IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.6, Issue.10, Oct. 2018 E-ISSN: 2347-2693

Enhanced Hybrid Techniques for Data Hiding

Sukhjeet kaur[1*] , Harpal Singh[2]

[1,2]Guru Kashi University, Talwandi Sabo, India

[*]*Corresponding Author: Sukhjeetkaursra9@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 20/Oct/2018, Published: 31/Oct/2018

***Abstract*—** Security is the occasions of anyone unfastened from hazard. Safety has very crucial difficulty in conversation. To solve the difficulty of security we arrange those integrate techniques. Cryptography is the artwork and science of observe of generating the secret message of the original message. As Steganography is the art and technological know-how of hiding verbal exchange, into some other media type file consisting of image, text and video. The numerous cryptography and steganography methods to cover statistics like LSB, DCT etc. However these strategies are wounded by a few problems like reduce quality of image, lower covering capacity. To success over this difficulty the proposed strategies use Substitution Encryption method to similarly encrypt the data and steganography method uses the Improved LSB Steganography technique which uses the formats like bmp, jpg and so forth. Performance of the proposed system is better than existing system.

***Keywords*—** Cryptography, Steganography, Encryption, LSB, Security

I. INTRODUCTION

As information are exchanged over the Internet so one must ensure about its security. Some techniques like cryptography and steganography are well known and widely used techniques for securing sensitive information [14].

A. Cryptography

Cryptography is a technique to generate the secret message from the original message for the security purpose. To make this secret code we use Encryption procedure. By using encryption original data or message is converted into different random forms and it seems meaningless. It can also be supposed that encryption is the process of transform plaintext into the cipher text where plaintext is the input to the encryption process and cipher text is the output of the encryption process [6, 14].

The fundamental objectives of cryptography are (1) Authentication, (2) Privacy, (3) Integrity, (4) Non-repudiation and (5) Access Control.

The basic components of cryptography: [6]

Plain text: Plain text is the original message before being transformed.

Cipher text: Cipher text is the output of an encryption process i.e. encrypted text or message in its coded individual readable form.

Encryption algorithm: An encryption algorithm transforms the plaintext into cipher text. The sender uses an encryption algorithm.

Decryption algorithm: A decryption algorithm transforms the cipher text back into plaintext. The receiver uses a decryption algorithm

Key: A key is an amount (or set of numbers) that the cipher, as an algorithm, operate on it.

B. Steganography

Steganography is a technique of hiding the data. The word steganography came from the combinations of two Greek words, stego means covert and graphic which means writing. Steganography hides the message in such a way that no one expects the recipient known about message existence. In this technique message is hidden into another file like image, text, sound or video [11].

II. RELATED WORK

Encryption Methods: Atish Jain et al. (2015), Caesar cipher is an ancient, basic method of encrypting plain text message into cipher text protecting it from adversaries. This paper aims to propose AN increased version of Caesar cipher substitution technique which may overcome all the limitations faced by classical Caesar Cipher [3]. Gurjeevan Singh, et al. (2011), presents the performance analysis of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. In future Encryption techniques in such a way that it can consume less time and power furthermore try to develop stronger Encryption Algorithm with high speed and minimum energy consumption [14].

Steganography Methods: Balvinder Singh et al. (2014), introduces a new approach for least significant Bit (LSB) based on image steganography that enhances the existing LSB substitution techniques to improve the security of hidden information. The proposed algorithm hides the secret data inside images using an efficient steganography technique [4]. Amritpal Singh et al. (2014), represent steganography is becoming an important area of research in recent years. Image steganography is that the means of secret communication through the digital images. It is an art and the science of embedding information into cover image, text, video, and audio etc. This paper discusses various image steganography techniques such as least significant bit, DWT, PVD, DCT [2].

Hybrid Methods: G.Prashanti et al. (2017), represent the sender encrypts the secret message using cipher algorithm which uses a secret key that should be known to both the sender and receiver. To produce twin security the encrypted message obtained from different encryption strategies is hidden in an image based on LSB steganography. From receiver side the encrypted message is extracted from the image. To provide better security both cryptography and steganography are combined. [13]. Dipti Kapoor Sarmah et al. (2016), introduces a system with the combination of cryptography and steganography using four (4) keys. AES Algorithm is used to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys. Steganography and Cryptography are two popular methods for sending vital information in a secret way. One hides the reality of the message and the other distorts the message itself. [7]. Marwa E. Saleh et al. (2016), represent a new secure communication model has been presented that combines cryptography and steganography techniques to provide two layer of security, so the steganalyst can't reach to plaintext without meaningful the secret key to decode the ciphertext. [20].

III. PROPOSED METHOD

The proposed methodology works in the following phases are as follows:

Embedding Phase: This algorithm is used for embedding the secret message in the host image using a transformation method.

The steps involved in this process are:

1. Select the image in which we want to embed the secret message. Image that is select to embed secret data is known as cover image which carries secret message from sender to receiver.
2. Select the text file which is en crypt in cipher form with the help of key.
3. Then encrypted file is hidden in image with Improved LSB method of image steganography.
4. After embedding process encrypted file is hidden in image. This image is called stego image. The Stego image is saved on disk.

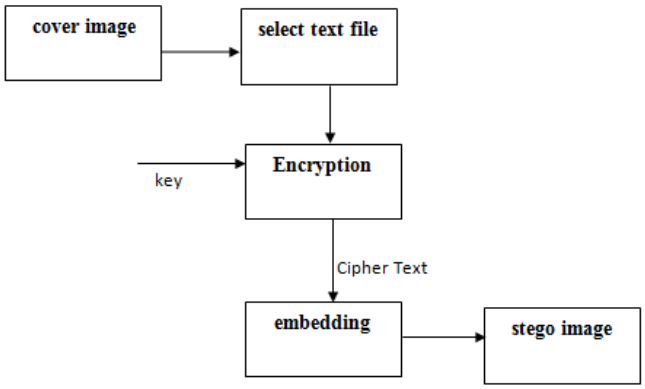

Figure1: Block Diagram of Embedding Phase

Extraction phase: Extraction phase is the process of retrieving the secret message from the stego image. The steps involved in this process are:

1. Select the Stego image from disk then extract the encrypted file with help of improved LSB decoding method.
2. After Extraction process encrypted file decrypt with same key and original message are shown.

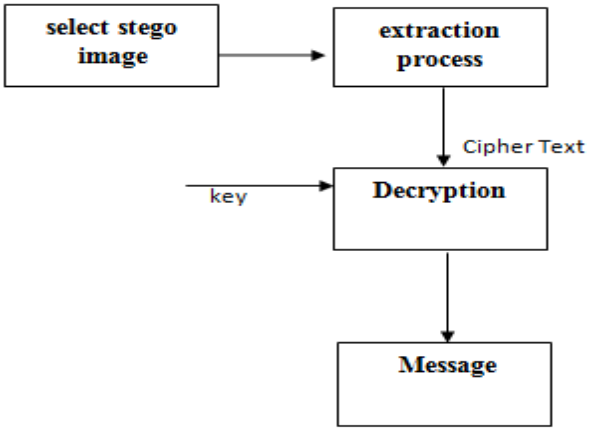

Figure2: Block Diagram of Extraction Phase

Embedding Algorithm: Embedding is the process of hiding the embedded message developing the stego image. Hiding information may require a Stego key which is additional secret information, such as password, required for embedding the information.

For example, when a secret message is hidden in a cover image, the resulting image is known as stego image.

The embedding algorithm steps can be listed as follow:

1. Select the cover image in which message is to be hidden.
2. Select the text file which is to hide in the cover Image.
3. Enter any key which you want to use as a secret key.
4. Encrypt the message using Substitution Encryption Algorithm.
5. Hide the text data into the cover image using Improved LSB As follows:

a) Compute the RGB values for all pixel of the cover image to embed the secret text
b) Find the smallest value from these three values of Red, Green and Blue.
c) Select this colour to be target colour to insert the secret message in it.
d) Embed the message and Repeat step 5 for complete secret message.

6. Store the stego image.
7. Exit

Extracting Algorithm: Extracting is the process of receiving the embedded message from the stego image.
The Extraction algorithm steps can be listed as follow:
1. Select the Stego Image in which encrypted text message is hidden.
2. Extract the text message using Reverse Improved LSB Technique as follows:
a) Compute the RGB values for every pixel of the cover image to embed the hidden text
b) Find the smallest value from these three values of Red, Green and Blue.
c) Select this colour to be target colour to extract the secret message from it.
d) Extract and concatenate the message to the final message and Repeat step 5 for complete secret message.
3. Enter the secret key which has you entered for encryption purpose.
4. Decrypt the message using Inverse Substitution Decryption Algorithm
5. Display the result to the user.
6. Exit.

IV. IMPLEMENTATION

Cryptography and Image steganography is implementing with the help of MATLAB. MATLAB (short for Matrix Laboratory) is a mathematical and graphical software package which has numerical, graphical and programming capabilities. MATLAB is very powerful software which provides various inbuilt function to problem solving. MATLAB provide interactive software in which group of commands are entered by the user and it respond immediately with a result. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

V. RESULTS AND DISCUSSION

This section defines the results developed by the proposed system. The proposed algorithm is implemented in MATLAB platform. Six different images are used to perform the test cases.

Two types of test cases have been performed as follows:
1. Mean Square Error (MSE): MSE dealings the average of the square of the error. The average squared dissimilarity between an original image and resulting (stego) image is called Mean Squared Error. To compute MSE we use procedure as:

$$MSE=1/mn\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2$$

2. Peak Signal to Noise Ratio (PSNR): PSNR is a common used to find out the difference between the carrier and stego data. The PSNR is the percentage between the maximum possible power of an indicator and the power of corrupting noise. PSNR is commonly expressed in terms of the logarithmic decibel scale. PSNR represent a compute of the peak error. It can be calculated as follow:

$$PSNR=10 * log10 \frac{Max\text{^}2}{MSE}*db$$

Table: 1 Comparison of proposed system with the existing on the basis of the PSNR

Cover Images	PSNR of Existing Method	PSNR of Proposed Method
Img1	81.8697	82.5279
Img2	83.2855	84.231
Img3	83.6805	84.0024
Img4	83.5919	84.7414
Img5	82.2775	82.7518
Img6	82.3696	82.8527
Average	82.8457	83.5178

The graphical representation of Proposed and Existing system with Average PSNR is shown below.

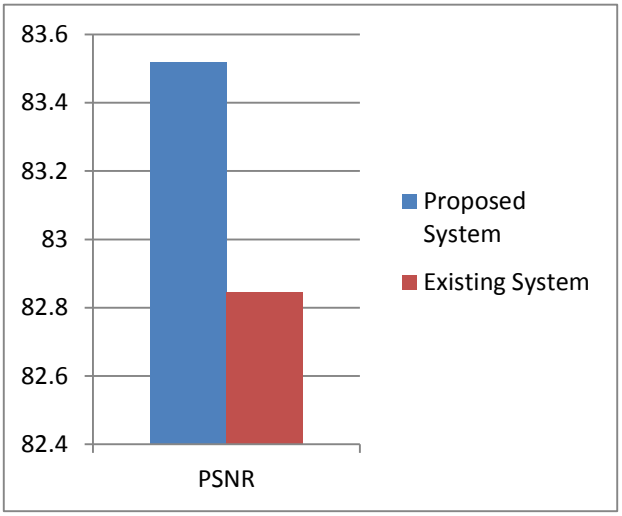

Figure3: Comparison Of proposed system and existing on the basis of PSNR.

Table: 2 Comparison of proposed system with the existing on the basis of the MSE

Cover Images	MSE of Existing Method	MSE of Proposed Method
Average	0.0003421	0.0002946

(a) Img1

(b) Img2

(c) Img3

(d) Img4

(e) Img5

(f) Img6

Fig. 4

VI. Conclusion and Future Scope

A. Conclusion

The main intention of the work is to extend a cryptography or steganography function that provides good security. The proposed approach provides higher security and can protect the secret data from attacks. In the proposed technique use Substitution Encryption method similarly encrypt the data and steganography method uses the special domain technique that is the Improved LSB Steganography technique which uses the formats like bmp, jpg etc. There are number of methods in cryptography and steganography and are different from each other. Each method has some pros and cons in comparison with other methods. The Least Significant Bit Insertion Method of Image Steganography provides an easy way to embed the information in the images. It is a very easy method to embed, so, it is used widely. But, it is very easy to decode also.

In addition the proposed technique improves the PSNR value of the proposed system. Performance of the proposed system is compared with the performance of the existing on the same input data set and it is concluded that the results of the proposed system are better than that of existing system.

B. Future Scope

There is a very brilliant future scope of this technique as it can be implemented in government sector and even in daily life. New strategies for the achievement of embed the secret message are always in demand.

As proposed system only encryption works with image file in future a more advanced system can developed that can work both on images as well as on audio and videos.

References

[1] Amritpal Singh, Harpal Singh " An improved LSB based Image Steganography Technique for TGB Images" , 978-1-4799-6085-9/15/$31.00 ©2015 IEEE.

[2] Amritpal Singh, Satinder Jeet Singh, "An Overview of Image Steganography Techniques", International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 3 Issue 7 July, 2014 Page No. 7341-7345.

[3] Atish Jain, Ronak Dedhia, Abhijit Patil, "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication ", International Journal of Computer Applications (0975 – 8887) Volume 129 – No.13, November2015.

[4] Balvinder Singh, Sahil Kataria, Tarun Kumar, Narpat Singh Shekhawat, "A Steganography Algorithm for Hiding Secret Message inside Image using Random Key", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTIJERT IJERTV3IS120844 www.ijert.org Vol. 3 Issue 12, December-2014.

[5] B.Ramesh Kumar, K.Suresh, S.K.Basheer, M. Raja Krishna Kumar, "Enhanced Approach to Steganography Using Bitplanes", International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012.

[6] Deepanshi Nanda, Sonia Sharma, "Security in Cloud Computing using Cryptographic Techniques", IJCST Vol. 8, Issue 2, April - June 2017

[7] Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for data hiding using Cryptography and Steganography", https://www.researchgate.net/publication/46585135. 15 April 2016.

[8] Dr.M.Umamaheswari, Prof.S.Sivasubramanian, S.Pandiarajan, " Analysis of Different Steganographic Algorithms for Secured Data Hiding", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010.

[9] Dr. Mohammed A. F. Al-Husainy, Dr. Diaa Mohammed Uliyan," Image Encryption Technique based on the Entropy Value of a Random Block", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No.7, 2017.

[10] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[11] Er. Munish Katoch, Reenu Jaswal, "Image Steganography: A Review", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2016.

[12] Gurpreet Singh, Supriya, "A Study of Encryption Algorithm(RSA,DES,3DES and AES) for information Security" ,

International Journal of Computer application, Vol. 67- No 19, april 2013.
[13] G.Prashanti, B.V.Jyothirmai, K.Sai Chandana, " Data Confidentiality Using Steganography and Cryptographic Techniques", 978-1- 5090-4967- 7/17/$31.00 © 2017 IEEE
[14] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 2011.
[15] Hayfaa Abdulzahra, Robiah Ahmad1, Norliza Mohd Noor, " Combining Cryptography And Steganography for Data Hiding in Images", ISBN: 978-960-474-368.
[16] Jagdish Mali1, Viraj Sonawane, Prof. R.N.Awale, "Image Steganography Using Block Level Entropy Thresholding Technique", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 4, Jul-Aug 2013, pp. 412-415.
[17] K.Thangadurai and G.Sudha Devi, "An analysis of LSB Based Image Steganography Techniques", 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.
[18] K. Arora, G. Gandhi, "A Review of Approaches for Steganography", International Journal of Computer Sciences and Engineering, Vol.2, Issue.5, pp.118-122, 2014.
[19] Mandeep Kaur Gill and Rupinder Kaur Randhawa , "Comparative Study of Multibit LSB Steganography with Cryptography", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.120-123, 2015.
[20] Manoj Kumar, Gursewak Singh, "Block based Image Steganography using Entropy with LSB and 2-bit Identical Approach", International Journal of Computer Application (0975-8887) Volume 171-No. 8, August 2017.
[21] Mehdi Hussain and Mureed Hussain, " A Survey of Image Steganography Techniques" , ", International Journal of Advanceed Science and Technology Vol. 54, May,2013.
[22] Marwa E. Saleh, Abdelmgeid A. Aly, Fatma A. Omara, " Data Security Using Cryptography and Steganography Techniques" , (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.
[23] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.
[24] Priyanka Haridas, Gouri Shankar Prajapati, " A Combined Approach of Steganography and Cryptography Techniques for Information Security: A Survey", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 4 Issue 12, December-2015.
[25] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication" IJCST Vol. 2, Iss ue 2, June 2011
[26] S Ushll, G A Sathish Kumal, K Boopathybagan, "A Secure Triple Level Encryption Method Using Cryptography and Steganography", 978-1-4577-1587-7/111$26.00 ©20111EEE.

