CRYPTO-STEG: A Hybrid Cryptology - Steganography Approach for Improved Data Security

ATIF BIN MANSOOR*, ZOHAIB KHAN*, AND SHOAB AHMED KHAN**

RECEIVED ON 20.11.2009 ACCEPTED ON 10.03.2010

ABSTRACT

Internet is a widely used medium for transfer of information due to its reach and ease of availability. However, internet is an insecure medium and any information might be easily intercepted and viewed during its transfer. Different mechanisms like cryptology and steganography are adopted to secure the data communication over an inherently insecure medium like internet. Cryptology scrambles the information in a manner that an unintended recipient cannot easily extract the information, while steganography hides the information in a cover object so that it is transferred unnoticed in the cover. Encrypted data may not be extracted easily but causes a direct suspicion to any observer, while data hidden using steganographic techniques go inconspicuous. Cryptanalysis is the process of attacking the encrypted text to extract the information, while steganalysis is the process of detecting the disguised messages. In literature, both cryptology and steganography are treated separately. In this paper, we present our research on an improved data security paradigm, where data is first encrypted using AES (Advanced Encryption Standard) and DES (Data Encryption Standard) cryptology algorithms. Both plain and encrypted data is hidden in the images using Model Based and F5 steganographic techniques. Features are extracted in DWT (Discrete Wavelet Transform) and DCT (Discrete Cosine Transform) domains using higher order statistics for steganalysis, and subsequently used to train a FLD (Fisher Linear Discriminant) classifier which is employed to categorize a separate set of images as clean or stego (containing hidden messages). Experimental results demonstrate improved data security using proposed CRYPTO-STEG approach compared to plain text steganography. Results also demonstrate that the Model Based steganography is more secure than the F5 steganography.

Key Words: **Cryptology, Steganography, Steganalysis, Classification**

1. INTRODUCTION

Data security is a paramount concern in today's networked society that has increased dependence on internet due to its ubiquity, cost effectiveness and availability. Information transfer on internet is inherently insecure due to its basic underlying model. Many application oriented security modules are developed to cater this shortcoming, most popular are cryptographic techniques. Cryptography can handle different aspects of information security like data confidentiality, integrity, origin authentication etc. In cryptography, the data is transformed into a form incognizable to an observer, but the intended recipient can recover the information using a secret key. The broader category of crypto systems is symmetric key and

* College of Aeronautical Engineering, National University of Sciences and Technology, Islamabad.

* Associate Professor, National University of Sciences and Technology, Islamabad.

asymmetric key cryptography. Same key is used for encryption and decryption in symmetric key cryptography. In asymmetric cryptography different keys are used for encryption and decryption, also known as public key and private key. Asymmetric key cryptography solves different problems present in symmetric key cryptography like key exchange over insecure media, authentication using digital signatures etc. Similarly, cryptography systems can also be categorized on the basis of encryption of plain text i.e., block cipher encrypt the input block by block while stream cipher processes the input one element at a time [1].

The word steganography comes from Greek meaning 'hidden writing' [2]. Steganography is used for hiding information in digital images and afterwards transferring them via internet without any hunch. Steganography is an age-old subject, having its origins in ancient Greece and China, where it was being used thousands of years ago. Steganography and cryptography are closely linked techniques for hiding information. The aim of cryptography is to muddle a message so that it cannot be apprehended, whereas that of steganography is to conceal a message so that it becomes invisible. Generally, a neutral observer will become suspicious of a message created with cryptographic tools, whereas a message created with steganographic tools will go unnoticed. Steganalysis techniques aspire at detecting the presence of hidden communication from unobtrusive stego images. Steganographers mean to hide communications and are neutralized by steganalysts who mean to disclose it. The precise field to counter steganography is called steganalysis. The objective of a steganalyst is to sense the presence of steganography in order to stop the secret message from being received. Then the steganography tool to obtain the secret message from the stego file is identified. Normally two techniques are utilized for steganalysis; first to form a speecial steganalysis technique for specific steganographic algorithm. These are also called technique specific steganalysis methods. Second is to work out universal steganalysis techniques that are not dependent upon the paricular steganographic algorithm.

This paper presents our research on a hybrid cryptography and steganography approach. The improved data security achieved through this approach is evaluated by our reported universal steganalysis method [3]-4]. The paper is structured as following: In Section 2, the details of a crypto-stego approach, along with the development of steganographic image datasets for experiments is presented. Description of our Steganalysis technique is given in Section 3. Section 4 contains experimental results. Finally, section 5 presents the conclusion.

2. THE CRYPTO-STEGAPPROACH

Fig. 1 depicts the basic model of the hybrid cryptology and steganography approach. A sender in order to transmit a confidential message to an intended receiver first enciphers the message using a secret key and cryptology algorithm to get the cipher text. The sender then selects a cover image and hides the cipher text in the image using a secret key and a steganographic tool to get the stego image. The stego image is sent securely and unnoticed over a public channel (e.g. internet) to the intended receiver. As the receiver gets the stego image, first the cipher text is extracted from the stego image by applying steganographic key using the same steganographic tool. Then the cipher text is deciphered using secret key to get the original message using the same cryptology tool.

2.2 Image Dataset Development

In our experiments, the Uncompressed Colour Image Database [5] constructed by Schaefer and Stich [6] was used to obtain 1338 images of size 512x384. These images provide a real and challenging environment for a steganalysis problem because they contain a wide range of indoor/outdoor, daylight/night scenes. We encrypted the message using DES and AES encryption algorithms. Details about DES and AES can be viewed in [1].

2.2.1 F5 Stego Image Dataset

Steganography software F5 by Andreas Westfeld is used to creat our first stego image database [7], utilising both plain text and cipher text. F5 steganography algorithm hides information bits by decrementing and incrementing the values of quantized DCT coefficients from compressed JPEG images [8]. F5 also makes use of 'matrix embedding' operation to reduce the number of changes done to the DCT coefficients, required to embed a message of a specific length. Three parameters are used in Matrix embedding (c,n,k) , where 'k' is the number of embedded bits and 'c' is the number of changes per group of 'n' coefficients. Embedding algorithm ascertains these parameter values. F5 was selected as reported in literature [9-10], F5 is difficult to detect than other steganography algorithms.

2.2.2 MB Stego Image Dataset

Model Based steganography method [11], proposed by Phil Sallee [12], is used to create the second stego image dataset. The algorithm divides the quantized DCT coefficients of JPEG image into two segments and then replaces the visually insignificant one with the secret message. There are two types of this algorithm; MB1 is ordinary steganography and MB2 is steganography with deblocking. The deblocking algorithm regulates the unused coefficients to lessen the blockiness of the stego image related to original blockiness. Model Based steganography algorithm, unlike F5, does not recompress the original image prior to embedding. Messages were embedded successfully selecting different quality factors. High resistance was offered by the model based steganography algorithm against steganalysis techniques [13-14]. This dataset contains a total of 21,408 cover and stego images equally. Maximum length message is embedded in each image. Model Based steganography without deblocking is utilized. A maximum length message is embedded in each image.

3. STEGANALYSIS APPROACHES

3.1 Discrete Cosine Transform Features

Fridrich's approach [13] is used to construct DCT based feature set. A vector functional F is applied to the JPEG image J_1. After decompressing the image in the spatial domain, 4 pixels are cropped in every direction and is then

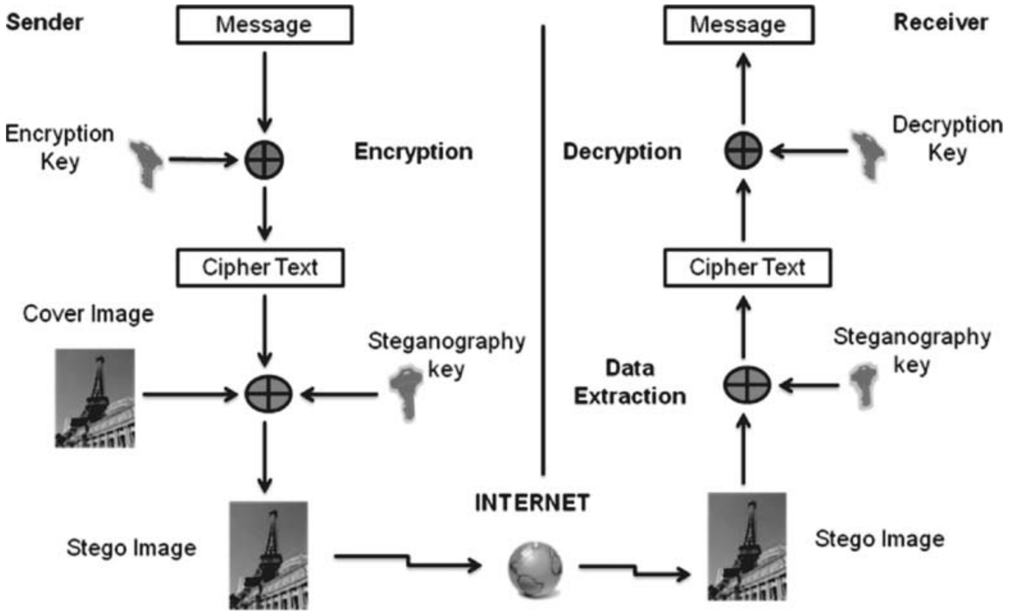

FIG. 1. THE CRYPTO-STEG MODEL

recompressed with the original quantization table to form J_2. J_2 is then acted upon by the same functional F . The L_1 norm of the difference of the functional applied to J_1 and J_2 is the final feature f, as depicted in Fig. 2.

The logic behind this approach is that the previous JPEG compression's 8x8 block boundary is lost due to cropping by 4 pixels in each direction and the previous quantization and hence embedding in the DCT domain doesn't affect the extracted features. Thus, J_2 is an estimate of the cover image containing the hidden data. The global, individual and dual histograms of the DCT coefficient array $d_{(k)}(i,j)$ were calculated as the first order functional. The symbol $d_{(k)}(i,j)$ represents the (i,j)th quantized DCT coefficient i,j=(1,2,...,8) in the kth block, (k=1,2,...,B). The global histogram of all 64B DCT coefficients is defined as, $H(m)^{L}_{m=L}$, where $L=\min_{k,i,j} d_{(k)}(i,j)$ and $R=\max_{k,i,j} d_{(k)}(i,j)$. We computed $H/\|H\|_{L1}$ the normalized global histogram of DCT coefficients as the first functional. Techniques that preserve global DCT coefficients histogram in steganography may not essentially preserve the individual DCT modes histogram [13]. Next, value found is $h^{i,j}/\|h^{i,j}\|$,the normalized individual histograms $h(m)^{R}_{m=L}$ of 5 low frequency DCT modes, (i,j) = (2,1), (3,1), (1,2), (2,2), (1,3) as the next five functionals. The dual histogram is an 8x8 matrix that shows the ocurrence of the value 'd' as the (i,j)th DCT coefficient in all blocks B present in the image. Next, $g^{d}_{ij}/\|g^{d}_{ij}\|_{L1}$ the normalized dual histograms where $g^{d}_{ij} = \sum_{k=1}^{B} \delta d,d_{(k)}(i,j) g^{d}_{ij}/\|g^{d}_{ij}\|_{L1}$ for 11 values of d=-5,-4,...,4,5 is calculated. The second order features variation and blockiness capture the inter block dependency. The entropy added to the DCT coefficients by steganographic algorithms is captured by the variation (V). The variation along rows (V_r) and columns (V_c) of blocks is:

$$V_r = \sum_{i,j=1}^{8} \sum_{k=1}^{|I_r|-1} \left| d_{I_r(k)}(i,j) - d_{I_{r(k+1)}}(i,j) \right| \tag{1}$$

$$V_c = \sum_{i,j=1}^{8} \sum_{k=1}^{|I_c|-1} \left| d_{I_c(k)}(i,j) - d_{I_{c(k+1)}}(i,j) \right| \tag{2}$$

where I_r and I_c give the vectors of block indices while scanning the image `by rows' and `by columns' respectively. The total variation (V) is then:

$$V = \frac{V_r + V_c}{|I_r| + |I_c|} \tag{3}$$

Blockiness that calculates the discontinuity along the block boundaries over all DCT modes in the image, is computed from the decompressed JPEG image. The L_1 and L_2 blockiness (B_α, α=1,2) is defined as:

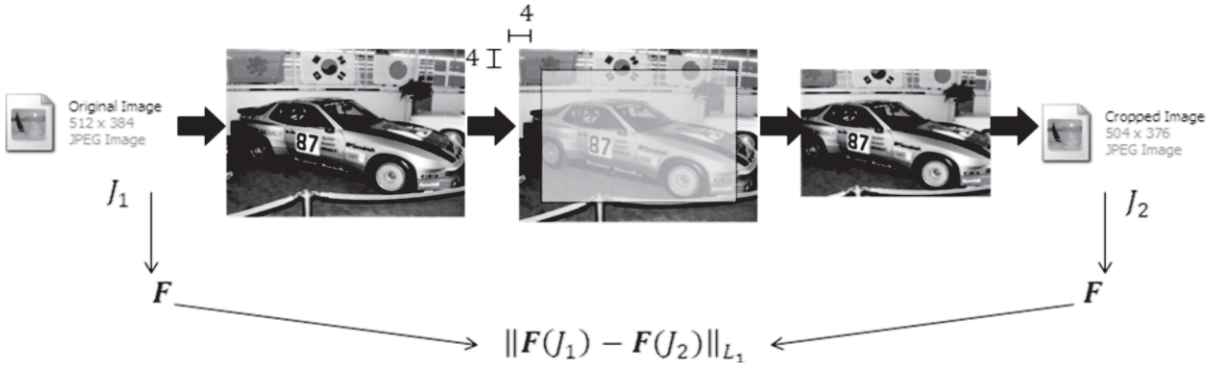

FIG. 2. EXTRACTION OF DISCRETE COSINE TRANSFORM BASED FEATURE

$$B_{\alpha} = \frac{\sum_{i=1}^{\tilde{M}} \sum_{j=1}^{N} \left| x_{8i,j} - x_{8i+1,j} \right|^{\alpha} + \sum_{j=1}^{\tilde{N}} \sum_{i=1}^{M} \left| x_{i,8j} - x_{i,8j+1,j} \right|^{\alpha}}{N\tilde{M} + M\tilde{N}} \qquad (4)$$

Where $\tilde{M} = \lfloor (M-1/8 \rfloor, \tilde{N} = \lfloor (N-1/8) \rfloor$ and $x_{i,j}$ are the grayscale intensity values of an image with dimensions MxN. Thus a final feature set is achieved having dimension 20-D, where seventeen features are histograms based; one global, five individual and eleven dual histograms as explained in above paragraph, one Variation feature given by Equation (3), two Blockiness features given by Equation (4).

3.2 Discrete Wavelet Transform Based Features

Three scale decomposition was chosen for extraction of features in the Discrete Wavelet Transform domain, as proposed by [10]. Fig. 3 depicts the levels and subbands selected.

Nine detail subbands (Horizontal H_1, Vertical V_i and Diagonal D_i, i=1,2,3) and three approximation subbands (Lowpass L_i, i=1,2,3) were obtained using wavelet. To improve the performance of features, the first scale diagonal subband D_1 was further decomposed. D_1 is the finest detail subband and each one of its coefficients involves diagonal differences in a four pixel block, so H_2', V_2', and D_2' will have additional information about the difference of differences between adjacent pixels.

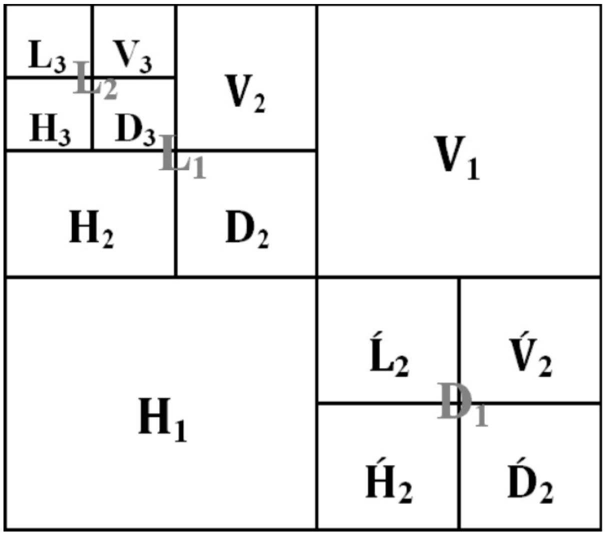

FIG. 3. A THREE SCALE WAVELET DECOMPOSITION

The -point discrete CF (Characteristic Function) is given as:

$$\Phi(k) = \sum_{m=0}^{M-1} h(m) e^{\left\{ \frac{j2\pi mk}{k} \right\}}, 0 \le k \le K-1 \qquad (5)$$

where $\{h(m)\}_{m=0}^{M-1}$ is the   bin histogram estimating the PDF, p(x) of the wavelet coefficients.

The nth absolute moment of discrete CF is given by:

$$M_n^A = \sum_{K=0}^{K-1} \left| \Phi(k) \right| \sin^n \left(\frac{\pi l}{k} \right) \qquad (6)$$

The normalized CF moment is given by:

$$\hat{M}_n^A = \frac{M_n^A}{M_o^A}$$

where M^A_0 is the zeroth order moment. A 48-D feature vector is formed consisting of the first three normalized CF moments for each of the 16 subbands.

3.2 Classifier

Two class FLD classifier [15] was used. Let x_i, i=1,.....N_x and y_i, j=1,.....N_y denote the samples from each of the two classes of the training set.

The within class means are given by:

$$m_x = \frac{1}{N_x} \sum_{i=1}^{N_x} x_i, m_y = \frac{1}{N} \sum_{j=1}^{N_y} y_j \qquad (8)$$

The between class mean is:

$$m = \frac{1}{N_x + N_y} \left(\sum_{i=1}^{N_x} x_i + \sum_{j=1}^{N_y} y_j \right) \qquad (9)$$

The within scatter matrix is:

$$S_{\omega} = M_{x}M^{T}_{x} + M_{y}M^{T}_{y} \tag{10}$$

where $M_x=x_i-m_x$, $M_y=y_j-m_y$ are the matrices containing the zero-meaned ith and jth samples respectively. The between class scatter matrix is:

$$S_{b} = N_{x}(m_{x}-m)\,(m_{x}-m)^{T} + N_{y}(m_{y}-m)\,(m_{y}-m)^{T} \tag{11}$$

The maximal generalized eigen value eigenvector 'e' related to S_b and S_w by:

$$S_{b}e=\lambda S_{\omega}e \tag{12}$$

By projecting the training samples x_i and y_j onto one dimensional linear subspace e($x_p=x^T_i e$, $y_p=y^T_i e$) , the between class scatter is maximized and the within class scatter is minimized. This effect is highly desirable in any classification problem because it maintains the discriminability while at the same time reduces the dimensions of data. An unknown sample 'z' can now be tested for its class by projecting it onto the same subspace 'e' ($z_p=z^T e$) and its class determined on the basis of a threshold T_h. We set the threshold at equal detection rate for both cover and stego images.

4. EXPERIMENTAL RESULTS

For experiments a database of JPEG images was developed which include cover images, stego images for both plain and encrypted text. The stego image database was developed using F5 and Model based steganography algorithms. For steganalysis image features were extracted in the DWT and the DCT separately. A FLD classifier was trained on the extracted features from 669 cover and 669 stego images. The FLD classifier was then tested on the features extracted from a different database of test images containing 669 cover and 669 stego images. The ROC (Receiver Operating Characteristics) curve, that gives the variation of the Detection Probability (P_d, the portion of rightly classified stego images) with the False Alarm Probability (P_f, the portion of cover images incorrectly classified as stego image), was computed for each steganographic algorithm and encrypted/plain text. The ROC Curves were formed for steganalysis of F5 with matrix embedding turned off (1,1,1), turned on F5(c,n,k), and Model based steganography with deblocking algorithms for both plain and cipher texts utilizing DWT and DCT features (Figs. 4-9). It is observed that detection accuracy of steganalysis reduces for cipher text compared to plain text steganography as the area under the curve is less for cipher text steganalysis than plain text.

Table 1 gives the summary of classification accuracy of steganalysis for detection of plain and cipher text. Results show that detection rate decreases for the cipher text embedding in the images than plain text embedding for the three steganography algorithms. Model based Steganography is stronger than F5 based steganography as its detection rate is less. DCT based steganalysis approach is better than DWT based approach as better detection rates are achieved by it.

5. CONCLUSION

This paper presents a hybrid CRYPTO-STEGANO technique for improved data security. Image database was developed in which data is encrypted using ASE and DES cryptology algorithms and then hidden in JPEG images using F5 and model based steganography techniques.

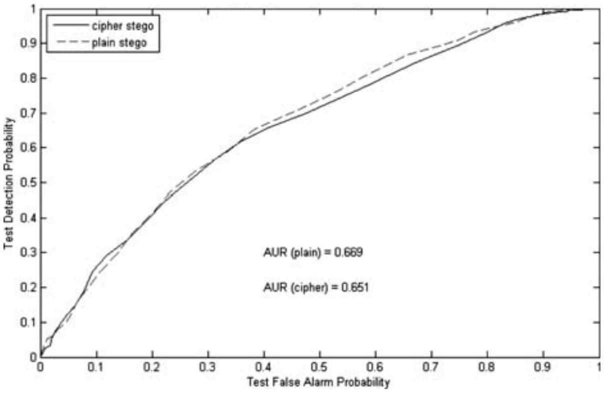

FIG. 4. RECEIVER OPERATING CHARACTERISTICS CURVE FOR F5(c,n,k) USING DISCRETE WAVELET TRANSFORM FEATURES

DWT and DCT based approaches were developed for steganalysis of plain and cipher text embedding. Statistical results based on ROC demonstrate that (a) Improved data security is achieved by embedding cipher texts compared to plain texts in the images (b) Model based steganography is stronger than F5 based steganography (c) DCT based steganalysis approach is stronger than DWT based approach.

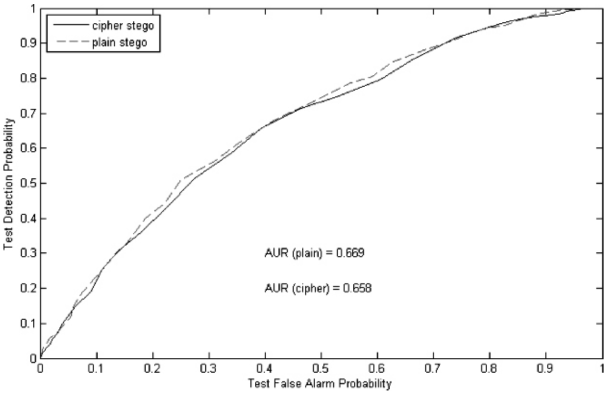

FIG. 5. RECEIVER OPERATING CHARACTERISTICS CURVE FOR F5(1,1,1) USING DISCRETE WAVELET TRANSFORM FEATURES

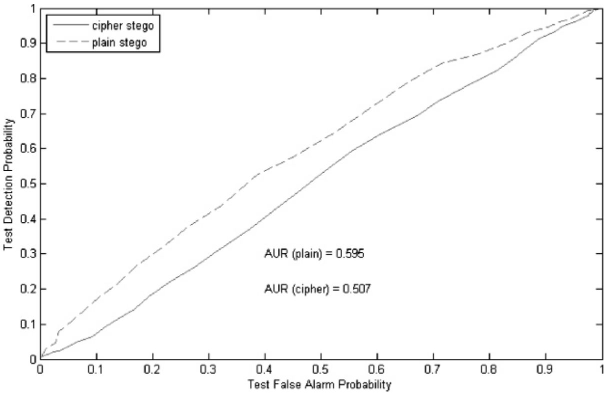

FIG. 6. RECEIVER OPERATING CHARACTERISTICS CURVE FOR MODEL BASED USING DISCRETE WAVELET TRANSFORM FEATURES

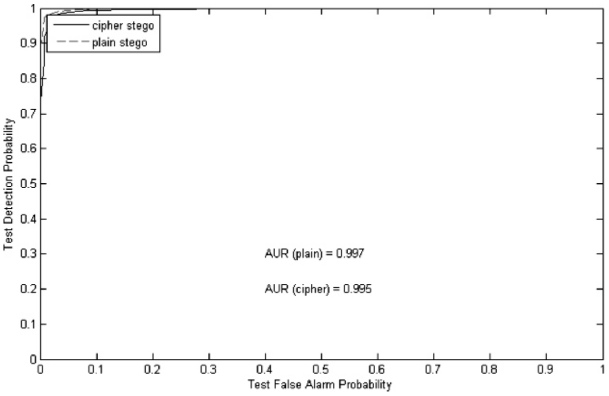

FIG. 7. RECEIVER OPERATING CHARACTERISTICS CURVE FOR F5(c,n,k) USING DISCRETE COSINE TRANSFORM FEATURES

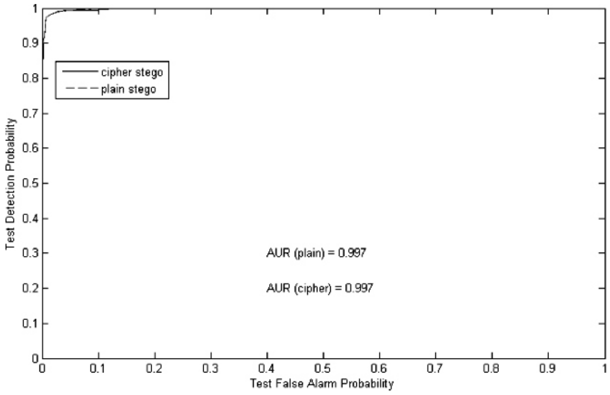

FIG. 8. RECEIVER OPERATING CHARACTERISTICS CURVE FOR F5(1,1,1) USING DISCRETE COSINE TRANSFORM FEATURES

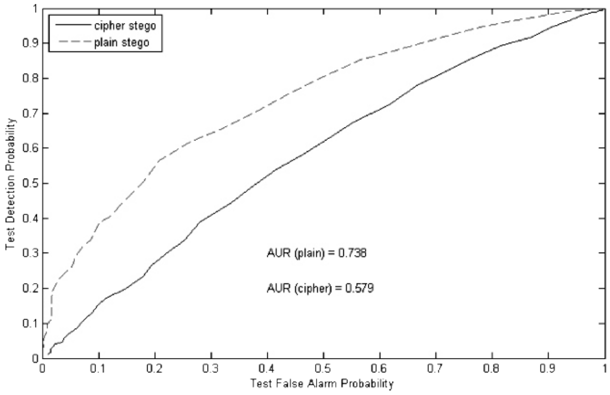

FIG. 9. RECEIVER OPERATING CHARACTERISTICS CURVE FOR MODEL BASED USING DISCRETE COSINE TRANSFORM FEATURES

TABLE 1. CLASSIFICATION ACCURACY FOR DETECTION OF PLAIN AND CIPHER TEXT EMBEDDEDIN IMAGES USING DWT AND DCT BASED STEGANALYSIS

Text Type	F5 (1,1,1)	F5 (c,n,k)	Model Based	Features
Plain	0.669	0.669	0.595	Discrete Wavelet Transform
Cipher	0.658	0.651	0.507	Discrete Wavelet Transform
Plain	0.997	0.997	0.738	Discrete Cosine Transform
Cipher	0.996	0.995	0.579	Discrete Cosine Transform

ACKNOWLEDGEMENTS

Authors are thankful to Higher Education Commission, Islamabad, Center for Advanced Studies in Engineering, University of Engineering and Technology, Taxila, and National University of Sciences and Technology, Islamabad, Pakistan, for providing support and facilities for this research. Authors are also thankful to the School of Computing and Mathematics, Nottingham Trent University, UK, for providing free UCID-An Uncompressed Colour Image Database.

REFERENCES

[1] Stallings, W., "Cryptography and Network Security: Principles and Practices", Prentice Hall, Chapter-3, pp. 63-64, New York, 2003.

[2] McBride, B.T., Peterson, G.L., and Gustafson, S.C., "A New Blind Method for Detecting Novel Steganography", Digital Investigation, Volume 2, pp. 50-70, February, 2005.

[3] Khan, Z., and Mansoor, A.B., "Steganalysis of JPEG Images with Joint Transform Features", Pacific-Rim Symposium on Image and Video Technology, Volume 1, pp. 965-975, Tokyo, Japan, 2009.

[4] Khan, Z., and Mansoor, A.B., "A New Hybrid DCT and Contourlet Transform Based JPEG Image Steganalysis Technique", 16th Scandinavian Conference on Image Analysis, Volume 1, pp. 91-98, Oslo, Norway, June, 2009.

[5] UCID (Uncompressed Colour Image Database), Online: http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html.

[6] Schaefer, G., and Stich, M., "UCID-An Uncompressed Colour Image Database", SPIE, Storage and Retrieval Methods and Applications for Multimedia, Volume 1, pp. 472-480, San Jose, USA, January, 2004.

[7] Steganography Software F5. Online : http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html.

[8] Westfeld, A. , "F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis", Information Hiding: 4th International Workshop, Lecture Notes in Computer Science, Moskowitz, I.S., (Editor), Volume 1, pp. 289-302, Springer-Verlag, Berlin Heidelberg, April, 2001.

[9] Farid, H., "Detecting Hidden Messages Using Higher-order Statistical Models", IEEE International Conference on Image Processing, Volume 1, pp. 905-908, New York, 2002.

[10] Wang, Y., and Moulin, P., "Optimized Feature Extraction for Learning-Based Image Steganalysis", IEEE Transactions on Information Forensics and Security, Volume 2, pp. 31-45, March, 2007.

[11] Model Based JPEG Steganography Demo. Online: http://www.philsallee.com/mbsteg/index.html.

[12] Sallee, P., "Model Based Steganography", International Workshop on Digital Watermarking, Volume 1, pp. 174-188, Seoul, Korea, October, 2003.

[13] Fridrich, J., "Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes", Sixth Information Hiding Workshop, Lecture Notes in Computer Science, Volume 1, pp. 67-81, Springer-Verlag, Berlin Heidelberg, 2004.

[14] Kharrazi, M., Sencar, H.T., and Memon, N., "Benchmarking Steganographic and Steganalysis Technique", SPIE Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents-VII, Volume 1, pp. 152-263, San Jose, USA, 2005.

[15] Duda, R.O, Hart, P.E., and Stork, D.G., "Pattern Classification", John Wiley & Sons, Chapter-3, pp. 117-120, New York, USA, 2001.