World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:9, 2014

A Robust Image Steganography Method Using PMM in Bit Plane Domain

Souvik Bhattacharyya, Aparajita Khan, Indradip Banerjee, Gautam Sanyal

***Abstract*—**Steganography is the art and science that hides the information in an appropriate cover carrier like image, text, audio and video media. In this work the authors propose a new image based steganographic method for hiding information within the complex bit planes of the image. After slicing into bit planes the cover image is analyzed to extract the most complex planes in decreasing order based on their bit plane complexity. The complexity function next determines the complex noisy blocks of the chosen bit plane and finally pixel mapping method (PMM) has been used to embed secret bits into those regions of the bit plane. The novel approach of using pixel mapping method (PMM) in bit plane domain adaptively embeds data on most complex regions of image, provides high embedding capacity, better imperceptibility and resistance to steganalysis attack.

***Keywords*—**PMM (Pixel Mapping Method), Bit Plane, Steganography, SSIM, KL-Divergence.

I. 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. The term information hiding can refer to either making the information undetectable or keeping the existence of the information secret. Steganography is an area of information hiding which means "secret or covered writing". As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. Another form of information hiding is digital watermarking; a process that embeds data known as watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. A famous illustration of steganography is **Simmons' Prisoners' Problem [**1]. An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as the secret key steganography where as pure steganography means that there is no prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [2]-[4]. For a more thorough knowledge of steganography methodology the reader may see [5], [6]. Some steganographic model with high security features has been presented in [7]-[9]. Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [6]. Fig. 1 shows the different categories of steganography techniques.

Fig. 1 Types of Steganography

A block diagram of a generic image steganographic system is given in Fig. 2. 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 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.

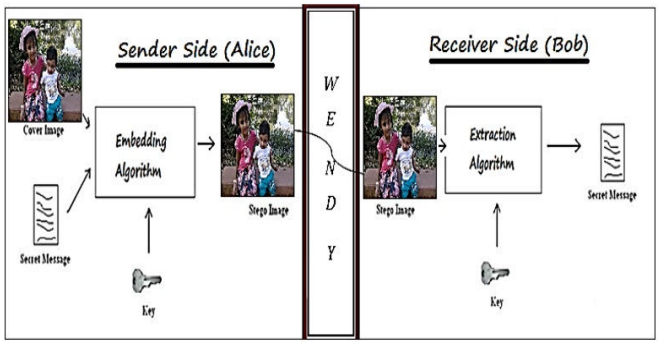

Fig. 2 Generic form of Image Steganography

In this work a specific image based steganographic method in the bit plane domain has been proposed which may be considered as the improved version of the author's previous work [10] in bit plane domain with an additional approach of showing resistivity of the proposed method against various steganalysis attacks with better imperceptibility. In this proposed method secret messages has been embedded through Pixel Mapping Method (PMM) in the bit planes of the cover

Souvik Bhattacharyya, Aparajita Khanis with the Department of CSE, University Institute of Technology, The University of Burdwan, West Bengal, India - 713104 (e-mail: souvik.bha@gmail.com, khanaparajita@yahoo.com).

Indradip Banerjee is with the Department of CSE, National Institute of Technology, Durgapur, Mahatma Gandhi Avenue, West Bengal, India - 713209 (e-mail: indradip.banerjee@yahoo.com)

GautamSanyal is the Professor of Department of CSE and Dean (FW), National Institute of Technology, Durgapur, Mahatma Gandhi Avenue, West Bengal, India - 713209 (e-mail: nitgsanyal@gmail.com)

image to generate the stego image. Experimental results demonstrate that the proposed embedding algorithm has high imperceptibility and better embedding capacity and produces satisfactory results in terms of security of the hidden data and robust enough to stay secure against some of the well known steganalysis attacks also.

This paper has been organized as following sections: Section II describes some existing works on image steganography. Section III deals with BPCS steganography approach. Proposed PMM based bit plane steganography method has been presented in section IV. Different algorithms are discussed in Section V and Experimental results are discussed and analyzed in Section VI. Different steganalysis attack on the stego images has been discussed in Section VII. Section VIII draws the conclusion.

II. Related Works

In this section some image based steganographic data hiding methods in spatial domain has been discussed.

A. Data Hiding by LSB

Various techniques about data hiding have been proposed in literatures. One of the common techniques is based on manipulating the least-significant-bit **(LSB)** [11] 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, compression and steganalysis. In order to overcome this problem Chan et al. [12] proposed an efficient method optimal Pixel adjustment Method **(OPAP)** which reduces the distortion occurs due to LSB replacement.

B. Data Hiding by PVD

The pixel-value differencing **(PVD)** method, proposed by Wu & Tsai [13] 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. A larger difference in the original pixel values allows a greater modification. In the extraction phase, the original range table is necessary. It is used to partition the stego-image by the same method as used to the cover image. Based on PVD method, various approaches have also been proposed. Among them Chang et al. [14] proposes a new method using tri-way pixel-value differencing **(TPVD)** which is better than original PVD method with respect to the embedding capacity and PSNR. Wang et al. [15] also proposed an improvement of PVD scheme where the secret data is hidden in pixel difference with the help of modulus function **(MPVD)** which greatly reduces the alteration caused by the hiding of the secret data.

C. Data Hiding by GLM

In 2004, Potdar et al. [16] proposed **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. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

D. Data Hiding by Pixel Pair Matching

The LSB and OPAP method use one pixel as an embedding unit, and hide the data bit into the right-most LSBs. Another group of data-hiding methods employs two pixels as an embedding unit to conceal a message digit in a n-ary notational system. These data-hiding methods are denoted as pixel pair matching **(PPM).**Two popular PPM approaches are exploiting modification direction **(EMD)** [17] method by Zhang and Wang and diamond encoding **(DE)** method proposed by Chao et al. [18] in 2009. The EMD embedding scheme hides each *(2n+1)*-ary notational secret digit into n cover pixels, and only one pixel value increases or decreases by 1 at most. The embedding method of EMD offers low payload and is limited to 5-ary notational system. For extraction, more than one pixel needs to be modified, which affects the overall performance of the method. The DE method is an extension of EMD with grater payload.DE employs an extraction function to generate diamond characteristic values (DCV).In DE embedding is done by modifying the pixel pairs in the cover image according to their DCVs neighborhood set and the given message digit. Chao used an embedding parameter k to control the payload, in which a digit in a N-ary notational system can be concealed into two pixels, where $N = 2k^2 + 2k + 1$, which implies significantly increase of N for one increase of k. Zhang et al. [19] have proposed a new method based on **Side Match** where the users can consult more than two neighboring pixels to determine the payload of each pixel.

E. Bhattachayya and Sanyal's Transformation

Bhattachayya and Sanyal proposed a new image transformation technique known as Pixel Mapping Method (**PMM**) [20], [21] a method for information hiding within the spatial domain of any gray scale image. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. 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. Figs. 3 and 4 show the mapping information for embedding two bits or four bits respectively.

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.

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

Fig. 3 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

Fig. 4 PMM Mapping Technique for embedding of four bits

F. HUGO Steganography Method

Hugo is a content-adaptive spatial steganography that over-comes 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 [22] 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.

G. ADAPTIVE ±1 Steganography in Extended Noisy Region

This is an adaptive steganography method [23] where message is embedded into the noisiest area using a noisy function measuring the texture complexity. Here double-layered embedding is implemented by fast matrix embedding in LSB plane and wet paper codes in second LSB plane hence reducing number of modifications.

III. BPCS Steganography

BPCS (Bit-Plane Complexity Segmentation) steganography was introduced by Eiji Kawaguchi & Richard O. Eason [24] to overcome the short comings of traditional steganographic techniques like Least Significant Bit (LSB) technique or transform domain embedding technique. The important aspect of this approach compared to those methodologies is that the embedding capacity is very large. BPCS steganography makes use of the important characteristic of human vision. Here, the vessel image is divided into informative region and also noise like region, the secret data is embedded in noise blocks of vessel image without degrading image quality [24], [25]. In LSB technique, data can be hidden in last four bits i.e. only in the 4 LSB bits [26]. But in BPCS technique, data can also be hidden in MSB planes along with the LSB planes provided, more complex region [24] are available for data embedding.

A. Basic Principle of BPCS Steganography

In BPCS, a multi-valued image (P) consisting of n-bit pixel planes can be decomposed into set of n binary pictures. e.g.: If P is a gray scale image then $n = 8$ and can be decomposed into P = [P7 P6 P5 P4 P3 P2 P1 P0] where P7 is the MSB bit plane and P0 is the LSB bit plane. Each bit plane can be segmented into informative and noisy region. An informative region consists of simple pattern while noise-like region consists of complex pattern. In BPCS, each noise-looking region is replaced with another noise-looking pattern without changing the overall image quality. Thus, BPCS steganography makes use of this nature of human vision system [25], [27].An example of bit plane slicing has shown in Fig. 5.

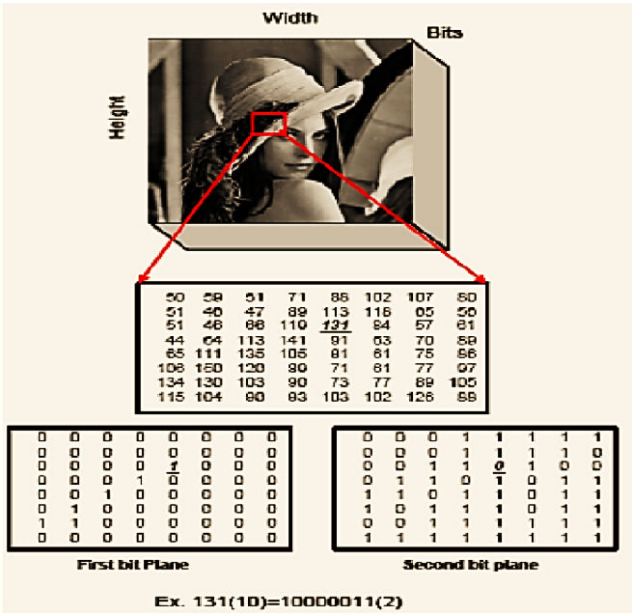

Fig. 5 Bit Plane slicing concept considering pixel having value 131

B. Mathematical formulation of BPCS Steganography

A bit plane of a digital discrete signal like image or sound can be represented as a set of bits corresponding to a given bit position in each of the binary numbers representing the signal. A $M \times N$ image can be sliced into n bit planes given by

$$B_i = \{b_i | b_i \text{ is the value of } i^{th} \text{ bit position in } (b_{n-1}, b_{n-2}, b_{n-3}, \ldots, b_0)\}^{M \times N}, \forall\, i = 0, 1, \ldots, n-1 \quad (1)$$

If a bit on the i^{th} bit plane on an m-bit dataset is set to 1, it contributes a value of 2^{m-i}, otherwise it contributes nothing. Define γ as the set of all possible binary messages of length l where $l \geq 1$. Mathematically it can be said $\gamma = \{0, 1\}^l | l \in N$.

Let $\chi = \{0, 1, 2, \ldots 255\}^{M \times N \times D}$ be the set of pixel intensity values such that a digital image is represented by,

$X = (x_{ijk}) \in \chi$ where D=1 corresponds of a gray scale image consisting of just the gray scale plane and D=3 corresponds to an RGB image, $\forall x_{ijk}$ k=1 refers to the red plane, k=2 green plane and k=3 blue plane. Now since each value of x_{ijk} is drawn from the set χ consisting of values within the range [0,255] so pixel intensities of each color plane of RGB image and the gray scale image itself can be represented by a corresponding 8 bit binary number. Thus for a $M \times N$ RGB image with 24 bits per pixel ($b_{23}, b_{22}, b_{21}, \ldots, b_0$) where the first 8 bits from rightmost end ($b_{23}, b_{22}, b_{21}, \ldots, b_{16}$) corresponds to the red plane intensity while next 8 bits ($b_{15}, b_{14}, b_{13}, \ldots, b_8$) and remaining ($b_7, b_6, b_5, \ldots, b_0$) corresponds to green and blue plane intensities respectively and b_{23}, b_{15} & b_7 being the MSB and b_{16}, b_8 and b_0 being the LSB of red, green and blue color planes respectively. While for gray scale image we have $b_7, b_6, \ldots, b_0$ representing the bit planes of the image, b_7 being MSB and b_0 being LSB.

C. Complexity of a Binary Image

Let B be a binary image of dimension $2^M \times 2^M$ .The complexity of the image is given by

$$\alpha = \frac{k}{2 \times 2^M \times (2^M - 1)} \quad (2)$$

k is the total number of black-and-white borders in the image. Consider 4-connectivity of pixels, the black-and-white border is defined as the sum of the color changes along the rows and columns of the image. The border length k can be computed as, say, a single white pixel surrounded by 4 black pixels, i.e., having all its 4-connected neighbors as black pixels, will have a border length of 4 (2 color changes each along the rows and columns). Thus for a square binary image of size $2^M \times 2^M$ the minimum border length possible is 0, obtained for an all-white or all-black image, and the maximum border length possible is $2 \times 2^M \times (2^M - 1)$ and α is the normalized value of the total length of the black and white border in the image. Clearly α lies in [0, 1].

IV. Proposed Data Embedding Method

In this approach, the secret message is embedded though pixel mapping method into the highly complex bit planes or noisy bit planes of the cover image. The proposed approach starts by extracting the R, G and B planes (for RGB image only) followed by selecting the embedding bit planes using some threshold value with application of the pixel mapping method (PMM) in a 8x8 blocks of the each selected plane. The integrated approach of PMM and BPCS steganography produces a robust image based steganographic technique, independent of the nature of the data to be hidden and produces a stego image with minimum degradation. Embedding in any of color planes of RGB image is quite similar in case of Gray Scale image. Figs. 6 and 7 show the block diagram of Sender Side System for GRAY SCALE and RGB image respectively. Also Figs. 8 and 9 are for Receiver Side System of GRAY SCALE and RGB image.

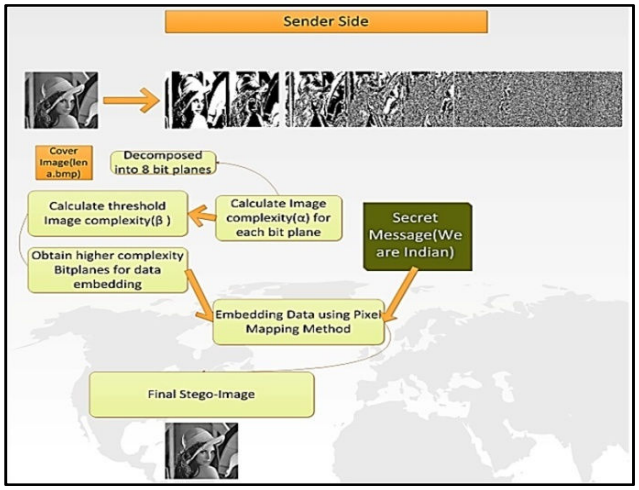

Fig. 6 Block Diagram of Sender Side System for GRAY SCALE image

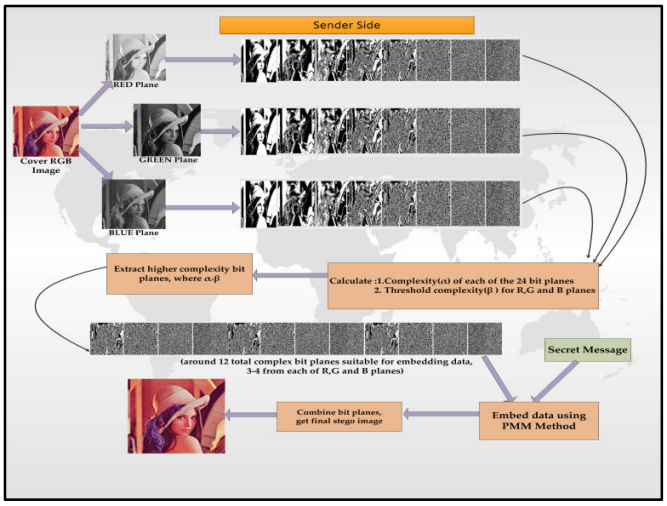

Fig. 7 Block Diagram of Sender Side System for RGB image

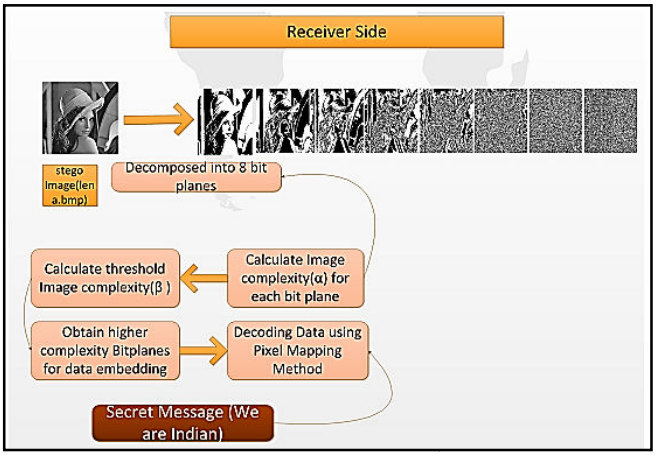

Fig. 8 Block Diagram of Receiver Side System GRAY SCALE

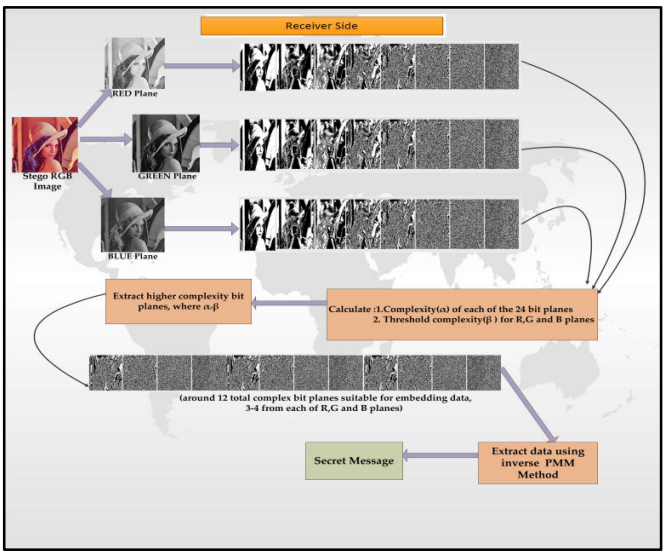

Fig. 9 Block Diagram of Receiver Side System for RGB image

Fig. 10 shows the R, G and B planes of LENA image of dimension 512 X 512 whereas Fig. 11 illustrates the various of bit planes of each of the R, G and B planes.

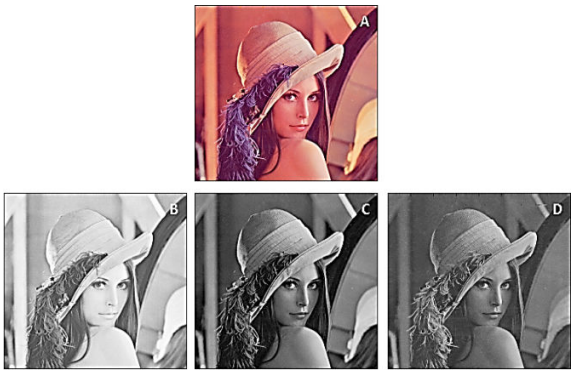

Fig. 10 A) Original Lena as Cover Image B) RED Plane of Lena before embedding C) GREEN Plane of Lena before embedding D) BLUE Plane of Lena before embedding

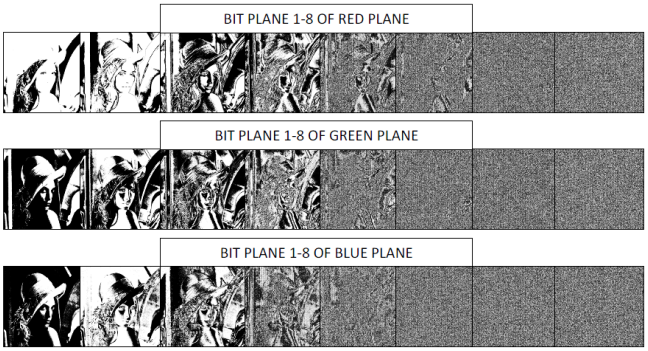

Fig. 11 Various Bit Planes of RED, GREEN and BLUE Plane

V. Algorithms

In this section, algorithms for different processes used in sender side and receiver side have been described.

A. Data Embedding Method

1. The cover image C = $(c_{ijk}) \in \chi$ with n bits per pixel is sliced into n binary images or logical matrices.
2. Let ρ be a secret message of length L characters where $L \geq 1$, to be embedded. Each character of ρ can be represented by a 8 bit binary sequence using ASCII encoding. Using this ρ is converted to a binary message stream m of length l=8L such that $m \in \gamma$.
3. For each bit plane B_i $i = 0, \ldots, n-1$ compute the overall plane complexity from (2) as $\{\alpha_{n-1}, \alpha_{n-2}, \ldots \alpha_0\}$ and next step is to find the color plane complexity δ_R, δ_G and δ_B for R,G and B planes of color image or δ_{Gry} for gray scale image as the average of the complexities of bit planes corresponding the color or gray plane.
4. Considering δ_R, δ_G and δ_B or δ_{Gry} as the threshold complexities determine bit planes with complexity α greater than its corresponding δ and add them to the set of message embedding planes ξ of the image.
5. Sort the elements of ξ according to decreasing order of their bit plane complexity α.
6. Let binary message stream m be given by the sequence of bits β_i, i = 1, 2, ..., *l*. While there are bits β_i, remaining to be embedded, i.e. $i \leq l$, the following procedure is used for embedding.
7. Select the next highest complexity bit plane B_i from the decreasingly sorted sequence of ξ as the next embedding plane E. Divide E into non-overlapping blocks of size $2^k \times 2^k$, $k \geq 3$.
8. Compute the complexities of each of the $\frac{MXN}{2^{2k}}$ blocks obtained from step 7. Take the mean value of these complexities as the threshold complexity say α_T to determine the complex or noise like blocks within the image. Consider all $2^k \times 2^k$ blocks having complexity $\alpha \geq \alpha_T$ for all embedding bits.
9. Let R be a selected $2^k \times 2^k$ block for embedding, then divide R into $\frac{2^{2k}}{64}$ non-overlapping blocks of size 8 × 8 and within each such block say T embed 16 bits as follows.

10. T is a logical matrix given by, T = (τ_{jk}), for j, k = 1, 2, ..8.. Let Dec_j be the decimal value of the j[th] row of T i.e., considering bit sequence τ_{j1}, ..., τ_{j8} and $count_j$ be the number of ones in j^{th} row of T excluding τ_{j8} i.e, number of ones in bit sequence τ_{j8}, ..., τ_{j7} . Within each row of T i.e for each j embed 2 bits β_i β_{i+1} by Pixel Mapping Method as,

a) Case 1: $\beta_i \beta_{i+1} = 01$ set Dec_j = x such that x%2 = 0 and $count_j$ = y such that y%2 ≠0.
b) Case 2: $\beta_i \beta_{i+1} = 10$ set Dec_j = x such that x%2 = 0 and $count_j$ = y such that y%2 = 0.
c) Case 3: $\beta_i \beta_{i+1} = 00$ set Dec_j = x such that x%2 = 0 and $count_j$ = y such that y%2 = 0.
d) Case 4: $\beta_i \beta_{i+1} = 11$ set Dec_j = x such that x%2 = 0 and $count_j$ = y such that y%2 ≠ 0.

11. After embedding 2 bits for each j=1,2,..8 consider next 8 × 8 block of S and so on, when S is filled consider next noisy block with α ≥ α_T and so on until all noisy blocks filled and then consider next highest complex plane from sorted sequence of ξ. Repeat this procedure until all bits of β_i have been embedded.
12. Finally transform from bit plane domain to spatial pixel intensity by merging the bit planes in correct order to obtain the final stego image S = (s_{ijk}) ∈χ.

B. Data Extraction Method

1. The stego image S = (s_{ijk}) ∈ χ is sliced into n bit planes.
2. For each bit plane B_i ∀i = 0, 1, ..., n − 1 compute the overall plane complexities from (2) as { $\alpha_{n-1}, \alpha_{n-2}, \ldots \alpha_0$ } and next step is to find the color plane complexity δ_R, δ_G and δ_B for R,G and B planes of color image or δ_{Gry} for gray scale image as the average of the complexities of bit planes corresponding the color or gray plane.
3. Considering δ_R, δ_G and δB or δ_{Gry} as the threshold complexities determine bit planes with complexity α greater than its corresponding δ and add them to the set of message extraction planes ξ of the image.
4. Sort the elements of ξ according to decreasing order of their bit plane complexity α.
5. The secret binary message stream m to be extracted be given by the sequence of bits $\beta_i, i = 1, 2, 3, ..., l$ where l is the length of the binary message to be extracted. While $i < l$ binary message bits are extracted from complex bit planes by 2-bit inverse Pixel Mapping Method (PMM) as follows.
6. Select the next highest complexity bit plane $B_{2^k i}$ from the decreasingly sorted sequence of ξ as the next extraction plane E. Divide E into non-overlapping blocks of size $2^k \times 2^k$, $k \geq 3$. Compute the complexities of each of the $\frac{M \times N}{2^{2k}}$ blocks obtained. Take the mean value of these complexities as the threshold complexity say α_T to determine the complex or noise like blocks within the image. Consider all $2^k \times 2^k$ blocks having complexity α ≥α_T for extraction of bits.
7. Let R be a selected $2^k \times 2^k$ block for extraction, then divide R into $\frac{2^{2k}}{64}$ non-overlapping blocks of size 8 × 8 and within each such block say T embed 16 bits as follows.
8. T be a logical matrix given by, T= (τ_{jk}), for j, k = 1, 2,...8. Let $count_j$ be the number of ones in j[th] row of T excluding τ_{j8} i.e., number of ones in bit sequence τ_{j1}, ..., τ_{j7} .From each row of T i.e for each j extract 2 bits β_i β_{i+1} by inverse Pixel Mapping Method (PMM) as

(a). $\beta_{i+1} = j_8$ and
(b). Case 1:if $count_j$ = y such that y%2 = 0 then β_i = 0.
(c). Case 2:if $count_j$= y such that y%2 ≠ 0 then β_i = 1.

9. After extraction of 2 bits for each j = 1,2,..,8 consider next 8 X 8 block of S and so on, when data has been extracted from all $\frac{2^k}{64}$ blocks of S then consider next noisy block with α ≥ α_T and so on until all noisy blocks have been covered and then consider next highest complex plane from sorted sequence of ξ. Repeat this procedure until all bits β_i have been extracted.

VI. Experimental Results

Experimental results of the proposed method have 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. All the experiments has been carried out by testing the steganographic algorithm on a set of 1328 uncompressed RGB images from Uncompressed Color Image Database (UCID) (Ucid image database) [28].

A. Embedding Capacity Test

Since the main application of information hiding and steganography is the secret communication, it is important to determine how many bits a steganographic system can embed imperceptibly in comparison to the other methods. Therefore, evaluating the capacity of a steganography technique means to find out the maximum number of bits that can be stays undetectable after hidden. The payload indicates the maximum number of bits that can be hidden with an acceptable resultant stego carrier quality. Embedding Capacity for the PMM in Bit Plane Domain in terms of number of bits per pixel can be calculated below.

As mentioned in the embedding algorithm ξ being the set of all complex planes of the cover image C let $n = |\xi|$ i.e., n is the cardinality of the set ξ . For each $e_i \in \xi$, ∀i = 1, 2, ..., n, let a_i be the number of noisy blocks of size $2^k \times 2^k$, $k \geq 3$ of plane e_i having complexity greater than average complexity of all blocks of plane. Each such noisy block can be divided into 8 × 8sub blocks yielding $2^{2(k-3)}$ sub blocks. Within each 8 × 8 sub blocks with **PMM (2 bit)** 8 × 2 bits can be embedded (2 bits in each row of 8 × 8 sub block) or with **PMM (4 bit)** 8 × 4 bits can be embedded. Embedding capacity (for 2 bit mapping) can thus be calculated as given in (5)

$$\text{No-of-bits} = \left(\sum_{i=1}^{n} a_i\right) \times 2^{2(k-3)} \times 16 \qquad (3)$$

Embedding capacity for 4 bit mapping can be calculated as

$$\text{No-of-bits} = (\sum_{i=1}^{n} a_i) \times 2^{2(k-3)} \times 32 \quad (4)$$

Maximum Bits Per Pixel (bpp) is given by

$$\text{bpp} = \frac{No-of-bits}{M \times N \times 3} \quad (5)$$

Most images are expected to yield 4 complex bit planes for each of the color planes R, G and B as half of the 8-bit color planes have complexity higher than threshold. For some images n is even as high as 18. Thus if for each complex plane on average half of the blocks of size $2^k \times 2^k$ are found to be noisy then there are $\frac{M \times N}{2^k \times 2^k \times 2}$ noisy blocks. In each noisy block $2^{2(k-3)} \times 32$ bits can be embedded with **PMM (4-bit)** and $2^{2(k-3)} \times 16$ bits embedded with **PMM (2-bit).** Thus Bits Per Pixel (bpp) for PMM (4 bit) comes out to be

$$bpp_{PMM(4\,bit)} = \frac{\frac{M \times N}{2^k \times 2^k \times 2} \times (2^{2(k-3)} \times 32) \times n}{M \times N \times 3} = \frac{n}{6} \quad (6)$$

From the experiments it has been identified that using **PMM (4 bit)** for 512x512 RGB image with 18 complex bit planes would give an embedding capacity 2359296 bits or 294912 characters where as 1179648 bits or 147456 characters can be embedded using **PMM (2 bit)** approach.

Fig. 12 shows the variation of no of complex planes (n) for different test set of the cover images and Fig. 13 shows the variation of maximum embedding capacity of the different test set of cover images.

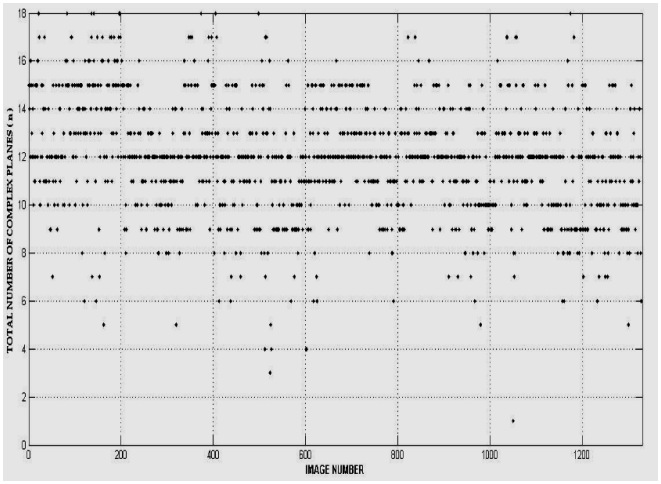

Fig. 12 No of complex planes for different test images

The embedding capacity of the proposed method has been compared with other existing methods like the Least-significant-bit (LSB) [11], Optimal Pixel Adjustment Method (OPAP) [12], Pixel-Value Differencing (PVD) method by Wu and Tsai [13], Tri-way Pixel Value Differencing (TPVD) [14], Pixel Difference with the help of modulus function (MPVD) [15], GLM (Gray level modification) by Potdar et al. [16] Exploiting Modification Direction (EMD) [17] and Diamond Encoding (DE) method [18].The comparison of the embedding capacity in terms of Byte and BPP has been shown in Figs. 14 and 15 respectively.

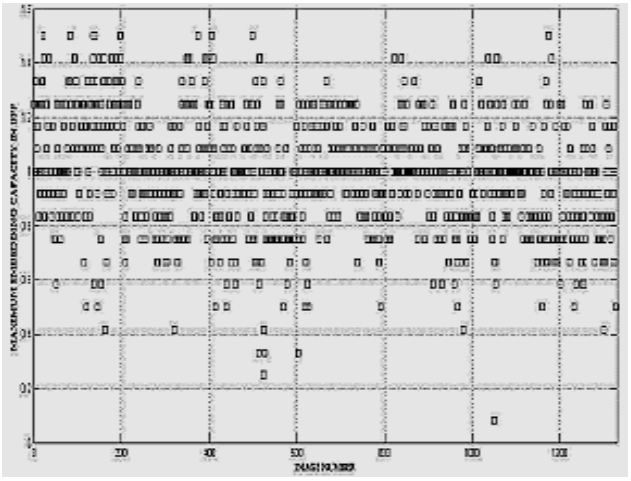

Fig. 13 Embedding capacity for different test images

Emb Cap	LSB(k=1)	GLM	PVD	OPAP (k=1)	TPVD	PMM(2 bit)_Bit Plane	PMM(4 bit)_Bit Plane	PMM(2 bit)_Bit Plane (RGB)	PMM(4 bit)_Bit Plane(RGB)
Bytes	32768	32768	50960	32768	75836	32768	65536	147456	294912

Fig. 14 Comparison of embedding capacity in terms of Byte

Embedding Capacity	LSB (k=1)	OPAP (k=1)	DE (k=1)	EMD	PMM(2 bit)_Bit Plane (RGB)	PMM(4 bit)_Bit Plane (RGB)
BPP	1	1	1.16	1.161	1.5	3

Fig. 15 Comparison of embedding capacity in terms of BPP

B. Imperceptibility Test

How to preserve the details of the cover carrier when the secret message is being embedded in so that the deference between the stego carrier and the cover carrier can be perfectly imperceptible to the human eye is the very first problem an ideal steganographic scheme has to face. Accordingly, the higher the quality of stego images, the larger the imperceptibility of the steganographic system. Therefore, the stego image quality is a very important criterion in order to evaluate the performance of a steganographic technique. 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.

1) 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. Engineers commonly use the PSNR to measure the quality of reconstructed signals that have been compressed. Signals can have a wide dynamic range, so PSNR is usually expressed in decibels, which is a logarithmic scale. In statistics, the mean squared error (MSE) of an estimator is one of many ways to

quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. MSE measures the average of the squares of the "errors." The error is the amount by which the value implied by the estimator differs from the quantity to be estimated. PSNR measures the quality of the image by comparing the original image or cover image with the stego image, i.e. it measures the percentage of the stego data to the image percentage. 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. RMSD is a good measure of accuracy. These individual differences are also called residuals, and the RMSD serves to aggregate them into a single measure of predictive power. 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 (7).

$$MSE = \frac{1}{[N \times N]^2} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(ij) - S(ij)]^2 \quad (7)$$

The PSNR is computed using the following formulae given in (8).

$$PSNR = 10\, log_{10} \left(\frac{255^2}{MSE} \right) db \quad (8)$$

The visual imperceptibility of the stego image produced by the proposed method has tested by computing PSNR and MSE values. Fig. 16 shows the PSNR of 1328 images at an embedding rate of 0.317 bpp. Figs. 17 and 18 show the comparison of PSNR value of the proposed method with the PSNR value of some other existing methods.

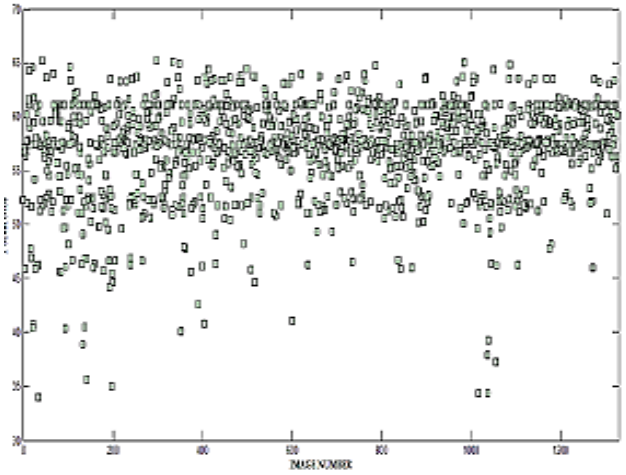

Fig. 16 PSNR value for different test images with an embedding rate of 250000 bits or 0.317 bpp

Cover Image	LSB	PVD	SIDE MATCH	OPAP	GLM	M-PVD	DE (k=1)	PMM (2 bit)_Bit Plane (RGB)
Lena	49.5	46.2	46.2	50.1	35.5	49.6	52.1	58.7
Baboon	49.5	46.1	43.4	50.1	35.5	49.4	52.0	60.1
Pepper	49.5	46.2	46.6	50.1	35.5	49.6	52.0	56.2
Airplane	49.5	46.1	46.5	50.0	35.5	49.5	52.0	61.3
Boat	49.5	46.1	45.4	50.1	35.5	49.4	52.1	58.4
Barbara	49.5	46.1	49.5	50.1	35.5	49.5	52.1	58.7
Tiffiany	49.4	46.1	46.7	50.0	35.5	49.7	52.1	62.6
Zelda	49.4	46.2	46.5	50.1	35.5	49.5	52.1	57.7

Fig. 17 Comparison results of PSNR among LSB, OPAP,SIDE MATCH PVD, MPVD,GLM,DE(k=1) and PMM in Bit Plane(RGB) on various test images with embedding payload = 300000 bits

Cover Image	LSB	PVD	SIDE MATCH	OPAP	GLM	M-PVD	DE (k=3)	PMM (2 bit)_Bit Plane (RGB)
Lena	42.3	37.5	46.2	45.7	NA	40.6	46.3	49.9
Baboon	42.5	37.1	43.4	45.3	NA	40.3	46.3	50.3
Pepper	42.3	37.8	46.6	45.4	NA	40.2	46.4	48.2
Airplane	42.4	37.4	46.5	45.3	NA	40.4	46.7	51.9
Boat	42.3	37.0	45.4	45.4	NA	40.2	46.3	48.6
Barbara	42.4	37.7	49.5	45.6	NA	40.5	46.2	49.1
Tiffiany	42.5	37.2	46.7	45.6	NA	40.3	46.6	51.9
Zelda	42.4	37.1	46.5	45.4	NA	40.5	46.2	47.2

Fig. 18 Comparison results of PSNR among LSB, OPAP,SIDE MATCH PVD, MPVD,GLM,DE (k=1) and PMM in Bit Plane(RGB) on various test images with embedding payload = 600000 bits

2) Structural Similarity (SSIM)

The structural similarity (SSIM) [29] index is a method for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measuring of image quality based on an initial uncompressed or distortion free image as reference. 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. The SSIM metric is calculated on various windows of an image. The measure between two images x and y of common size $N \times N$ is:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (9)$$

where μ_x is the average of x and μ_y is the average of y; 2. σ_x^2 is the variance of x; 3. σ_y^2 is the variance of y; 4. σ_{xy} is the covariance of x and y; 5. $c_1 = (k_1 L)^2$ *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.

The Structured Similarity Measure between each pair of cover and stego image for the entire set of test images is given by Fig. 19.

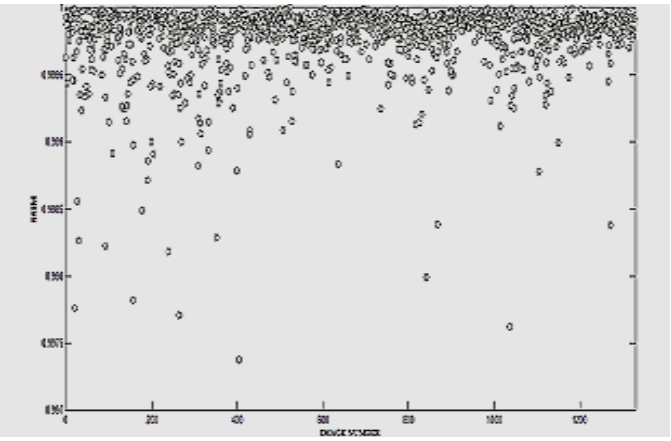

Fig. 19 Structured Similarity Measure between each pair of cover and stego image at embedding rate 0.3 bpp

SSIM value for most of the cove stego pair being near to 1, shows the high degree of similarity between each pair thus establishing the imperceptibility of the steganographic algorithm.

3) Kullback Leibler Divergence

In probability theory and information theory, the Kullback Leibler Divergence [30] (also information divergence, information gain, relative entropy, or KLIC) is a non-symmetric measure of the difference between two probability distributions P and Q. KL measures the expected number of extra bits required to code samples from P when using a code based on Q, rather than using a code based on P. Typically P represents the "true" distribution of data, observations, or a precisely calculated theoretical distribution. The measure Q typically represents a theory, model, description, or approximation of P.

Although it is often intuited as a metric or distance, the KL divergence is not a true metric? For example, it is not symmetric: the KL from P to Q is generally not the same as the KL from Q to P.

For probability distributions P and Q of a discrete random variable their KL divergence is defined to be

$$D_{KL}\left(P \parallel Q\right) = \sum_{i} P\left(i\right) \ln \frac{P(i)}{Q(i)} \tag{10}$$

In words, it is the average of the logarithmic difference between the probabilities P and Q, where the average is taken using the probabilities P. The K-L divergence is only defined if P and Q both sum to 1 and if Q(i) > 0 for any i such that *P(i)>0*. If the quantity *0log0* appears in the formula, it is interpreted as zero. For distributions P and Q of a continuous random variable, KL-divergence is defined to be the integral

$$D_{KL}\left(P \parallel Q\right) = \int_{-\infty}^{\infty} p\left(x\right) \ln \frac{p(x)}{q(x)} dx \tag{11}$$

where p and q denote the densities of P and Q. More generally, if P and Q are probability measures over a set X, and Q is absolutely continuous with respect to P, then the Kull back Leibler divergence from P to Q is defined as

$$D_{KL}\left(P \parallel Q\right) = \int_{X} \ln \frac{dP}{dQ} dP = \int_{X} \frac{dP}{dQ} \ln \frac{dP}{dQ} dQ \tag{12}$$

where $\frac{dQ}{dP}$ is the Radon Nikodym derivative of Q with respect to P, and provided the expression on the right hand side exists. Likewise, if P is absolutely continuous with respect to Q, then

$$D_{KL}\left(P \parallel Q\right) = -\int_{X} \ln \frac{dQ}{dP} dP \tag{13}$$

which we recognize as the entropy of P relative to Q. Continuing in this case, if is any measure on X for which p $=\frac{dP}{d\mu}$ and q $=\frac{dQ}{d\mu}$ then the Kullback Leibler Divergence from P to Q is given as

$$D_{KL}\left(P \parallel Q\right) = \int_{X} p \ln \frac{p}{q} d\mu \tag{14}$$

The logarithms in these formulae are taken to base 2 if information is measured in units of bits, or to base e if information is measured in nats. Most formulas involving the KL divergence hold irrespective of log base.

4) Steganography Security using Kullback Leibler Divergence

Denoting C the set of all covers c, Cachin's definition of steganographic security [30] 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 ×M ×K → C that assigns a new (stego) object, s ϵ C, to each triple (c,M,K), where M ϵM is a secret message selected from the set of communicable messages, M, and K ϵK 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 detect ability is the KullbackLeibler divergence or relative entropy.

$$D_{KL}\left(P \parallel Q\right) = \sum_{c \in C} P\left(c\right) \log \frac{P\left(c\right)}{Q\left(c\right)} \tag{15}$$

When D_{KL} *(P||Q)* <ϵ, the stego system is called ϵ secure.

Fig. 20 shows the values of relative entropy of different stego images at embedding rate of 0.3 bpp.

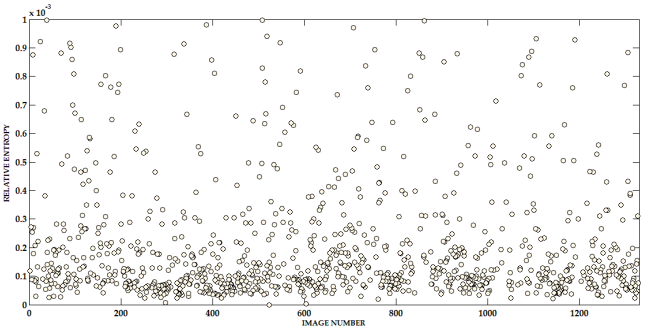

Fig. 20 Relative entropy between each pair of cover and stego image at embedding rate 0.3 bpp

Low Relative Entropy of most of the test images proves the imperceptibility of the steganographic algorithm.

C. 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:

$$r = \frac{\sum(C(i,j)-m_1)(S(i,j)-m_2)}{\sqrt{(C(i,j)-m_1)^2}\sqrt{(S(i,j)-m_2)^2}} \quad (16)$$

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. 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. It has been seen that the correlation coefficient computed here for all the images is almost one which indicates the both the cover image and stego image are of highly correlated i.e. both of these two images are same.

Comparison of PMM Bit Plane and others methods have been furnished at a glance in Fig. 21.

Image	Performance Metrics	LSB(k=1)	GLM	PVD	OPAP(k=1)	TPVD	PMM(2 bit)_Bit Plane (RGB)	PMM(4 bit)_Bit Plane (RGB)
LENA (512x512)	EMB Cap (in byte)	32768	32768	50960	32768	75836	147456	294912
	PSNR	51.1410	35.50	41.79	51.1410	38.89	40.7	41.67
	MSE	0.50	18.32	4.30	0.50	8.39	5.52	4.42
	Correlation	Not Considered	0.92	0.8	Not Considered	0.9995	0.9955	0.9968
	SSIM	Not Considered	Not Considered	Not Considered	Not Considered	Not Considered	0.9466	0.9332
	Security of Hidden data	Not Considered	Not Considered	Not Considered	Not Considered	Not Considered	0.0568	0.0547
PEPPER (512x512)	EMB Cap (in byte)	32768	32768	50685	39034	75579	147456	294912
	PSNR	51.1410	34.00	40.97	51.1410	38.50	39.9874	42.8
	MSE	0.50	25.88	5.20	0.50	9.18	6.52	3.41
	Correlation	Not Considered	0.93	0.75	0.9	0.9997	0.995	0.9952
	SSIM	Not Considered	Not Considered	Not Considered	Not Considered	0.9943	0.936	0.947
	Security of Hidden data	Not Considered	Not Considered	Not Considered	Not Considered	0.0018	0.0475	0.0518

Fig. 21 Results of PMM Bit Plane at a glance with a comparison

VII. Steganalysis Attack

Steganalysis is the science of detecting hidden information. The main objective of Steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on the Steganographic algorithms introducing statistical differences between cover and stego image. The majority of steganographic utilities for the camouflage of confidential communication suffer from fundamental weaknesses. On the way to more secure steganographic algorithms, the development of attacks is essential to assess security. In quantitative steganalysis the detector outputs not only a binary decision regarding weather the tested object is a stego object or not but also returns an estimate of the lengths of the secret message, which can be zero for clean covers. These methods are reliable only when parts of the covers steganographic capacity have been used. Quantitative detectors are functions that estimate the net embedding rate p. Let $x^{(0)}$ represent the cover object and $x^{(1)}$ be the stego object. If $x^{(p)}$ be the stego object with embedding rate p. Then estimated embedding rate $\hat{p}$ can be given by,

$$\hat{p}=\text{Detect}_{\text{Quant}}(x^{p}) \quad (17)$$

In this section all the stego images produced by PMM Bit Plane (RGB) algorithms has been tested against some of well known LSB detectors like Chi-square Analysis, RS Steganalysis and Sample Pair Analysis. Finally the stego images produced by this method have been tested through extracting the SPAM features (dimensionality 686).

A. Statistical Attack: Chi-Square Analysis

Andreas Pfitzmann and Andreas Westfeld [31] introduced a method based on statistical analysis of Pair of Values (PoVs) that are exchanged during sequential embedding. This attack works on any sequential embedding type of stego system such as EzStego and Jsteg. Sequential embedding makes PoVs in the values embedded in. For example, embedding in the spatial domain makes PoVs (2i, 2i +1) such that 0↔ 1, 2 ↔ 3, 4 ↔ 5… 252 ↔ 253, 254 ↔ 255. This will affect the histogram Y_k of the images 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 given in (18) and the χ^2 value for the difference between distributions with v-1 degrees of freedom is in (19). From (18) and (19) χ^2 statistic can be obtained for the PoVs as given in (20).

$$E(Y_{2i}) = \frac{1}{2}(Y_{2i} + Y_{2i+1}) \quad (18)$$

$$X^2 = \sum_{i=1}^{v} \frac{(F-E(F))^2}{E(F)} \quad (19)$$

$$X^2_{PoV} = \sum_{i=1}^{127} \frac{\left((Y_{2i})-\left(\frac{1}{2}(Y_{2i}+Y_{2i+1})\right)\right)^2}{(Y_{2i}+Y_{2i+1})} \quad (20)$$

Chi-Square Analysis calculates the average LSB and constructs a table of frequencies and Pair of Values [32]; it takes the data from these two tables and performs a chi-square test. It measures the theoretical vs. calculated population difference. This Analysis calculates the chi-square for every 128 bytes of the image and this calculation becomes more and

more accurate until too large of a data set has been produced. Figs. 22 and 23 show the results related to chi-square analysis.

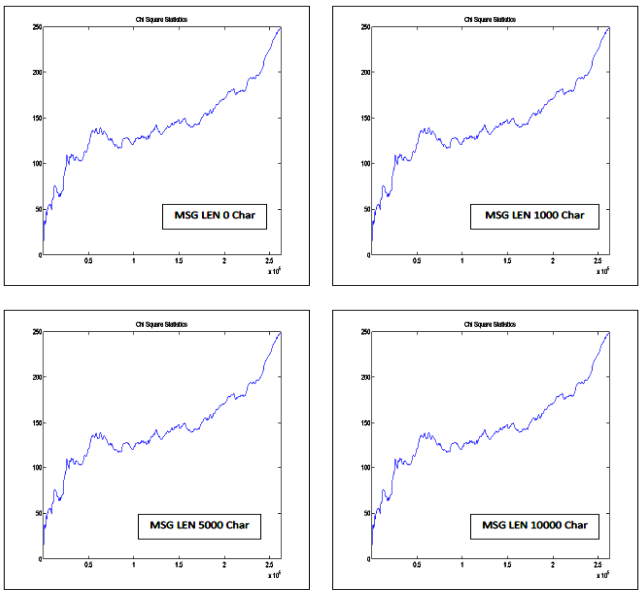

Fig. 22 Chi Square Statistics for LENA image of Various Embedding Capacity

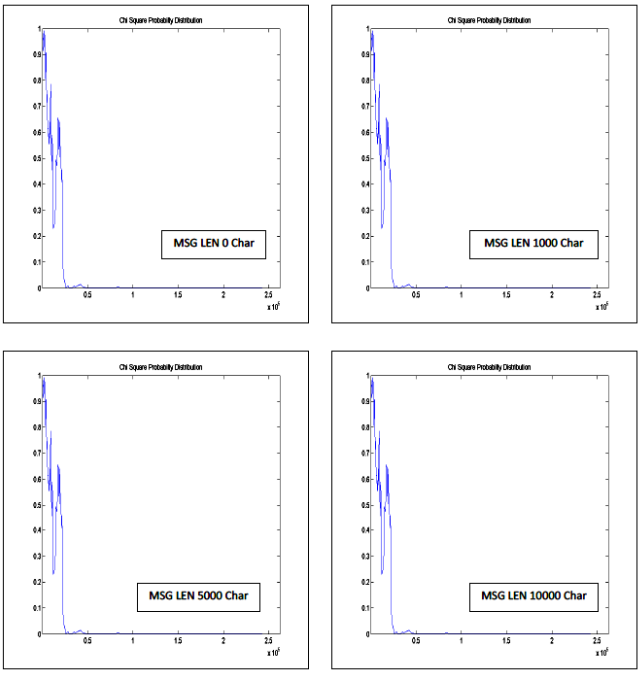

Fig. 23 Chi Square Probability Distribution for LENA image of Various Embedding Capacity

B. RS Analysis

Fridrich et al. [33] introduced an efficient LSB steganalytic method able to estimate the length of the embedded message accurately on a digital image. The method has been designed based on the fact that the content of each bit plane of an image is correlated with the remaining bit planes. In particular, for an 8-bit image, there is some degree of correlation between the LSB plane and the other remaining seven bit planes and when a message is inserted in the LSB plane, its content is considered to become randomized, and thus the correlation between the LSB planes with the remaining bit planes is reduced or lost. Let I be the image to be analyzed having width W and height H pixels. Each pixel has been denoted as P i.e. for a Gray Scale Image (8 bits per pixel image), value of P = 0, 1, . . ., 255. Next step is to divide I into G disjoint groups of n adjacent pixels. For instance consider $n = 4$. Define a discriminant function f which is responsible to give a real number $f(x_1, ..., x_n) \varepsilon R$ for each group of pixels $G = (x_1, ..., x_n)$. The objective is to capture the smoothness of G using f. Let the discrimination function can be defined as

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \quad (21)$$

Furthermore, let F_1 be a flipping invertible function F_1: 0 ↔ 1, 2 ↔3, . . ., 254 ↔255, and F_{-1} be a shifting function denoted as F_{-1} : -1 ↔0, 1 ↔2, . . ., 255 ↔256 over P. For completeness, let F_0 be the identity function such as $F_0(x) = x \; \forall x \; \varepsilon \; P$. Define a mask M that represents which function to apply to each element of a group G. The mask M is an n-tuple with values in -1, 0, 1. The value -1 stands for the application of the function F_{-1}, 1 stands for the function F_1 and 0stands for the identity function F_0 . Similarly, define –M as M's compliment.

Next step is to apply the discriminant function f with the functions $F_{-1\ ;0\ ;1}$ defined through a mask M over all G groups to classify them into three categories 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: $G \epsilon U_M \Leftrightarrow f(F(G)) = f(G)$

In similar manner R_{-M}, S_{-M} *and* U_{-M} can be defined for -M such that $(R_M + S_M)/2 \leq T$ and $(R_{-M} + S_{-M})/2 \leq T$, where T is the total number of G groups. RS Analysis method describes 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 of various stego images with different embedding capacity have been shown in Figs. 24 and 25 respectively.

Insertion Rate (in bpp)	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
0.2	32717	21081	77274	32547	21046	77481
0.3	32719	21081	77270	32549	21048	77479
0.4	32720	21084	77269	32550	21050	77475
0.5	32720	21084	77266	32550	21053	77473

Fig. 24 RS Parameter at various insertion rate for PMM Bit Plane (RGB) stego images (LENA 512x512)

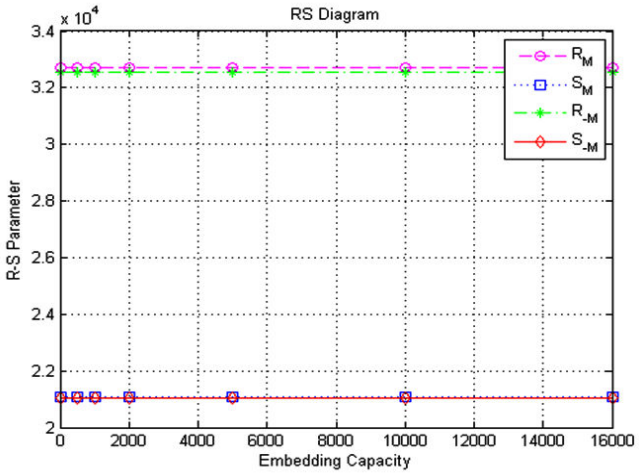

Fig. 25 RS Diagram at various insertion rate for PMM Bit Plane (RGB) stego images (LENA 512x512)

C. Sample Pair Analysis

Sorina Dumitrescu et al. [34] proposed SPA, a method to detect LSB steganography via sample pair analysis. When the embedding ratio is more than 3%, this method can estimate the embedded length with relatively high precision. The principle of SPA method is based on finite-state machine theory. The states of finite state machine are selected multisets of sample pairs. If sample pairs were drawn from images, there are some inherent relations. But after random LSB embedding, these multisets will change, and it causes changes to these statistics relations. Assuming that the pixel value of an image is represented by the succession of samples $s_1, s_2, ..., s_N$ (the index represents the location of a sample in the image), a sample pair means a two tuple (s_i, s_j), $1 \le i, j \le N$. Let P be a set of sample pairs drawn from an image, then P can be seen as a multiset of two-tuples (u, v), where u and v are the values of two adjacent samples, $0 \le u \le 2^b - 1$, $0 \le v \le 2^b - 1$, and b is the number of bits to represent each sample value. Denote by D_n the submultiset of P that consists of sample pairs of the form $(u, u + n)$ or $(u + n, u)$, i.e., where n is a fixed integer, $0 \le n \le 2b - 1$. Although sample pair analysis (SPA) was first introduced by Dumitrescu et al. [34] but the more extensible alternative approach has been proposed by Ker [35].

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

$$C_i = \left\{(x_1, x_2) \epsilon \chi^2 \left| \left\lfloor \frac{x_2}{2} \right\rfloor - \left\lfloor \frac{x_1}{2} \right\rfloor = i \right\}, \text{ where } |i| \le \lfloor (max\chi - min\chi)/2 \rfloor \quad (22)$$

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 $i = x2 - x_1$ and whose first elements x_1 are even belong to ε_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 o_i.

Consequently, the union of trace subsets $\epsilon_{2i+1} \cup \epsilon_{2i} \cup o_{2i} \cup o_{2i-1} = C_i$ constitutes a trace set (shown in Fig. 26).

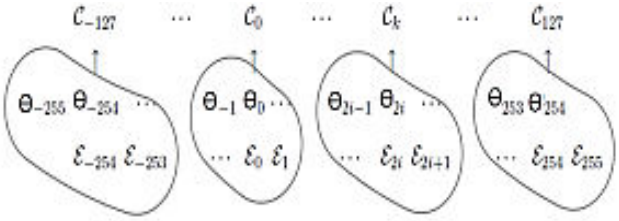

Fig. 26 Relation of trace sets and subsets in SPA (X = [0, 255])

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, where as $|\varepsilon_i|$ and $|o_i|$ are sensitive. The transition probabilities between trace subsets depend on the net embedding rate p as depicted in the transition diagram of Fig. 27. 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 in Fig. 27):

$$\begin{bmatrix} |\varepsilon_{2i+1}^{(p)}| \\ |\varepsilon_{2i}^{(p)}| \\ |\theta_{2i}^{(p)}| \\ |\theta_{2i-1}^{(p)}| \end{bmatrix} = \begin{bmatrix} \left(1-\frac{p}{2}\right)^2 & \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p^2}{4} \\ \frac{p}{2}\left(1-\frac{p}{2}\right) & \left(1-\frac{p}{2}\right)^2 & \frac{p^2}{4} & \frac{p}{2}\left(1-\frac{p}{2}\right) \\ \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p^2}{4} & \left(1-\frac{p}{2}\right)^2 & \frac{p}{2}\left(1-\frac{p}{2}\right) \\ \frac{p^2}{4} & \frac{p}{2}\left(1-\frac{p}{2}\right) & \frac{p}{2}\left(1-\frac{p}{2}\right) & \left(1-\frac{p}{2}\right)^2 \end{bmatrix} \begin{bmatrix} |\varepsilon_{2i+1}^{(0)}| \\ |\varepsilon_{2i}^{(0)}| \\ |\theta_{2i}^{(0)}| \\ |\theta_{2i-1}^{(0)}| \end{bmatrix} \quad (22.1)$$

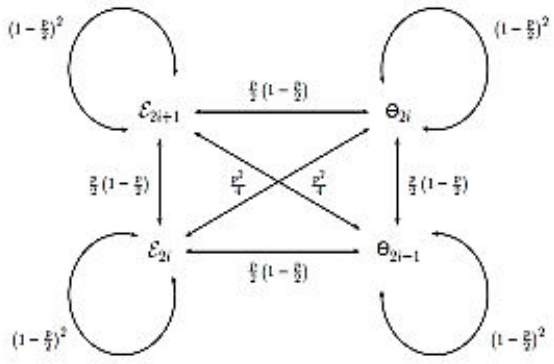

Fig. 27 Transition diagram between trace subsets under LSB replacement

Trace subsets $\varepsilon^{(p)}$ and $o^{(p)}$ are observable from a given stego object. An approximation of the cardinalities of the cover trace subsets $\varepsilon^{(0)}$ and $o^{(0)}$ can be rear ranged as a function of p by inverting as shown in equation (22.1). The transition matrix is invertible for $p < 1$ is given in equation (22.2):

$$\begin{bmatrix} |\hat{\varepsilon}_{2i+1}^{(0)}| \\ |\hat{\varepsilon}_{2i}^{(0)}| \\ |\theta_{2i}^{(0)}| \\ |\theta_{2i-1}^{(0)}| \end{bmatrix} = \frac{1}{(2-2p)^2} \begin{bmatrix} (2-p)^2 & p(p-2) & p(p-2) & p^2 \\ p(p-2) & (2-p)^2 & p^2 & p(p-2) \\ p(p-2) & p^2 & (2-p)^2 & p(p-2) \\ p^2 & p(p-2) & p(p-2) & (2-p)^2 \end{bmatrix} \begin{bmatrix} |\varepsilon_{2i+1}^{(p)}| \\ |\varepsilon_{2i}^{(p)}| \\ |\theta_{2i}^{(p)}| \\ |\theta_{2i-1}^{(p)}| \end{bmatrix} \quad (22.2)$$

With one additional cover assumption, namely $\left|\hat{\varepsilon}_{2i+1}^{(0)}\right| \approx \left|\hat{o}_{2i+1}^{(0)}\right|$, 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.

$$\left|\hat{\varepsilon}_{2i+1}^{(0)}\right| = \left|\hat{o}_{2i+1}^{(0)}\right| \tag{23}$$

$$O = \frac{(2-p)^2}{(2-2p)^2}\left(\left|\varepsilon_{2i+1}^{(p)}\right| - \left|o_{2i+1}^{(p)}\right|\right) + \frac{(p)^2}{(2-2p)^2}\left(\left|o_{2i-1}^{(p)}\right| - \left|\varepsilon_{2i+3}^{(p)}\right|\right) + \frac{(p(p-2))}{(2-2p)^2}\left(\left|\varepsilon_{2i}^{(p)}\right| + \left|o_{2i}^{(p)}\right| - \left|\varepsilon_{2i+2}^{(p)}\right| - \left|o_{2i+2}^{(p)}\right|\right) \tag{24}$$

$$O = p^2(|C_i| - |C_{i+1}|) + 4\left(\left|\varepsilon_{2i+1}^{(p)}\right| - \left|o_{2i+1}^{(p)}\right|\right) + 2p\left(\left|\varepsilon_{2i+2}^{(p)}\right| + \left|o_{2i+2}^{(p)}\right| - \left|\varepsilon_{2i+1}^{(p)}\right| + \left|o_{2i+1}^{(p)}\right| - \left|\varepsilon_{2i}^{(p)}\right| - \left|o_{2i}^{(p)}\right|\right) \tag{25}$$

The smaller root of (25) 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 (25) for a fixed interval around C_0, such as -30 =i = 30, and calculates a single root $\hat{p}$ from the aggregated quadratic coefficients. Fig. 28 shows percentage of deviation in estimated embedding rate from the actual embedding rate $\hat{p}$ obtained by Sample pair analysis of the PMM Bit Plane based stego images.

It's evident from Fig. 28 that for most values of p the estimated rate is quiet incorrect due to high deviation percentage. Only for few values of p around 0.18 the estimate is good, for rest there lies a huge difference between p and $\hat{p}$.

D. Triples Analysis

Triples analysis [36] 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. Fig. 29 shows how 3-tuples are moved amongst the trace subsets when a single sample has the LSB altered.

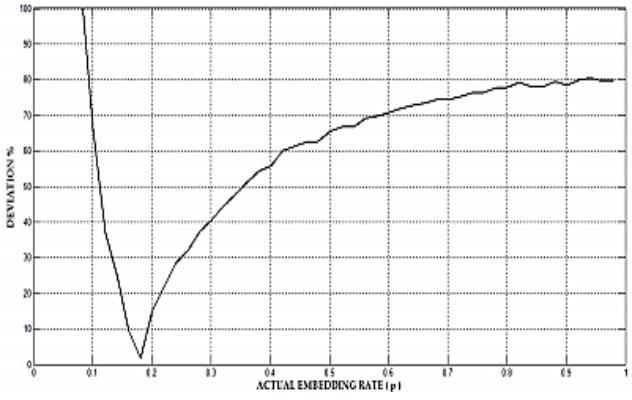

Fig. 28 Sample Pair Analysis Graph for PMM Bit Plane for (LENA 512x512 (RGB))

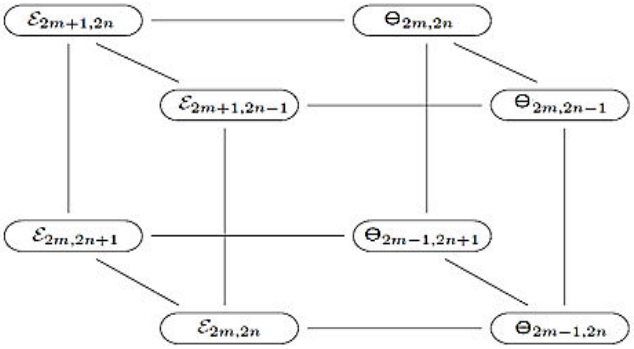

Fig. 29 The 8 trace subsets of $C_{m,n}$

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 one trace subset to another is $p^i(1-p)^{(3-i)}$, where i is the length of the shortest path between them. If the trace subsets are enumerated as 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 can be 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,

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

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 (26).

$$\hat{X} = T_3^{-1}\acute{X} \tag{26}$$

For the analogous property or the parity symmetry, $\xi_{2m.2n} = \Theta_{2m.2n}$ for 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

$$\epsilon_{m,n} = \hat{\xi}_{2m+1.2n+1} - \hat{\Theta}_{2m+1.2n+1} \tag{27}$$

Final step is to find the value of embedding rate p which minimizes the error rate. Fig. 30 shows percentage of deviation in estimated embedding rate from the actual

embedding rate $\hat{p}$ obtained by Triples analysis of the PMM Bit Plane based stego images.

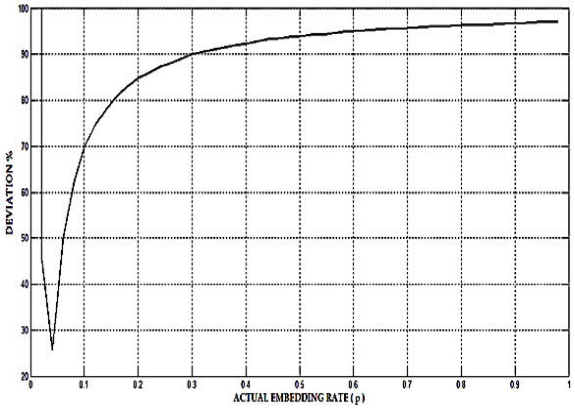

Fig. 30 Triples Analysis Graph for PMM Bit Plane for (LENA 512x512(RGB))

E. Steganalysis Using SPAM Features

Steganalysis through rich model [37] analysis using 2nd order SPAM features [38] with dimensionality 686 with the help of ensemble classifiers [39] has been used for evaluating the performance of the proposed method. The minimum average classification error P_E has been computed as

$$P_E = min(P_{FA})\left[\frac{P_{FA}+P_{MD}(P_{FA})}{2}\right] \quad (28)$$

where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate.

The steganalysis performance of the for PMM Bit Plane method has been compared with HUGO and Adaptive steganography method and the plots of P_E have been shown in Fig. 31.

From Fig. 31, it can be concluded that for SPAM steganalyzer the performance of the proposed method is quite comparable with HUGO and Adaptive scheme.

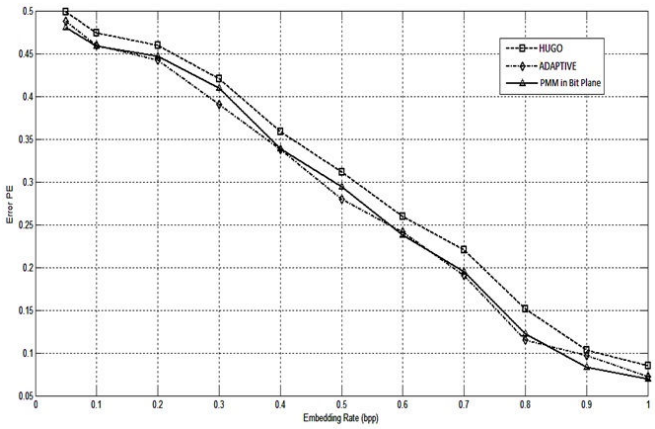

Fig. 31 Minimum average classification errors of different methods using 2nd order SPAM feature (dim 686) using ensemble classifier

VIII. Conclusion

In this article the authors proposes an efficient image based steganography method for hiding information through the Pixel Mapping Method (PMM) in Bit Plane Domain. Efficiency of the proposed method has been compared with some of the existing methods. From the experimental results it has been identified that the embedding capacity of the proposed method is much better compared to other existing ones. This methods shows a significant achievements compared to others in terms of MSE, PSNR and other different similarity measure metrics. From the security aspects PMM in Bit Plane domain gives an excellent result as the relative entropy distance (KL divergence) is very low and the secret messages are embedded in highly complex planes of the cover image. The hidden message also stays undetected against some well known steganalysis attacks like Chi-Square, RS Analysis, Sample Pair and Triples Analysis .This method also gives a moderate result against RICH Model analysis based on SPAM features.

References

[1] G. J. Simmons., The prisoners' problem and the subliminal channel, Proceedings of CRYPTO. 83 (1984) 51–67.
[2] R. Anderson., Stretching the limits of steganography, Information Hiding, Springer Lecture Notes in Computer Science 1174 (1996) 39–48.
[3] R. J. Anderson., F. A.P.Petitcolas., On the limits of steganography, IEEE Journal on Selected Areas in Communications (J-SAC), Special Issueon Copyright and Privacy Protection 16 (1998) 474–481.
[4] S. Craver., On public-key steganography in the presence of an active warden, in: Proceedings of 2nd International Workshop on Information Hiding., Portland, Oregon, USA, 1998, pp. 355–368.
[5] N.F.Johnson., S. Jajodia., Steganography: seeing the unseen, IEEE Computer 16 (1998) 26–34.
[6] J. E. T Mrkel., M. Olivier., An overview of image steganography, in: Proceedings of the fifth annual Information Security South AfricaConference., 2005.
[7] S. Bhattacharyya., G. Sanyal., Study of secure steganography model, in: Proceedings of International Conference on Advanced Computing and Communication Technologies (ICACCT-2008), Panipath, India, 2008.
[8] S. Bhattacharyya., G. Sanyal., An image based steganography model for promoting global cyber security, in: Proceedings of International Conference on Systemics, Cybernetics and Informatics, Hyderabad, India, 2009.
[9] S. Bhattacharyya., G. Sanyal., Implementation and design of an image based steganographic model, in: Proceedings of IEEE InternationalAdvance Computing Conference, Patiala,India, 2009.
[10] S. B. A. K. et al., G. Sanyal., Pixel mapping method (PMM) based bit plane complexity segmentation (bpcs) steganography, in: Proceedings of WICT 2011, Mumbai, India, 2011.
[11] Y. K. Lee., L. H.Chen., High capacity image steganographic model, IEEE Proc.-Vision, Image and Signal Processing 147 (2000) 288–294.
[12] C. Chan., L. M.Cheng, Hiding data in images by simple lsb substitution, Pattern Recognition 37 (2004) 469–474.
[13] D. Wu., W. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24 (2003) 1613–1626.
[14] P. H. K.C. Chang., C.P Chang., T. Tu., A novel image steganography method using tri-way pixel value differencing, Journal of Multimedia 3.
[15] C.-S. T. C.-M. Wang, N.-I. Wu, M.-S. Hwang., A high quality steganographic method with pixel-value differencing and modulus function, The Journal of Systems and Software 81(1) (2008) 150–158.
[16] P. V. C. E., Gray level modification steganography for secret communication, in: IEEE International Conference on Industrial Informatics.,Berlin, Germany, 2004, pp. 355–368.
[17] X. Zhang, and S. Wang, Efficient steganographic embedding by exploiting modification direction, Journal of IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, 2006.

[18] Ruey-Ming Chao, Hsien-Chu Wu, Chih-Chiang Lee, and Yen-Ping Chu A Novel Image Data Hiding Scheme with Diamond Encoding EURASIP Journal on Information Security Volume 2009, Article ID 658047, 9 pages
[19] X. Zhang, S. Wang. C. C. L. R.M. Chao, H. C. Wu, Y. P. Chu.T. H. Chang, C.C., A steganographic method for digital images using side match., Pattern Recognition Letter 25 (2004) 1431–1437
[20] S. Bhattacharyya., G. Sanyal., Hiding data in images using pixel mapping method (PMM), in: Proceedings of 9th annual Conference onSecurity and Management (SAM) under The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing (WorldComp 2010), LasVegas, USA, July 12-15,2010.
[21] L. K. Souvik Bhattacharyya, G. Sanyal., A novel approach of data hiding using pixel mapping method (PMM), International Journal Ofcomputer Science and Information Security(IJCSIS) 8.
[22] P. B. T. Pevn, J. Fridrich., Steganalysis by subtractive pixel adjacency matrix., IEEE Transactions on Information Forensics and Security,5(2):215-224.
[23] C. W. N. Y. Tao Han, Weiming Zhang, Y. Zhu., Adaptive steganography in extended noisy region.
[24] R. O. E. E. Kawaguchi, Principle and applications of bpcs-steganography, in: Proc. SPIE 3528, Multimedia Systems and Applications, 464. Conference Volume 3528, November 01, 1998.15
[25] H. N. M. Niimi, E. Kawguchi., A steganography based on region segmentation by using complexity measure., Trans. of IEICE, J81-D-II, pp.1132-1140,1998.
[26] A. Habes, 4 least significant bits information hiding implementation andanalysis, in: Proc. GVIP 05 Conference, CICC,Cairo, Egypt,2005.
[27] B. P. Pevn, T., J. Fridrich, Review: Steganography bit plane complexity segmentation (bpcs) technique, International Journal of Engineering Science and Technology,Vol. 2(9), 2010, 4860-4868.
[28] Ucid image database [online].URL http://vision.cs.aston.ac.uk/datasets/UCID/ucid.html
[29] I. A. C. B. F. I. H. R. S. S. M. I. Zhou Wang, Member, I. EeroP. Simoncelli, Senior Member, Image quality assessment: From error visibility to structural similarity, IEEE Transactions on Imageprocessing. 3
[30] 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.
[31] A. Westfeld, A. Pfitzmann., Attacks on steganographic systems., In Proceedings of the Third Intl. Workshop on Information Hiding, Springer-verlag. (1999) 61–76.
[32] Guillermito., Steganography: A few tools to discover hidden data.
[33] G. M. D. R. Fridrich, J., Detecting lsb steganography in color, and gray-scale images, IEEE Multimedia 8. (2001) 22–28.
[34] W. X. W. Z. Dumitrescu, S., Detection of lsb steganography via sample pair analysis, in: Proceedings of 5th Information Hiding Workshop, Vol.2578, 2002, pp. 355–372.
[35] A. Ker, Improved detection of lsb steganography in grayscale images in: Proc.6th Information Hiding Workshop. Volume 3200 of Springer LNCS, 2004, pp. 97–115.
[36] A. D. Ker, Optimally weighted least-squares steganalysis, in: Proc. SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX, 650506 (February 27, 2007).
[37] Fridrich, J. Kodovsk., Rich models for steganalysis of digital images., IEEE Transactions on Information Forensics and Security. 7(3) 868–882.
[38] S. K. et. al., Steganalysis by subtractive pixel adjacency matrix, IEEE Trans. Inf. Forensics and Sec., 5, 215-224, 2010.
[39] J. F. J. Kodovsk, V. Holub., Ensemble classifiers for steganalysis of digital media., IEEE Transactions on Information Forensics and Security.

Souvik Bhattacharyya 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 his Ph.D in Engineering. 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 various 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.

Indradip Banerjee is a Research Scholar at National Institute of Technology, Durgapur, West Bengal, India. He received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. He is registered and pursuing his PhD. in Engineering at Computer Science and Engineering Department, National Institute of Technology, Durgapur, West Bengal, India. His areas of interest are Steganography, Cryptography, Text Steganography, Image Steganography, Quantum Steganography and Steganalysis. He has published 25 research papers in International and National Journals / Conferences.

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. Four 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 (Faculty Welfare) at National Institute of Technology, Durgapur, India.