Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

LSB Steganography Based on Encryption

Mrs. K.Rajasri, Ms. T.Indhumathi
M. Tech.,
Department of CSE,
Christ College of engineering and Technology, India

Mrs. G.Shoba
M.E.,
Department of CSE,
Christ College of engineering and Technology, India

Abstract— Steganography, introduced in 2003, is a techniques employed for concealed message transfer among two secret parties. It is an ability of hidden message transfer. It also relates to the areas like network protocols and security for practical data hiding in communication networks using Transmission Control Protocol/Internet Protocol. The distinctive steganographic technique utilizes digitized media files as a cover medium for hiding data. Network steganography uses message transfer protocols such as TCP/IP. Such methods make it harder to discover and eradicate. In a typical steganography using network the alteration of a distinct network protocol occurs. Such alteration can be applied to the Protocol Data Unit. Network steganography shelters a broad spectrum of techniques. Sampling is used for selection of pixels. Then Gray level Co-occurrence matrix is calculated. The GLCM is the matrix containing information about the relationship between values of adjacent pixel in an image. This is used to classify the original and stego images.

Keywords— Steganography, LSB, Steganalysis, Embedding, GLCM

I. INTRODUCTION

Steganography is a process that involves hiding communication in a suitable carrier for example an image or an audio file. The carrier can then be sent to a recipient with nobody else knowing that it contains a hidden communication. The phrase steganography means "covered or hidden writing". The purpose of steganography is to transmit communication through some inoffensive carrier. Computer based Steganography allows alterations to be prepared to what are recognized as digital carriers such as images or sounds. The changes characterize the hidden message, but outcome if triumphant in no visible change to the carrier. The information may not be able to do anything by means of the carrier sound or picture or it might be information about the carrier such as the writer or a digital watermark or fingerprint.

Cryptography and steganography are dissimilar. Cryptographic techniques can be used to jostle a communication so that if it is exposed it cannot be read. But, Steganography aims at hiding the existence of a message within the carrier. Images are the most extensive carrier medium used in the field of steganography. Pictures are the most familiar and well-situated means of conveying or transmitting information. A picture is worth a thousand words. Images quickly express information about positions, sizes and inter relationships between things. They depict spatial information that can be able to identify as objects. Human beings are good at deriving information from such images, because of our innate visual and mental abilities. About 75% of the information received by human is in pictographic category. A picture is digitized to change it to a type which can be stored in a computer's memory or on some form of storage media such as a hard disk or CD-ROM. This digitization process can be prepared by a scanner, or by a video camera linked to a frame grabber board in a PC. Once the picture has been digitized, it can be operated upon by a variety of image processing operations.

A digital image is a photograph in that the values are all discrete. Usually they take on only integer values. The brightness values also range from 0 to 255. A digital image can be considered as a large array of discrete dots, each of which has a brightness associated with it. These dots are called picture elements, or more only pixels. The pixels contiguous to a given pixel comprise its neighbourhood. A neighbourhood can be characterized by its form in the same way as a matrix. Except in very special circumstances, neighbourhoods have odd numbers of rows and columns; this ensures that the existing pixel is in the centre of the neighbourhood.

Watermarking is embedding a hidden message within the original data "host image". A digital watermark is a type of indicator secretly embedded in a noise-tolerant signal such as audio or image information. It is characteristically employed to recognize possession of the patent of such signal. "Watermarking" is the process of hiding digital information in a carrier signal. The hidden information should not be required to hold a relation to the carrier signal. Digital watermarks may be employed to confirm the authenticity or integrity of the carrier signal or to explain the uniqueness of its owners. It is notably employed for tracing copyright infringements and for banknote verification. Like traditional watermarks, digital watermarks are just detectable under certain situations.

Our main contribution in this paper is to employ the GLCM which provides the relationship between values of adjacent pixel in an image. This can be used in the effective steganalysis method. The organization of this paper is as follows. In the subsequent part a number of preceding steganography and steganalysis methods are concisely discussed.

Section III is dedicated to the explanation of the existing process. Section IV is dedicated to the proposed steganalytic system. In this section, we first introduce our inspiration and then present GLCM which is helpful in deciding the pixel values relationship. The conclusions are drawn in Section V.

II. LITERATURE SURVEY

Data hiding is a technique of concealing clandestine information into a cover media and preventing a viewer from being aware of the survival of the hidden message as in [6]. The only function of steganography is to hide the fact that any communication is taking place as in [7]. Steganography can be used to store information on a locality. While digital steganography aims to embed top secret communication into digital media for covert message transfer, the reason of steganalysis is to notice the existence of clandestinely hidden data in a digital media as in [2]. Steganalysis involves detecting the employ of steganography inside of a file with little or no knowledge about the steganography algorithm and/or its parameters. The objective of steganalysis is to notice the existence of clandestinely concealed data in an object as in [3]. Steganography is not equal to watermarking as in [9]. Steganographic algorithms sometimes leave a signature in the file that is encoded. With this knowledge, the presence of secret communiqué can be detected. It is reasonable to say that steganalysis is both an art and a science. The art of steganalysis plays a foremost function in the selection of characters or features to check for hidden messages while the science helps in designing the tests themselves.

The picture gradient information is disintegrated into local histograms over contrast intensity as in [5]. Many steganalytic techniques which have been developed in recent times may fall under one of these two classes: ad hoc schemes and feature based schemes that are generic and that use classifiers to differentiate original and stego images. Feature based steganalysis is the growing division in information forensics and protection. Its ultimate aspire is to recognize the existence of a secret message. This can be done by employing the statistical features of the cover and stego image as clues/evidences. The feature based system works in two steps – extraction of generic feature vectors and training a classifier with these features to separate stego images from original images. Support vector machines is utilized to build the blind classifiers as in [1]. Feature based schemes have been studied more recently and found to be more reliable. Since the amount of audit facts and the features that such a steganalyzers needs to inspect is very bulky, categorization by hand is unfeasible. Analysis is not easy even with computer assistance because superfluous characters can make it harder to detect suspicious behaviour patterns.

Steganalysis can be universal or specific. Universal steganalysis enables to recognize stego images whatever the steganographic system be used. Universal steganalysis is also known as blind steganalysis. It is more applicable and sensible than the specific steganalysis. This is for the reason that it can notice a larger class of stego images; it is generally less accurate for one given steganographic algorithm. There are several reasons to scale the target values while training the classifiers as in [4].

LSB-based steganography uses the lowest bit plane of an image to communicate the secret data as in [8]. This method has been used by many Steganographer. This is because the eye cannot notice the very little perturbations which are introduced into an image by this method. It is also enormously easy to execute.

III. EXISTING SYSTEM

Two inputs are necessary for the embedding procedure as in Fig.1.

- Secret message: generally a text file that contains the message the user wants to transfer.
- Cover work: used to create a stegogramme that contains a secret message, it may be text, image, video clips or sounds.

The next step is to pass the inputs through the Stego-system encoder, which will be cautiously engineered to embed the message within an exact copy of the cover work. The resultant output from the stego-system encoder is the stegogramme, which is planned to be as close to the cover work as doable, apart from it will contain the secret message. This stegogramme is then sending over some communications channel. So, steganography is concerned with hiding information in some cover medium, by manipulating properties `of the medium in such a way that the hidden information is not easily visible by an observer.

Also it is one of the information hiding techniques that can be categorized into linguistic steganography and technical steganography. Linguistic steganography can defined as "the art of using written natural language to conceal secret communication". A more specific definition explains linguistic steganography as a medium which required not only the steganographic cover that is composed of natural language text, but the text itself can be also generated to have a cohesive linguistic structure, or the cover text that begin with natural language. On the other hand, technical steganography is explained as a carrier rather than a text.

In existing scheme a reversible data hiding system based on histogram alteration is employed for the steganography process. The histogram modification method involves generating histogram and finding the peak point and the zero point and shifting histogram bins to embed message bits. For a given host image, we primarily create its histogram and find a peak point and a zero point. A peak point corresponds to the gray scale value which the maximum number of pixels in the given image assumes. On the converse, a zero point corresponds to the gray scale value which no pixel in the given image assumes. Let P be the value of peak point and Z be the value of zero point. The range of the histogram, [P+1, Z-1], is shifted to the right-hand side by 1 to leave the zero point at P+1. Once a pixel with value P is encountered, if the message bit is "1," increase the pixel value by 1. Otherwise, no conversion is essential. We note that the number of message bits that can be embedded into an image equals to the amount of pixels which are associated with the peak point. For recovering data, the side information, namely peak points and the location map, should be sent to the recipient.

In several blind statistical steganalyzer, the classifier used for pattern identification plays an essential role. In this work we use three different classifiers to evaluate the features extracted. They are Artificial Neural Networks, Support Vector Machines and Random Forests. The well-designed freedom for these classifiers consists of five variables, the four Huffman Length Statistics; H**2**, H**3**, H**4** and H**5**and FR Index and is designed for binary classification to differentiate stego images from genuine ones. To teach and test each classifier for each of the 16 combinations of YASS settings, the following steps are followed:

The image database is separated into a number of combinations of training and testing sets for each of the 16 YASS settings tested. In each trial, 60% of the data is used for training the classifier. To evaluate the accuracy of the model, the minimal total average probability of error is computed and is given by:

$P_e = (P_{FP} + P_{FN})/2$ where P_{FP} and P_{FN} are the probability of false positives and false negatives of the test images correspondingly.

The drawback of this approach, especially in the watermark embedding is that a watermark should be inserted at the occasion of demo, which would limit this approach to specifically equipped digital cameras and there is a chance of distortion to occur in histograms.

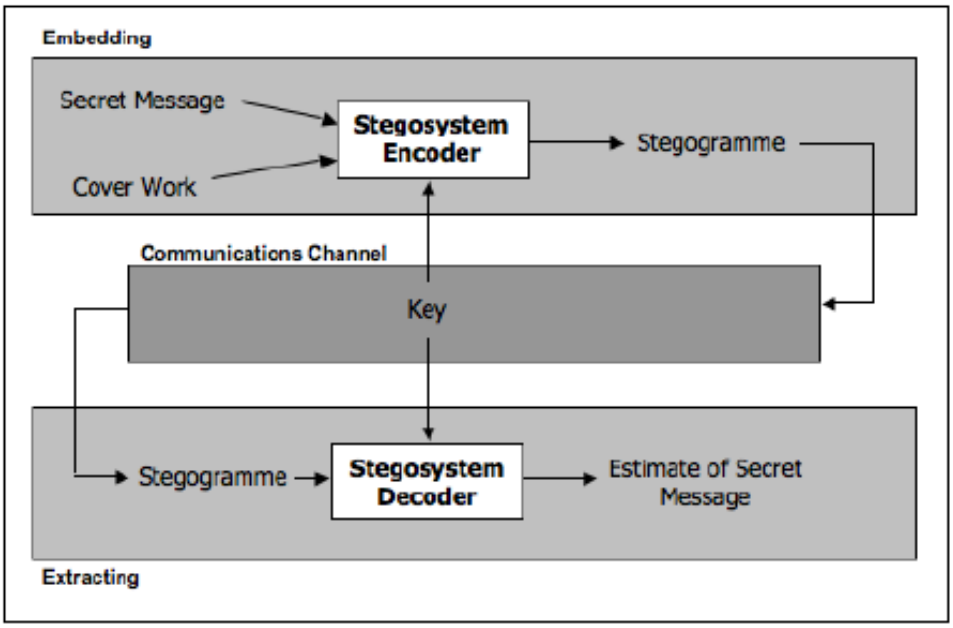

Fig. 1: Basic steganography system

IV. **PROPOSED SYSTEM**

The robust steganalytic scheme is proposed in this paper. After sampling is completed, GLCM is constructed. The GLCM is the matrix containing information about the relationship between values of adjacent pixel in an image. Number of fields in the header of TCP/IP is complimentary and optional. This can be worked for the spread of information secretly.

In our technique we have mostly four components as sampling, encryption, embedding and decryption. Sampling plays a key function here in our process. It involves the uniform choice of pixels for encryption which strengthen the steganography process. Encryption is the process where implementing algorithms, we apply our tricks to match all steganographic features. Then we embed the communication in the sampled pixels with well-built and efficient algorithm. Subsequently use the decryption method to retrieve the image in the receiver end.

A. Sampling

Sampling is intricately connected with victorious steganography and plays an essential responsibility in the procedure. In this paper, we have explored an extremely protected and weight balanced algorithm to obtain variable samples spread evenly throughout the cover image. This paper explores a highly secure method of image steganography. The samples are selected based on the input cover object, secret massage and the stego key. Further, a striking feature of the sampling purpose is that the sample count decreases exponentially as we move inwards from the periphery to the Centre of the picture. This is based on the idea that the centre of the picture is typically more meticulously noticed and focused on by the human eye, and peripheral parts generally attract lesser meticulous keen notice. The sampling is strengthened keeping in mind the visible changes in the histogram, thereby repulsing steganalysis cleverly. Further, the purpose ensures that roughly equal number of pixel samples have been selected from all four quadrants, to prevent clustering of samples from a single one.

Then, we obtained the GLCM from a cover image. It is calculated by the addition of the main breadth values and named it as S-image. We then use this for embedding process.

B. Encryption

We encrypt the secret message using a 2 – level encryption task. The first level of encryption is based on the secret message and stego-key. The second level encryption parameters consist of the intermediate message and the secret message. We perform a stego- key based cyclic alterations of the secret message followed by inter operable second level encryption.

C. Decoding And Decryption

The initial phase consists of retrieving the necessary information necessary for decoding from the corner pixels. In the first step it is required to recover two significant parameters from the encrypted image as secret message size and order of the stego images. Then we intend decoding the original message from the stego image and concatenate them in order to obtain the secret message. We first, apply the sampling algorithms to obtain the samples used for encoding.

The PSNR and MSE values are also better in this method as compared to prior techniques.

V. CONCLUSION

PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error) and histogram analysis of stego image is calculated. With the raise in cover image dimension extra secret information can be embedded. As only very last bit of each pixel get changed so there is insignificant alter is histogram which makes stego-image visually impossible to differentiate from the unique cover-image. In addition PSNR value is extremely high and MSE is reasonably small which explain stego quality is very excellent. Since the quality of stego-image is better, it makes it tough for illegitimate person to identify that information has been embedded in the image. By increasing the payload ability, large amount of clandestine bits can embed in cover image. The performance of the projected scheme is better-quality than those of previous schemes, leading to the development of new steganalytic technique. The image quality will be retained until the process is fulfilled.

REFERENCES

[1] Zhuo Li, Kuijun Lu, Xianting Zeng and Xuezeng Pan, *A Blind Steganalytic Scheme Based on DCT and Spatial Domain for JPEG Images* , Journal of Multimedia, Vol. 5, No. 3, June 2010.

[2] Fengyong Li, Xinpeng Zhang, Bin Chen, and Guorui Feng, *JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier*, IEEE Signal Processing Letters, Vol. 20, No. 3, March 2013.

[3] Jan Kodovský, Jessica Fridrich and Vojtech Holub, *Ensemble Classifiers for Steganalysis of Digital Media*.

[4] Chih-Chung Chang and Chih-Jen Lin, *Training v-Support Vector Regression: Theory and Algorithm*.

[5] Silvio Borer, *New support vector algorithms for multicategorical data applied to real-time object recognition*.

[6] Parisa Gerami, Subariah Ibrahim and Morteza Bashardoost, *Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment* , International Journal of Computer Applications (0975 – 8887) Volume 55– No.2, October 2012.

[7] Menka Goswami, Vishal Gupta and Anil Kumar, *LSB Steganography based on Variable Key Encryption*, International Journal of Computer Applications (0975 – 8887) Volume 78 – No.2, September 2013.

[8] Sedighe Ghanbari, Manije Keshtegary and Najme ghanbari, *New Steganalysis Method using Glcm and Neural Network*, International Journal of Computer Applications (0975 – 8887) Volume 42– No.7, March 2012.

[9] Firas A. Jassim, *A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method*, International Journal of Computer Applications (0975 – 8887) Volume 72– No.17, June 2013.

[10] Joshi Rana, Amanpreetkaur and Nitin Malik, *Network-based Steganography using Encryption in TCP/IP Header*, International Journal of Computer Applications (0975 – 8887) Volume 74– No.4, July 2013.

