ISSN:0975-9646

A Study on Different JPEG Steganograhic Schemes

Alphy Ros Mathew, Sreekumar K

Department of Computer Science, College of Engineering,Ponjar,
Cochin University of Science And Technology
Kottayam,Kerala,India

***Abstract*-Steganography is an art of secret communication in which the information to be exchanged is hiding in some kind of media where it is not easily noticeable by the third party. Among different kinds of steganography, image steganography is the kind in which images are used as the medium of communication in which secret messages are embedded in the image. Several types of mechanisms are available for efficiently implementing steganography using images. Also different formats of images can be used for steganography, among which JPEG is the most suitable one. Since steganography is used for covert communication purposes, the security of the data that is being shared is very important, so that it should not be easily recoverable. So the mechanisms for implementing steganography are very important. In this paper, we analyze different types of JPEG steganographic schemes.**

***Keywords*-Statstical Embedding, Distortion Function, Steganalysis**

I. Introduction

Steganography is the way of secret communication in which messages are concealed within a media. So there may not be any chance to identify the existence of communication. Steganography is contrast to cryptography in which the message can be identified and modified against certain security goals provided by the cryptographic algorithms, in steganography the message is hidden inside another message which will hide the existence of the actual message. Both of them has its own advantages and disadvantages, but they can be used in combination to provide multiple layers of security.

Steganography can be used with different types of media. The media can be anything such as audio, video, image, text, network protocol etc in their digital form. These can be called as cover object and after the hiding process it is called as stego-object. Steganography is an information hiding process i.e. the actual content of the information is not altered, but the information is hiding into information which is the carrier. A key is also used to restrict the detection of the hidden information from external parties. Steganography has wide range of applications especially in the internet area where security and privacy are very important factors.

II. Overview Of Image Steganography

Image steganography one the main types of steganography in which the message is hidden inside an image. The four main terminologies in the image steganography are:

i. Cover image – the original image in which the message is embedded.
ii. Message – the data that is to be exchanged between two parties. It can be in the form of text or image.
iii. Stego image – the cover image after the embedding operation.
iv. Stego key – the key for embedding and extracting the message to and from cover image.

The main classifications of image steganography are:

i. High capacity – the maximum size of message that can be embedded into the image.
ii. Perceptual transparency - After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover-image.
iii. Robustness – after embedding operation, the stego-image should be inert against operations such as cropping, scaling, transformation, addition of noise etc.
iv. Temper Resistance – once the message has been embedded into stego – image, it should be difficult to alter the message.
v. Computation Complexity – computational expense for embedding and extracting a hidden message.

Main image steganographic techniques are:

i. Spatial domain methods - directly change some bits in the image pixel values for hiding data. Spatial domain techniques are broadly classified into:
   - Least significant bit (LSB)
   - Pixel value differencing (PVD)
   - Edges based data embedding (EBE)
   - Random pixel embedding (RPE)
   - Mapping pixel to hidden data
   - Labelling or connectivity
   - Pixel intensity based method
   - Texture based method
   - Histogram shifting methods

ii. Transform domain methods – this is the complex way of steganography in which different steganographic algorithms are used. These are more appropriate than spatial methods because they are less exposed to cropping, compression and image processing. Transform domain techniques are classified into:

- Discrete Fourier transformation (DFT).
- Discrete cosine transformation (DCT).
- Discrete Wavelet transformation (DWT).
- Lossless or reversible method (DCT)
- Embedding in coefficient bits

iii. Distortion techniques – the data is stored by applying a series of changes to the cover image. This technique needs information about the stego image in order to retrieve the original data.

iv. Masking and filtering – works in the same way as watermarks.

III. JPEG STEGANOGRAPHY

JPEG stands for Joint Photographic Experts Group which is a lossy compression technique in which redundant bits are eliminated in order to perform compression. Since it is a lossy compression technique, it may not be suitable for steganography. But in real cases, JPEG compression algorithm is divided into two phases – DCT[1] and the quantization phase forms the lossy stage, and lossless stage is the Huffman encoding used to further compress the data. Steganography can take place between these two stages.[2] The figure shows basic steganographic process.

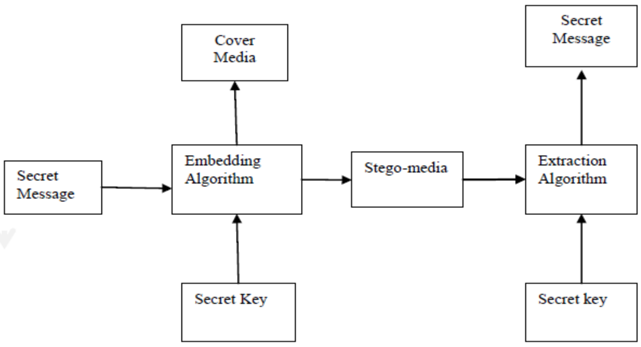

Fig.1 Basic steganographic process

As stated earlier, there will be cover image for embedding data and after embedding the cover image will become stego image. To conceal the occurrence of the secret communication, the stego image must be statistically undetectable from its cover image. So, undetectability and embedding payload are two important parameters while considering the steganographic schemes. While designing a steganograhic scheme, the important factor to consider is the cost or distortion function, i.e. minimizing the embedding distortion for a given payload. With a properly designed distortion function, the stego images will become statistically undetectable.

JPEG is the widely used format for image storage and transmission. There are several schemes that developed for JPEG steganography such as F5, nsF5, MME and several other schemes. All these schemes came under minimal distortion embedding which consists of a coding unit and distortion function. In F5, the impact of embedding is treated equally for each co-efficient. So minimizing the distortion for a given payload results in minimizing the number of co-efficient to be modified. This will maximize the embedding efficiency i.e. the no of co-efficients to be modified.nsF5 is an improved version of F5 in which wet paper code (WPC) is used instead of Hamming code used in F5. This will help to avoid the shrinkage problem associated with F5. In MME (Modified Matrix Encoding) side information of the uncompressed image is used to construct the distortion function. Co-efficients with less distortion are only modified. Another scheme is the one which uses the block entropy of DCT co-efficients and syndrome trellis coding. The proposed cost function explores both the block complexity and distortion effects due to flipping and rounding errors.

Corresponding to the development of steganography, steganalysis also is of vital importance. Steganalysis is the study of detecting messages hidden using steganography. Steganalysis is done by rich models using steganalysis feature sets like CC-PEV-548D.Use of ensemble classifiers leads to the detection of even most efficient steganographic algorithms with high accuracy. Hence, the secure payload of JPEG steganography is decreased, which results in new challenges on modern JPEG steganography. Therefore, developing more secure JPEG steganographic algorithm is of vital importance.

A good JPEG steganographic scheme involves an efficient steganographic coding unit and an effective distortion function. Here, we focus on the design of a new additive distortion function for JPEG steganography. An efficient JPEG steganographic scheme is then developed by incorporating the distortion function in the STC framework, which has better working capability against the popular steganalyzers with various feature sets, e.g., CC-PEV-548D, IBC-EM-882D, MP-486D[4], and the recently emerged CC-JRM- 22,510D In addition, the original BMP image can be used as precover (side information) to further improve the security performance of our method.

IV. DIFFERENT JPEG STEGANOGRAPHIC SCHEMES

A. F5

Visual and statistical attacks are the important attacks affect the steganography. Those systems without these problems offer only a relatively small capacity for steganographic messages. F5 is the scheme that withstands both visual and statistical attacks, in addition to large steganographic capacity. Matrix encoding is used to improve the efficiency of embedding which reduces the number of necessary changes[2]. To uniformly spread out the changes over the whole steganogram, F5 use permutative straddling.

Image files provide a limited steganographic capacity comparing to streaming media (especially video). Part of the file remains unused in many cases since the embedded message does not require full capacity. The start of the file is used for embedding and the unused part is usually the end of the file. To prevent attacks, the embedding function should use the carrier medium as regular as possible and embedding density should be the same everywhere.

To increase the embedding efficiency, several schemes are used such as permutative straddling and matrix encoding. First, all those co-efficients used in the straddling mechanism of F5 shuffles all the co-efficients using the permutation[2]. Then, F5 is embedded into the permuted sequence. The numbers of co-efficients are not changed due to the shrinkage (only their values). The permutation depends on a key derived from a password. F5 delivers the steganographically changed coefficients in its original sequence to the Huffman coder. With the correct key, the receiver is able to repeat the permutation. The permutation has linear time complexity *O*(*n*). If most of the capacity is unused in a steganogram,[2] matrix encoding decreases the necessary number of changes. For example, if we embed a very short message comprising only 217 bytes (1736 bits), F4 changes 1157 places in the *Expo* image. F5 using matrix encoding embeds the same message with only 459 changes, which results in an embedding efficiency of 3.8 bits per change.

B. nsF5

F5 decreases the absolute value of DCT coefficients and incorporates matrix embedding - a coding scheme that decreases the number of changes and consequently increases the steganographic security. F5 embeds only into nonzero AC DCT coefficients; if a coefficient becomes zero after embedding (the so called *shrinkage*), the same bit is re- embedded at the next coefficient [3]. Shrinkage substantially decreases the embedding efficiency as the values +1 and -1 are the most frequent nonzero DCT coefficients in natural images. The effect of shrinkage can be alleviated by applying more sophisticated coding schemes, such as wet paper codes (WPC) or syndrome trellis codes (STC).The algorithm nsF5 was introduced as an improved version of F5, which uses wet paper codes to overcome the negative effect of shrinkage [3]. The theoretical bound on the embedding efficiency of the nsF5 algorithm is equal to,

$$e = \frac{\alpha}{H-1_{(\alpha)}}$$

where alpha is the relative payload with respect to the number of changeable coefficients (the number of nonzero AC DCT coefficients in the image) and H^{-1} stands for the inverse of the binary entropy function. From a given value of the embedding efficiency e, one can easily calculate the number of embedding changes that nsF5 would introduce.

Side information unavailable to the decoder can be used by wet paper codes. In F5, the decoder reads the message from non-zero DCT coefficients [3]. Thus, when a DCT coefficient is zeroed out, the decoder does not know that it was originally nonzero. This problem can be overcome using syndrome coding similar to matrix embedding. Wet paper codes can eliminate the shrinkage problem by using random matrix. Routine that simulates the embedding changes as they would be carried out in the F5 algorithm coupled with wet paper codes is called no-shrinkage F5(nsF5).

C. MME

MME stands for modified matrix embedding which is an enhancement of matrix encoding. In this mechanism, the message is embedded into the LSB's of the cover image. The advantage of this method is that distortion of the stego - image is less comparing to cover image. The main advantage of the matrix encoding was only one bit from a block of bits are needed to embed several bits. In the modified matrix scheme, the size of the block is increased as two compared to F5 [4]. All non-zero AC co-efficients are marked for embedding after computing the DCT and this form rounding error after embedding. The block size is increased by improved versions of MME such as MME3, MME4 etc [4].

Using modified LSB for information hiding results in distortion of cover images. Steganalysis algorithms use these distortions to detect whether the object is modified or not. Those co-efficients which does not result in large distortion can be used for embedding. This algorithm introduces a new method for information hiding in the LSB's of JPEG co-efficients. This algorithm uses modified matrix encoding to choose the coefficients whose modifications introduce minimal embedding distortion. We derive the expected value of the embedding distortion as a function of the message length and the probability distribution of the JPEG quantization errors of cover images [4]. The experiments show close agreement between the theoretical prediction and the actual embedding distortion. The algorithm can be used for both steganography and fragile watermarking as well as in other applications in which it is necessary to keep the distortion as low as possible.

D. Steganographic scheme based on block entropy of DCT co-efficients

The block entropy of DCT coefficients are used to find the local complexity of the JPEG image and are adopted for the design of the cost function in JPEG steganography. Entropy in information theory refers to the uncertainty of the information source. As the entropy increases the structure of the information source decreases. The main feature of this mechanism is that the cost function is associated with Syndrome Trellis Codes which in effect improves the performance in terms of secure payload. The cost function in this mechanism analyzes both the distortion effects and block complexity due to flipping errors and rounding errors. There are many ways to embed messages to the block of co-efficients using STC. Among which STC uses only the method which have minimal distortion effect. Because of this, the total distortions are significantly reduced, which leads to less detectability of message in steganalysis.

In this scheme, the messages are embedded in the hard to predict area of images thus by achieving less detectability [7]. The image regions with high complexity correspond to the ones of less predictability. High complexity areas can be texture and edges. The block entropy of the quantized DCT coefficients in JPEG compressed domain can be used as the metric to evaluate the complexity of the corresponding 8*8 image block. The proposed cost function takes into account both distortion effects due to rounding and block entropy. With this cost function the blocks with higher entropy and small flipping errors have the highest priority to get modified. This framework for JPEG steganography utilizes the syndrome-trellis coding (STC) [1] for data hiding and the new distortion function for embedding efficiency optimization, which includes the encoder and decoder. The encoding process is described as follows:

i. Input
ii. Compute block entropy cost and cost due to flipping error
iii. STC coding
iv. Stego JPEG image

The decoding is the reverse of the encoding procedure.

E. Heuristic optimization and BCH syndrome coding

Here we presents an efficient JPEG steganography method based on heuristic optimization and BCH syndrome (Bose-Chaudhuri-Hochquenghem) coding [5]. Traditional data hiding approaches hide data into each block, where all the blocks are not overlapping each other. However, in the proposed method, two consecutive blocks can be overlapped to form a combined block which is larger than a single block, but smaller than two consecutive non-overlapping blocks in size. In order to embed more amounts of data into the combined block than a single block, the BCH-based data hiding scheme has to be redesigned. The proposed scheme reduces the distortion by adding or removing AC co-efficients 1 or -1 in the most appropriate locations. This technique for data hiding is based on structured BCH syndrome coding. This method finds solutions to hide data in a block of co-efficients and it chooses the best method with minimum distortion effect [5].So, the total distortion can be reduced, which results in less detectability of the steganalysis. The proposed heuristic optimization significantly decreases detectability of the steganalysis. The proposed methods also outperform the existing steganography methods.

V. Steganalysis

Steganalysis is the study of detection of hidden images in a media. This is similar to that of cryptanalysis in cryptography. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. Steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a payload. The steganalyst is usually something of a forensic statistician, and must start by reducing this set of data files (which is often quite large; in many cases, it may be the entire set of files on a computer) to the subset most likely to have been altered.

A. Using Rich Models

Rich model is built systematically as a union of smaller sub models formed as joint distributions of DCT coefficients from their frequency and spatial neighbourhoods covering a wide range of statistical dependencies [8]. Due to its high dimensionality, combine the rich model with ensemble classifiers and construct detectors for six modern JPEG domain steganographic schemes: nsF5, model-based steganography, YASS, and schemes that use side information at the embedder in the form of the uncompressed image: MME, BCH, and BCHopt[8]. The resulting performance is contrasted with previously proposed feature sets of both low and high dimensionality. We also investigate the performance of individual sub models when grouped by their type as well as the effect of Cartesian calibration[8]. The proposed rich model delivers superior performance across all tested algorithms and payloads.

B. Using Ensemble Classifiers

Today, the most accurate steganalysis methods for digital media are built as supervised classifiers on feature vectors extracted from the media. The tool of choice for the machine learning seems to be the support vector machine (SVM)[9]. A new method of machine learning tool known as ensemble classifier which is implemented as random forests is a better choice for steganalysis. Ensemble classifiers have large no of training examples and the performance is lie complex comparing to SVM. Because of the lower training complexity, the steganalyst has to work with high-dimensional cover models and train on larger training sets – two key elements that appear necessary to reliably detect modern steganographic algorithms. Ensemble classification is a powerful developer tool that allows fast construction of steganography detectors with improved detection accuracy across a wide range of embedding methods. The power of the proposed framework is demonstrated on three steganographic methods that hide messages in JPEG images.

VI. Conclusion

Various mechanisms for implementing JPEG steganography such as F5, nsF5, MME, mechanism based on block entropy of DCT co-efficients and BCH syndrome are studied. The most basic mechanism is F5 and nsF5 (also known as no-shrinkage F5) is an enhancement of F5 in which the shrinkage problem is eliminated. Another mechanism is modified matrix encoding in which an uncompressed image format is used for generating distortion function. The other mechanism is the one which uses the block entropy of DCT co-efficients in which problems due to flipping and rounding errors are eliminated. In steganography, steganalysis is important which is used for finding the secret message and to measure the security of the algorithms. Steganalyzers uses various feature sets for analyzing the security features of steganographic algorithms. Ensemble classifiers results in finding weak steganographic algorithms which in turn leads to the development of more efficient JPEG steganographic schemes.

Acknowledgement

I sincerely express my gratitude to everyone who supported me to prepare this paper. I am thankful for their aspiring guidance, invaluably constructive criticism and friendy advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the work.

REFERENCES

[1] T. Filler, J. Judas, and J. Fridrich, “Minimizing additive distortion in steganography using syndrome-trellis codes,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 920–935, Sep. 2011.

[2] A. Westfeld, “F5—A steganographic algorithm,” in *Proc. 4th Inf. Hiding Conf.*, vol. 2137. 2001, pp. 289–302.

[3] J. Fridrich, T. Pevný, and J. Kodovský, “Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities,” in *Proc. 9th ACM Workshop Multimedia Security*, Dallas, TX, USA, Sep. 2007, pp. 3–14.

[4] Y. Kim, Z. Duric, and D. Richards, “Modified matrix encoding technique for minimal distortion steganography,” in *Proc. 8th Inf. Hiding Conf.*, vol. 4437. Jul. 2006, pp. 314–327.

[5] V. Sachnev, H. J. Kim, and R. Zhang, “Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding,” in *Proc. 11th ACM Workshop Multimedia Security*, Sep. 2009, pp. 131–140.

[6] T. Filler and J. Fridrich, “Design of adaptive steganographic schemes for digital images,” *Proc. SPIE*, vol. 7880, p. 78800F, Jan. 2011.

[7] C. Wang and J. Ni, “An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients,” in *Proc. IEEE ICASSP*, Kyoto, Japan, Mar. 2012, pp. 1785–1788.

[8] J. Kodovský and J. Fridrich, “Steganalysis of JPEG images using rich models,” *Proc. SPIE*, vol. 8303, p. 83030A, Jan. 2012.

[9] J. Kodovský, J. Fridrich, and V. Holub, “Ensemble classifiers for steganalysis of digital media,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.