of the modulus n and the public (or encryption) exponent e. And the private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

Encryption in RSA

1. A sends his/her public key (n, e) to B but keeps the private key d secret.

2. If B now wants to send a message M to A, B computes the cipher text C as C = Me mod n and B then transmits C to A.

Decryption in RSA

1. A recovers the integer M from C as M=Cd mod n.

DWT Steganography: The two dimensional Discrete Wavelet Transform (DWT) is an important function in many multimedia applications, such as JPEG2000 and MPEG-4 standards, digital watermarking, and content based multimedia information retrieval systems. The DWT shows its appropriateness for information hiding application.

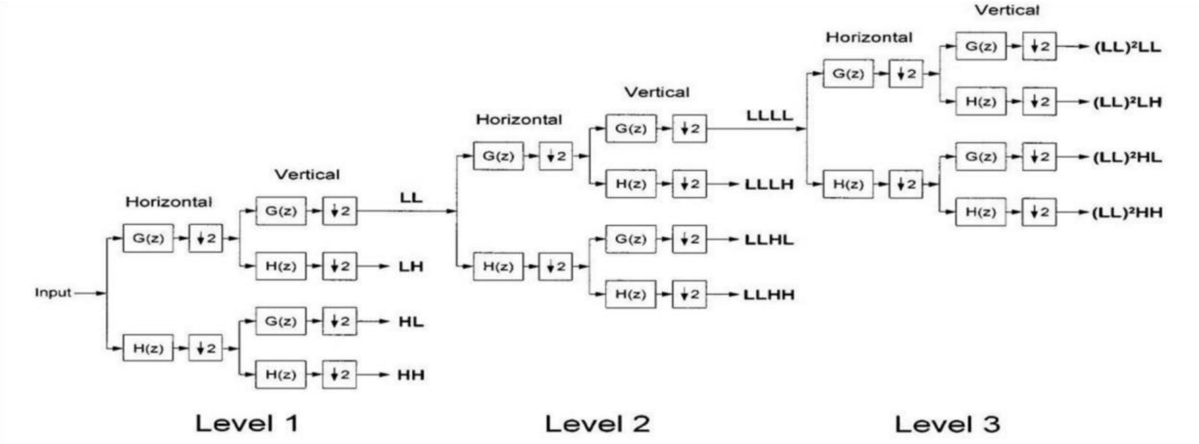

Figure 9: DWT Steganography Model

The secret message can be embedded in the higher level frequencies, which are not perceptible to the human eye, by reaching the wavelet coefficients in the HL and LH detail sub-bands. The 2D DWT is computationally intensive than other functions, for instance, in the JPEG2000 standard. Here two dimensional discrete wavelet transform is used to produce stego object for multilevel security.

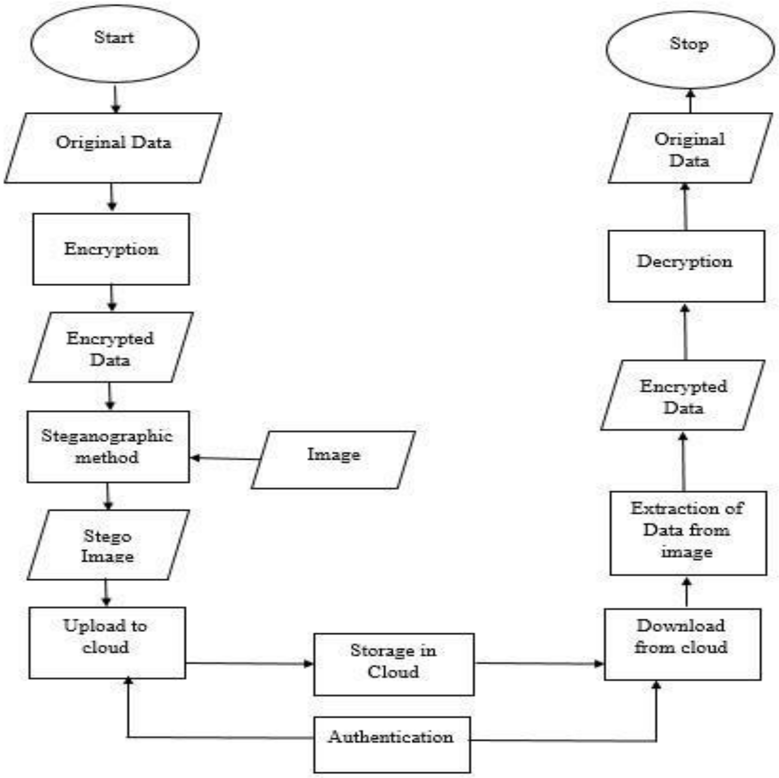

Figure 10: Flowchart of the System

To ensure data security secret message is encrypted via RSA encryption algorithm. Then DWT Steganography method is used to hide the encrypted message by producing stego object. Then this stego image is uploaded to the cloud. One can download the image file when necessary and decrypt the information to get the original file.

IV. Conclusion

This paper studied about five recent research papers about two major techniques of data security, Cryptography and Steganography and combination of both in different sectors. This paper will help a reader to have a look on the working methodology of these research at relatively short period. Although several methods are proposed earlier any of them cannot provide maximum guarantee of data security. So we still need to build a system that will provide us maximum secure platform. Further study will try to build a secure method merging both cryptographic algorithm (with hash function) and steganographic algorithm to ensure higher security.

References

1. A.G Palathingal, A. George, B. A. Thomas and A. R. Paul, "Enhanced Cloud Data Security using Combined Encryption and Steganography," International Research journal of Engineering and Technology (IRJET), Volume 5, Issue 13, 2018.
2. G. Sateesh, E. S. Lakshmi, M.Ramanimma, K. Jairam and A. Yeswanth, "Assured Data Communication using Cryptography and Steganography,"IJLTEMAS, Volume 5, Issue 3, 2016.
3. S. Almuhammadi and A. Al-Shaaby, "A Survey on Recent Approaches Combining Cryptography and Steganography," Computer Science & Information Technology (CS & IT), 2017.
4. B. Chauhan, S. Borikar, S. Aote and Prof. V. Katankar, "A Survey on Image Cryptography Using Lightweight Encryption
5. Algorithm," International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Volume 4, Issue 4, 2018.
6. A. Agath, C. Sidpara and D. Upadhyay, "Critical Analysis of Cryptography and Steganography," International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Volume 4, Issue 2, 2018.
7. R. S. Phadte and R. Dhanraj, "Enhanced Blend of Image Steganography and Cryptography," International Conference on Computing Methodologies and Communication (ICCMC), 2017.
8. S. Akolkor, Y. Kokulware and A. Neharkar, "Secure Payment System using Steganography and Visual Cryptography," International Journal of Computing and Technology (IJCAT), Volume 3, Issue 1, 2016.
9. S. Kaur, S. Bansal and R. K. Bansal, "Steganography and Classification of Image Steganography Techniques," International Conference on Computing for Sustainable Global Development (INDIACom),2014.
10. S. Roy and P. Venkateswaran, "OnlinePayment System using Steganography andVisual Cryptography,"Proceeding of IEEEStudents'
11. Conference on Electrical, Electronicsand Computer Science, Jadavpur University,Kolkata-700032, India, 2014
12. B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, \Image steganography method using k-meansclustering and encryption techniques,"
13. Advances in Computing, Communications and Informatics(ICACCI), 2016 International Conference on. IEEE, 2016, pp. 1206{1211
14. B. Karthikeyan, A. C. Kosaraju, and S. Gupta, \Enhanced security in steganography using encryptionand quick response code," Wireless Communications, Signal Processing and Networking(WiSPNET), International Conference on. IEEE, 2016, pp. 2308{2312.
15. A. Kumar, V. Nagare, S. Dhakane and Prof. S. Y. Kanawade, "Secured Wireless Communication Through Zigbee using
16. Cryptography and steganography," International Journal for Innovation Research in Science and Technology (IJIRST), Volume 2, Issue 11, 2016.
17. J. V. Karthik and B. V. Reddy, \Authentication of secret information in image stenography,"International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58,2014