Enhanced LSB method to hide and transferring of information

Krutik V. Poojara[1], Jasmine Jha[2]
[1]Department of Computer Engineering, LJIET, Gujarat, India
[2]Asst.Professor, PG Department, LJIET, Gujarat, India

***Abstract* - Steganography is the art of hiding information behind information. The digital images are the most popular because of their frequency on the Web among all different carrier file formats. Image steganography, achieves the secrecy by embedding data into cover image and generating a stego-image. There are many types of steganography techniques each have their advantages and disadvantages. In this paper, we propose a new approach for information hiding based on cryptography and steganography. It also attempts to identify and briefly reflects on which steganographic techniques are more suitable for which applications. The various results obtained for different cover images demonstrate that the stego image obtained by applying this technique is not visually distorted because the PSNR is high. Thus, experimental results demonstrate that the technique performs well as compared to other image steganography techniques.**

Key Words — Steganography; PSNR; MSE; encrypt; Communication, Information, Secrecy, Techniques.

I. Introduction

Under the rapid development of the Internet and multimedia techniques, digital data such as texts, images, videos, and audios now have been widely used in our daily life. The process of the digital information makes human lives become more convenient. People can transmit huge information via computer networks. However, the security of the computer networks is insufficient, and the transmitted data could be intercepted or grabbed by an illegal user. Therefore, how to ensure the digital data to be securely transmitted via the Internet is an important issue.If a person views the digital object that the information is hidden inside, he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information, this is the main objective behind the steganography.

Steganography is a Greek word which means concealed writing. The word "steganos" means "covered " and "graphical" means "writing" . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data.
Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data [3]

II. Steganography concepts

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [5], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [6]. The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the

other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information.

III. CRYPTOGRAPHY CONCEPTS

Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'. The message may be converted using a 'code' (in which case each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual characters).Cryptology is the science underlying cryptography. Cryptanalysis is the science of 'breaking' or 'cracking' encryption schemes, i.e. discovering the decryption key. Cryptographic systems are generically classified along three independent dimensions [7].

1. Methodology for transforming plain text to cipher text.

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

2. Methodology for number of keys used.

There are some standards methods [8] which are used with cryptography such as secret key, public key, digital signature and hash function.

Secret Key (Symmetric): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called as symmetric encryption.

Public Key: Public key cryptography has been said to be the most significant new development in cryptography in the last 300400 years. Modern Public Key Cryptography was first described publicly by Standford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their study describe a two-key crypto system in which two parties could engage in a secure communication over a insecure communications channel without having to share a secret key.

Digital Signature: The use of digital signature came from the need of ensuring the authentication. The digital signature is more like stamp or signature of the sender which is embedded together with the data and encrypts it with the private key in order to send it to the other party. In addition, the signature assures that any change made to the data that has been signed is easy to detect by the receiver.

Hash Function: The hash function is a one way encryption, the hash function is a well defined procedure or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes. The generating of hash code is faster than other methods which make it more desired for authentication and integrity. Cryptographic hash functions are much used for digital signature and cheap constructions are highly desirable. The use of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols. The authentication and the integrity considered as main issues in information security, the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if it’s similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side.

3. Methodology for processing plain text.
A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

IV. Steganography techniques

1. Spatial Domain Methods:

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories:

i)Least significant bit (LSB)

ii) Pixel value differencing (PVD)

iii) Edges based data embedding method (EBE)

iv) Random pixel embedding method (RPE)

v)Mapping pixel to hidden data method

vi) Labelling or connectivity method

vii) Pixel intensity based.

i. LSB: this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii. BPCP: In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

iii. PVD: In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. Spread Spectrum Technique:

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3. Statistical Technique:

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

4. Transform Domain Technique:

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as

i) Discrete Fourier transformation technique (DFT)

ii) Discrete cosine transformation technique (DCT)

iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT)

iv)Embedding in coefficient bits

5. Distortion Techniques:

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

6. Masking and Filtering:

These techniques hide information by marking an image. Steganography only hides the information where as watermarks becomes a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

V. Combined Crytography-Stegnography

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time.

Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2.

In figure 2, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

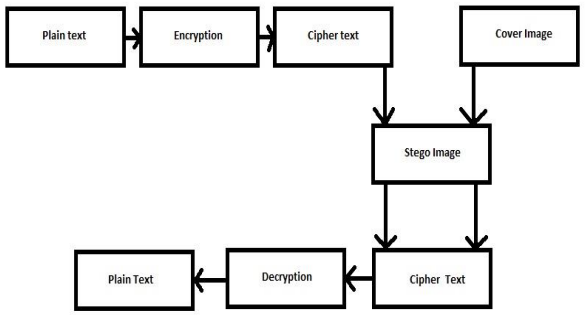

Figure : 2

Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types [8]:

1. **Pure Steganography:** This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

2. **Secret Key steganography:** The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

3. **Public Key Steganography:** The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

VI. Proposed system

Enhance LSB

A new image steganography scheme based on first component Alteration technique. In a computer, images are represented as arrays of values. These values represent the intensities of the three colors R (Red), G (Green) and B (Blue), where a value for each of three colors describes a pixel. Each pixel is combination of three components(R,G and B). In this scheme, the bits of first component (blue component) of pixels of image have been replaced with data bits. Blue channel is selected because a research was conducted by Hecht, which reveals that the visual perception of intensely blue objects is less distinct that the perception of objects of red and green.

Embedding Process

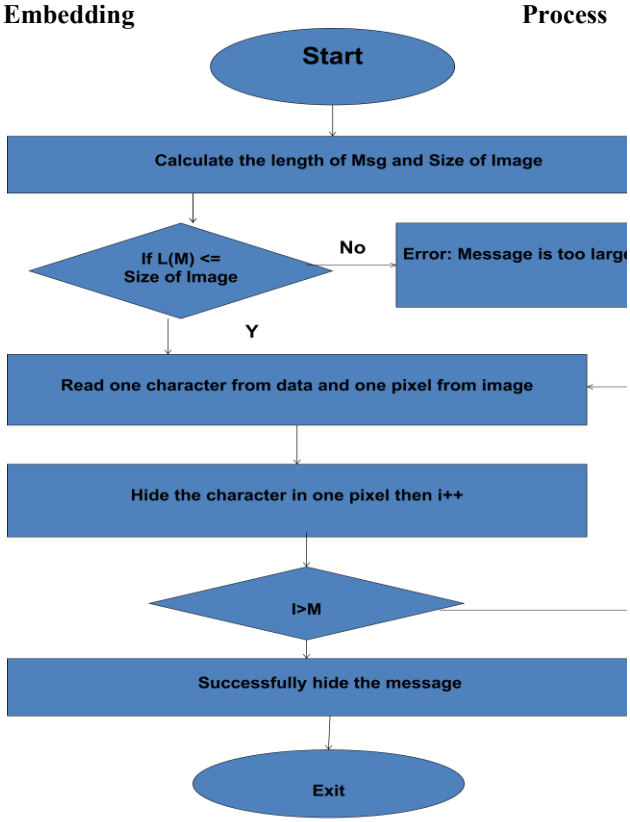

Fig.1 : Proposed Model

The Proposed embedding algorithm:

Step-1: Read the encrypted message and convert into binary form using AES algorithm
Step-2: Read the cover image and secret image you want to hide in cover image
Step-3: Store the binary message into secret image
Step-4: Conver into rgb to gray color
Step-5: Conversions need to spread the image value on 256gray scale
Step-6: Determine the size of cover image used embed
Step-7: determine the Size of message to embed
Step-8: Set the LSB of cover image to the value of the MSB
Step-9: by applying the method of LSB we obtain Stego image

Fig. 2: Cover image and Stego image

Data Retrieval

Proposed Retrieval Algorithm

Step-1: Retrieve the least significant bits of each potential pixel of the stego image to get the bits stream
Step-2: Determine size of cover image
Step-3: Construct the Secret Image.
Step-4: Apply AES decryption algorithm.
Step-5: End

VII. Performance Evaluation

The experimental results determined required to be executed for measuring the performance of the system.

A The mean square error

It is used to measure the difference between estimated value and the true value for estimated quantity.
It is used to measure the distortion in the image using equation

$$MSE = \sum_{i=1}^{all\ pixcel} \sum_{j=1}^{all\ pixel} \frac{[CI(i,j) - SI(i,j)^2}{N * N}$$

Where CI (i, j) represent the pixel of the cover image.

SI (i, j) represent pixel of the stego image.

N * N represent the cover image size.

B Peak Signal to Noise Ratio (PSNR):

Peak Signal to Noise Ratio is the ratio of original signal in the image to the noise introduced due to

data embedding.PSNR is the measurement of the quality between the cover image and stego-image and can be measured in db in using equation:

PSNR = 10_X_ log(255-/MSE)

VIII. Experiment and Performance Results

In this , asecret image / data shown in fig 3 is embedded into original cover image of fig 4 and converted to stego image which is passed from sender's side.

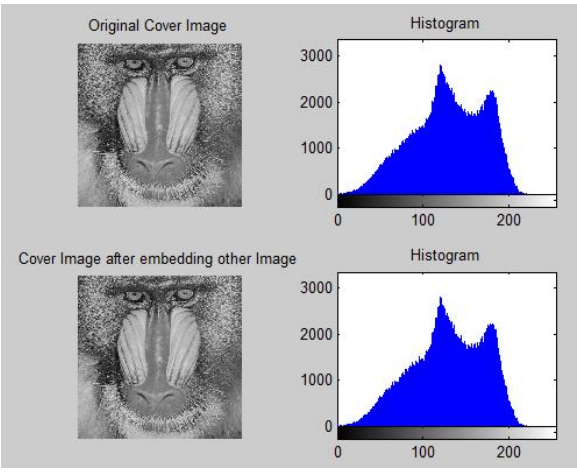

Fig 3: Comparison

In proposed work so there is no big difference in the visibile quality of original image and stego image . This shows that visual differences will appear indistinguishable for human visual senses and negligible to human eye. As results are shown above.

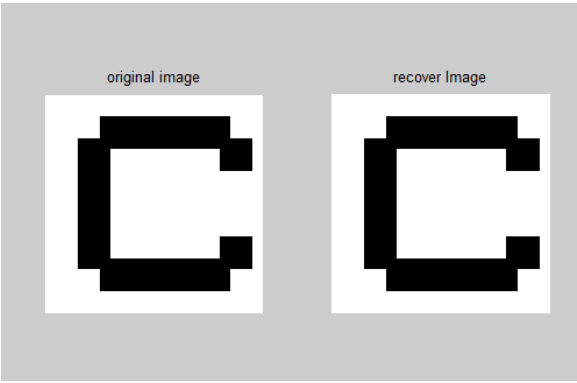

Fig 4 : Hidden Image

IX. Comparison between existing methods and proposed algorithm

Table 1 shows the comparison of PSNR value for existing methods and proposed algorithm. The algorithm improves the security and the quality of the stego image. It is show that the PSNR is high in the case of proposed algorithm compared to existing algorithms.

ıage	LSB	First Component alteration technique	Improved LSB	Proposed System
ena	26.08	46.11	68.10	78.125

Table 1

X. Conclusion and future scope

The main objective of LSB steganography is that to pass a message to receiver without intruder even knowing that message has been passed.The existing Least Significant Bit Algorithm has been analyzed and found to have a more amount of distortion, so a new method has been proposed "Enhanced Least Significant Bit (ELSB)". It improves the performance of the LSB method.The results obtained shows significant improvement in the PSNR(Peak Signal-to-Noise Ratio) than the existing work. PSNR is the most popular metric to measure the distortion in an original image and a reconstructed image.PSNR represents a measure of the peak error.The results also shows decrease in MSE(mean square error). The MSE represents the cumulative squared error between the compressed and the original image. The lower the value of MSE, the lower the error.Results

show that proposed method is better than existing methods. According to the results, stego images are almost identical to cover images and it seems very difficult to differentiate them.

Proposed technique can be extended for other forms of digital media. The technique was implemented here for images but same can be extended to be used with other digital media available.The technique requires some variations that are cover object specific.Combination of other techniques can be tried to get comparable results.

XI. References

[1] A.Joseph Raphael,Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[2] I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12

[3] Jasleen Kour , Deepankar Verma , International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-3, Issue- 5)

[4] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[5] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983

[6] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[7] Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, " An Encrypto-Stego Technique Based secure data Transmission System", PEC, Chandigarh..

[8] B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010

[9] Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, "A Survey on Cryptography and Steganography Methods for Information Security", Internaltional Journal of Computer Applications(0975-8887), Volume 12 – No. 2,November 2010.

[10]DiptiKapoorSarmah,Nehabajpai,"ProposedSyste m for Data hiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.

[11] Nitin Kanzariya,Ashish Nimavat,Hardik Patel, "Security of digital images using steganography techniques based on LSB, DCT and Huffman encoding" ELSEVIER 2013

[12] Jyoti Gaba, Mukesh Kumar"Implementation of Steganography Using CES Technique"Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)

[13] Dilip Kumar Nayak and Prof. Chakravarthy Bhagvati"A Threshold-LSB Based Information Hiding Scheme Using Digital Images" 2013 4th International Conference on Computer and Communication Technology (ICCCT)

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