Information Hiding Technique Using Lsb Substitution

Amit Patel[1] Alpesh Dafda[2]
[2]Assistant Professor,E.C.Department
[1,2] V.G.E.C, Chandkheda, Gandhinagar,Gujarat,India.

Abstract---Since the rise of the internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a new method or technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. But it is not enough to keep the contents of a message secret, it is also important to keep the existence of the information secret. The technique which provides this features, is called steganography. Steganography is the art and science of invisible communication. This accomplished through hiding information in other medium, thus hiding the existence of the information which is communicated. The word steganography is comes from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing"[6]. In image hiding using steganography the information is hidden exclusively in images.

Keywords:- Steganography, Cryptography, Peak-Signal-to-Noise-Ratio (PSNR)

I. INTRODUCTION

The word steganography comes from the Greek word Stego, means hidden or secret and graphy means drawing or writing. So, steganography is a system with hidden writing. Steganography is a technique and science of information hiding such that its presence cannot be detected[4] and a communication is happening. A secret information is encoding in a manner such that the very existence of the information is hidden. With existing communication methods, steganography can be used to exchange hidden messages. The main goal of steganography is to communicate securely in a completely undetectable manner[4] and to avoid drawing suspicion to the transmission of a hidden data. It is not sufficient to keep adversary people from knowing the hidden information, but it is to keep adversary people from thinking that the information even exists. If for a steganography method someone suspects the carrier object, then the steganography system has failed.

Until some recently development, information hiding techniques received very much less attention than cryptography from the research community and from industry. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996. There has been a rapid growth of interest in steganography for two main reasons [6].

- The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in audio recordings, books, digital films, and multimedia products.
- Action taken by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

A possible formula of the process may be represented as : cover medium + message object + stego key = stego object.

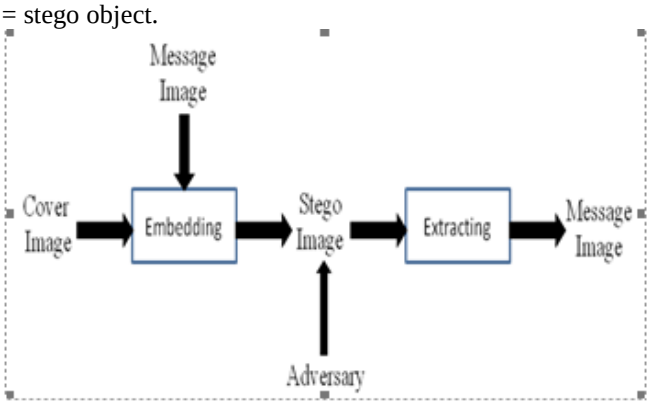

Fig. 1: Graphical Version of the Steganographic System

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered by adversary people. Often, using encryption technique might identify the sender or receipient as somebody with something to hide. For example, the picture of sunset could conceal the plans for our company's latest information.

II. HISTORY OF STEGANOGRAPHY

It is believed that steganography was first practiced during the Golden Age in Greece[3]. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood, giving the appearance of a new, unused tablet. The resulting tablets could be innocently transported without anyone suspecting the presence of a message beneath the wax. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood.[3]

III. APPLICATION OF STEGANOGRAPHY

There are many applications for digital steganography of image,including feature tagging, copyright protection, and secret communication[1,6]. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark. In feature tagging, time stamps, captions, annotations, and other descriptive elements can be embedded inside an image. Copying the stego image also copies of the embedded features and only parties who posses the decoding stego key will be able to extract and view the features of object. On the other hand, secret communication does not display a covert communication by using steganography. So, it can avoid information of the message, sender, and recipient. This can be effective only if the hidden communication is not detected by the others people.

IV. STEGANOGRAPHY AND CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret exchange of information. However, steganography is different than cryptography. In cryptography system hides the secret message from a malicious people[2], whereas steganography even conceals the existence of the message information. Steganographic system must not be confused with cryptography, in which we modify the message information so as to make it meaning obscure to a malicious people who intercept it contents. Therefore, the meaning of breaking the system is different from steganography[7]. In cryptography, the system is broken when the attacker can read the secret or hidden message. Successful attack on a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message.

V. STEGANOGRAPHY OF A CRYPTOGRAPHIC MESSAGE

Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted information data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several techniques by which we can encrypt data before hiding it in the chosen object. In some situations, sending an encrypted message will across suspicion while an invisible message will not arouse suspicion. Both methods can be combined to produce better protection of the message. In case, when the steganographic system fails and the message can be detected, it is still can be of no use as it is encrypted using cryptographic techniques.

VI. STEGANOGRAPHY APPLICATION

There are many applications for digital image steganography, including feature tagging, protection of copyright, and secret communication[1,6]. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission of the owner, they can prove it by extracting the watermark.

In feature tagging time stamps, annotations, captions, and other descriptive objects can be embedded inside the cover image. Copying the stego image also copies of the embedded features and only parties who posses the decoding stego key will be able to extract and view the features hidden inside the cover. On the other hand, hidden or secret communication does not advertise a covert communication by using steganographic system. So, it can avoid checking of the sender, information message and people at receiver side. This is effective only if the hidden communication is not detected by the others people.

VII. STEGANOGRAPHIC TECHNIQUES

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed[8]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches include[6, 8]:

- Least significant bit insertion (LSB)
- Masking and filtering
- Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in cover image. The simplest steganographic method hide the bits of the information message directly into least significant bit plane of the cover-image in a specified deterministic sequence. Modifying the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering techniques of information hiding, usually restricted to 24 bits and gray scale images, hide information message by marking the cover image, in a similar way to paper watermarks method. The techniques of masking and filtering performs analysis of the cover image, thus embed the message information in significant areas so that the hidden message is more integral to the carrier image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Wavelet Transform, or Discrete Fourier Transform. These transform methods hide information messages in significant areas of the carrier image, which make them more robust to attack on system. Transformations technique can be applied over the entire portion of the image, through out the image, to block of the image, or other variants.

VIII. GOALS OF STEGANOGRAPHY

There are mainly three concerns of the steganography

- Security (Imperceptibility)
- Capacity
- Robustness

A. 8.1 Security: It is secure if it cannot be detected, extracted or removed even with full knowledge of the embedding algorithm without knowledge of the secret key. It should not be detected by human perception or it should be invisible to human eye that something is passing on in particular image.

It should not be statistically detectable. So, It should not leave the easily detectable signatures.

The levels of failures of steganographic system :

- Detection - Proof of existence of message
- Extraction – removing without destroying the cover
- Destruction – destroying the message without destroying the cover

B. 8.2 Capacity : The usefulness of the steganographic system depends on the capacity of the system to hold the message. There is a physical limit on the capacity until the size of the cover object is increased. Beyond limit the data will be noticeable, it will be visible and so the system will become failure. So, as the capacity of the steganographic system tends to increase, it lowers the security and robustness.

C. 8.3 Robustness: The robustness of a stegnographic system implies that the data of the message should maintain the integrity of the message in case of the modification. If the cover image get the image processing operation like cropping or compression which can be happened in todays environment of internet era, the data hidden in the image

pixel get modified or can be destructed which will result in the failure of stegnographic system.

The concerned modifications that are quite common like :

- Images: cropping, scaling, blurring, sharpening, contrast, gamma, brightness, rotation, skewing, recoloring, printing/copying/scanning, etc.
- Audio: filtering (think bass/treble), volume adjustment, stereo to mono, etc.
- Video: add/delete frames, any image/audio modification, frame swapping, frame averaging, temporal adjustments.
- Also: A/D and D/A conversion, lossy compression, and sophisticated attacks

Robustness of a steganographic system is achieved through redundant encoding of the message which reduces the capacity.

As shown in fig.2 there exists the trade off among the capacity, robustness and security of the information message image to be hide. Depending on the application requirement one can select the technique of image hiding providing required parameters of the system.

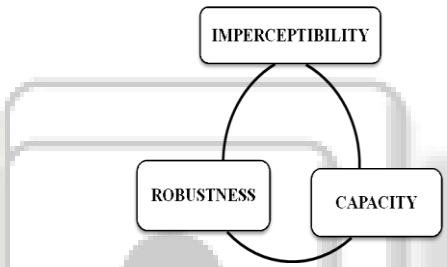

Fig. 2: Trade-off between Capacity, Robustness and Imperceptibility

IX. LSB SUBSTITUTION

A. 9.1 Introduction: In LSB steganography, the least significant bits of the cover media's digital data are used to hide the information message. The simplest of the Least Significant Bit Substitution steganography techniques is LSB replacement[4,5]. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hide in the cover image. Now, Consider an 8-bit image where each pixel is stored as a byte representing a grayscale value of the image. Suppose the value for first eight pixel of the original image have the following grayscale values:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 00001100, we would replace the LSBs of these pixels to have the following new grayscale values:

11010010
01001010
10010110
10001100
00010101
01010111
00100110
01000010.

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.

Both LSB replacement and LSB matching leave the LSB unchanged if the message bit matches the LSB of the cover image. When the information message bits does not match the LSB of the cover image, the LSB replacement technique replaces the LSB of the cover image with the message information bits. The method of LSB matching randomly increments or decrements the data value by one[3]. LSB matching is also known as ±1 embedding. In the case of still grayscale images, every pixel is represented using 8 bits, with 11111111 (=255) representing white and 00000000 (=0) representing black color. Thus, there are levels of 256 different grayscale shades between black and white which are used in grayscale images. In LSB stegonography, the LSB's of the cover image is to be changed. As the message bit to be substituted in the LSB position of the cover image is either 0 or 1, one can state without any loss of generality that the LSB's of about 50 percent pixel changes.

There are three possibilities[3]:

- Intensity value of any pixel remains unchanged.
- Even value can change to next higher odd value
- Odd Value change to previous lower even value

B. 9.2 Simulation Result: Simulations are computed on matlab for image hiding for LSB substitution technique.The results are shown in fig.3.

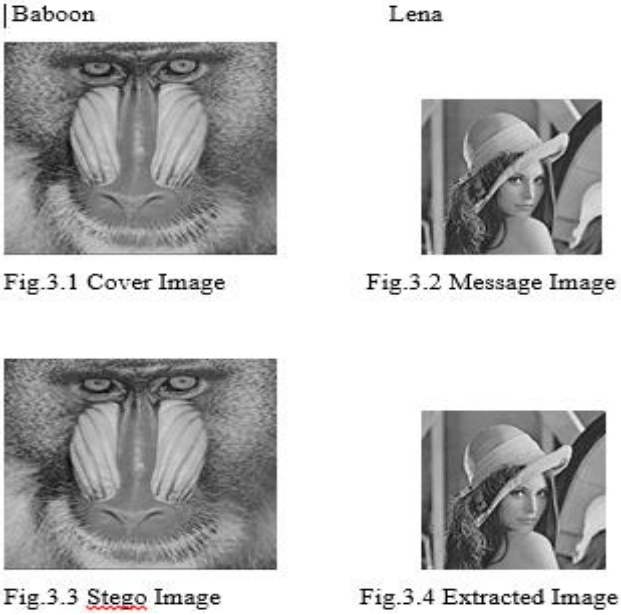

Fig. 3: Image hiding by LSB substitution

The PSNR(db) of message image to extracted image using this technique is 31.7273db.

X. CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a

secret. Digital image steganography and its derivatives are growing in use and application.By observing result, the Least Significant Bit substiution method has higher embedding capacity and generates very high visual quality of image interms of PSNR and well embedding capacity also.

REFERENCES

[1] Vijay kumar sharma ,Vishal shrivastava, "A Steganography algorithm for hiding image in image by improved lsb substitution by minimize detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1, ISSN: 1992-8645.
[2] Shailender Gupta, Ankur Goyal and Bharat Bhushan,"Information Hiding Using Least Significant Bit Steganography and Cryptography",I.J.Modern Education and Computer Science, June 2012, 27-34,DOI: 10.5815/ijmecs.2012.06.04.
[3] Arvind Kumar, Km. Pooja,"Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887),Volume 9– No.7, November 2010.
[4] Toony, Z.; Sajedi, H.; Jamzad, M., "A high capacity image hiding method based on fuzzy image coding/decoding",Computer Conference, 2009, IEEE. CSICC 2009.14th International CSI, vol., no., pp.518,523, 20-21 Oct. 2009 doi:10.1109/CSICC.2009.5349632.
[5] Gutta Sadhana, "Strengthening the Security of Information using Steganography", International Journal of Computer Science and Information Technology Research, Vol. 2, Issue 1, pp: (27-35), Month: January-March 2014.
[6] Muhalim Mohamed Amin,Subariah Ibrahim,Mazleena Salleh,Mohd rozi katmin " Information hiding using steganography ", Universiti Teknologi Malaysia,2003.
[7] Ramadhan Mstafa, Christian Bach, "Information Hiding in
[8] Images Using Steganography Techniques", Norwich University March 14-16, 2013. ASEE Northeast Section Conference 2013.
[9] Jayeeta Majumder, Sweta Mangal, "An Overview of Image Steganography using LSB Technique", IJCA Proceedings on National Conference on Advances in Computer Science and Applications (NCACSA 2012) NCACSA(3):10-13, May 2012.

