Steganography Using Edge Adaptive Image

G.Karthigai Selvi, Leon Mariadhasan, K. L. Shunmuganathan
Department of Computer Science and Engineering
R.M.K Engineering College
Chennai, India
g.karthibe@gmail.com
leon.mariadhasan@in.ibm.com
hod.cse@rmkec.ac.in

***Abstract*— The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. This paper is a tutorial review of the steganography techniques appeared in the literature. Various image steganography techniques have been proposed. In this paper, we investigate steganography techniques and steganalysis techniques. We state a set of criteria to analyze and evaluate the strengths and weaknesses of the presented techniques. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image with high capacity, while it is detectable by statistical analysis such as RS and Chi-square analyses. This paper has proposed a novel LSB image steganography algorithm that can effectively resist image steganalysis based on statistical analysis.**

***Keywords*— Encrypting the text, Locating the edges, Data extraction, Decoding the data.**

I. INTRODUCTION

Steganography is the art and science of writing the hidden data in such a way that no one, apart from the sender and intended recipient, suspects the existence of the data, a form of security through obscurity. Generally, the data will be appearing to be something else: image, articles, shopping lists or some other cover text and classically, the hidden data may be in the form of invisible ink between the visible lines of a private letter.

While steganography is compared to the watermarking, steganography wish to communicate the data in a completely unidentified manner where it does not occur in the watermarking. In watermarking is a recognizable image or pattern in paper that appear as various shades of lightness/darkness when viewed by transmitted light, caused by thickness or density variations in the paper. A watermarking is very useful in the examination of paper because it can be used for dating, identifying sizes, mill trademarks and locations and the quality of a paper. There are two types of watermarking named as visible watermarking and invisible watermarking. Visible watermarking that an object can be seen whereas in invisible watermarking that an object cannot be seen. A watermarked image in which the watermarking is imperceptible, or the watermarked image is visually identical to its original constitutes of invisible watermarking. Examples include images distributed over internet with watermarks embedded in them for copyright protection. Those which fail can be classified as visible watermarks. Examples include logos in the papers in currencies.

One of the most important applications of steganography is digital watermarking. A watermark is the replication of an image, logo, or text on paper stock so that the source of the document can be at least partially authenticated. A digital watermark can accomplish the same function; an artist can post sample images on his website with an embedded signature so that he can prove her ownership in case others attempt to steal his work or try to show as their work.

The following formula can provide a very generic description of the steganography process:

Cover data + hidden data + stego key = stego data

In this formula, the cover data is the file in which we will hide the hidden data, which may also be encrypted using the stegos key. The resultant file is the stegos data which will be of the same type as the cover data. The cover data and stegos data are typically image.

In steganography they have two properties named as, unidentified and fixed data capacity, should be carefully considered while we are going to design with steganography algorithm. Normally, the large amount is fixed in a cover image; the more identified artifacts would be introduced into the stegos. As per many applications, the most important requirement for steganography is unidentified, which means that the stegos should be visually and statistically same to the cover image while keeping the fixed rate as high as possible.

978-1-4673-0210-4/12/$31.00 ©2012 IEEE

LSB replacement is a well-known for steganography method. In this fixing model, only the LSB plane of the cover image is in an original form is kept safe and considered a duplicate form that is made to be overwritten with the help of the secret bit stream according to a Pseudo Random Number Generator (PRNG).

LSB Matching (LSBM) which develops a minor identification to LSB replacement. Suppose the secret bit (unit of information expressed as either a 0's or 1's in an binary notation) that does not match the LSB of the cover image, then insert one or remove one is shuffled to add the corresponding to the picture element of its value is made. Statistically, the probability of increasing or decreasing for each identified picture element value is the same and its clearly understood that is not balanced with artifacts introduced by LSB replacement can be easily reduced.

The pixel values is not dependent, LSB Matching Revisited (LSBMR) uses a pair of picture element as an fixing device, in which the LSB of the first picture element carries one bit of secret data and relationship of the second picture element values carries another bit of secret dat. It is shown that such a new scheme can avoid the LSB replacement style is not balanced, and thus it should make the identification slightly tougher than the LSBM approach based on our experiments.

The LSB-based approaches, includes LSB replacement, LSBM and LSBMR, that deal with each given the picture element / picture element-pair without considering the difference between the picture element and its neighbors.

The edge adaptive scheme has another kind is called as Pixel- Value Differencing (PVD) in which the number of fixed secret data can be extracted the result of stego-image without referring the original cover image, in which the determined by the difference between a picture element and its neighbor. The larger number of secret bits that can be fixed by using the lager values.

The most common of steganography method is by picture element/picture element-pair selection is mainly used to find by PRNG while neglecting the relationship between the image content and size of the secret data.

On the other side, steganalysis can serve as an effective way to judge the security performance of steganography by identifying the hidden data and extracting it from stego-image. The text will be hidden in an image by an invisible ink by using steganography the that particular hidden text is extracted from it an it's brought to a original image it's known to be as cipher text is converted into an plain text and so on.

In the following section we discuss about the related works in section II, system overview in section III and the index terms in section IV, V, VI, VII respectively, conclusion in section VIII and future contribution in the section IX is when in detail.

II. RELATED WORK

In this section we review past work relevant to the problem of hidden the text in an image file and covering it through the video frame and then extracting the hidden file. A literature survey in this area finds an amount of work is done in encrypting the text and decoding the text from an image and video file. In each case we summarize the approach and highlights of contributions, assumptions and limitation.

An approach proposed by M. Goljan in [1] cryptography, which aims to make communication unintelligible to those who don't possess the right keys. Once a third party can reliably identify which images contain secret messages, the stenographic tool becomes useless. Another important factor is the choice of the cover image. The selection is at the discretion of the person who sends the message. Images with a low number of colors, computer art, and images with unique semantic content should be avoided as cover images.

In Zhe Wang [2] proposed to identifying the least - significant- bit (LSB) steganography in the digital signals such as images and audio that the length of hidden data can fix signal samples can be estimated with high precision. The new steganalysis approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. To evaluate the robustness of the proposed steganalysis approach, bounds on estimation errors are developed.

In Andrew D. Ker [3] proposed to identify the spatial domain Least Significant Bit Matching (LSBM) steganography in gray scale images, which is proved much harder than for its counterpart, LSB replacement. The Histogram Characteristic Function (HCF), for the detection of steganography in color images but ineffective on gray scale images. In A.Daneshkhah [4] proposed the two bits of message is embedded in a pixel in a way that not only the Least Significant Bit (LSB) of picture element is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, but the point is in each embedding process only one alternation in one bit plane is allowed to happen. It is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm.

In Q.Huang [5] proposed the problem in LSB Matching Revisited (LSBMR) algorithm to make regions selection on images to find suitable area. By counting on each pixel we can decide if it should be protected. It can improve the visual imperceptibility and detectability of the LSB matching method. By adjusting the parameters of neighbor pixels, the max embedding capacity can be increased as needed.

In A.D.Ker [6] proposed the general framework for detection and length estimation of these hidden messages, which potentially makes use of all the combinatorial structure. It is necessary to screen the Triples method by first applying a standard estimator, because of inaccurate results when the hidden message length is high. A range of experiments verify that this makes for a reliable detector and estimator of hidden messages, performing somewhat better than the standard detectors on uncompressed covers, and very much better on images where the cover has artifacts.

In P.Marwaha [7] proposed the Cryptography and steganography are the most widely used techniques. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

In Andrew D. Ker [8] proposed the This paper draws together two methodologies for the detection of bit replacement steganography: the principle of maximum likelihood, which is statistically well-founded but has led to weak detectors in practice, and so-called structural detection, which is sensitive but lacks optimality and can suffer from complicated exposition. Bringing together the statistical foundations of the maximum likelihood method with the sensitivity of structural steganalysis has been fruitful in terms of new and more accurate payload estimators for bit replacement steganography.

In A.Almohammad [9] proposed the performance of both gray scale and color versions of a given cover image when they are used with a given steganography method. The capability and impact of using the chrominance components for data hiding. There are two steganography methods are used as test methods, JSteg and JMQT. As a result, using color images is better than using gray scale images for data hiding.

In J.Milelikainen [10] proposed the modification to the least-significant-bit Matching (LSBM) choice of whether to add or subtract one from the cover image pixel is random. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. Therefore, the modified method allows embedding the same payload as LSB matching but with fewer changes to the cover image.

In Xinpeng Zhang [11] a novel steganography scheme that employs human vision sensitivity to hide a large amount of secret bits into a still image with a high imperceptibility. In this method, data to be embedded are converted into a series of symbols in a notation system with multiple bases. The specific bases used are determined by the degree of local variation of the pixel magnitudes in the host image so that pixels in busy areas can potentially carry more hidden data. The amount of information carried by individual pixels is adapted to the gray value variation in the immediate neighborhood, realized by using a novel multiple-base notational system. As more data are embedded in busy areas and on edges that can tolerate more changes, the method provides a good imperceptibility with a large quantity of embedded data.

In Ying Wang [12] the purpose of image steganalysis is to detect the presence of hidden messages in cover photographic images. Supervised learning is an effective and universal approach to cope with the twin difficulties of unknown image statistics and unknown steganography codes. A crucial part of the learning process is the selection of low-dimensional informative features. We investigate this problem from three angles and propose a three-level optimization of the classifier. First, we select a sub band image representation that provides better discrimination ability than a conventional wavelet transform. Second, we analyze two types of features—empirical moments of Probability Density Functions (PDFs) and empirical moments of characteristic functions of the PDFs—and compare their merits. Third, we address the problem of feature dimensionality reduction, which strongly impacts classification accuracy.

III. SYSTEM OVERVIEW

The main objective of the proposed system is to hide the data and extract the data from the image. The data hidden in the image is kept secret to the unknown user and file is protected in safety manner. The proposed system consists of mainly two stages: data embedding stage and data extraction stage. Both the data embedding stage and data extraction stage is to cover the data and protect the data in secure manner. The data embedding stage and data extraction stage are used to transfer the data.The figure 1 that shows the proposed system architecture diagram that is given below:

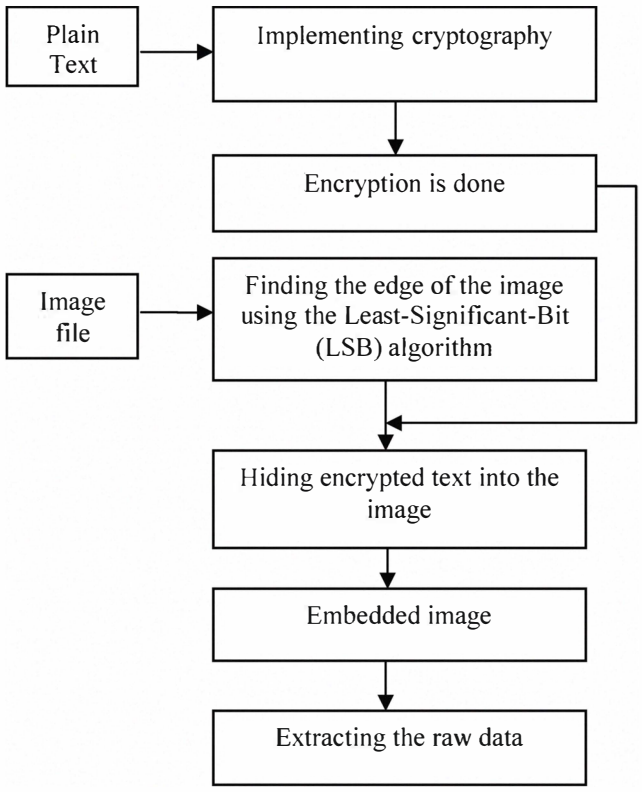

Figure 1 Block diagram of the proposed system

In the data embedding stage, the scheme first initializes some parameters, which are used for subsequent data pre-

processing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message M, then data hiding is performed on the selected regions. Finally, it does some post processing to obtain the stegos image. Otherwise the scheme needs to revise the parameters, and then repeats region selection and capacity estimation until M can be embedded completely.

In data extraction, the scheme first extracts the side information from the stegos image. Based on the side information, it then does some pre-processing and identifies the regions that have been used for data hiding. Finally, it obtains the secret message according to the corresponding extraction algorithm.

At first we are going to encrypt the data into a plain text, by using the Least-Significant-Bit (LSB) algorithm. Then the Least-Significant-Bit (LSB) algorithm used to give safe and protection to the text its encryption in safe location. Normally an encoding is a device that converts information from one format to another format, for the purposes of standardization, speed, security, or saving space by shrinking size. The encrypted data is used to store and recall the information that is unknown to the person cannot read the data.

Algorithm

Input: hide the data.
Output: data is hidden safely in an image file that the unknown is unable to see the hidden data file.
Begin
1. Plain text
2. Encrypting text
3. Implementing the Least-Significant-Bit (LSB)
4. Edge detection
5. Data hiding on sharper edges
6. Stegos image
7. Extraction of information
8. Preprocessing
9. Identification of region
10. Secret message generation
11. Decryption
12. Original image
End

Taking an image file and finding the edge location of an image whether the data can be stored in sharper region/smooth region. Edge detection is a fundamental tool; in image processing and compute vision, particularly in the area of features detection and feature extraction, which aim at identifying the points in a digital image at which the images is made to changes sharply and its more formally has discontinuities.

In data extraction, the scheme first extracts the side information from the stegos image. Based on the side information, it then does some preprocessing and identifies the regions that have been used for data hiding. Finally, it's used to obtain the secret message according to the corresponding extraction algorithm.

Decoding is normally made to be the opposite process -- the conversion of an encoded format back into the original sequence of characters. Decryption, or decipherment, is the process of converting cipher text back into its original format.

IV. ENCRYPTING THE TEXT

Encryption is done normally for recalling the data later from the short term or long term memory. The algorithm or person that converts information from one format or code to another. The purpose of encryption is used for standardization, speed, secrecy, security. Plaintext is the information, which the sender wishes to transmit to the receivers. Plain text simply meant text in the language of the communicating parties. Encryption is the process of transforming information using an algorithm to make it unreadable to anyone. The result of the process is to encrypt the information. It incorporates security where the data resides or the medium through which data is transmitted. In computers, encoding is the process of putting a sequence of characters into a specialized format for efficient transmission or storage. The data chunk is a sequence of integers, one per sample, whose range is specified by the sample rate.

V. LOCATING THE EDGES

There are 2 main ways to hide information in an image file: binary encoding and non- binary encoding. Binary encoding involves modifying certain bits of the cover file to cover the plain text secret message while attempting to make these changes in a way that will not alter the sound file so much that the difference is audible to an observer. Non-binary encoding involves taking advantage of the properties of the sound waves themselves to hide information. It's a fundamental tool in image processing and computer vision. Its aims are to identifying points in a digital image at which the image changes sharply. For lower embedding rates in LSB algorithm, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. In this embedding method which first employs a Laplacian detector is used to detect edges, and then performs data hiding on center pixels whose blocks are located at the sharper edges.

VI. DATA EXTRACTION

Data extraction is the act or process of the retrieving data out of data sources for further data processing or data storage . The import into the intermediate extracting system is thus usually followed by data transformation and possibly the addition of metadata prior to export to another stage in the data workflow. Usually, the term data extraction is applied when data is first imported into a computer by using the primary sources that is used to

measure the data or record the data. The scheme first extracts the side information from the stegos image. Based on the side information, it then does some pre-processing and identifies the regions that have been used for data hiding. Finally, it will obtain the secret message or data according to the corresponding extraction algorithm.

VII. DECODING THE DATA

Decoding is the reverse of encoding. Decoding is the process of translating received messages into code words of a given code. Both the communication theory and coding theory are used for decoding the data. It's the process of translating received message into the code words of a given code. There have been many common methods of mapping messages to code words. These are often used to recover messages sent over a noisy channel, such as a binary symmetric channel. The conversion of an encoded format back into the original sequence of characters. Decryption, or decipherment, is the process of converting cipher text back into its original format. In many contexts, the word encryption also implicitly refers to the reverse process, decryption to make the encrypted information readable again.

VIII. CONCULSION

This project describes an edge adaptive image stenographic scheme in the spatial LSB domain they usually exists some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. To preserve the statistical and visual features in cover images, we have proposed a novel scheme which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges.

IX. FUTURE CONTRIBUTION

In this paper we focused data embedded and data extract from an image using Least-Significant-Bit (LSB) algorithm and then it's hidden the data in an video frame. In future we will try out it in audio steganography in the spatial or frequency domains when the embedding rate is less than the maximal amount.

REFERENCES

[1] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray- Scale Images", IEEE Multimedia, vol.8, no.4, pp.22-28, Oct.2001.

[2] S.Dumitrescu, X.Wu, and Z.Wang,"Detection of LSB Steganography via Sample Pair Analysis", IEEE transactions on signal processing, vol.51, no. 7, Jul.2003.

[3] Andrew D. Ker, "Steganalysis of LSB Matching in Gray scale Images" , IEEE signal processing letters, vol. 12, no. 6, pp. 441-444, Jun. 2005.

[4] Ali Daneshkhah, Hassan Aghaeinia and Seyed Hamed Seyedi, "A More Secure Steganography Method in Spatial Domain", Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.

[5] Qinhua Huang and Weimin Ouyang, "Protect Fragile Regions in Steganography LSB Embedding", 3rd International Symposium on Knowledge Acquisition and Modelling, 2010.

[6] Andrew D. Ker, "A General Framework for Structural Steganalysis of LSB Replacement", in Proc.7th Int. Workshop on Information Hiding, 2005, vol.3427, pp. 296-311.

[7] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in images", 2nd International conference on Computing, Communication and Networking Technologies, 2010.

[8] Andrew D. Ker, "A Fusion of Maximum Likelihood and Structural Steganalysis", in Proc.9th Int. Workshop on Information Hiding, 2007, vol. 4567, pp. 204-219.

[9] Adel Almohammad and Gheorghita Ghinea, "Image Steganography and Chrominance Components", 10th IEEE International Conference on Computer and Information Technology, 2010.

[10] Jarno Mielikainen, "LSB Matching Revisited", IEEE signal processing letters, vol. 13, no. 5, May 2006.

[11] Xinpeng Zhang and Shuozhong Wang,"Steganography Using Multiple-Base Notational System and Human Vision Sensitivity" IEEE signal processing letters.

[12] Ying Wang, Student Member, IEEE, and Pierre Moulin, Fellow, IEEE, "Optimized Feature Extraction for Learning-Based Image Steganalysis" IEEE transactions on information forensics and security, 2007.

[13] Weiqi Luo, member, IEEE, Fangjun Huang member, IEEE, and Jiwu Huang, senior member, IEEE, " Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010.