A Survey on Crystanography: A Secured Multilayered Data Hiding Technique

Bhushan S. Bafna[1], Prof. P. N. Kalavadekar [2]

[1]*PG Student, Computer Engineering, SRES' COE Kopargaon, Maharashtra, India*
[2] *Assistant Professor, PG Coordinator, Computer Engineering, SRES' COE Kopargaon, Maharashtra, India.*

Mail: {erbhush007, kprak3004}@gmail.com

ABSTRACT

Now a days there is a challenges faced by Data or Information Security Field. We have to make this data free from harm during transmission. The primary aim is to built an application which enables sensitive information by covering securely in statistically undetectable communication channel. The two important concepts of securely transmitting information or data over a medium like internet are Steganography and Cryptography. Steganography is the art of secure communication which aims to hide the secret or sensitive information into a cover medium while observing the least possible statistical detectability. Cryptography is a scheme which decodes secret messages into several encrypted forms and distributes them. Both of them are used to ensure security. But none of them can simply fulfill the basic requirements of security i.e. the features such as robustness, undetectability and capacity etc.

A new technique based on the merging of both Cryptography and Steganography named as "Crystanography" is necessary which overcomes each other's limitations and make difficult for the intruders to attack or steal sensitive information is being proposed. To extend this new method of Crystanography a new technology is added to it which is named as "Multilayer Steganography". This new technique makes use of two cover files to strongly hiding of the Crypto-Stego file for providing very strong security in transmission of important data. The trouble of the size of file during transmission is also resolved by "Data Compression". Application of this widens the horizon of data and file embedding and privacy of data. Thus the scope is better than the existing Cryptography and Steganography systems which only the operations of data hiding and message embedding in the file.

Keywords: - *DES Cryptography, LSB Steganography, Crystanography, Multimedia file steganography like PDF Steganography, XML, WAV, HTML, GIF, FLV, etc. Steganography, Multilayer Steganography, Data Compression, Deffie-Helman Key Exchange Algorithm,*

---

1. INTRODUCTION

The speedy evolution of data transfer through internet has made it simpler to send the data exact and quicker to the destination. To transfer the data to destination there are many transmission media like e-mails, social sites etc. At the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the sensitive data securely to the destination excluding any alteration, there are many methodologies like Cryptography and Steganography. One of the reasons why the attackers become successful in intrusion is that they have an opportunity to read and comprehend most of the information from the system. Intruders may reveal the information to others, misuse or modify the information, misrepresent them to an individual/ organization or use them to plan even some more severe attacks. One of the solutions to this problem is through the use of steganography and cryptography. But among them some methods are implemented to break these approach security. So there is need to
make the communication more secure among the existing one.

1.1 Cryptography

Cryptography encodes information in such way that nobody can read it, except the person who holds the key. Cryptography comes from Greek word where "Crypto" means "Secret" and "Graphy" means "Writing"[5]. As shown in Figure 1.1 the cryptography provides the security to the data file.The Sender sends the data in plain text which is readable manner then using one of encryption algorithm the plain text converts into cipher text which is in unreadable form.

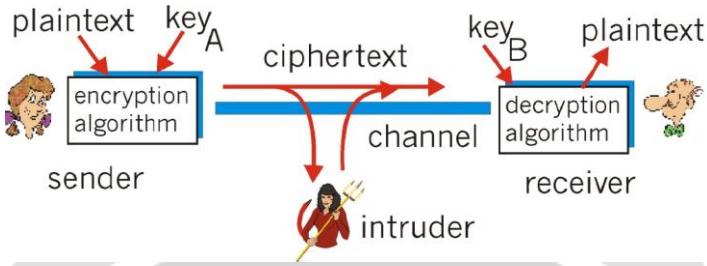

Figure 1.1: Working of Cryptography

So intruders cant see the actual data.When the plain text reached to the receiver, at receiver side the decryption algorithm used to converting cipher text back to plain text and actual data is observed at receiver side. This whole process of cryptography is performed be the "key" which decided by both for the purpose of encryption and decryption.

1.2 Existing Steganography

Steganography is not truly a method of encrypting message but hiding them within something else to enable them to pass unobserved. The word steganography comes from Greek word where "Steganos" means "Covered" and "Graphy" means "Writing"[5]. The various forms of data in steganography can be audio, video, text, images etc. The basic model of Steganography consists of three components:

- The Carrier image: The carrier image is also called the cover object that will carry the message that is to be hidden.
- The Message: A message can be anything like data, file or image etc.
- The Key: A key is used to decode/decipher/discover the hidden message.

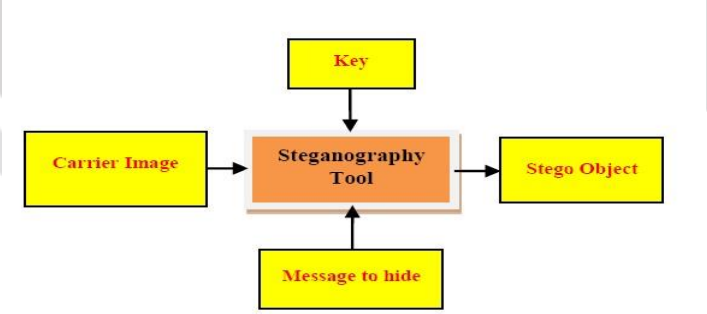

Figure 1.2: Working of Steganography

As shown in Figure 1.2, The Steganography just put a one carrier image or cover file among the encrypted data so the real file is hide among the medium which hides real file form attacker.

1.3 Crystanography

Cryptography + Steganography
Cover file + Message to be hidden (cipher meassage) ------> CryptoStego file .... (Secure)
Merging of Cryptography and new advance Steganography wich can be named as "Crystanography".

1.4 Advance Steganography

Now,

Master cover file + CryptoStego file -------> Multilayer or Double –layer CryptoStego file .... (More Secure)

The Master cover file is again applied on cover file under which already encrypted data is embedded.So in this way Advance Steganography is increases more privacy and secure data transmission.

1.5 Multilayer Crystanography Compression

Multilayer Crystanography Compression is the art of reducing the number of bits needed to store or transmit data. Compression can be either lossless(text or programs) or lossy(image,audio,video)[13].

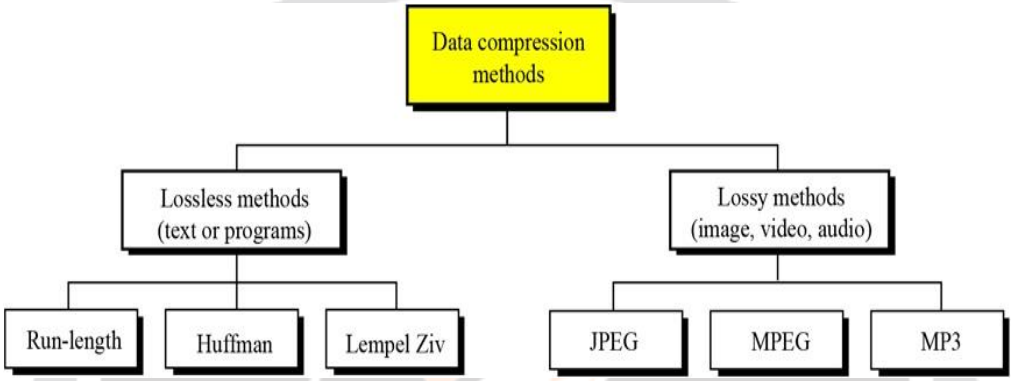

Figure 1.3: Data Compression Methods

There are different Data Compression Methods as shown in above Figure 1.3.

2. LITERATURE SURVEY

Steganography is the art of secret communication. For this purpose, it use recent results on the statistics of natural images and investigate the effect of some popular steganography techniques. it found that these fundamental statistics of natural images are, in fact, generally altered by the hidden non natural information [1].

Constructing and implementing new algorithm based on hiding a large amount of data (image, audio, text) file into color BMP image. Here used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially by using new concept defined by main cases with their sub cases for each byte in one pixel [2].

Storing vast amounts of multidimensional telemetry data presents a challenge. Telemetry data being relayed from sensors to the ground station comes in the form of text, images, audio, and various other formats. Compressing this data would optimize bandwidth usage during transmission and reduce storage resources needed at the ground level [3].

The features such as robustness, undetectability and capacity etc. So a new method based on the combination of both cryptography and steganography known as Crypto-Steganography which overcome each others weaknesses and make difficult for the intruders to attack or steal sensitive information is being proposed [4].

In past few decades the data transmission is not secure because of attacks by intruder or attacker. In public communication system Data transmission is not secure because of interception and improper manipulation by eavesdropper. So Steganography is the attractive solution for this problem, which is a method of writing hidden, messages apart from the sender and receiver in such a way that no one, suspects the existence of the message, a form of security through obscurity [5].

The combination of a randomly generated Symmetric Key along with LSB technique of Audio Steganography sends a secret message unrecognizable through an insecure medium. The Stego File generated is almost lossless giving a 100 percent recovery of the original message. This paper also presents a detailed experimental analysis of the algorithm with a brief comparison with other existing algorithms and a future scope. The experimental verification and security issues are promising [6].

Image steganography is the process when the cover medium used is an image. The proposed algorithm is a modulation of the standard Least Significant Bit Algorithm (LSB). In the proposed algorithm the information to be hidden is considered to be text. This text is taken and first encrypted using the Data Encryption Standard Algorithm (DES) with the help of a key. This key to encrypt the data is then encrypted using the RSA algorithm [7].

In this paper, They conduct a comparative study of steganography and cryptography. They survey a number of methods combining cryptography and steganography techniques in one system. Moreover, we present a classification of these methods, and compare them in terms of the algorithm used for encryption, the steganography technique and the file type used for covering the information [10].

- **Existing System:**

Only Image, Audio, Video Steganography.

- **Proposed System:**
  In Advanced Crystanography…

Not only Image, Audio, Video Steganography but also other multimedia files can be used for Steganography like PDF Steganography, XML, WAV, HTML, GIF, FLV, etc. Steganography.

- **Existing System:**

We provide the security to message by embedding message.
Message-→ Cryptography-→ Encrypted Message-→ Multilayer Steganography.

- **Proposed System:**
  In Advanced Crystanography…

We provide the security not only to message but also to whole file by embedding it.
Message/File-→Cryptography-→Encrypted Message/File-→ Multilayer Steganography.

3. SYSTEM OVERVIEW

There are two sides of communication as sender side and receiver side. Encoder encodes the information at sender side and decoder decodes the information at receiver side.

Following Figure 3.1 and 3.2 shows the working of Crystanography at sender side and receiver side respectively.

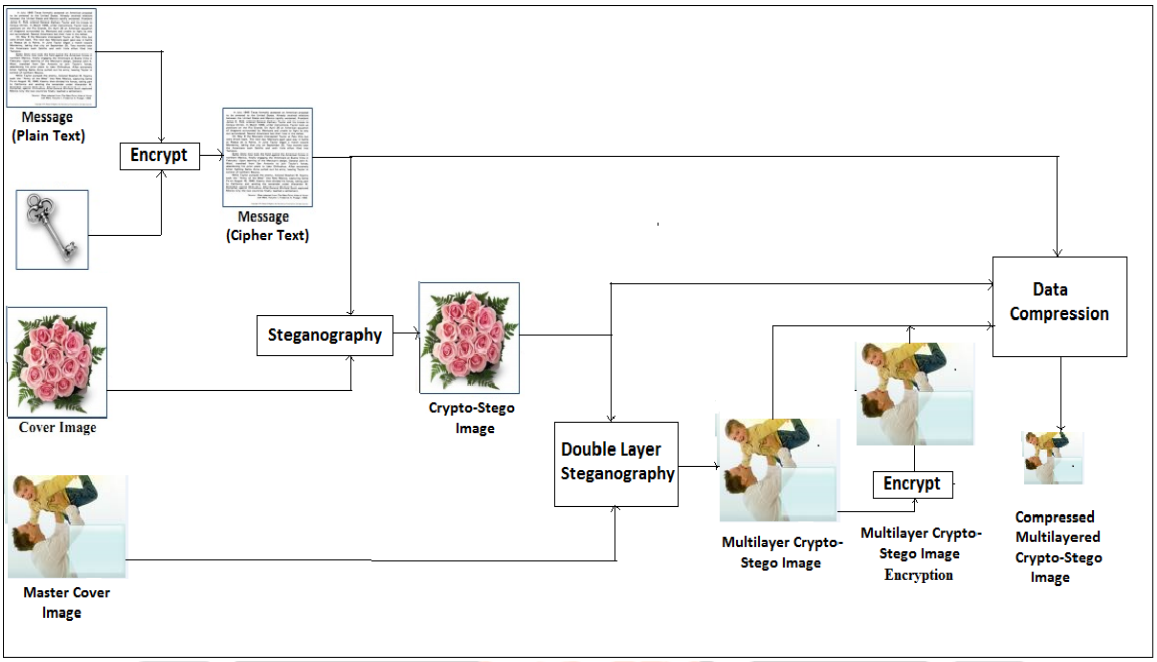

Figure 3.1. The Working of a Multilayer Crystanography Data Hiding Encoder

Crypto-Stego-encoder as in Figure 3.1 collects user information such as the message file, cover file and the secret key to be used for the message encryption and perform the necessary action depending on the user requirement. The encoder encrypt the message file content using the key provided, then may compress the file before encoding the message under the original image using the key supplied to form stego-image and then send it via the communication medium to the destination.

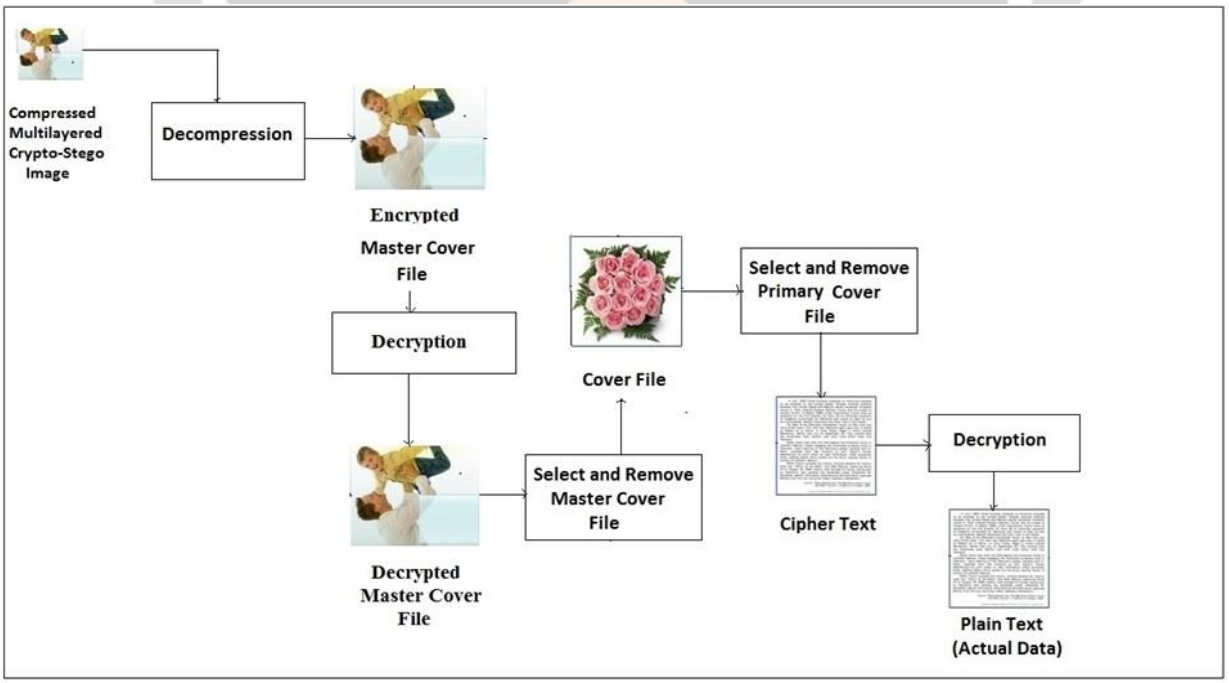

Figure 3.2 The Working of a Multilayer Crystanography Data Hiding Decoder

The Crypto-Stego-decoder as in Figure 3.2 on the other hand, decodes the stego-image file using the same key as specified by the sender to get the message file, decompress the message file if need be and then decrypt it with the suitable key to get the message content.

Modules

Sender Side Modules:

1. User Login Module

- It will accept the user id and password for login into the system.

2. Encryption of data file

- It converts the plain text data into cipher text data.

Cryptography Basis:

The algorithms under the Cryptography are

1) Secret Key Cryptography(SKC):

Uses a single key for both encyption and decyption.

Symmetric algorithm like DES,AES,etc.

2)Public key Cryptography(PKC):

It Uses one key for encryption and another for decryption.

The Asymmetric algorithm like Diffie-Helman,etc.

3) Hash Functions:

Uses a mathematical transformation to irreversibly encrypt information.

Hashing algorithm

Selected:

- DES (Data Encryption Standard) algorithm.

The one of the reason behind selection of this as it has invariant key of 56 bit and invariant rounds of 6 where extended algorithm like AES has invariant key size and number of rounds and it is necessary that system is of invariant nature to support the multi-layer Cryptography.

3. Double Layer Steganography

- It hides the encrypted data along with two cover files.

Steganography Basis:

The algorithms under the Steganography are

Algorithm like

a) LSB (Least Significant Bit)

It is a old but efficiently simple and useful working on Least bit.

b) ELSB (Enhanced Least Significant Bit)

It is extended version of LSB which overcomes the simplicity of LSB by enhancing it.

Selected:

- LSB (Least Significant) algorithm.

The reason behind the selection of this among existed are the simplicity which is essential for the purpose of multi-layer Steganography.

– The simplest and most common type of steganography is LSB (least significant bit). The ones bit of a byte is used to encode the hidden information.

– Suppose we want to encode the letter A (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.

4. Multilayer Crystanography

- It Combines/Merge the all above three files.

5. Data Compression

- It reduces the size of the file.

Compression Basis:

-Data Compression algorithm.

The data should be lossless so designed the compression based on it.

6. Secret Key Sharing

-Sharing secret private key between sender and receiver securely.

Key Sharing Basis:

Deffie-Hellman Key Exchange Algorithm.

Receiver Side Modules:

1. Data Decompression

- It will Resize the file.

2. Extraction of Master and primary cover file

- Selection and removal of master and primary cover file.

3. Decryption of Data File

- It converts the cipher text data back into plain text data.

4. CONCLUSION

A new high capacity and highly secure data hiding has been presented. The master cover file is most essential for providing more data security as multi-layer Steganography including Cryptography provide a wide range of data

security. The experimental results carried out show that the system produces a good quality stego images for a fairly high amount of payload. The double layer security coupled with high capacity and good perceptual transparency make the proposed system a very good candidate system for convert communications.

ACKNOWLEDGEMENT

"**Crystanography: A Secured Multilayered Data Hiding Technique**" has been a wonderful subject to research upon, which leads ones mind to explore new heights in the field of Computer Engineering. I dedicate all my dissertation works to my esteemed guide and PG Coordinator, **Prof. P. N. Kalavadekar**, whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to **Dr. D. B. Kshirsagar** (H.O.D. Computer Engineering Department) who has provided facilities to explore the subject with more enthusiasm.

REFERENCES

[1] Alvaro Martn, Guillermo Sapiro, and Gadiel Seroussi, Fellow, IEEE., "Is Image Steganography Natural?",In IEEE Transaction On Image Processing, VOL. 14, NO. 12, DECEMBER 2005, pp. 2040 - 2050.

[2] Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm", Journal of Computer Science 3 (4): 223-232, 2007 ISSN 1549-3636, pp.223 - 232.

[3] Intell. Syst. Div., NASA AmesMaluf, D.A. Res. Center, Moffett Field, CA ; Tran, P.B. ; Tran, D., "Effective Data Representation and Compression in Ground Data Systems", In Aerospace Conference, 2008 IEEE ,pp. 1 - 7.

[4] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "A Crypto-Steganography: A Survey", In IJACSA, Vol.5, No.7, 2014, pp. 149 - 155.

[5] Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar, Shahrukh Qureshi, "A Technique for Data Hiding using Audio and Video Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016 ISSN: 2277 128X pp. 568-571.

[6] Smita Paira and Sourabh Chandra, "Audio Cryptanalysis - An Application of Symmetric Key Cryptography and Audio Steganography ", Ictact Journal on Communication Technology, September 2016, Vol. 07, Issue 03 pp. 1345-1350.

[7] Shreyank N Gowda, "Dual Layered Secure Algorithm for Image Steganography" 978-1-5090-2399-8/16/$31.00 c_2016 IEEE.

[8] B.Karthikeyan, A. Deepak, K.S. Subalakshmi, Anishin Raj M M, V.Vaithiyanathan, "A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm", 978-1-5090-5434-3©2017 IEEE.

[9] Sourabh Chandra, Bidisha Mandal, Sk. safikul Alam, Siddhartha Bhattacharyya, "Content based double encryption algorithm using symmetric key Cryptography", ScienceDirect Procedia Computer Science 57 (2015) 1228 – 1234.

[10] Sultan Almuhammadi and Ahmed Al-Shaaby, "A Survey On Recent Approches Combining Cryptography and Steganography", in IEEE David C. Wyld et al. (Eds) : ITCS, SIP, CST, ARIA, NLP – 2017 pp. 63– 74, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.70306