An Extensive Survey on Image Steganography with Encryption Techniques

Sawan Soni[1], Prof. Arpit Solanki[2]

[1]M. Tech. Scholar, [2]Research Guide

Department of Computer Science and Engineering, RKDF Indore

Abstract- Steganography is a technique of hiding information within the information or hiding one form of information into another form of information. Steganography word is the combination of two Greek word "stegos" and "grafia". Stego means "cover" and grafia means "writing" whereas Steganalysis is a technique to detect the existence of steganography. Steganography is the art and science of secret communication this paper proposed an extensive review of the novel approach of encryption the plain text into cipher text and embedding it in to color image.

Keywords – Chaos theory ,has function ,data hiding ,LSB replacement, encryption.

I. INTRODUCTION

Image steganography is the the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2]. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which supposed to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques.

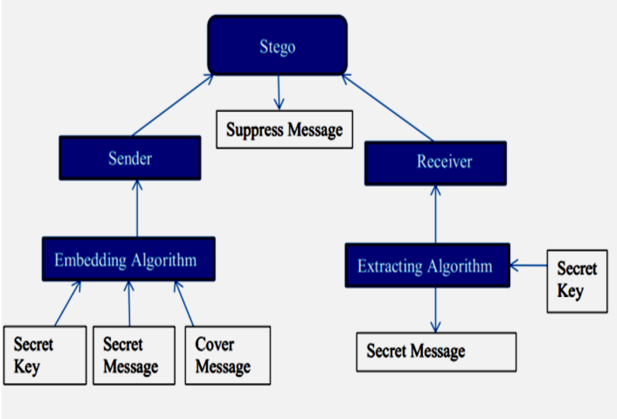

Figure: 1.1 Steganography System Scenarios.

The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender. The Steganography system scenario is shown above in the Figure 1.1.

"Steganography is the ancient art of embedding a secret message into a seemingly harmless message. This art, in contrast to cryptography, does not use ciphers or codes to scramble a message, and therefore is not obvious. U.S. and foreign officials suspect that Osama bin Laden is using steganography to pass embedded maps and photographs of terrorist targets through chat rooms and pornographic Web sites"

Data Hiding Techniques

There are three different approaches that can be used to hide information in a cover object: injection, substitution and generation.

- Injection

The data can be hidden in sections of a file that are ignored by the processing application using injection technique. Therefore file bits that are relevant to an end-user are not modified—leaving the cover file perfectly usable. For example, we can add additional harmless bytes in an executable or binary file. Because those bytes don't affect the process, the end-user may not even realize that the file contains additional hidden information. However, using an insertion technique changes file size according to the amount of data hidden and therefore, if the file looks unusually large, it may arouse suspicion.

- Substitution

Substitution technique is used to replace the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion. The main advantage of this technique is that the cover file size does not change after the execution of the algorithm. On the other hand, this approach has at least two drawbacks. First, the resulting stego object may be adversely affected by quality degradation—and that may arouse suspicion.

Second, substitution limits the amount of data that you can hide to the number of insignificant bits in the file.

- Generation

Unlike injection and substitution, generation techniques do not require an existing cover file. This technique generates a cover file for the sole purpose of hiding the message. The main flaw of the insertion and substitution techniques is that people can compare the stego object with any pre-existing copy of the cover object (which is supposed to be the same object) and discover differences between the two. We will not have that problem when using a generation approach, because the result is an original file, and is therefore immune to comparison tests. Figure 1.2 shows an images stenography system.

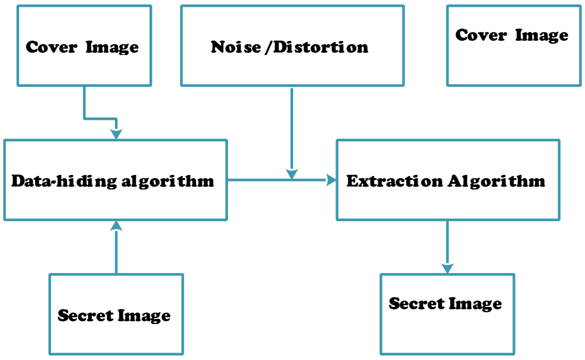

Figure 1.2 Image Steganography System.

II. LITERATURE SURVEY

Table 1: Summary of Literature Review

Sr. No.	Title	Authors	Year	Proposed methodology
1.	A novel LSB based image steganography with multi-level encryption,	G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K,	2015	A novel approach of encrypting the plain text into cipher text and embedding it into a color image.
2.	An efficient arithmetic coding data compression with steganography,	M. Gomathymeenakshi, S. Sruti, B. Karthikeyan and M. Nayana,	2013	The most reliable technique called arithmetic coding is used for compressing the information.
3.	Secret Communication Using JPEG Double Compression	J. M. Guo and T. N. Le,	2010	Show that the quality factor in a JPEG image can be an embedding space, and we discuss the ability of embedding a message to a JPEG image by managing JPEG quantization tables (QTs).
4.	Matrix factorizations for reversible integer mapping,	Pengwei Hao and Qingyun Shi	2001	Prove that there exist some approaches to factorize a matrix into TERMs or SERMs. The advantages of the integer implementations of an invertible linear transform are (i) mapping integers to integers, (ii) perfect reconstruction, and (iii) in-place calculation.
5.	Steganalysis of LSB encoding in color images,	J. Fridrich and M. Long,	2000	Introduce a powerful steganalytic technique that enables us to reliably detect the presence of a pseudorandom binary message randomly spread in a color image

G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K [1] Steganography is an art of hiding the existence of secret information by embedding it in a cover and hence preventing the unauthorized access of confidential information. This paper proposes a novel approach of encrypting the plain text into cipher text and embedding it into a color image. Encryption is done in two stages, during first stage it is encrypted by Ceaser cipher technique and in the second stage it is encrypted based on

chaos theory. The cipher text obtained after encryption is embedded using 3, 3, 2 LSB replacement algorithm.

M. Gomathymeenakshi, S. Sruti, B. Karthikeyan and M. Nayana, [2] Data transmission must be secure enough to be used in a channel medium without any loss and tampering of data. Data sent in a compact way adds to the efficiency in sustaining the aspects of secure transfer. Practically, compactness is achieved through data compression which reduces the storage space or the transmission capacity of the information. In this paper, the most reliable technique called arithmetic coding is used for compressing the information. Secure medium is achieved by concealing the compressed information into the image using Steganography. This paper provides an inter-platform between data compression and steganography for increasing the secrecy of the information.

J. M. Guo and T. N. Le,[3] Protecting privacy for exchanging information through the media has been a topic researched by many people. Up to now, cryptography has always had its ultimate role in protecting the secrecy between the sender and the intended receiver. However, nowadays steganography techniques are used increasingly besides cryptography to add more protective layer to the hidden data. In this letter, we show that the quality factor in a JPEG image can be an embedding space, and we discuss the ability of embedding a message to a JPEG image by managing JPEG quantization tables (QTs). In combination with some permutation algorithms, this scheme can be used as a tool for secret communication. The proposed method can achieve satisfactory decoded results with this straightforward JPEG double compression strategy.

Pengwei Hao and Qingyun Shi,[4] Reversible integer mapping is essential for lossless source coding by transformation. A general matrix factorization theory for reversible integer mapping of invertible linear transforms is developed. Concepts of the integer factor and the elementary reversible matrix (ERM) for integer mapping are introduced, and two forms of ERM-triangular ERM (TERM) and single-row ERM (SERM)-are studied. We prove that there exist some approaches to factorize a matrix into TERMs or SERMs if the transform is invertible and in a finite-dimensional space. The advantages of the integer implementations of an invertible linear transform are (i) mapping integers to integers, (ii) perfect reconstruction, and (iii) in-place calculation. We find that besides a possible permutation matrix, the TERM factorization of an N-by-N nonsingular matrix has at most three TERMs, and its SERM factorization has at most N+1 SERMs. The elementary structure of ERM transforms is the ladder structure. An executable factorization algorithm is also presented. Then, the computational complexity is compared, and some optimization approaches are proposed. The error bounds of the integer implementations are estimated as well. Finally, three ERM factorization examples of DFT, DCT, and DWT are given.

J. Fridrich and M. Long,[5] Analyzes the security of least significant bit (LSB) embedding for hiding messages in high-color-depth digital images. We introduce a powerful steganalytic technique that enables us to reliably detect the presence of a pseudorandom binary message randomly spread in a color image. We estimate the probability of both false detections and missing a secret message. The method is based on statistical analysis of the image colors in the RGB cube. It is shown that, even for secret message capacities of 0.1-0.3 bits per pixel, it is possible to achieve a high degree of detection reliability.

III. PROPLEM IDENTIFICATION

Based on novel LSB image stenography with multi-level Encryption. chaos based image steganography has been added to the base stenography technique . The proposed Algorithm uses cover in the spatial domain for hiding secret information. Proposed algorithm has added security and better performance when compared with base 3, 3, 2 LSB steganography techniques. Future works includes extending this approach to various cover and secret formats. the performance and security of the methodology can be enhanced by further enhancement of the level of encryption .

IV. CONCLUSION

To make information secure LSB based steganography with multi level in encryption has studied and discussed there are many techniques of encryption is already exist like chaos theory of encryption ,ceaser cipher technique ,embedding technique. In the technique discussed a secret image has divided in segments of L part of size 1*B the embedding has done by LSB replacement technique discussed is secure and further can enhance by increasing the level.

REFERENCES

[1] G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K, "A novel LSB based image steganography with multi-level encryption," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.

[2] Gomathymeenakshi,M., Sruthi, S .,Karthikeyan,B .,N ayana,M. ”An efficient arithmetic coding data compression with steganography”, in 2013 IEEE International.

[3] Guo,J,-M.,Le,T,-N, “Secret Communication Using JPEG Double Compression”, IEEE Signal Processing Letters, 17(10),5556462,pp.879-882.

[4] Hao,P.,Shi,Q. “Matrix factorizations for reversible integer mapping”, IEEE Transactions on Signal Processing. 49 (I0),pp. 2314-2324.

[5] J. Fridrich and M. Long, "Steganalysis of LSB encoding in color images," 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No.00TH8532), New York, NY, 2000, pp. 1279-1282 vol.3.

[6] Singla,D., Juneja,M. ”New information hiding technique using Features of image”, Journal of Emerging Technology in Web Intelligence, 6(2),pp.237-242.

[7] Mainberger,M.,Schmaltz,c.,Berg,M.,Weickert,J.,Backes,M. Diffusion-based image compression in steganography” 7432 LNCS (PART 2),pp.219-228..

[8] Conference on Emerging Trends in Computing and Nanotechnology,ICE-CCN 2013 6528520,pp. 342-345.

[9] Lin, Y.-K. “A data hiding scheme based upon DCT coefficient modification”, Computer Standards and Interfaces 36(5),pp.855- 862.

[10] Chen,Y.,Hao,P. “Integer Reversible Transformation to make JPEG lossless” 2004 7th International Conference on Signal Processings,ICSP. pp.837-840.

[11] Karthikeyan,B.,Vaithiyanathan,V.,Thamotharan,B.,Gomath yme enakshi,M.,Smthi,S.“LSB replacement steganography in an image using pseudorandomised key generation” Research Journal of Applied Sciences, and Engineer and Technology,4(5),pp.491-494.

[12] Hu,Y.,Wang,K.,Z.-M.” An improved VLC-based lossless data hiding scheme for JPEG images” Journals of Systems and Software 86 (8),pp.2166- 2173.

[13] Dr. K. L. Sudha, and Manjunath Prasad, (2011) “Chaos image encryption using pixel shuffling with Henon map,” in Proc. of Elixir Elec. Engg. 38, pp. 4492-4495.

[14] Kousik Dasguptaa, Jyotsna Kumar Mondal and Paramartha Dutta,” Optimized video Steganography using Genetic Algorithm (GA)” First International Conference on Computational Intelligence:Modelling Techniques and Applications,Vol lO (2013),pp. 131 - 137.

[15] Chang,C.-C.,Lin,C.-C.,Tseng,C.-S.,Tai,W.-L” Reversible hiding in DCT-based compressed images” information Sciences 177 (l3),pp. 2768-2786.

[16] Qian,Z.,Zhang,X.” Lossless data hiding in JPEG bitstream”, Journal of Systems and Software 85 (2),pp. 309-313.

[17] Bandyopadhyay,D.,Dasgupta,K.,Mandal,J,K.,Paramartha Dutta.”A Novel secure Image Steganography method based on Chaos theory in spatial domain”,International Journal Of Security,Privacy and Trust Management,Vol 3,No I.

[18] Karthikeyan,B. ,Ramakrishnan,S.,V aithiyanathan,V. ,Sruthi,S., Gomathymeenakshi,M. “An improved steganography technique using LSB replacement on a scanned path image”, International Journal of Network Security, 16(l),pp.14-18.

[19] Jovanovic,V,T.,Kazerounian,K, “Using Chaos to Obtain Global Solutions in Computational Kinematics”, in Proc. of Journal of Mechanical Design, 120(2), pp. 299-304.

[20] Amigo,J.M.,Kocarev,L.,Szczepanski,J., “Theory and Practice of Chaotic Cryptography”, Physics Letters, Section A:General Atomic and Solid State Physics,366(3),pp.211-216.

[21] Fridrich,J.,Du,R.,Long,M.“Steganalysis and LSB Encoding in Color Images”, IEEE International Conference on Media and Expo,(III/WEDNESDAY),pp.1279-1282.

[22] Saeed,M.J “A new technique based on chaotic steganography and encryption text in DCT domain for color images”, in Proc. of Journal of Engineering Science and Technology,8(5),pp.508-520.

[23] Arun A.S. and George M. Joseph, (2013) “High Security Cryptographic Technique using Steganography and Chaotic Image Encryption”, in Proc. of Journal of Computer Engineering (IOSRJCE), Vol 12, pp 49-54.