Eigenvalue Steganography Based on Eigen Characteristics of Quantized DCT Matrices

Yasser M. Behbahani, *Member*, *IEEE*, Parham Ghayour, *Member*, *IEEE*, Amir Hossein Farzaneh
Department of Electrical and Computer Engineering
Shahid Beheshti University
Tehran, Iran

***Abstract*—In this paper we propose a new JPEG-based steganography technique, using eigenvalues' properties of matrices of quantized DCT coefficients. We call this new approach, Eigenvalue Steganography. Usual steganography techniques based on JPEG images, hide data by changing the least significant bit (LSB) of DCT coefficients. Eigenvalue Steganography technique hides confidential data employing the eigenvalues of quantized DCT matrices and manipulating them. This technique suggests the subdivision of quantized DCT coefficients blocks into smaller submatrices in DCT domain. Afterwards, this technique efficiently hides confidential information among DCT submatrices, by employing the proposed algorithms and manipulating the eigenvalues of these submatrices. Experiments done in this paper, depicts that the two proposed methods to implement Eigenvalue Steganography show appropriate resistance against Subtractive Pixel Adjacency Matrix (SPAM) steganalyzer. This steganalysis model doesn't have the capability of proper detection for the suggested methods.**

Keywords-Eigenvalue; Steganography; Information Security; Quantized DCT

I. INTRODUCTION

Digital steganography is a subset of communication science in which a confidential cryptic data or a message is hidden inside an innocent object via a transmitter. With the knowledge of steganography technique and having the stego key (password used in transmitter), the receiver tends to extract and reveal the confidential information from stego object (object carrying a confidential information). As we move toward the age of information technology, we interfere with developed modern steganography techniques which take the multimedia communication as a host in order to send confidential data securely. In modern steganography techniques these hosts are introduced as video, image, and audio files; and among them, graphical and pictorial files are of the most popularity. There are many steganography techniques based on JPEG compressed images (JPEG-based steganography techniques) inherited from their universality in use and comprehensive continuous tone [1], [2], [3], [4].

Alongside the steganography techniques which are predicated upon JPEG images, there exist intelligent JPEG-based steganalysis techniques whose duties are to detect the stego images (images which carry a message) [5], [6], [8]. Various touchstones exist to compare developed steganography techniques based on JPEG compressed images; the most important of them all are:

1) Resistance against steganalysis techniques.
2) Embedding Capacity and Embedding Efficiency of steganography technique (Embedding Efficiency is said to be the ratio of hidden message bits to the scale of changes in image).

In prevalent JPEG-based steganography techniques, the confidential message bits are hidden by manipulating the least significant bit (LSB) of DCT coefficients in frequency domain of image.

In this paper, we propose new technique to hide confidential information in DCT domain of JPEG compressed images by using eigenvalues' characteristics of matrices of quantized DCT coefficients. We call this technique, Eigenvalue Steganography. In this technique, we subdivide 8×8 DCT blocks of image into smaller non overlapping submatrices of size 2×2. Each of these submatrices carries attributes named eigenvalues and eigenvectors. In Eigenvalue Steganography, changing these attributes, the transmitter hides the desired data in DCT coefficients of image. The receiver terminal is able to extract the confidential message by utilizing proper division of 8×8 blocks in DCT domain and generating 2×2 submatrices and calculating their eigenvalues afterwards.

In this paper, we design and implement Eigenvalue Steganography in two methods. The experimental results which are presented in Section IV, shows that these two methods has a great resistance against SPAM steganalysis method. Also Eigenvalue Steganography technique increases Embedding Capacity and Efficiency.

The paper is organized as follows. In Section II we provide technical background of JPEG compression algorithm and we briefly review the relevant prior work in the field. In Section III, we describe our proposed methods and sketch the theoretical analysis of these methods. In Section IV we present our experimental results. Finally, in Section V we present the concluding remarks.

978-1-4577-0989-0/11/$26.00 ©2011 IEEE

II. JPEG COMPRESSION ALGORITHM AND DCT-BASED EMBEDDING TECHNIQUES

Several steganography embedding techniques are proposed, with the goal of minimizing the statistical artifacts exerted to the DCT coefficients during embedding procedure. In this section, after brief introduction of JPEG compression algorithm, we study three of these techniques, which are F5, OutGuess and JPHS.

A. JPEG Compression Algorithm

To ease up our efforts, we use JPEG images in grayscale. Early in JPEG compression algorithm, the image luminance matrix is subdivided to non-overlapping blocks of 8×8. Thence, pixels are decremented 128 units in value. The two dimensional Discrete Cosine Transform (2D DCT) is applied on each of the blocks. These blocks whose elements are now DCT coefficients, are put together again and form the frequency domain of image.

In spatial domain, an 8×8 block is shown as $P_{8\times8}$. We subtract the elements by 128 units and show the given matrix as $P_{8\times8}$ again. Applying 2D DCT on $P_{8\times8}$, the generated $C_{8\times8}$ matrix contains the DCT coefficients of the manipulated block of the image. The element (1, 1) of $C_{8\times8}$ (is shown as c_{11}) is the DC component or zero frequency and represents as average value of the matrix $P_{8\times8}$. Manipulating the DC coefficient causes dramatically drastic changes on $P_{8\times8}$. Remaining DCT coefficients of $C_{8\times8}$, are described as AC or frequency coefficients. In this paper the matrices are demonstrated with capital letters and elements and their subscripts with small letters. Each $C_{8\times8}$ blocks is element-wise divided by quantization table $Q_{8\times8}$. After the rounding procedure, the outcome is a matrix of size 8×8 with quantized DCT coefficients shown as $Z_{8\times8.}$

B. DCT-Based Embedding Techniques

Westfeld [3] proposed a popular steganography technique, called F5. F5 contains two different message embedding concepts [2]. In the first concept, it uses syndrome coding and minimizes the changes of LSB of the DCT coefficients. This concept has a main drawback. It changes number of non-zero DCT coefficients. This drawback leads to design new specific steganalysis technique [8]. In the second concept, F5 uses AC and non-zero DCT coefficients and embeds message bits into them, by decreasing absolute value of them. Shrinkage problem occurs when F5 tries to embed message bits in the DCT coefficients with value of +1 and -1.

Outguess [4] is an embedding technique proposed by Provos to defend against statistical steganalyzers. This technique embeds confidential message into image, in two steps. First, it identifies the DCT coefficients that have minimum effect on the image. Then according to the information obtained in the first step, it determines changeable DCT coefficients in which it would embed the confidential message bits. During embedding process, Outguess preserve some DCT coefficients. After embedding all message bits, it changes LSB of these preserved coefficients to remain histogram of DCT coefficient constant. Outguess increases the blockiness between 8×8 DCT blocks.

JPHS stand for JPEG Hide and Seek [9], proposed by Allan Latham, is one of the simplest JPEG-based steganography techniques. It chooses changeable DCT coefficients in luminance and chrominance matrices, according to a constant tables and rules. JPHS embeds confidential bits by replacing them with LSB of specific DCT coefficients.

III. EIGENVALUE STEGANOGRAPHY

In this section, we describe the two proposed methods of Eigenvalue Steganography technique. $Z_{8\times8}$ quantized DCT block is given which is considered to be divided in 16 sub matrices of size 2×2, Fig. 1. We are trying to embed the confidential message in the matrices whose attribute doesn't affect what is visual in our primary image. We are attempting to devise two new methods of embedding a message in an image. The methods are explained with details in Sections III-A and III-B. Both of these methods expose their primary goal as manipulation of a selected 2×2 matrix to a certain extent that the receiver terminal reveals the hidden message, after calculating the eigenvalue of the retrieved matrix.

A. Method One

Assuming the selected 2×2 block of matrix is:

$$A_{2\times2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \tag{1}$$

Embedding an arbitrary hexadecimal value m which contains 4 bits of our message, is given by means of exchanging the values of a_{21} and a_{22}, with $a_{11} - m$ and $a_{12} + m$ respectively. As follows, the manipulated matrix is:

$$A'_{2\times2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{11} - m & a_{12} + m \end{bmatrix} \tag{2}$$

Possessing the above matrix, the receiver calculates its eigenvalues and extracts two values. The problem is what eigenvalue to consider as the message carrier m. Subsequently the receiver compares the values of $a_{11} + a_{12}$ and m; then uses the Table I to help him choose the proper eigenvalue.

TABLE I
CHOOSING PROPER EIGENVALUE IN THE RECEIVER

Condition	Decision (Decisions are made considering signed values)
$a_{11} + a_{12} > m$	The smaller *eigenvalue* holds the message
$a_{11} + a_{12} < m$	The greater *eigenvalue* holds the message
$a_{11} + a_{12} = m$	Both of eigenvalues are equal and hold the message

B. *Method Two*

The second method for embedding the message is to exchange the elements a_{12} and a_{22} with $a_{11}-m$ and $a_{21}+m$ respectively; the manipulated matrix is found to be:

$$A'_{2\times2}=\begin{bmatrix} a_{11} & a_{11}-m \\ a_{21} & a_{21}+m \end{bmatrix} \quad (3)$$

The receiver calculates its eigenvalues and extracts two values. As in the previous method, this time the receiver terminal compares the values of $a_{11}+a_{21}$ and m and uses the Table II.

TABLE II
CHOOSING PROPER EIGENVALUE IN THE RECEIVER

Condition	Decision (Decisions are made considering signed values)
$a_{11}+a_{21}>m$	The smaller *eigenvalue* holds the message
$a_{11}+a_{21}<m$	The greater *eigenvalue* holds the message
$a_{11}+a_{21}=m$	Both of eigenvalues are equal and hold the message

As shown in Fig. 1, In each $Z_{8\times8}$ quantized DCT block, we use 6 submatrices to embed 4 bits of message into each of them. This architecture makes us capable to embed 24 message bits into each $Z_{8\times8}$ quantized DCT block of image. Changing quantized DCT coefficients which are close to the DC value of the DCT block, have the maximum effect in the spatial domain of image. Also statistical analyzers always analyze these coefficients and use them for their feature extraction of image. As a result, changing these coefficients increases the detectability of Eigenvalue Steganography technique. We do not embed into submatrices with index number of 1, 2, 5, and 6. In this paper we manipulate submatrices with index number of 3, 7, 8, 9, 10, and 14. Also we can limit useful submatrices to 7 and 10 to increase security of Eigenvalue Steganography technique.

IV. EXPERIMENTAL RESULTS

In this section, we evaluate the resistivity of proposed Eigenvalue Steganography methods in Section III, against steganalyzers. For this cause, we implement the process of proposed methods on a database containing 5000 JPEG compressed images. The steganalysis techniques used here, are Subtractive Pixel Adjacent Matrix (SPAM) [5] and Merged Markov and DCT Features [6]. We abbreviate Merged Markov and DCT Features steganalysis technique as MMDF. Initially, using our methods, an arbitrary confidential message is hidden inside the images of database. The messages are generated randomly for each image. The length of the message equals a percentage of non-zero DCT coefficients for each image. We call this significant percentage as Embedding Rate. Process of message embedding is done with Embedding Rates of 5%, 10% and 20% respectively. After generating database

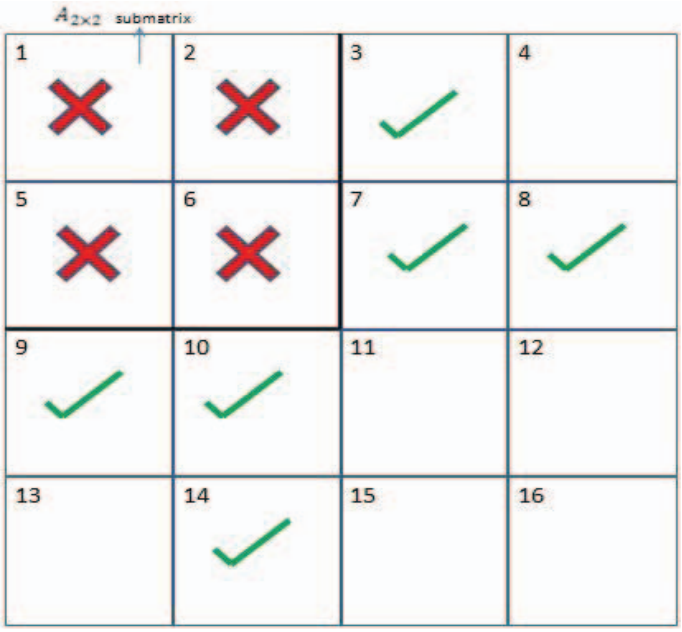

Fig.1. 8×8 quantized DCT block. Useful submatrices are shown by indexes 3, 7, 8, 9, 10, and 14.

of stego images for each specific method and specific Embedding Rate, we train steganalyzers and generate steganalysis models. Feature extraction of clean and stego images are done employing SPAM and MMDF steganalysis techniques. The MMDF steganalyzer detects the generated stego images with high precision. This steganalyzer completely classifies stego and clean images.

In Fig. 2 and Fig. 3, Receiver Operating Characteristic (ROC) curves [7] resulted from SPAM steganalysis technique are shown based on True Positive and False Positive variables. The outcome depicted in Fig. 2 and Fig. 3 illustrates that the SPAM is not able to properly detect the stego images with Embedding Rate of 5%. The SPAM steganalyzer has high error rate detecting stego images with Embedding Rate of 10%. Also the results indicate that the first method shows more resistance against SPAM steganalyzer than the second method does.

V. CONCLUSION

In this paper we proposed new steganography technique which uses eigenvalues' characteristics of quantized DCT matrices of JPEG compressed images to embed the confidential message. We called this technique as Eigenvalue Steganography. We designed two methods to implement Eigenvalue Steganography. These two methods divide 8×8 quantized DCT blocks to submatrices of size 2×2. Then, they embed 4 bits of confidential message in each submatrix by modifying two elements of it. After embedding procedure, Eigenvalue of each stego submatrix carries a hexadecimal value of message. As a result, the major advantage of Eigenvalue steganography technique in contrast to the other common DCT based steganography techniques was improvement of image capacity which resulted in higher embedding capacity.

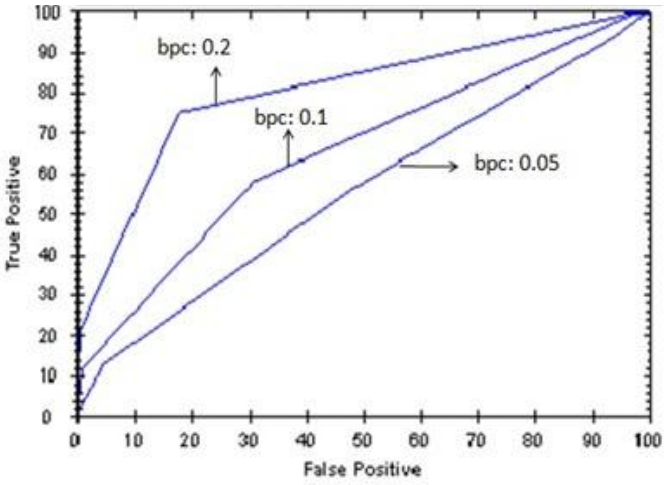

Fig.2. ROC for images embedded using method one of Eigenvalue Steganography technique with embedding rates of 0.2, 0.1 and 0.05 bpc for SPAM steganalysis technique.

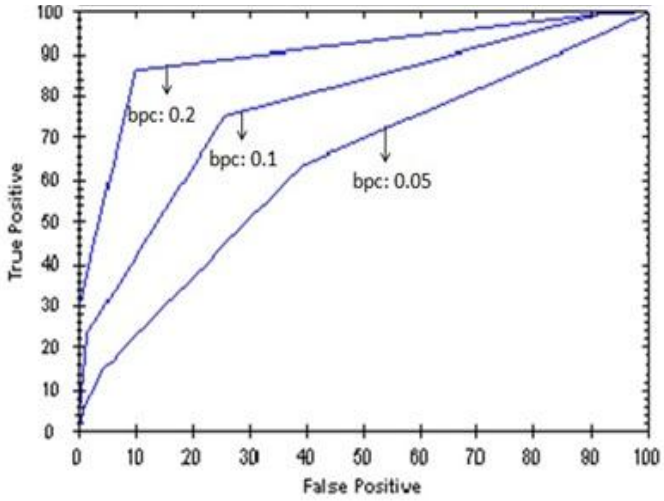

Fig.3. ROC for images embedded using method two of Eigenvalue Steganography technique with embedding rates of 0.2, 0.1 and 0.05 bpc for SPAM steganalysis technique.

We evaluated the detectability of our proposed methods by using SPAM steganalysis technique. Our experimental results showed that these two methods have acceptable resistance against this steganalyzer.

The SPAM steganalyzer is trained based on a database including stego and clean images, using Support Vector Machine (SVM) tool. The confidential message is embedded in images using Eigenvalue steganography and the corresponding model is produced. The SPAM steganalyzer is able to detect the proposed method given that the amount of true positive (proper detection of stego image) is far more than the amount of false positive (improper detection of a clean image instead of a stego image). The ROC diagram presented in figures 2 and 3 express that with the embedding rate of 5% the amount of true positive and false positive are approximately equal; meaning that with this rate of embedding, the SPAM steganalyzer has no decision. As a result the SPAM steganalyzer lacks the ability to classify stego and clean images properly. This steganalyzer does not employ exact decision with the embedding rate of 10%.

REFERENCES

[1] Mehdi Kharrazi,Husrev T. Sencar,Nasir Memon "Performance study of common image steganography and steganalysis techniques" Journal of Electronic Imaging vol.15(4), pp 041104,Oct–Dec 2006.

[2] J. Fridrich, T. Pevny, and J. Kodovsky, "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities," Proc. ACM MM&Workshop, Dallas, TX, Sept. 2007, pp. 3-14, doi:10.114511288869.1288872.

[3] Westfeld, A.: F5—a steganographic algorithm: High capacity despite better steganalysis. In: Moskowitz, I.S. (ed.) Information Hiding. LNCS, vol. 2137, pp. 289–302. Springer, Heidelberg (2001).

[4] Provos, N. "Defending Against Statistical Steganalysis," Proc. 10th USENIX Security Symposium. Washington, DC, 2001.

[5] T. Pevný, P. Bas, and J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. In J. Dittmann, S. Craver, and J. Fridrich, editors, Proceedings of the 11th ACM Multimedia & Security Workshop, pages 75–84, Princeton, NJ, September 7–8, 2009.

[6] T. Pevn´y and J. Fridrich. Merging Markov and DCT features for multi-class JPEG steganalysis. In E. J. Delp and P. W. Wong, editors, Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505, pages 3 1–3 14, San Jose, CA, January 29– February 1, 2007.

[7] T. Fawcett, "ROC graphs: notes and practical considerations for researchers," http://www.hpl.hp.com/personal/Tom_Fawcett/papers/ROC101.pdf.

[8] Fridrich, J.: Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In: Proc. 6th Information Hiding Workshop, Toronto, Canada, 2004 (2004).

[9] http://linux01.gwdg.de/~alatham/stego.html