Institute of Advanced Engineering and Science

International Journal of Information & Network Security (IJINS))
Vol. 3, No. 1, February 2014, pp. 40 – 63
ISSN: 2089-3299

DCT Difference Modulation(DCTDM) Image Steganography

Souvik Bhattacharyya[*], Aparajita Khan[*], and Gautam Sanyal[**]
[*]Department of CSE, University Institute of Technology,, The University of Burdwan,West Bengal, India - 713104
[**]Department of CSE ,National Institute of Technology, Durgapur,, Mahatma Gandhi Avenue, West Bengal, India - 713209

Article Info

Article history:
Received Dec 21th, 2013
Revised Jan 10th, 2014
Accepted Feb 27th, 2014

Keyword:
Steganography
PMM(Pixel Mapping Method)
DCTDM (DCT Difference Modulation)
Image Similarity Metrics
SSIM

ABSTRACT

Many different carrier file formats can be used to pursue steganography, but digital images are the most popular because of their frequency over the Internet. In this work a new transform domain image steganography method has been proposed which embeds secret message by modulating adjacent DCT coefficient differences. This approach works for both Gray Scale and RGB images in both uncompressed and lossless compressed domain , yielding a high performance in terms of embedding capacity,imperceptibility and resistivity against some of the well-known steganalysis methods.Experimental results demonstrate the effectiveness and accuracy of the proposed technique in terms of security of hidden data and various image similarity metrics.

Corresponding Author:
Dr.Souvik Bhattacharyya
Assistant Professor
Department of CSE, University Institute of Technology,The University of Burdwan,West Bengal, India - 713104
souvik.bha@gmail.com

1. INTRODUCTION

Over the past few decades information hiding has gain popularity with the aid of Internet. The security and fair use of the information with guaranteed quality of services are important, yet challenging topics. One of the most important sub disciplines of it is steganography. It is an ancient art of hiding information in ways a message is hidden in an innocent-looking cover media so that will not arouse an eavesdropper's suspicion .Compared with cryptography ,which attempts to conceal the content of the secret message, steganography conceals the very existence of that [1]. Another form of information hiding is digital watermarking [39], which is the process that embeds data called a watermark, tag or label into a multimedia object. Steganography works have been carried out on different transmission media like images, video , text, or audio.Among them image steganography is the most popular due its high degree of redundancy [27, 33].In video steganography,same method may be used to embed a message in each of the video frames [44, 10]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [16]. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio [18, 31]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [30].Some steganographic model with high security features has been presented in [3] and [37].

1.1. Image Steganography System

In image steganography system a message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key. The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key.During transmission of the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message.The block diagram of a generic image steganographic system is given in figure 1.

Rest of the paper has been organized as following sections: Section II describes some related works on image steganography.Section III deals with proposed DCTDM methodology.Algorithms are described in section IV.In the section V , different experimental results are discussed and analysed.Section VI describes the performance of

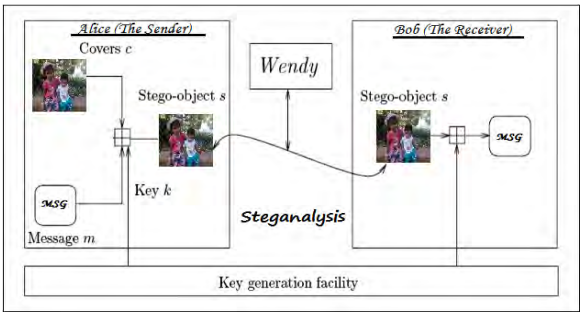


Figure 1. Generic form of Image Steganography

the DCTDM approach against various image attacks. Section VII deals with the impact of steganalysis methods on DCTDM approach.Comparision with other techniques has been illustrated in section VIII.Section IX contains the computational complexity analysis of the embedding methods.Section X draws the conclusion.

2. RELATED WORKS ON IMAGE STEGANOGRAPHY

In this section various steganographic data hiding methods both in spatial domain and transform domain has been discussed.

2.1. Spatial Domain Steganographic Method

Different spatial domain steganography techniques has been presented in this section.

2.1.1. HUGO Steganography Method

Hugo [41] is a content-adaptive spatial steganography that overcomes the shortcomings of other spatial techniques by using a general high-dimensional image model covering various dependencies of natural images.HUGO hides messages in the least significant bit of gray scale images following the minimum-embedding-impact principle. The design is decomposed in two parts-image model which is largely inspired by the Subtractive Pixel Adjacency Matrix (SPAM) steganalytic feature [40] and the coder. The optimal coder uses the distortion function generated by the image model to determine which cover elements to be changed. HUGO focuses on the image model such that distortion function can be generated more adaptively to the image content without changing the coder.

2.1.2. Data Hiding by LSB

This is one of the common techniques of image steganography , based on manipulating the least-significant-bit (LSB) [5, 7] and [34] planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression.

2.1.3. Data Hiding by PVD

The pixel-value differencing (PVD) method proposed by Wu and Tsai [48] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding.

2.1.4. Data Hiding by GLM

In 2004, Potdar et al.[12] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image.

2.1.5. Bhattachayya and Sanyal's Transformation

Bhattachayya and Sanyal devised a new image transformation technique in [4, 38] known as Pixel Mapping Method (PMM) for information hiding within the spatial domain of any gray scale image.Embedding pixel generation depends on the intensity value of the previous pixel selected. It includes a decision factor, dependent on intensity with a fixed way of calculating the next pixel. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbors lies at the boundary of the image or not. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel. Figure 2 and 3 shows the mapping information for embedding two bits or four bits respectively.

PAIR OF MSG BIT	PIXEL INTENSITY VALUE	NO OF ONES (BIN)
01	EVEN	ODD
10	ODD	EVEN
00	EVEN	EVEN
11	ODD	ODD

Figure 2. PMM Mapping Technique for embedding of two bits

MSG BIT SEQ	2nd SET – RESET BIT	3rd SET – RESET BIT	PIXEL INTENSITY VALUE	NO OF ONES(BIN)
0000	EVEN	EVEN	EVEN	EVEN
0001	EVEN	EVEN	EVEN	ODD
0010	EVEN	EVEN	ODD	EVEN
0011	EVEN	EVEN	ODD	ODD
0100	EVEN	ODD	EVEN	EVEN
0101	EVEN	ODD	EVEN	ODD
0110	EVEN	ODD	ODD	EVEN
0111	EVEN	ODD	ODD	ODD
1000	ODD	EVEN	EVEN	EVEN
1001	ODD	EVEN	EVEN	ODD
1010	ODD	EVEN	ODD	EVEN
1011	ODD	EVEN	ODD	ODD
1100	ODD	ODD	EVEN	EVEN
1101	ODD	ODD	EVEN	ODD
1110	ODD	ODD	ODD	EVEN
1111	ODD	ODD	ODD	ODD

Figure 3. PMM Mapping Technique for embedding of four bits

Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operations has been carried out to get back the original information.

2.2. Transform Domain Steganographic Method

Transform domain steganography method hides messages in significant areas of cover image which makes them robust against various image processing operations like compression, enhancement etc. The widely used transformation functions include Discrete Cosine Transformation (DCT), Fast Fourier Transform (DFT), and Wavelet Transformation.

2.2.1. DCT based Data Hiding

DCT technique used in JPEG compression algorithm to transform successive 8×8 pixel blocks of image from spatial domain to 64 DCT coefficients each in frequency domain. The least significant bits of the quantized DCT

coefficients are used as redundant bits into which the hidden message can be embedded. The modification of a single DCT coefficient affects all 64 image pixels. Because this modification happens in the frequency domain and not the spatial domain, there are no noticeable visual differences.The advantage DCT has over other transforms is the ability to minimize the block-like appearance resulting when the boundaries between the 8×8 sub-images become visible (known as blocking artifact).

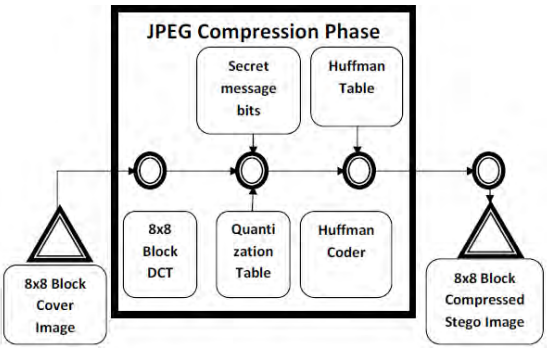


Figure 4. Steganography Principle in transform (DCT) domain

J-Steg [42] and JPHide [28] are the two classical JPEG steganographic tools developed based on LSB embedding technique.JSteg embeds the secret information into the cover image by sequentially replacing the LSBs of non-zero quantized DCT coefficients with the secret message bits where as JPHide not only modifies the LSBs of the selected coefficients but also modifies the bits of the second least significant bit-plane.F5 steganographic algorithm was introduced by Westfeld [47] where instead of replacing the LSBs of quantized DCT coefficients with the message bits, it modifies the randomly-chosen coefficient by decreasing the absolute value of the coefficient by one.

OutGuess [32] has been developed through UNIX. Yet Another Steganographic Scheme (YASS) [20] works based on the principle of JPEG steganography but does not directly embed data in JPEG DCT coefficients. Instead an input image in spatial domain is divided into blocks with a fixed large size known as the big blocks (or B-blocks). Within each B-block, an 8x8 embedding host block (or H-block) is selected randomly with a secret key for performing DCT. Next step is to encode the secret data by error correction codes and embedded in the DCT coefficients of the H-blocks by QIM technique. Finally, after performing the inverse DCT to the H-blocks, the whole image is compressed and distributed as a JPEG image.

Model Based Steganography [35] designed through an information-theoretic approach for performing steganography and steganalysis using a statistical model of the cover medium. This methodology is general and can be applied to virtually any type of media. MB steganography methods has been proposed for JPEG images, achieves a higher embedding efficiency and message capacity than the previous methods also remains secure against first order statistical attacks. MME [49] utilizes side information at the sender in terms of the uncompressed image and employs matrix embedding to minimize an appropriately defined distortion function.

BCH and BCHopt [43] are side-informed algorithms that employ BCH codes to minimize the embedding distortion in the DCT domain defined using the knowledge of non-rounded DCT coefficients. BCHopt is an improved version of BCH that contains a heuristic optimization and also hides message bits into zeros.

Wang et al. [45] presents an efficient JPEG steganography scheme based on the block entropy of DCT coefficients and syndrome trellis coding (STC).Danti et al. [9] proposes a novel image steganography method based on randomized bit embedding.In this approach the Discrete Cosine Transform (DCT) of the cover image is obtained and the stego image is constructed by hiding the given secrete message image in Least Significant Bit of the cover image in random locations based on threshold.

To enhance the embedding capacity Chia-Chen Lin et al. [29] proposes a new data hiding scheme based on a notation transformation concept. The image quality of stego-images with their proposed scheme remains above 30 dB for most test images when the hiding capacity is above 90000 bits. KB Raja et al. [19] proposes Bit Length Replacement Steganography Based on DCT Coefficients (BLR). It is observed that the BLR algorithm has better PSNR, security and capacity compared to the existing algorithm.

2.2.2. DWT based Data Hiding

Wavelet-based steganography [2] and [26] is a new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information

is stored in the wavelet coefficients of an image,instead of changing bits of the actual pixels.

3. THE PROPOSED METHODOLOGY: DCT DIFFERENCE MODULATION (DCTDM) STEGANOGRAPHY

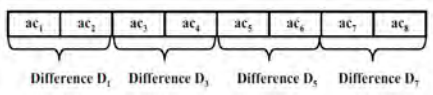
This work presents a novel DCT difference based stenographic method in transform domain , an enhanced idea of the Bhattacharyya and Sanyal's Transformation [4, 38].The main idea of this approach is to store data by modulating the difference between the DCT coefficients.In the selected cover image a plane of embedding is selected first , for a gray scale image is the image itself while for the RGB cover image is the middle green plane to minimize the distortion. The raw pixel data of targeted cover plane in transformed by taking 8×8 block DCT thus yielding $(n^2/64)$ blocks of 64 DCT coefficients each.The results of a 64-element DCT transform are 1 DC coefficient and 63 AC coefficients. The DC coefficient represents the average color of the 8×8 region. The 63 AC coefficients represent color change across the block. So since the DC coefficient gives vital information about the overall color characteristics of the 8X8 region so we exclude it and eventually the remaining 7 AC coefficients of the first row of the block from embedding data. Within each of the remaining 7 rows of 8 AC coefficients each, the binary encoding of a secret message character is embedded. This is a 2-bit embedding process where arithmetic operation is used to map a pair of binary bits into the computed difference between two adjacent AC coefficients. In order to make the algorithm resistant to compression, during extraction the range of the coefficient differences is considered to fetch the secret message bits. Further DCTDM approach shows the resistivity against different image attacks like noise addition and compression. Additionally the embedded message based on this algorithm stays undetected against some state of the art steganalysis attacks also.

4. ALGORITHM

This section describes the algorithms of the embedding and extraction process of the proposed DCTDM method.

4.1. Embedding Algorithm

1. Fetch the embedding plane of the cover image.
2. Get the 8-bit binary representation of each secret message character.
3. Transform the raw pixel data of embedding plane into DCT coefficients by taking 8X8 block DCT.
4. Take the absolute values of DCT coefficients.
5. Within each block of 64 coefficients, exclude the first row and consider the remaining matrix of 56 AC coefficients.
6. For each of the 7 rows of 8 AC coefficients embed the binary encoding of a secret message character as follows:
7. Compute the difference between non-overlapping adjacent pairs of AC coefficients thus yielding 4 difference values:



8. Perform arithmetic computations as shown in figure 5 to map 2-bits of secret message say B_i and B_{i+1} by modulating each difference D_j for $j = 1, 3, 5, 7$, where D_j = ac_j - ac_{j+1} to two distinct values of ε_1 and ε_2 such that $|\varepsilon_2 - \varepsilon_1|$ = δ
   Case 1: B_i = 0 and B_{i+1} = 0
   Magnitude of difference D_j= ε_1 & Sign of difference D_j = Positive
   Case 2: B_i = 0 and B_{i+1} = 1
   Magnitude of difference D_j= ε_2 & Sign of difference D_j = Positive
   Case 3: B_i = 1 and B_{i+1} = 0
   Magnitude of difference D_j= ε_2 & Sign of difference D_j = Negative

Case 4: B_i = 1 and B_{i+1} = 1

Magnitude of difference D_j= ε_1 & Sign of difference D_j = Negative

Message Bits	Sign of DCT Coefficient Difference	Magnitude of DCT Coefficient Difference
00	Positive	ε_1
01	Positive	ε_2
10	Negative	ε_2
11	Negative	ε_1

Figure 5. DCT difference table for data embedding

9. Update the changes to the DCT coefficients and take inverse DCT to transform back to spatial domain.
10. Integrate the inverse DCT blocks to get the Stego plane with embedded data .
11. For RGB cover image, attach the two enclosing Red and Blue planes with the stego plane to get stego image.
12. Apply lossless compression to stego image like JPEG compression with Quality Factor 100 or PNG or GIF compression techniques for ease of transmission and obtain final compressed stego image.

Figure 6 below shows the pictorial description of the embedding process.

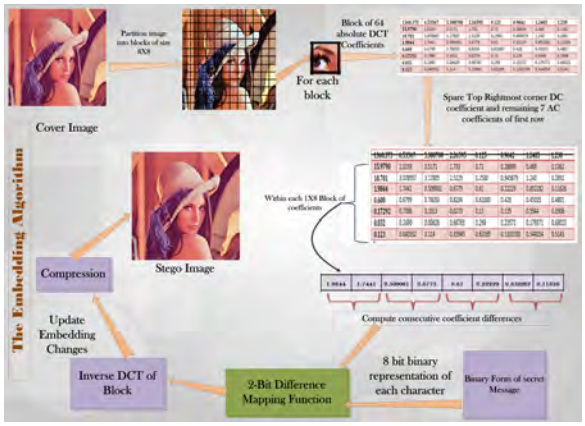
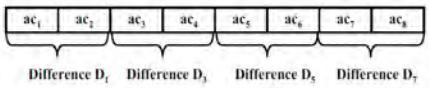


Figure 6. Pictorial Description of embedding algorithm

4.2. Extraction Algorithm

1. Get the compressed stego image.
2. Fetch the extraction plane of the stego image which is the image itself for gray scale image and the green plane for an RGB image.
3. Transform the raw pixel data of extraction plane into DCT coefficients by taking 8X8 block DCT.
4. Take the absolute values of DCT coefficients.
5. Within each block of 64 coefficients, exclude the first row as it does not contain any relevant secret message and consider the remaining matrix of 56 AC coefficients.
6. From each 8 element row of AC coefficients extract the binary code for a secret character as follows



7. Compute the difference between non-overlapping adjacent pairs of AC coefficients thus yielding 4 difference values as given below.
8. Consider the magnitude and sign of each difference D_j for $j = 1, 3, 5, 7$, where D_j = ac_j - ac_{j+1} to extract 2 secret bits of message B_i and B_{i+1} .
9. Due to distortion of the exact values of D_j while compression consider the range of difference values for D_j and its sign in extraction phase as follows in figure 7

   Case 1 : if D_j is positive and $abs(D_j) > 0$ and $abs(D_j) < \delta$ then B_i = 0 and B_{i+1} = 0

   Case 2 :if D_j is positive and $abs(D_j) \geq \delta$ then B_i = 0 and B_{i+1} = 1

   Case 3 :if D_j is negative and $abs(D_j) \geq \delta$ then B_i = 1 and B_{i+1} = 0

   Case 4 :if D_j is negative and $abs(D_j) > 0$ and $abs(D_j) < \delta$ then B_i = 1 and B_{i+1} = 1
10. Combine the binary bits together and get the ASCII values of the embedded character and eventually the secret character.
11. Continue the Extraction steps of 6 to 10 until all the secret characters have been extracted.

Sign of DCT coefficient Difference	Magnitude Range of DCT coefficient Difference	Extracted Message Bits
Positive	(0,δ)	00
Positive	[δ,∞)	01
Negative	[δ, ∞)	10
Negative	(0,δ)	11

()-open interval, []-closed interval, [)-closed to left open to right

Figure 7. DCT difference table for data extraction

Figure 8 below shows the pictorial description of the extraction process.

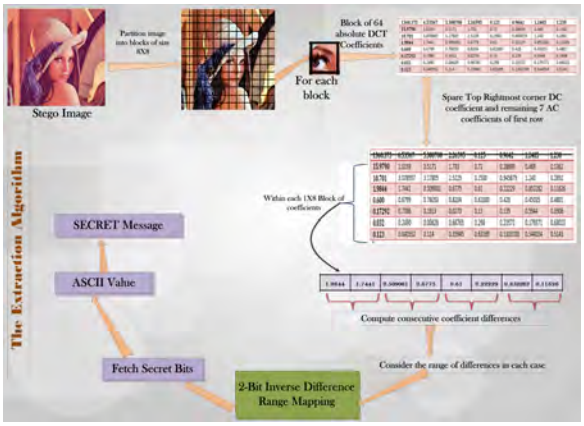


Figure 8. Pictorial Description of extraction algorithm

5. EXPERIMENTAL RESULTS

Experimental results of the proposed method has been evaluated based on two benchmarks techniques.First one is the capacity of hidden data and the second one is the imperceptibility or the quality of the stego image.

5.1. Embedding Capacity Test

Evaluating the capacity of a steganography technique means to find out the maximum number of bits that can undetectably be hidden. The payload indicates the maximum number of bits that can be hidden with an acceptable resultant stego-carrier quality.The embedding capacity of the DCTDM method has been compared with other existing methods like J-Steg [42] ,F5[47], Outguess [32] , Methods by Liu et al [8] and Lin et al [29].Some of the standard test gray images of 512×512 dimensions have been taken as the cover images for the experimental basis.

Test Image	J-Steg	F5	OutGuess	Liu et al.	Lin et al.	DCTDM
Barb	45363	45513	22699	59229	90112	131072
Boat	38374	38506	19105	50042	90112	131072
F16	35373	35295	17721	46079	90112	131072
Goldhill	45196	45505	22639	60890	90112	131072
Lena	32998	33026	16375	44131	90112	131072
Mandrill	75751	75837	37867	98989	90112	131072
Pepper	34295	34074	17016	46346	90112	131072
Tank	44417	44329	22195	61220	90112	131072
Tiffiany	31674	31516	15729	43300	90112	131072
Zelda	27557	27630	13724	37086	90112	131072

Figure 9. Comparison of embedding capacity in terms of bits

5.2. Imperceptibility Test

The deference between the cover and stego carrier should be perfectly imperceptible to the human eye, is the feature of an ideal steganographic scheme.The higher the quality of stego images, the larger the imperceptibility of the steganographic system. The quality of stego image produced by the proposed method has been tested exhaustively based on various image similarity metrics namely MSE,RMSE,PSNR,SSIM,Shannon's Entropy,KL divergence distances and Normalized Cross-correlation.

5.3. Mean Squared Error (MSE),Root Mean Squared Error (RMSE) and Peak Signal to Noise Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is the ratio between a signal's maximum power and the power of the signal's noise where as the mean squared error (MSE) measures the average of the squares of the "errors". The error is the amount of value implied by the estimator , differs from the quantity to be estimated.The root-mean-square deviation (RMSD) or root-mean-square error (RMSE) is a frequently used measure of the differences between values predicted by a model or an estimator and the values actually observed from the thing being modeled or estimated. The PSNR is used to evaluate the quality of the stego-image after embedding the secret message in the cover. Assume a cover image C(i,j) that contains N by N pixels and a stego image S(i,j) where S is generated by embedding / mapping the message bit stream. Mean squared error (MSE) of the stego image is calculated as equation 1.

$$MSE = \frac{1}{[N \times N]^2} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(ij) - S(ij)]^2 \tag{1}$$

The PSNR is computed using the following formulae given in equation 2:

$$PSNR = 10 \log_{10} 255^2 / \ MSE \ db. \tag{2}$$

A comparative study of PSNR with some other existing techniques has been shown in figure 10 below. PSNR values has been calculated by embedding same amount of secret bits as per the embedding capacity of Outguess.

5.4. Structural Similarity Measures (SSIM)

The structural similarity (SSIM) [50] index is a method for measuring the similarity between two images. SSIM is designed to improve on traditional methods like peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proved to be inconsistent with human eye perception.

Test Image	J-Steg	F5	OutGuess	Liu et al.	DCTDM
Boat	35.67	36.23	35.47	34.53	41.35
F16	36.79	37.33	36.57	35.89	44.79
Lena	36.36	36.94	36.37	35.67	40.74
Pepper	35.45	35.86	35.32	34.75	34.61
Tiffiany	35.93	36.36	35.81	35.07	37.88
Zelda	38.31	38.82	38.22	37.64	40.36

Figure 10. Comparison of PSNR with other existing ones

The SSIM metric is calculated on various windows of an image. The measure between two images x and y of common size $N \times N$ given in equation 3.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{3}$$

- where μ_x is the average of x and μ_y is the average of y.
- σ_x^2 is the variance of x.
- σ_y^2 is the variance of y.
- σ_{xy} is the covariance of x and y.
- $c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ are two variables to stabilize the division with weak denominator.
- L is the dynamic range of the pixel-values.
- $k_1 = 0.01$ and $k_2 = 0.03$ by default.

5.5. Shannon's Entropy

The term Entropy usually refers to the Shannon's Entropy, which quantifies the expected value of the information contained in a message, usually in units such as bits.The concept was introduced by Claude E.Shannon in his 1948 paper "A Mathematical Theory of Communication" [36].Named after Boltzmann's H-theorem , Shannon denoted the entropy H of a discrete random variable X with possible values $x_1, x_2, ..., x_n$ as,

$$H(X) = E(I(X)) \tag{4}$$

Here E is the expected value, and I is the information content of X.I(X) is itself a random variable. If p denotes the probability mass function of X then the entropy can explicitly be written as

$$H(X) = \sum_{i=1}^{n} p(x_i)\, I(x_i) = \sum_{i=1}^{n} p(x_i) \log_b \frac{1}{p(x_i)} = \tag{5}$$

$$-\sum_{i=1}^{n} p(x_i) \log_b p(x_i) \tag{6}$$

5.6. Steganography Security using Kullback Leibler Divergence

Denoting C the set of all covers c, Cachin's definition of steganographic security [6] is based on the assumption that the selection of covers from C can be described by a random variable c on C with probability distribution function (pdf) P. A steganographic scheme S is a mapping $C \times M \times K \rightarrow S$ that assigns a new (stego) object s, $s \epsilon C$, to each triple (c,M,K), where $M \epsilon M$ is a secret message selected from the set of communicable messages, M,

and $K \epsilon K$ is the steganographic secret key.Assuming the covers are selected with pdf P and embedded with a message and secret key both randomly (uniformly) chosen from their corresponding sets, the set of all stego images is again a random variable s on C with pdf Q. The measure of statistical detectability is the Kullback Leibler divergence

$$D_{\mathrm{KL}}(P\|Q) = \sum_{c \epsilon C} P(c) \log \frac{P(c)}{Q(c)}. \tag{7}$$

when $D_{\mathrm{KL}}(P\|Q) < \epsilon$,the stego system is called ϵ secure.

The level of security of the hidden information of developed embedding algorithm has been calculated using Kullback Leibler Divergence (KLD) and measured within a range of 0 to 1, where the value nearest to 0 indicates more secure information.

5.7. Cross Correlation

Similarity measure of two images can be done with the help of normalized cross correlation generated from the above concept using the following formula:

$$r = \frac{\sum_{(C(i,j)-m_1)(S(i,j)-m_2)}}{\sqrt{(\sum_{C(i,j)-m_1})^2}\sqrt{(\sum_{S(i,j)-m_2})^2}} \tag{8}$$

Here C is the cover image, S is the stego image,m_1 is the mean pixel value of the cover image and m_2 is the mean pixel value of stego image.

Figure 11 and 12 shows the calculated value of various image similarity metrics for LENA Gray Scale and RGB image at different payload.

Payload (in bpac)	PSNR	MSE	RMSE	SSIM	KL-Divergence	Correlation	Entropy
0	Inf	0	0	1	0	1	7.0880
0.1	44.2872	2.4230	0.9892	0.9947	0.00022367	0.9991	7.0937
0.2	40.7405	5.4832	1.4617	0.9887	0.0009905	0.9980	7.0967
0.3	38.6153	8.9445	1.8678	0.9814	0.0050	0.9968	7.1022
0.4	36.6770	13.9758	2.2875	0.9742	0.0165	0.9950	7.1064
0.5	35.2582	19.3757	2.6742	0.9675	0.0269	0.9930	7.1102
0.6	34.4235	23.4816	2.9501	0.9625	0.0361	0.9916	7.1142
0.7	33.5308	28.8401	3.2541	0.9551	0.0425	0.9896	7.1200
0.8	32.9237	33.1672	3.4735	0.9495	0.0568	0.9880	7.1249
0.889 (Max)	32.4100	37.3322	3.7229	0.9429	0.0662	0.9865	7.1312

Figure 11. Different Image Similarity Metrics for Lena (512x512) Gray Scale Image at different payload

6. ATTACKS ON THE STEGO IMAGES

Spatial methods falter from most types of image attacks and the robustness of the spatial techniques limits the overall effectiveness.The transform domain representation of an image serves as a stronger channel for transmitting information covertly while minimizing distortion of the container image.DCTDM based steganographic image has been tested against various image attacks like noise addition, image compression and results are simulated in different subsections below.

6.1. Noise attack on the DCTDM Images

Two types of noise namely Gaussian and Salt & Pepper noise ,has been added to the DCTDM stego images before the extraction operation takes place and the final results is quite promising and has given a satisfied performance.Figure 13 and 14 shows the results of noise attack.

Payload in bpac (no of char)	PSNR	MSE	RMSE	SSIM	KL-Divergence	Correlation	Entropy
0	Inf	0	0	1	0	1	7.7507
0.1(3225)	47.4739	1.1633	1.0698	0.9982	0.00021323	0.9998	7.5975
0.2(6450)	43.4474	2.9400	1.6408	0.9960	0.0011	0.9996	7.5990
0.3(9675)	41.0821	5.0684	2.1791	0.9931	0.0054	0.9993	7.6019
0.4(12900)	38.9960	8.1938	2.6640	0.9905	0.0154	0.9988	7.6044
0.5(16125)	37.5266	11.4925	3.1103	0.9882	0.0236	0.9983	7.6059
0.6(19350)	36.6912	13.9303	3.4318	0.9865	0.0351	0.9980	7.6079
0.7(22575)	35.7448	17.3221	3.7759	0.9838	0.0397	0.9975	7.6102
0.8(25800)	35.1598	19.8200	4.0196	0.9819	0.0533	0.9971	7.6120
0.889(28672) (Max)	34.7437	21.8126	4.2741	0.9800	0.0577	0.9969	7.6154

Figure 12. Different Image Similarity Metrics for Lena (512x512) RGB Image at different payload

Noise Type	Noise Scalar Value	Char error rate (in %)
Gaussian	Mean= 0.001,Variance= 0.000001	4.3436
Salt & Pepper	0.0002	2.6748
Gaussian	Mean= 0.002,Variance= 0.000002	7.2393
Salt & Pepper	0.0003	4.3190
Gaussian	Mean= 0.003,Variance= 0.000003	7.5644
Salt & Pepper	0.0004	4.8589
Gaussian	Mean= 0.004,Variance= 0.000004	9.4785
Salt & Pepper	0.0005	4.8405
Gaussian	Mean= 0.01,Variance= 0.00001	22.5460
Salt & Pepper	0.001	7.3006
Gaussian	Mean= 0.05,Variance= 0.00005	70.4049
Salt & Pepper	0.005	29.2086

Figure 13. Noise Attack on DCTDM Gray images

Noise Type	Noise Scalar Value	Char error rate (in %)
Gaussian	Mean= 0.001,Variance= 0.000001	3.1472
Salt & Pepper	0.0002	3.6258
Gaussian	Mean= 0.002,Variance= 0.000002	4.8957
Salt & Pepper	0.0003	4.1043
Gaussian	Mean= 0.003,Variance= 0.000003	5.4847
Salt & Pepper	0.0004	4.7055
Gaussian	Mean= 0.004,Variance= 0.000004	7.2515
Salt & Pepper	0.0005	5.3313
Gaussian	Mean= 0.01,Variance= 0.00001	20.2945
Salt & Pepper	0.001	8.3742
Gaussian	Mean= 0.05,Variance= 0.00005	70.1411
Salt & Pepper	0.005	27.2638

Figure 14. Noise Attack on DCTDM RGB images

6.2. Compression on DCTDM Images

DCTDM stego images (both Gray and RGB) has also been tested exhaustively against image compression attack. Figure 15 below shows the compression ratio of different DCTDM based stego images at different embedding rates.

Embedding Rate in bpac										
Image	0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	Max
Lena (Gray)	1	0.5828	0.5964	0.6090	0.6210	0.6322	0.6453	0.6576	0.6707	0.6963
Lena (RGB)	1	0.6108	0.6121	0.6131	0.6142	0.6154	0.6173	0.6189	0.6206	0.6250
Mandrill (RGB)	1	0.7961	0.7942	0.7929	0.7919	0.7909	0.7897	0.7886	0.7874	0.7874
Pepper (RGB)	1	0.6465	0.6479	0.6490	0.6501	0.6508	0.6516	0.6521	0.6527	0.6568

Figure 15. Image Compression Ratio for DCTDM Stego Images at different embedding rates

7. STEGANALYSIS ON THE STEGO IMAGES

Steganalysis is the science of detecting hidden information. On the way to design secure steganographic algorithms, the development of attacks is essential to assess security.In this work all the stego images produced by DCTDM algorithms has been tested against some of well known steganalysis attack namely Chi-square Analysis , RS Steganalysis , Sample Pair Analysis, Triples and Weighted Stego Analysis.Finally DCTDM algorithms has been tested with present day state of the art steganalysis technique using RICH Model.

7.1. Chi-Square Analysis

Andreas Pfitzmann and Andreas Westfeld [46] developed a method from the statistical analysis of Pair of Values (PoVs), exchanged during sequential embedding. Sequential embedding makes PoVs in the values embeded in. For example, embedding in the spatial domain makes PoVs (2i,2i +1) such that $0 \leftrightarrow 1$, $2 \leftrightarrow 3$, $4 \leftrightarrow 5$, $252 \leftrightarrow 253$, $254 \leftrightarrow 255$. This will affect the histogram Y_k of the image pixel value k , while the sum of $Y_{2i} + Y_{2i+1}$ will remain unchanged. Thus the expected distribution of the sum of adjacent values obtained from (9) and the χ^2 value for the difference between distributions with v -1 degrees of freedom obtained from (10). From (9) and (10) the χ^2 statistic PoVs are obtained as given in (11).

$$E(Y_{2i}) = \frac{1}{2}(Y_{2i} + Y_{2i+1}) \tag{9}$$

$$\chi^2 = \sum_{i=1}^{v} \frac{(F - E(F))^2}{E(F)} \tag{10}$$

$$\chi^2_{PoV} = \sum_{i=1}^{127} \frac{((Y_{2i}) - (\frac{1}{2}(Y_{2i} + Y_{2i+1})))^2}{(Y_{2i} + Y_{2i+1})} \tag{11}$$

Figure 16 and 17 below shows the various plots based on the Chi Square Analysis.

7.2. RS Analysis

Fridrich et al. [13] devised an efficient LSB steganalytic method,able to estimate the length of the embedded message accurately on a digital image. In a 8-bit image, there lies some degree of correlation between the LSB and the other seven bit planes and insertion of a message in the LSB plane in a randomized manner, reduces correlation between the LSB and remaining bit planes or even lost. Let I be the 8 bit gray scale image to be analyzed having width W and height H pixels. Each pixel has been denoted as P having value 0,1, . . . ,255. Next step is to capture the spatial correlations using a discrimination function f that assigns a real number $f(x_1, ..., x_n) \in R$ to a group of pixels $G = (x_1, ..., x_n)$. Let the discrimination function defined in equation 12 which measures the smoothness of G the noisier the group G is, the larger the value of the discrimination function becomes.

$$f(x_1, ..., x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \tag{12}$$

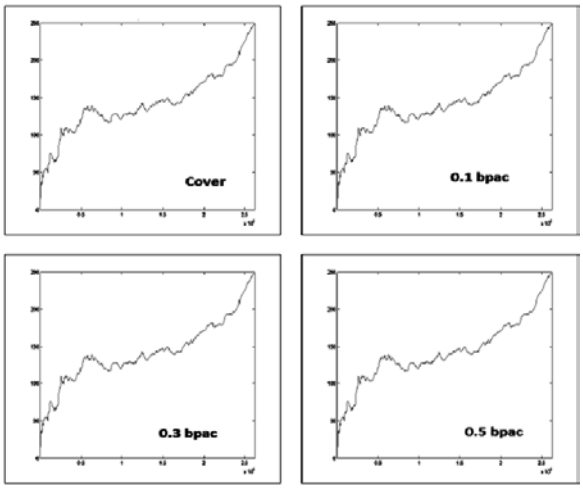


Figure 16. Plot of Chi Square Statistics for DCTDM stego images (LENA 512x512)

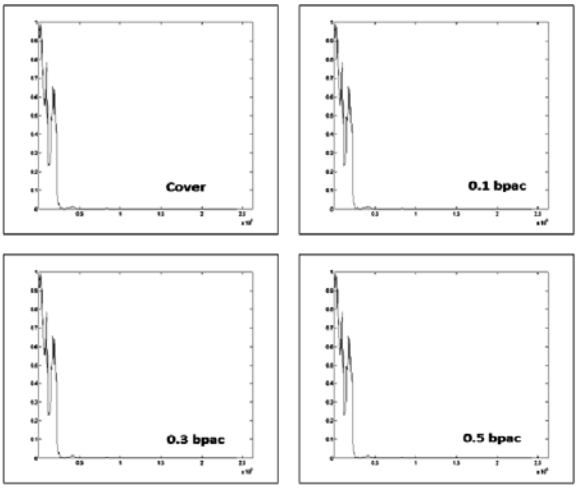


Figure 17. Plot of Chi Square Probability Distribution for DCTDM stego images (LENA 512x512)

The LSB embedding increases the noisiness in the image, and thus we expect the value of f to increase after LSB embedding. The LSB embedding process can be conveniently described using a flipping function $F_1 : 0 \leftrightarrow 1$, $2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$, and F_{-1} be a shifting function denoted as $F_{-1} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256$ over P. For completeness,F_0 be the identity function such as $F_0(x) = x, \forall x \varepsilon P$. Next step is to apply a mask M , used to represents which function is to apply to each element of a group G. The mask M is an n-tuple with values -1, 0, 1. Similarly, define -M as M's compliment. The discrimination function f and the flipping operation F define three types of pixel groups:Regular (R), Singular (S)and Unchanged (U) depending on how the flipping changes the value of the discrimination function.

- Regular groups: $G \epsilon R_M \Leftrightarrow f(F(G)) > f(G)$
- Singular groups: $G \epsilon S_M \Leftrightarrow f(F(G)) < f(G)$
- Unusable groups: $G \epsilon U_M \Leftrightarrow f(F(G)) = f(G)$

RS Analysis method concludes that, for typical images $R_M \approx R_{-M}$ and $S_M \approx S_{-M}$ and no change in R and S value for embedding character of various sizes.Results of RS analysis in various stego images having different embedding capacity has been shown in figure 18 and 19.

Insertion Rate (in bpac)	F_1 flipping			F_{-1} flipping		
	R_M	S_M	U_M	R_{-M}	S_{-M}	U_{-M}
0	32716	21079	77277	32545	21044	77483
0.1	32716	21079	77277	32545	21044	77483
0.3	32716	21079	77277	32545	21044	77483
0.5	32716	21079	77277	32545	21044	77483
0.7	32716	21079	77277	32545	21044	77483
0.8	32716	21079	77277	32545	21044	77483
0.889(max)	32716	21079	77277	32545	21044	77483

Figure 18. RS Parameter at various insertion rate for DCTDM stego images (LENA 512x512)

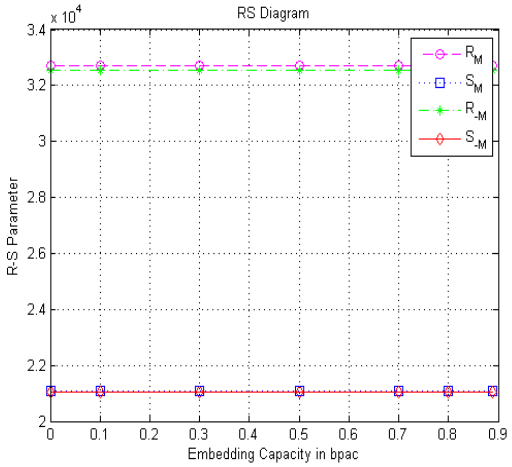


Figure 19. RS Diagram at various insertion rate for DCTDM stego images (LENA 512x512)

7.3. Sample Pair Analysis

Sample Pair Analysis (SPA) was first introduced by Dumitrescu et al. [11] but the more extensible alternative approach has been proposed by Ker [21].Similar to RS analysis, SPA evaluates groups of spatially adjacent pixels. It assigns each pair (x_1, x_2) to a trace set C_i, so that

$$C_i = \{(x_1, x_2) \in \chi^2 | \lfloor \frac{x_2}{2} \rfloor - \lfloor \frac{x_1}{2} \rfloor = i\} \; where \; |i| \; \leq \lfloor (max\chi - min\chi)/2 \rfloor \xi \tag{13}$$

Each trace set C_i can be further partitioned into up to four trace subsets, of which two types can be distinguished:

- Pairs (x_1, x_2) whose values differ by $i = x_2 - x_1$ and whose first elements x_1 are *even* belong to ξ_i.
- Pairs (x_1, x_2) whose values differ by $i = x_2 - x_1$ and whose first elements x_1 are *odd* belong to Θ_i.

Consequently, the union of trace subsets $\xi_{2i+1} \cup \xi_{2i} \cup \Theta_{2i} \cup \Theta_{2i-1} = C_i$ constitutes a trace set (shown in Figure 20 below).

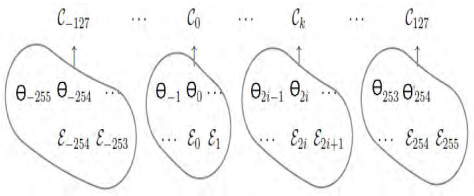


Figure 20. Relation of trace sets and subsets in SPA (X = [0, 255])

This definition of trace sets and subsets ensures that the LSB replacement embedding operation never changes a sample pair's trace set, i.e., $C_i^{(o)} = C_i^{(p)} = C_i$, but may move sample pairs between trace subsets that constitute

the same trace set. So cardinalities $|C_i|$ are invariant to LSB replacement,whereas $|\xi_i|$ and $|\Theta_i|$ are sensitive. The transition probabilities between trace subsets depend on the net embedding rate p as depicted in the transition diagram of Figure 21.

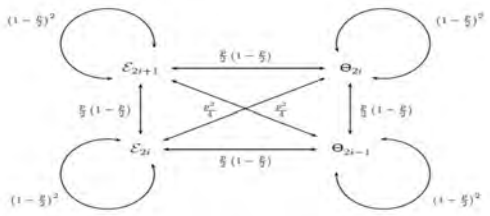


Figure 21. Transition diagram between trace subsets under LSB replacement

So the effect of applying LSB replacement with rate p on the expected cardinalities of the trace subsets can be written as four quadratic equations (as shown in matrix notation form in equation 13.1 below)

$$\begin{bmatrix} |\mathcal{E}^{(p)}_{2i+1}| \\ |\mathcal{E}^{(p)}_{2i}| \\ |\Theta^{(p)}_{2i}| \\ |\Theta^{(p)}_{2i-1}| \end{bmatrix} = \begin{bmatrix} \left(1-\frac{p}{2}\right)^2 & \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p^2}{4} \\ \frac{p}{2}\left(1-\frac{p}{2}\right) & \left(1-\frac{p}{2}\right)^2 & \frac{p^2}{4} & \frac{p}{2}\left(1-\frac{p}{2}\right) \\ \frac{p}{2}\left(1-\left|\frac{p}{2}\right.\right) & \frac{p^2}{4} & \left(1-\frac{p}{2}\right)^2 & \frac{p}{2}\left(1-\frac{p}{2}\right) \\ \frac{p^2}{4} & \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p}{2}\left(1-\frac{p}{2}\right) & \left(1-\frac{p}{2}\right)^2 \end{bmatrix} \begin{bmatrix} |\mathcal{E}^{(0)}_{2i+1}| \\ |\mathcal{E}^{(0)}_{2i}| \\ |\Theta^{(0)}_{2i}| \\ |\Theta^{(0)}_{2i-1}| \end{bmatrix} \tag{13.1}$$

Trace subsets $\xi^{(p)}$ and $\Theta^{(p)}$ are observable from a given stego object. An approximation of the cardinalities of the cover trace subsets $\xi^{(0)}$ and $\Theta^{(0)}$ can be rearranged as a function of p by inverting Equation (13.1). The transition matrix is invertible for $p < 1$ is given in Equation (13.2).

$$\begin{bmatrix} |\hat{\mathcal{E}}^{(0)}_{2i+1}| \\ |\hat{\mathcal{E}}^{(0)}_{2i}| \\ |\Theta^{(0)}_{2i}| \\ |\Theta^{(0)}_{2i-1}| \end{bmatrix} = \frac{1}{(2-2p)^2} \begin{bmatrix} (2-p)^2 & p(p-2) & p(p-2) & p^2 \\ p(p-2) & (2-p)^2 & p^2 & p(p-2) \\ p(p-2) & p^2 & (2-p)^2 & p(p-2) \\ p^2 & p(p-2) & p(p-2) & (2-p)^2 \end{bmatrix} \begin{bmatrix} |\mathcal{E}^{(p)}_{2i+1}| \\ |\mathcal{E}^{(p)}_{2i}| \\ |\Theta^{(p)}_{2i}| \\ |\Theta^{(p)}_{2i-1}| \end{bmatrix} \tag{13.2}$$

With one additional cover assumption, namely $|\xi^{(0)}_{2i+1}| \approx |\Theta^{(0)}_{2i+1}|$, the first equation of this system for i can be combined with the fourth equation for $i+1$ to obtain a quadratic estimator $\hat{p}$ for p.

$$|\hat{\xi}^{(0)}_{2i+1}| = |\hat{\Theta}^{(0)}_{2i+1}| \tag{14}$$

$$\begin{aligned} 0 = {} & \frac{(2-p)^2}{(2-2p)^2}(|\xi^{(p)}_{2i+1}| - |\Theta^{(p)}_{2i+1}|) \\ & + \frac{(p)^2}{(2-2p)^2}(|\Theta^{(p)}_{2i-1}| - |\xi^{(p)}_{2i+3}|) \\ & + \frac{(p(p-2))}{(2-2p)^2}(|\xi^{(p)}_{2i}| + |\Theta^{(p)}_{2i}| - |\xi^{(p)}_{2i+2}| - |\Theta^{(p)}_{2i+2}|) \end{aligned} \tag{15}$$

$$\begin{aligned} 0 = {} & p^2(|C_i| - |C_{i+1}|) + 4(|\xi^{(p)}_{2i+1}| \\ & - |\Theta^{(p)}_{2i+1}|) \\ & + 2p(|\xi^{(p)}_{2i+2}| + |\Theta^{(p)}_{2i+2}| - 2|\xi^{(p)}_{2i+1}| \\ & + |\Theta^{(p)}_{2i+1}| - |\xi^{(p)}_{2i}| - |\Theta^{(p)}_{2i}|) \end{aligned} \tag{16}$$

The smaller root of Equation (21) is a secret message length estimate $\hat{p}_i$ based on the information of pairs in trace set C_i. Standard SPA sums up the family of estimation equation (21) for a fixed interval around C_0, such as $-30 = i = 30$, and calculates a single root $\hat{p}$ from the aggregated quadratic coefficients. Results of SPA analysis in DCTDM image at different embedding capacity has been depicted in figure 22.

ORIGINAL EMBEDDING BIT RATE p	0%	10%	20%	30%	40%	50%	60%	70%	80%	86%
DETECTED EMBEDDING BIT RATE $\hat{p}$	0.00424 %	0.5546 %	0.4589 %	0.2301 %	0.4592 %	0.5322 %	0.8421 %	1.394 %	4.03 %	5.027 %

Figure 22. Sample Pair Detection Rate for DCTDM stego images (LENA 512x512)

7.4. Triples and Weighted Stego Analysis

Triples analysis [23] considers 3-tuples of sample values.First step is to fix a trace set $C_{m,n}$ and then it will be divided into 8 trace subsets. Subsets connected by an edge are related by the flipping of the LSB of exactly one sample in the 3-tuple.Generally the probability of transition from onetrace subset to another is $p^i(1-p)^{(3-i)}$, where i is the length of the shortest path between them as shown in Figure 28.If the trace subsets are enumerated in the order $\xi_{2m,2n}, \Theta_{2m-1,2n}, \xi_{2m+1,2n-1}, \Theta_{2m,2n-1}, \xi_{2m,2n+1}, \Theta_{2m-1,2n+1}, \xi_{2m+1,2n}, \Theta_{2m,2n}$ then the transition matrix is computed as,

$$T_3 = \begin{pmatrix}
(1-p)^3 & p(1-p)^2 & p(1-p)^2 & p^2(1-p) & p(1-p)^2 & p^2(1-p) & p^2(1-p) & p^3 \\
p(1-p)^2 & (1-p)^3 & p^2(1-p) & p(1-p)^2 & p^2(1-p) & p(1-p)^2 & p^3 & p^2(1-p) \\
p(1-p)^2 & p^2(1-p) & (1-p)^3 & p(1-p)^2 & p^2(1-p) & p^3 & p(1-p)^2 & p^2(1-p) \\
p^2(1-p) & p(1-p)^2 & p(1-p)^2 & (1-p)^3 & p^3 & p^2(1-p) & p^2(1-p) & p(1-p)^2 \\
p(1-p)^2 & p^2(1-p) & p^2(1-p) & p^3 & (1-p)^3 & p(1-p)^2 & p(1-p)^2 & p^2(1-p) \\
p^2(1-p) & p(1-p)^2 & p^3 & p^2(1-p) & p(1-p)^2 & (1-p)^3 & p^2(1-p) & p(1-p)^2 \\
p^2(1-p) & p^3 & p(1-p)^2 & p^2(1-p) & p(1-p)^2 & p^2(1-p) & (1-p)^3 & p(1-p)^2 \\
p^3 & p^2(1-p) & p^2(1-p) & p(1-p)^2 & p^2(1-p) & p(1-p)^2 & p(1-p)^2 & (1-p)^3
\end{pmatrix}$$

The inverse of T_3 consists of third order rational polynomials in p. So after substitution $q = \frac{1}{1-2p}$ the simplified matrix is,

$$T_3^{-1} = \frac{1}{8}\begin{pmatrix}
(1+q)^3 & (1-q)(1+q)^2 & (1-q)(1+q)^2 & (1-q)^2(1+q) & \cdots \\
(1-q)(1+q)^2 & (1+q)^3 & (1-q)^2(1+q) & (1-q)(1+q)^2 & \cdots \\
(1-q)(1+q)^2 & (1-q)^2(1+q) & (1+q)^3 & (1-q)(1+q)^2 & \cdots \\
(1-q)^2(1+q) & (1-q)(1+q)^2 & (1-q)(1+q)^2 & (1+q)^3 & \cdots \\
(1-q)(1+q)^2 & (1-q)^2(1+q) & (1-q)^2(1+q) & (1-q)^3 & \cdots \\
(1-q)^2(1+q) & (1-q)(1+q)^2 & (1-q)^3 & (1-q)^2(1+q) & \cdots \\
(1-q)^2(1+q) & (1-q)^3 & (1-q)(1+q)^2 & (1-q)^2(1+q) & \cdots \\
(1-q)^3 & (1-q)^2(1+q) & (1-q)^2(1+q) & (1-q)(1+q)^2 & \cdots
\end{pmatrix}$$

For a given stego image , considering each trace set $C_{m,n}$ and counting the trace subsets to form a vector $\acute{X}$. Next step is to hypothesize a value of p and form estimate for the sizes of the trace subsets of the cover image using the following

$$\hat{X} = {T_3}^{-1}\acute{X} \tag{17}$$

For the analogous property or the parity symmetry,$\xi_{2m,2n} = \Theta_{2m,2n}$ each m,n and considering just one case of parity symmetry, $\xi_{2m+1,2n+1} = \Theta_{2m+1,2n+1}$.Error terms for each m and n can be computed as

$$\epsilon_{m,n} = \hat{\xi}_{2m+1,2n+1} - \hat{\Theta}_{2m+1,2n+1} \tag{18}$$

Final step is to find the value of embedding rate p which minimizes the error rate.

Introduced by Fridrich and Goljan [15], WS steganalysis estimates the hidden payload, more precisely, the embedding rate p, of a stego object created by applying the LSB replacement embedding operation to uniformly distributed positions of the cover. The method has been extended to detect sequential embedding by Ker [24], further refined in [22].

Sample Pair ,Triples and WS analysis has been tested over the pepper 512×512 gray scale image and the overall observations are notified.Over a wide range of p varying from 0.00305 to 0.875 the percentage of deviation in estimated embedding rate made by WS Analysis with bias correction is above 97.95% where as without bias correction yields slightly better and less deviation % of 28.155 and 65.0123 for actual embedding rates of 0.00152 and 0.00305 respectively.For a wide span of p ranging from 0.122 to 0.875 the deviation rate is above 97%. Similar observation is obtained considering steganalysis performed by lsb detectors like SP and Triples. Triples analysis is quiet close to WS Analysis with bias correction, yielding a high deviation % of 98.60 and above for the range of 0.0152 to 0.875. While even SP analysis yielding a high deviation % of 85.39 and above for all p above 0.0305 which proves that DCTDM method is resistant to attacks of different LSB detectors like WS , SP and Triples.Results of SP,Triples and WS analysis on DCTDM images has been shown below on figure 23 and 24 respectively.

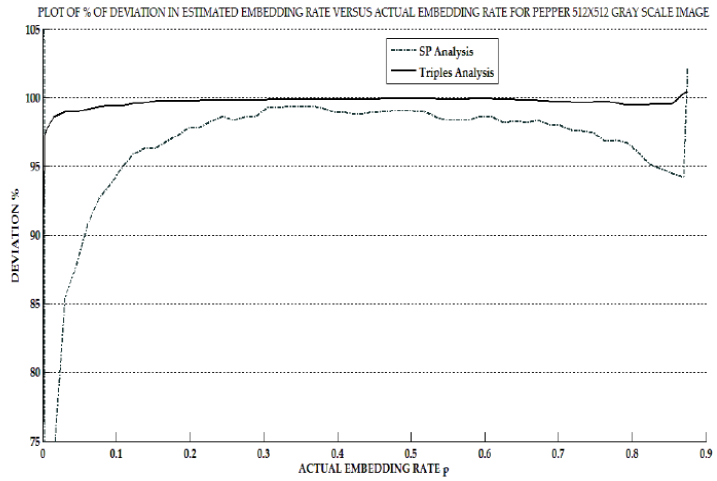


Figure 23. Plot of Deviation of the estimated rate vs actual embedding rate for Pepper 512x512 image for SP and Triples Analysis

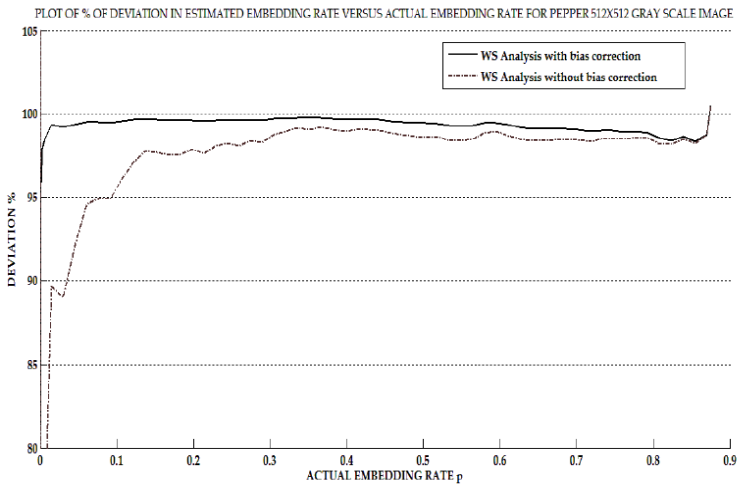


Figure 24. Plot of Deviation of the estimated rate vs actual embedding rate for Pepper 512x512 image for WS Analysis

7.5. Steganalysis using RICH Model

To demonstrate the robustness of the proposed DCTDM image steganographic algorithm the stego images produced at different payloads has been tested using the features of JPEG rich model [14, 25].Rich models require a scalable machine learning algorithm and designed based on the ensemble classifier [17] for all experiments as it enables fast training in high-dimensional feature spaces and its performance on low-dimensional feature sets is comparable to the much more complex SVMs [17].

The performance of DCTDM method has been compared with some other like F5[47] , MB[35], YASS[20], MME[49], BCH, and BCHopt[43].

For evaluating the performance of every steganographic method, stego images using a range of different payload sizes expressed in terms of bits per nonzero AC DCT coefficient (bpac), and trained using a separate classifier to detect each of them. Before classification, all cover-stego pairs were divided into two halves for training and testing, respectively. The minimal total error P_E under equal priors achieved on the testing set as

$$P_E = min(P_{FA})[\frac{P_{FA} + P_{MD}(P_{FA})}{2}] \tag{19}$$

where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate. The steganalysis performance of the proposed DCTDM method has been compared with different JPEG steganalysis method mentioned above using the following feature spaces (models), the numbers in brackets denote their dimensionality:

- CHEN (486) = Markov features utilizing both intra- and inter-block dependencies.
- CC-CHEN (972) = CHEN features improved by Cartesian calibration.
- LIU (216) = the union of diff-absNJ-ratio and ref-diff-absNJ features published in.
- CC-PEV (548) = Cartesian-calibrated PEV feature set.
- CDF (1,234) = CC-PEV features expanded by SPAM features [16] extracted from spatial domain.
- CC-C300 (48,600) = the high-dimensional feature space proposed in.
- CF* (7,850) = compact rich model for DCT domain proposed in.
- JRM (11,255) = the rich model proposed in this paper, without calibration.
- CC-JRM (22,510) = Cartesian-calibrated JRM.
- J+SRM (35,263) = the union of CC-JRM and the Spatial-domain Rich Model (SRM) proposed in.

Resulting errors P_E of different embedding methods are reported in figure 25.From the steganalysis point of view it can be said that the performance of the DCTDM method based on RICH model analysis is quite promising compared to other existing one except the BCHopt method.

Algorithm	Payload (bpac)	CHEN (486)	CC-CHEN (972)	LIU (216)	CC-PEV (548)	CDF (1,234)	CC-C300 (48,600)	C*F (7,850)	JRM (11,255)	CC-JRM (22,510)	J+SRM (35,263)
nsF5	0.050	0.4153	0.3816	0.3377	0.3690	0.3594	0.3722	0.3377	0.3407	0.3298	0.3146
	0.100	0.3097	0.2470	0.1732	0.2239	0.2020	0.2207	0.1737	0.1782	0.1616	0.1375
	0.150	0.2094	0.1393	0.0706	0.1171	0.0906	0.1127	0.0720	0.0793	0.0663	0.0468
	0.200	0.1345	0.0708	0.0273	0.0549	0.0360	0.0486	0.0273	0.0338	0.0255	0.0150
MBS	0.010	0.4070	0.3962	0.3826	0.3876	0.3786	0.4038	0.3710	0.3478	0.3414	0.3260
	0.020	0.3178	0.2962	0.2780	0.2827	0.2684	0.3120	0.2560	0.2156	0.2122	0.1832
	0.030	0.2395	0.2100	0.1925	0.1965	0.1795	0.2241	0.1684	0.1266	0.1195	0.0983
	0.040	0.1770	0.1437	0.1288	0.1298	0.1135	0.1594	0.1087	0.0751	0.0670	0.0494
	0.050	0.1243	0.0946	0.0812	0.0833	0.0704	0.1176	0.0684	0.0427	0.0373	0.0282
YASS (12)	0.077	0.2009	0.1825	0.2324	0.2279	0.1268	0.9030	0.0532	0.0324	0.0303	0.0173
YASS (11)	0.114	0.1989	0.1585	0.2118	0.1573	0.0718	0.0701	0.0437	0.0349	0.0227	0.0111
YASS (8)	0.138	0.2520	0.1911	0.1886	0.1827	0.0742	0.0500	0.0271	0.0287	0.0178	0.0104
YASS (10)	0.159	0.2334	0.1476	0.1793	0.1341	0.0507	0.0370	0.0164	0.0210	0.0103	0.0054
YASS (3)	0.187	0.1277	0.0876	0.1301	0.0723	0.0224	0.0350	0.0146	0.0165	0.0081	0.0045
MME	0.050	0.4678	0.4546	0.4479	0.4492	0.4340	0.4427	0.4443	0.4424	0.4307	0.4194
	0.100	0.3001	0.2611	0.2574	0.2613	0.2501	0.3026	0.2466	0.2286	0.2091	0.1891
	0.150	0.2165	0.1735	0.1677	0.1721	0.1586	0.2299	0.1608	0.1404	0.1221	0.1027
	0.200	0.0217	0.0104	0.0127	0.0127	0.0124	0.0726	0.0153	0.0112	0.0080	0.0059
BCH	0.100	0.4599	0.4496	0.4448	0.4426	0.4390	0.4497	0.4290	0.4305	0.4229	0.4060
	0.200	0.3594	0.3124	0.3087	0.2974	0.2752	0.2958	0.2629	0.2707	0.2369	0.1946
	0.300	0.1383	0.0889	0.0862	0.0779	0.0697	0.0912	0.0663	0.0715	0.0536	0.0390
BCHopt	0.100	0.4726	0.4683	0.4558	0.4618	0.4595	0.4684	0.4550	0.4515	0.4480	0.4306
	0.200	0.4032	0.3712	0.3583	0.3548	0.3368	0.3517	0.3265	0.3253	0.3030	0.2582
	0.300	0.2400	0.1711	0.1719	0.1605	0.1356	0.1681	0.1289	0.1389	0.1102	0.0830
DCTDM	*0.100*	*0.4421*	*0.4541*	*0.4326*	*0.3948*	*0.4543*	*0.4278*	*0.3342*	*0.4537*	*0.4213*	*0.3109*
	0.200	*0.4034*	*0.3369*	*0.3671*	*0.3432*	*0.3290*	*0.3541*	*0.3126*	*0.3211*	*0.3043*	*0.2791*
	0.300	*0.2876*	*0.2314*	*0.1861*	*0.1507*	*0.1125*	*0.1654*	*0.1271*	*0.1364*	*0.1094*	*0.0764*

Figure 25. Median Testing Error for Different JPEG steganographic methods

8. COMPARISON WITH OTHER EXITING METHOD

This section compares the developed DCTDM with the existing methods like Least-significant-bit (LSB) [5, 7], PVD [48], GLM [12] all in Spatial domain and methods like JSteg [42] , F5 [47], Outguess [32] , Liu et al [8] , KB Raja et al.[19], Danti et al.[9] and Chia-Chen Lin et al. [29] all in DCT domain.Table 1 and 2 shows the comparison of DCTDM method with other existing methods in Spatial and DCT domain respectively.

Table 1. Comparison of DCTDM with other Spatial Domain Methods

LSB, PVD and GLM	DCTDM
i) All are spatial domain techniques. Data can be easily tractable from raw pixel intensities and falter from most types of image attacks.	i) It is a transform domain technique, extraction is done from dct coefficients which is far more complex but robust against any type of image attacks.
ii) Works only on uncompressed image.	ii) Works on both uncompressed and compressed image.
iii) For evaluating performance only MSE and PSNR has been incorporated.	iii) In addition to MSE and PSNR various other image similarity metrics has been incorporated.
iv) Embedding capacity is low.	iv) Embedding capacity is high.
v) Security of hidden data has not tested	v) Security of hidden data has been tested with Kullback Leibler Divergence and the security is very high.
vi) Falters from steganalysis techniques	vi) Tested against steganalysis attack like Chi-Square [46] , RS analysis [13] and Sample Pair Analysis [11, 21] and the performance is satisfactory.

8.1. Comparative Study between HUGO Steganography Method and DCTDM

1. HUGO is a content adaptive spatial domain algorithm while DCTDM in order to enhance its security embeds bits in transform domain. It achieves higher security than transform domain techniques that directly manipulate

Table 2. Comparison of DCTDM with other Transform Domain Methods

JSteg ,F5 ,Outguess ,Liu et al. ,Raja et al. , Danti et al. and Lin et al.	DCTDM
i) All works only on uncompressed image.	i) Works on both uncompressed and compressed image.
ii) For evaluating the performance only MSE and PSNR has been incorporated.	ii) In addition to MSE and PSNR various other image similarity metrics has been incorporated.
iii) Embedding capacity is low.	iii) Embedding capacity is high.
iv) Security of hidden data has not tested	iv) Security of hidden data has been tested with Kullback Leibler Divergence and the security is very high.
v) Not tested against various steganalysis attacks	v) Tested against steganalysis attack like Chi-Square [46] , RS analysis [13] and Sample Pair Analysis[11, 21].

DCT coefficient values as DCTDM embeds into adjacent DCT coefficient differences thus manipulating two coefficients together to hide bits and direct extraction merely from single DCT value may not be possible in existing DCT based steganographic approach like F5[47], Danti et al[9] etc.

2. As HUGO relies on minimal impact embedding similarly DCTDM attempts to adjust the modified DCT coefficient values optimally so as to have minimum diversion while performing inverse DCT.
3. DCTDM extraction additionally is noise and lossless compression resistant while HUGO and other spatial domain method is unable to deal with.
4. Average classification error P_E of DCTDM for different payload using 2nd order SPAM feature is quite comparable with HUGO classification error as shown in the plots of figure 26.

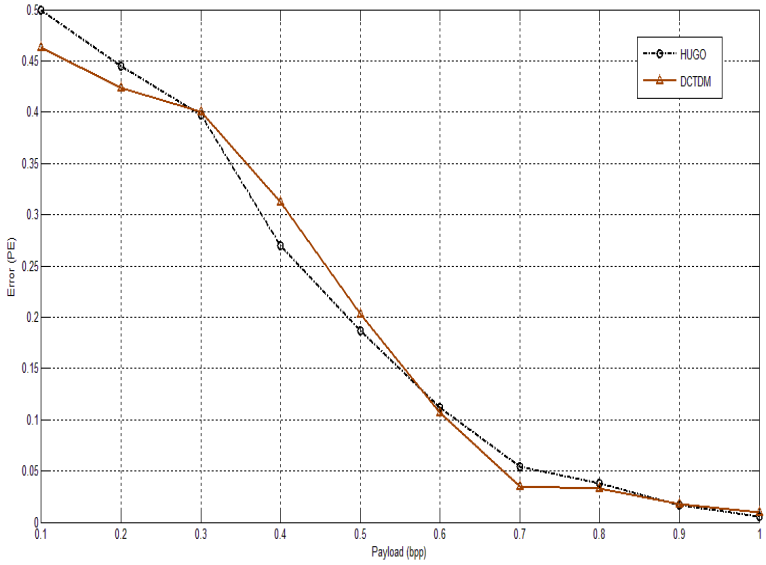


Figure 26. Comparative study of steganalysis of HUGO and DCTDM using 2nd order SPAM feature (dim 686) using ensemble classifier

9. CONCLUSION

This work dealt with an efficient image steganography method in Discrete Cosine Transform domain.From the comparative study it has been identified DCTDM method performs better compared to some other existing methods in terms of various performance detectors like embedding capacity,PSNR,SSIM etc. Additionally DCTDM approach is robust against different image attacks like noise addition,compression.From the security aspects the relative entropy

distance (KL divergence) is very low between the cover and stego image which yields a very high security value of the hidden data.The hidden message also stays undetected after application of some well known steganalysis like ChiSquare,RS Analysis , Sample Pair and Triples Analysis method on it.DCTDM gives a moderate results against RICH Model analysis also. In summary it can be concluded that the proposed DCTDM method has the following advantages:

- The embedding capacity provided by the DCTDM method is much larger than those provided by JSteg, F5, OutGuess and others steganographic methods mentioned above.
- Value of different similarity metric parameters are quite promising .
- Security of the hidden data is very high.
- This approach can avoid different image attacks also including some state of the art different modern steganalysis methods also.

REFERENCES

[1] Ross J. Anderson. and Fabien A.P.Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection*, 16:474–481, 1998.
[2] Ali Al Ataby and Fawzi Al Naima. A modified high capacity image steganography technique based on wavelet transform. *The International Arab Journal of Information Technology*, 7:358–364, 2010.
[3] Souvik Bhattacharyya. and Gautam Sanyal. Implementation and design of an image based steganographic model. In *Proceedings of IEEE International Advance Computing Conference*, Patiala ,India, 2009.
[4] Souvik Bhattacharyya. and Gautam Sanyal. Hiding data in images using pixel mapping method (pmm). In *Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer Engineering, and Applied Computing(WorldComp 2010)*, LasVegas,USA, July 12-15,2010.
[5] J.Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36 (7):1583–1595, 2003.
[6] C.Cachin. An information theoretic model for steganography. *Proceedings of 2nd Workshop on Information Hiding. D. Aucsmith (Eds.). Lecture Notes in Computer Sciences, Springer-verlag.*, 1525, 1998.
[7] C.K. Chan. and L. M.Cheng. Hiding data in images by simple lsb substitution. *Pattern Recognition*, 37:469–474, 2004.
[8] Shiang-Rong Liao. Chiang-Lung Liu. High-performance jpeg steganography using complementary embedding strategy. *Pattern Recognition , Science Direct*, 41:2945–2955.
[9] Ajit Danti and Preethi Acharya. Randomized embedding scheme based on dct coefficients for image steganography. *IJCA Special Issue on Recent Trends in Image Processing and Pattern Recognition*, 2010.
[10] G. Doerr and J.L. Dugelay. Security pitfalls of frameby-frame approaches to video watermarking. *IEEE Transactions on Signal Processing, Supplement on Secure Media*, 52:2955–2964, 2004.
[11] Wu X.-Wang Zs Dumitrescu, S. Detection of lsb steganography via sample pair analysis. In *Proceedings of 5th Information Hiding Workshop*, volume 2578, pages 355–372, 2002.
[12] Potdar V.and Chang E. Gray level modification steganography for secret communication. In *IEEE International Conference on Industrial Informatics INDIN.*, pages 355–368, Berlin, Germany, 2004.
[13] Goljan M.-Du R. Fridrich, J. Detecting lsb steganography in color, and gray-scale images. *IEEE Multimedia 8.*, pages 22–28, 2001.
[14] J. Fridrich and J. Kodovsk. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security.*, 7(3):868–882.
[15] Jessica Fridrich and Miroslav Goljan. On estimation of secret message length in lsb steganography in spatial domain. In *Proc. SPIE*, pages 23–34. Addison-Wesley, 2004.
[16] K. Gopalan. Audio steganography using bit modification. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03)*, volume 2, pages 421–424, 6-10 April 2003.
[17] J. Fridrich J. Kodovsk and V. Holub. Ensemble classifiers for steganalysis of digital media. *IEEE Transactions on Information Forensics and Security.*, 2012.
[18] N.F. Maxemchuk J.T. Brassil, S. Low and L. O.Gorman. Electronic marking and identification techniques to discourage document copying. *IEEE Journal on Selected Areas in Communications*, 13:1495–1504, 1995.
[19] R K Chhotaray K B Shiva Kumar, K B Raja and Sabyasachi Pattanaik. Bit length replacement steganography based on dct coefficients. *International Journal of Engineering Science and Technology*, 2:3561–3570, 2010.

[20] A. Sarkar K. Solanki and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In *In Proceedings of the 9th Information Hiding Workshop, volume 4567 of LNCS*, pages 16–31. Sprinnger, 2007.

[21] A Ker. Improved detection of lsb steganography in grayscale images. In *Proc.6th Information Hiding Workshop. Volume 3200 of Springer LNCS*, pages 97–115, 2004.

[22] A. D. Ker and R Bohme. Revisiting weighted stego-image steganalysis. In *Proc. SPIE*, volume 6819, pages 5–17, 2008.

[23] Andrew D. Ker. Optimally weighted least-squares steganalysis. In *Proc. SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX, 650506 (February 27, 2007)*.

[24] Andrew D. Ker. A weighted stego image detector for sequential lsb replacement. In *Proceedings of THIRD INTERNATIONAL SYMPOSIUM ON INFORMATION ASSURANCE AND SECURITY*.

[25] J. Kodovsk and J. Fridrich. Steganalysis of jpeg images using rich models. In *Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics*, volume XIV, 2012.

[26] V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. In *Proceedings of Advance Computing Conference (IACC), 2010 IEEE 2nd International*, pages 223–228, 2010.

[27] Jr. L. M. Marvel, C. G. Boncelet and C. T. Retter. Spread spectrum image steganography. *IEEE Trans. on Image Processing*, 8:1075–1083, 1999.

[28] Allan Latham. Jphide., 2008.

[29] Chia-Chen Lin. High capacity data hiding scheme for dct-based images. *Journal of Information Hiding and Multimedia Signal Processing*, 1, 2010.

[30] G. Davida M. Chapman and M. Rennhard. A practical and effective approach to large-scale automated linguistic steganography. In *Proceedings of the Information Security Conference*, pages 156–165, October 2001.

[31] N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. *IEEE Computer*, 16:26–34, 1998.

[32] N. Provos. Defending against statistical steganalysis. In *Proceedings of the 10th USENIX Security Symposium*, pages 323–325, 2001.

[33] Nasir Memon R. Chandramouli. Analysis of lsb based image steganography techniques. In *Proceedings of IEEE ICIP*, 2001.

[34] C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm. *Pattern Recognition*, 34:671–683, 2001.

[35] P. Sallee. Model-based steganography. In *In Proceedings of the 2nd International Workshop on Digital Watermarking of LNCS*, pages 154–167. Sprinnger, 2003.

[36] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal.*, 27:379–423.

[37] Avinash Prasad Kshitij. Souvik Bhattacharyya. and Gautam Sanyal. A novel approach to develop a secure image based steganographic model using integer wavelet transform. In *Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (Indexed by IEEE Computer Society)*, Cochin ,India, 2010.

[38] Lalan Kumar Souvik Bhattacharyya and Gautam Sanyal. A novel approach of data hiding using pixel mapping method (pmm). *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION SECURITY(IJCSIS)*, 8, 2010.

[39] S.P.Mohanty. *Digital Watermarking: A Tutorial*. 1999.

[40] P. Bas T. Pevn and J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security,5(2):215-224.*, 2010.

[41] T. Filler T. Pevn and P. Bas. Using high-dimensional image models to perform highly undetectable steganography. *In Information Hiding, 12th Int. Conf., volume 6387 of Springer LNCS.*, pages 161–177, 2010.

[42] Derek Upham. Jsteg, 2008.

[43] HJ Kim V Sachnev and R Zhang. Less detectable jpeg steganography method based on heuristic optimization and bch syndrome coding. In *In proceedings of ACM Workshop on Multimedia and Security, volume 4437 of Lecture Notes in Computer Science*, pages 131–139, 2009.

[44] N. Morimoto W. Bender, D. Gruhl and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35:313–316, 1996.

[45] C. Wang and J. Ni. An efficient jpeg steganographic scheme based on the block-entropy of dct coefficents. In *In proceedings of IEEE ICASSP, Kyoto, Japan, 2012*.

[46] Andreas Westfeld and Andreas Pfitzmann. Attacks on steganographic systems. In *In Proceedings of the Third Intl.Workshop on Information Hiding, Springer-verlag.*, pages 61–76, 1999.

[47] Andrew Westfeld. F5-a steganographic algorithm: high capacity despite better steganalysis. In *In Proceedings of the 4th Information Hiding Workshop,LNCS*, volume 2137, pages 289–302, 2001.

[48] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24:1613–1626, 2003.

[49] Z. Duric Y. Kim and D. Richards. Modified matrix encoding technique for minimal distortion steganography. In *In proceedings of Information Hiding, 8th International Workshop, volume 4437 of Lecture Notes in Computer Science*, pages 314–327. Springer-Verlag, 2006.

[50] Hamid Rahim Sheikh Zhou Wang, Alan Conrad Bovik and Eero P. Simoncelli. Image quality assessment: From error visibility to structural similarity. *IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 4, APRIL 2004*.

BIOGRAPHY OF AUTHORS

Souvik Bhattacharyya has received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. He has received Ph.D (Engg.) from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor and In-Charge in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Natural Language Processing, Network Security and Image Processing. He has published nearly 65 papers in International and National Journals / Conferences.

Aparajita Khan has received her B.E in Computer Science and Engineering from University of Burdwan, Burdwan, India and is currently perusing her M.Tech in Computer Technology from Jadavpur University, Kolkata, India.Currently she is working on inference of Gene Regulatory Network from Gene Expression Data.Her research interests include Information Security, Bioinformatics and Pattern Recognition.

Gautam Sanyal has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 150 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (S.W) at National Institute of Technology, Durgapur, India.