International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 5 01 - 06

Image Steganography with Dual Layer Security Using Fragment and Unite Technique

Mr. Umesh Mohite.
Research Scholar of Computer Engineering
Department ,Y.T.I.E.T, KARJAT
umeshmohite2311@gmail.com

Prof. Vaishali Londhe
H.O.D. Department of Computer Engineering
Y.T.I.E.T, KARJAT
vaishali.londhe@tasgoankartech.com

Abstract—At the present time where a regularly increasing number of data is made in different structures, kept and transferred, online security is the most vigorous factor. Different ways such as Cryptography, Steganography and Digital Watermarking are used to defend the data. The proposed framework gives additional dual layer of security as Cryptography and Steganography have been combined. Here data will be encrypted by using Encryption Algorithm AES. Then the encrypted data is embedded into a system's Defaulting image using least significant byte LSB Algorithm. Steganographed Default image is then fragmented into uniform parts and gets unite into reverse sequence using Uniform Fragment and Unite Technique. Reverse Steganographed Default image is then hidden (unseen) into another image. The proposed framework has summarized the goal to be safety and security factors.

Keywords-*AES, LSB, SHA-256, Fragment and Unite Technique, Steganography.*

*****

I. INTRODUCTION

Steganography is a word composed of two words. The word steganos means significance secured, disguised or ensured, and graphy means composing or drawing [1]. Steganography implies act of covering messages or data inside other non-mystery information. Cryptography word is composed of word crypto which means importance concealed, mystery, and graphy which means composing. Cryptography implies mystery composing which is the science and specialty of changing information to make them secure and safe to assaults by unapproved client. The Steganography and Cryptography concept can be utilized separately or together. By using these concepts together, the system gets more secure.

Cryptography algorithms are generally of two types Symmetric key and the second one is Asymmetric key algorithms. In Symmetric key algorithm one key is there for both encryption as well as decryption and in Asymmetric key algorithm two distinctive keys are utilized, one for concealing and the other for decrypting [2]. Symmetric key algorithm is otherwise called public key algorithm and the asymmetric key algorithm is also known as private key algorithm. The proposed framework is concerned for providing security to the user to transfer and store sensitive information.

- Information Hiding: Information Hiding is classified into two sections Steganography and Watermarking [3]. In the proposed structure Steganography is utilized for data covering. As steganography's communications are usually point-to-point while watermarking techniques are usually one-to-many. Figure. 1 describes the two information hiding techniques.
- Steganography limits unauthorized access and gives superior security during information transmission.

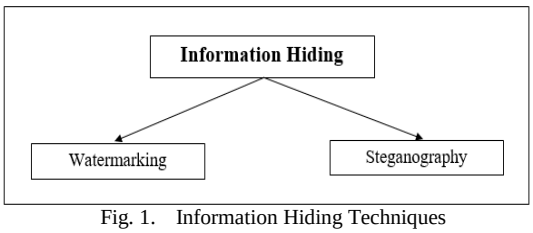

Fig. 1. Information Hiding Techniques

- Image Steganography: Steganography is used for many file formats such as picture, audio, video and text. The proposed framework utilizes picture; because those with high level of repetition are more reasonable for Steganography [4].

- Spatial Domain vs. Frequency Domain: The proposed framework uses Spatial Domain technique. Frequency Domain technique is more secure than Spatial Domain technique but it leads to more distortion [3, 4].

- Cryptography: The Proposed framework utilizes Advanced Encryption Standard (AES) algorithm for encryption-decryption. The computation time of AES is high, but still it is more secure than Data Encryption Standard (DES) algorithm [5] and as the size of data increases DES takes more computation time than AES.

- Secure Hash Algorithm (SHA-256) Vs. Message Digest (MD5): SHA-256 and MD5 algorithms are used as a Cryptographic hash function. SHA-256 is slower but provides high security compare to MD5.In proposed framework SHA-256 algorithm is used.

II. RELATED WORK

Cryptography calculations are utilized from most recent couple of decades. There exist plentiful cryptographic calculations accessible and they are characterized through the mean of their qualities [6].

Image Steganography can also be performed by segmenting the image unevenly [7]. In this technique three layers' security is provided for embedding the secret message into the image. At first the information is encoded utilizing AES calculation and thenNon-Uniform Block Adaptive Segmentation on Image (NUBASI) algorithm is used for generating segments of the cover image. Encrypted data is stored in these segments using Randomized Secret Sharing Algorithm (RSS). Data is stored in non-uniform segments of image.

LSB and AES is used together [8] where image is encrypted and not the data. The first layer encodes the data into acover image using Least Significant Bit (LSB) algorithm and the second layer encrypts the stego image using Advance Encryption Standard (AES) algorithm. The two layers are termed as Steganography Layer and Encryption Decryption layer.

Image can also be embedded in image as in [9]two ways are given one for 8 bit and other for 24-bit color image. For embedding image bits of LSB of shield image are replaced with bits of MSB of secret image. For 8-bit image 2 bits of LSB are replaced with 2 bits of MSB of secret image and for 24 bit 4 bit of LSB is changed by 4 bit of MSB of secret image.

For storing more information inside the image Lossless compression helps [10]by sinking the dimension of the file by removing the redundancy that occurs in the image. Itnever removes any information from the original image. The initial picture's integrity is kept up and the decompressed picture yield is bit-by-bit identical to the original image input.

Security of data is enhanced when Steganography is used along with cryptography [11]. The system encrypts data by taking advantage of AES and then embedding data into LSB of each pixel. For embedding text inside an image initially a total number of pixels in the image are calculated. A loop is applied through each pixel to get the RGB value of each one. The LSB value of each RGB pixel is made zero. The character which is to be hidden is converted in binary form and the 8-bit code is hidden in LSB of each pixel. The process is repeated until all the characters of the secret data are hidden inside the image. The extraction stage searches for 8 consecutive zero's and extracts the data from LSB and converts it into character.

Hash algorithms can be combined with both Steganography as well as Cryptography. In this system the data gets express in code using AES and SHA-512 is helps to produce a hash [12]. Cipher text, hash code is mixed using mixing algorithmtoform a mingled code.This code is then embedded in refuge image, after embedding process Steganographed image gets generated.

III. PROPOSED SYSTEM

The Proposed system is based on Image Steganography. Lossless Compression LSB embedding algorithm is used for storing the data inside the image. Along with Steganography, proposed system also uses cryptography for data encryption. AES Algorithm is unable to provide integrity for that purpose; the proposed system uses SHA-256 hashing algorithm for providing integrity. Later on for providing more security Fragment and Unite technique is used. This technique Fragments the image into uniform partitions and then unite them in a different sequence. The proposed system uses Lossless compression LSB technique for storing information in the image and image inside image. Reverse Steganographed Default image is stored in cover image that provides better security because the reverse image is difficult to decrypt. The proposed system provides extra layer security. The basic aim of the proposed system is to provide more security to secret data without the image getting distorted.

A. Least Significant Bit (LSB):

LSB Algorithm is basically divided in two sections i.e. Replacement and matching. Proposed system uses LSB replacement method for embedding data inside an image. The proposed system also uses lossless compression which is provided by LSB algorithm. Image compression techniques are used to reduce the redundancy of data. In the given system this technique is used to reduce the size of Steganographyimage.

B. Advanced Encryption Standard (AES):

AES [13] is symmetric encryption algorithm and is quicker than DES. AES divides the message and key size of 128,192 or 256 bits. Depending on the key size there are different numbers of rounds. The rounds consist of Sub Bytes, Shift Rows, Mix Columns and Add Round Key.

C. Secure Hash Algorithm(SHA-256):

Secure Hash Algorithm is one of the cryptographic hash functions that generate a settled size 256-bit hash value. The input data is segmented into blocks each of 512 bits. If the size of data is less than 512 bits then 1's are appended in the data. The segmented blocks undergo 64 rounds with initialized hash values after which final hash value is generated.In the proposed system AES Algorithm is used along with SHA Algorithm.

D. Uniform Fragment and Unite Technique:

Image Fragmenting and Unite is the main motive of the proposed system. Fragmenting procedure partitions an image in number of small regions. The number of regions (r) depends upon the estimation of 'm' and 'n', where m is total rows and n is total columns.

$$r = m*n \quad (1)$$

In Fragment and Unite technique image gets divided into uniform parts and gets merged in reversed order.

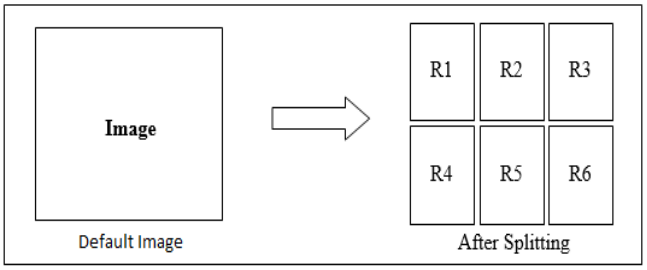

Fig. 2. Image Fragmenting Process

The merging process is more complex than the Fragmenting process. It combines all the regions and forms a single image. The regions which are formed after Fragmenting an image, only those regions are used to Unite into a single image.

Figure 3 shows that the regions of image get merged again.

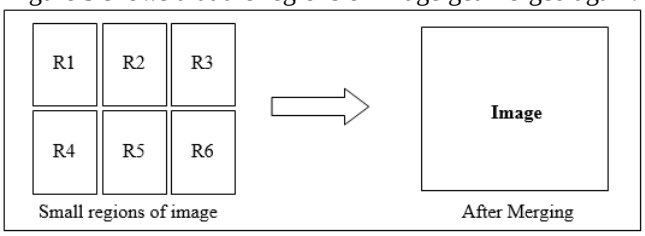

Fig. 3. Image Merging Process

The Fragment and Unite Technique is the main part of the proposed system, which is used to make the system more robust. The image is Fragment into a number of regions and the regions get merged in another sequence but after merging it will look like an original image.

Fig. 4. Fragment and Unite technique

The Figure. 4 describes how the image will get Fragment and merged again. The proposed system will provide another image which look's similar to an original image after Fragmenting and merging, so that the user won't come to know that the image has been Fragmentted and merged.

Encoding Process:

1. The system uses Lossless compression LSB algorithm, AES algorithm, SHA-256 algorithm and Fragment and Unite Algorithm.

2. In the 1st step of encoding process user will give input as an Original image, the Secret information user wants to covert within an image and the password.

3. The password is converted into message digest using SHA-256 algorithm.

4. The information taken as input from the system will get encrypted with the help of AES algorithm and for encryption secret key is obtained from the message digest generated by SHA-256 algorithm.

5. Now proposed system select random default image which is stored in it and encodes encrypted text into that image using Lossless compression LSB algorithm.

6. The encoded image is Fragment into uniform parts and then gets merged into another sequence.

7. After that, the generated image gets encoded using Lossless compression LSB algorithm into the Original image which is selected by the user and the final image will be generated.

Figure 5 describes the flowchart of the encoding process.

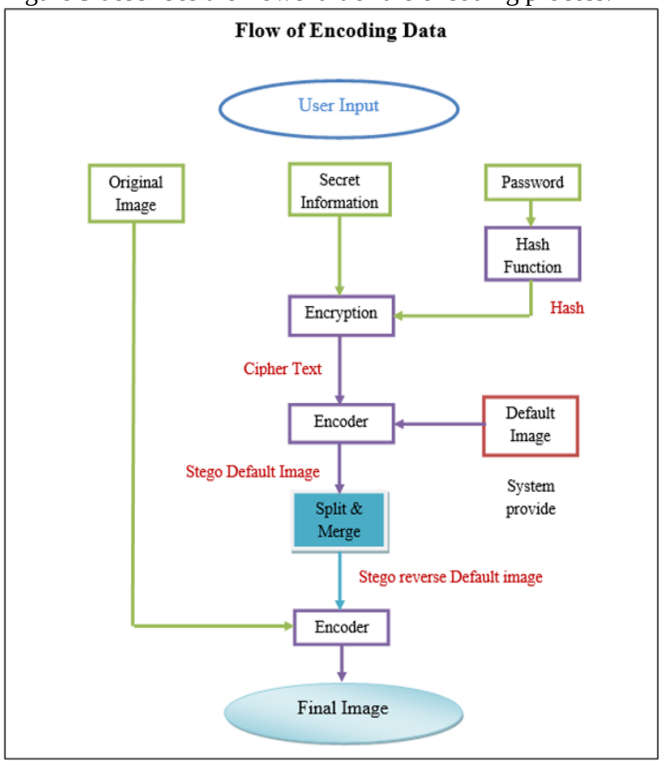

Fig. 5. Flowchart of encoding process

Decoding Process:

1. Decoding procedure is the precisely turnaround of encoding procedure.

2. The user input is the final image which contains secret information and password that was used to encode data in the image.

3. Using Lossless Compression LSB algorithm we extract the default image from the final image, then that default image gets Fragment into the uniform part and Unite into right sequence.

4. From the default image using Lossless compression LSB algorithm the encrypted text is separated out.

 ISSN: 2321-8169
01 - 06

5. The message digest which is generated from the password is used to decrypt the message.

6. Finally, the encrypted text is decrypted using AES algorithm and plain text is given which is secret information.

Figure 6 describes the flowchart of the decoding process.

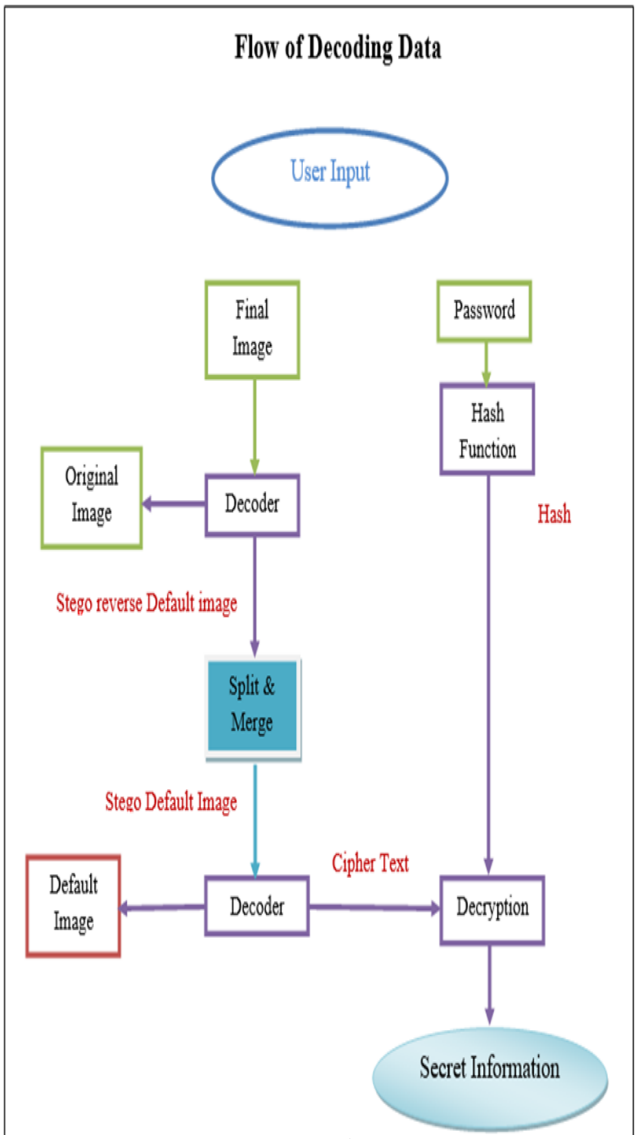

Fig. 6. Flowchart of decoding process

IV. EXPERIMENTALRESULT AND DISCUSSION

A. Histogram Analysis:

One of the way of analyzing the Steganography algorithm is Histogram Analysis. Histogram represents the intensity value of each channel.

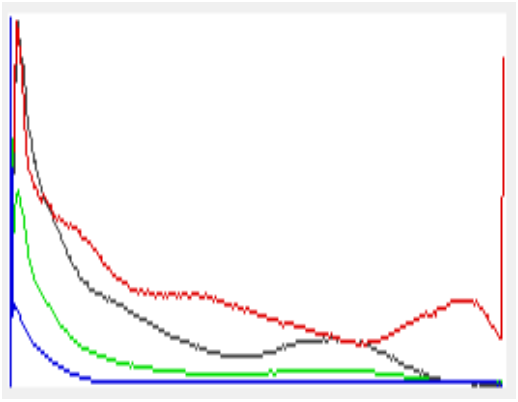

Fig. 7. Histogram of cover image

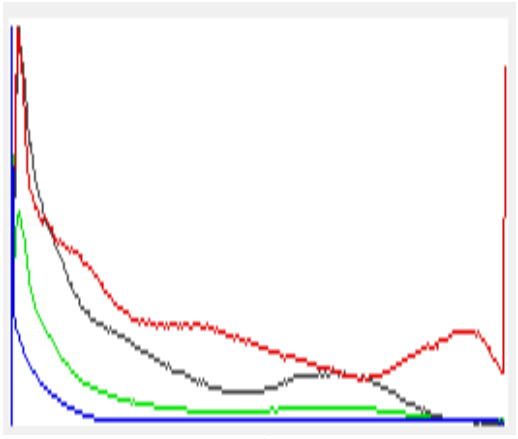

Fig. 8. Histogram of Steganography image

After comparing the histogram of cover image in the Figure. 7 with the histogram of Steganographed image in the Figure. 8 it can be seen that they are almost similar to each other, which means embedding the data leads to slight change or no change in the intensity values of the color pixels.

B. Peak Signal to Noise Ratio

The proposed system provides multiple features. They are less distortion, maximum security, minimum storage space, and maximum storage capacity. The developing system is java application based.

Greater the PSNR esteem better is the quality of the compressed or reconstructed image [14].
The given system is tested for various size image. For testing an image of size 1280*960 resolution is used and 6 kb of data is embedded into it. The PSNR value lies above 75 db. The PSNR value of three different images of the proposed system is given in the Table I.

 ISSN: 2321-8169
01 - 06

TABLE I. PSNR VALUE

Original Image	Secret Message	Steganographed Image	PSNR (dB)
	Steganography is a word composed of two words. The word steganos means significance secured, disguised or ensured, and graphy means composing or drawing. Steganography implies act of covering messages or data inside other non-mystery information. Cryptography word is composed of word crypto which means importance concealed, mystery, and graphy which means composing.		76.98
	The Steganography and Cryptography concept can be use separately or together. By using these concepts together, the system gets more secure. As the world has now become excited about the need of any secret communication and there are rules to limit uses of encryption.		76.99
	The Steganography and Cryptography concept can be use separately or together. By using these concepts together, the system gets more secure. As the world has now become excited about the need of any secret communication and there are rules to limit uses of encryption.		76.90

C. User Interface of a System:

Fig. 9. Home Page

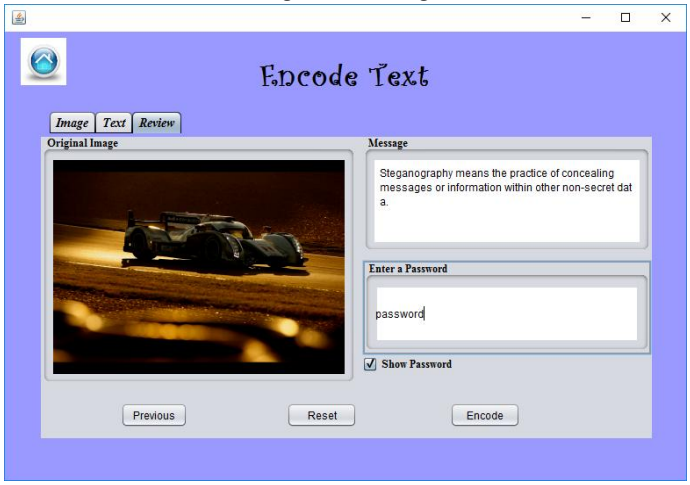

Fig. 10. Encoding Message

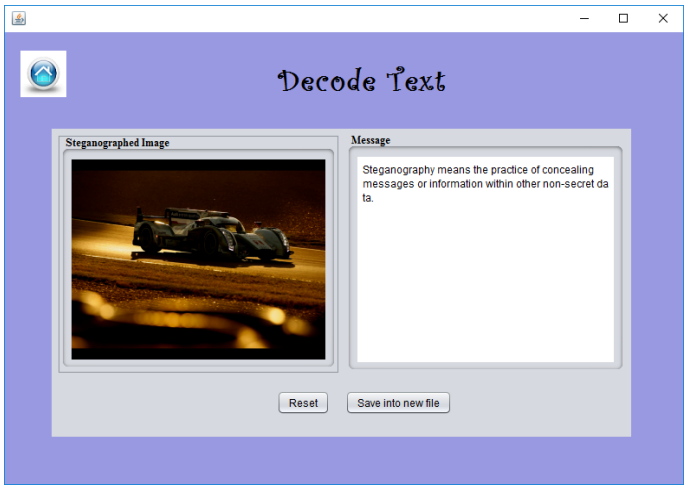

Fig. 11. Decoding Message

V. CONCLUSION

The proposed system provides improvement in the security factor by improving the PSNR value while not resulting to distortion of the Steganographed image. The proposed framework helps for concealing the instant message in the picture. Additionally, the message that is sent can be encoded, to strengthen secure steganography.AES algorithm doesn't provide integrity which is provided in the proposed framework by taking advantage of SHA-256 along with AES. The image hich contains undisclosed information is in reverse sequence and can't be detected by third party. After performing experiment on the system; the results show that the system provides an honest PSNR value for the generated Steganographed image.

REFERENCES

[1] https://en.wikipedia.org/wiki/Steganography,last accessed on 30/01/2017.
[2] D. D. Lad, Sindhu M. R., "A Survey on Data Hiding in Encrypted Images", International Journal of Science and Research (IJSR), Volume 4, Issue 11, pp. 389-392, November 2015.
[3] N. Choudhary,R. Gandhi, "A Review of Different Approach to Reduce Distance Error between Cover and Stego Image", International Journal ofEmerging Research in Management &Technology, Volume 4, Issue 8, pp. 27-30, August 2015.
[4] S. Mohan and S. Singh, "Image Steganography: Classification, Application and Algorithms", International Journal of Core Engineering &Management, Volume 1, Issue 10, pp. 93-97, January 2015.
[5] A. Devi, A. Sharma, A. Rangra,"A Review on DES, AES and Blowfish for ImageEncryption&Decryption",International Journal of Computer Science and Information Technologies, Volume 6, pp. 3034-3036, 2015.
[6] Md. A. Hossain, Md. B. Hossain, Md. S. Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research inComputer Science and Software Engineering, Volume 6, Issue 3, March 2016
[7] Srinivasan, S. Arunkumar, K. Rajesh, "A Novel Approach for Color Image, Steganography Using NUBASI and Randomized, Secret Sharing Algorithm", Indian Journal of Science and Technology, Volume 8, April 2015.
[8] S. Singh and V. K.Attri , "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", International Journal of Signal Processing, Image Processing and Pattern Recognition, Volume 8, 2015.
[9] D. Rawat and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Volume 64, February 2013.
[10] R. Kamboj and S.Kumari, "Remove Redundancy Technique of Lossless Image Compression", International Journal of Advanced Research in Computer and Communication Engineering, Volume 5, Issue 7, July 2016.
[11] S. Panghal, S. Kumar and N. Kumar, "Enhanced Security of Data using Image Steganography and AES Encryption Technique", International Journal of Computer Applications, Volume 42, 2016.
[12] C. Mehto, R. Kamble and Dr. B. Gour, "An Enhanced Digital Text passing system using SHA-512 and AES", IISTE, 2015, Volume 6, pp. 35-43.
[13] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm, last accessed on 10/02/2017.
[14] https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio,last accessed on 10/02/2017.