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 gained 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](image)

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](image)

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.
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 PPM 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 greater 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.
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 \( P = [P_7 P_6 P_5 P_4 P_3 P_2 P_1 P_0] \) where \( P_7 \) is the MSB bit plane and \( P_0 \) 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.

F. HUGO Steganography Method

Hugo 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 [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 shortcomings of traditional steganographic techniques like Least Significant Bit (LSB) technique or
If a bit on the $l^{th}$ bit plane on an m-bit dataset is set to 1, it contributes a value of $2^{m-l}$, otherwise it contributes nothing. Define $\gamma$ 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 $X = \{0, 1, 2, ..., 255\}$ be the set of pixel intensity values such that a digital image is represented by, $X=(x_{ijk})$ where $D=1$ corresponds to a gray scale image consisting of just the gray scale plane and $D=3$ corresponds to an RGB image. $X_{ijk}$, $k=1$ 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 $\chi$ 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 ($b_{23}, b_{22}, b_{21}, ..., b_{0}$) where the first 8 bits from rightmost end ($b_{23}, b_{22}, b_{21}, ..., b_{16}$) corresponds to the red plane intensity while next 8 bits ($b_{15}, b_{14}, b_{13}, ..., b_{8}$) and remaining ($b_{7}, b_{6}, b_{5}, ..., b_{0}$) corresponds to green and blue plane intensities respectively and $b_{23}, b_{15} & b_{7}$ being the MSB and $b_{14}, b_{6}$ and $b_{0}$ being the LSB of red, green and blue color planes respectively. While for gray scale image we have $b_{7}, b_{6}, ..., b_{0}$ 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

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

$k$ 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 $\alpha$ is the normalized value of the total length of the black and white border in the image. Clearly $\alpha$ lies in $[0, 1]$.

IV. PROPOSED DATA EMBEDDING METHOD

In this approach, the secret message is embedded through 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 $8 \times 8$ 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.
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 \( C = (c_{i,k}) \in \chi \) with \( n \) bits per pixel is sliced into \( n \) binary images or logical matrices.

2. Let \( \rho \) be a secret message of length \( L \) characters where \( L \geq l \), to be embedded. Each character of \( \rho \) can be represented by a 8 bit binary sequence using ASCII encoding. Using this \( \rho \) is converted to a binary message stream \( m \) of length \( l=8L \) such that \( m \in \gamma \).

3. For each bit plane \( B_i, i = 0, ..., n-l \) compute the overall plane complexity from (2) as \( \{\sigma_{n-1}, \sigma_{n-2}, ..., \sigma_{0}\} \) and next step is to find the color plane complexity \( \delta_R, \delta_G \) and \( \delta_B \) for \( R,G \) and \( B \) planes of color image or \( \delta_{\text{gray}} \) for gray scale image as the average of the complexities of bit planes corresponding the color or gray plane.

4. Considering \( \delta_R, \delta_G \) and \( \delta_B \) as the threshold complexities determine bit planes with complexity \( \alpha \) greater than its corresponding \( \delta \) and add them to the set of message embedding planes \( \xi \) of the image.

5. Sort the elements of \( \xi \) according to decreasing order of their bit plane complexity \( \alpha \).

6. Let binary message stream \( m \) be given by the sequence of bits \( \beta_i, i = 1, 2, ..., l \). While there are bits \( \beta_i \) remaining to be embedded, i.e. \( i \leq l \), the following procedure is used for embedding.

7. Select the next highest complexity bit plane \( B_k \) from the decreasingly sorted sequence of \( \xi \) 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 \( \frac{MN}{2^k} \) blocks obtained from step 7. Take the mean value of these complexities as the threshold complexity say \( \alpha_T \) 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 \( \frac{2^k}{10} \) non-overlapping blocks of size \( 8 \times 8 \) and within each such block say \( T \) embed 16 bits as follows.
10. T is a logical matrix given by, $T = (\tau_{i,j})$, for $j, k = 1, 2, \ldots, 8$. Let $Dec_j$ be the decimal value of the $j^{th}$ row of T i.e., considering bit sequence $\tau_{1,j} \ldots \tau_{s,j}$ and $count_j$ be the number of ones in $j^{th}$ row of T excluding $\tau_{1,j}$ i.e., number of ones in bit sequence $\tau_{2,j} \ldots \tau_{s,j}$. Within each row of T i.e. for each $j$ embed 2 bits $\beta_i \beta_{i+1}$ 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 $y%2 \neq 0$.

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 $y%2 \neq 0$.

d) Case 4: $\beta_i \beta_{i+1} = 11$ set $Dec_j = x$ such that $x%2 = 0$ and $count_j = y$ such that $y%2 \neq 0$.

11. After embedding 2 bits for each $j=1, 2, \ldots, 8$ consider next 8 × 8 block of S and so on, when S is filled consider next noisy block with $\alpha \geq \alpha_0$ and so on until all noisy blocks filled and then consider next highest complex plane from sorted sequence of $\xi$. Repeat this procedure until all bits of $\beta_i$ 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 $S = (s_{ijk}) \in \chi$.

B. Data Extraction Method

1. The stego image $S = (s_{ijk}) \in \chi$ is sliced into n bit planes.

2. For each bit plane $B_i$, $\forall i = 0, 1, \ldots, n - 1$ compute the overall plane complexities from (2) as $\{a_{n-1}, a_{n-2}, \ldots, a_0\}$ and next step is to find the color plane complexity $\delta_R, \delta_G$ and $\delta_B$ for R,G and B planes of color image or $\delta_{\text{Gry}}$, for gray scale image as the average of the complexities of bit planes corresponding the color or gray plane.

3. Considering $\delta_R, \delta_G$ and $\delta_B$ or $\delta_{\text{Gry}}$ as the threshold complexities determine bit planes with complexity $\alpha$ greater than its corresponding $\delta$ and add them to the set of message extraction planes $\xi$.

4. Sort the elements of $\xi$ according to decreasing order of their bit plane complexity $\alpha$.

5. The secret binary message stream $m$ be given by the sequence of bits $\beta_i, i = 1, 2, \ldots, I$ where $I$ 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 $B_j$ from the decreasingly sorted sequence of $\xi$ 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 $2^{kN}/2^k$ blocks obtained. Take the mean value of these complexities as the threshold complexity say $\alpha_t$ 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 extraction of bits.

7. Let $R$ be a selected $2^k \times 2^k$ block for extraction, then divide $R$ into $2^{2k}$ non-overlapping blocks of size $8 \times 8$ and within each such block say $T$ embed 16 bits as follows.

8. $T$ be a logical matrix given by, $T = (\tau_{i,j})$, for $j, k = 1, 2, \ldots, 8$. Let $count_j$ be the number of ones in $j^{th}$ row of T excluding $\tau_{1,j}$ i.e., number of ones in bit sequence $\tau_{2,j} \ldots \tau_{s,j}$. From each row of T i.e for each $j$ extract 2 bits $\beta_i \beta_{i+1}$ by inverse Pixel Mapping Method (PMM) as

(a) $\beta_i = j$ and

(b) Case 1: if $count_j = y$ such that $y%2 = 0$ then $\beta_i = 0$.

(c) Case 2: if $count_j = y$ such that $y%2 \neq 0$ then $\beta_i = 1$.

9. After extraction of 2 bits for each $j=1, 2, \ldots, 8$ consider next 8 × 8 block of S and so on, when data has been extracted from all $2^k \times 2^k$ blocks of S then consider next noisy block with $\alpha \geq \alpha_t$ and so on until all noisy blocks have been covered and then consider next highest complex plane from sorted sequence of $\xi$. Repeat this procedure until all bits of $\beta_i$ 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 $\xi$ being the set of all complex planes of the cover image $C$ let $n = |\xi|$ i.e., $n$ is the cardinality of the set $\xi$. For each $e_i \in \xi, \forall i = 1, 2, \ldots, n$, 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 $8 \times 8$ sub blocks yielding $2^{(k-3)} \times 16$ sub blocks. Within each $8 \times 8$ sub blocks with PMM (2 bit) 8 × 2 bits can be embedded (2 bits in each row of $8 \times 8$ 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)

$$\text{No-of-bits} = (\sum_{i=1}^{n} a_i) \times 2^{(k-3)} \times 16$$ (3)
Embedding capacity for 4 bit mapping can be calculated as

$$\text{No-of-bits} = (2^m a_i) \times 2^{2(k-3)} \times 32$$  \hspace{0.5cm} (4)

Maximum Bits Per Pixel (bpp) is given by

$$\text{bpp} = \frac{\text{No-of-bits}}{MN \times N \times 3}$$  \hspace{0.5cm} (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 $2^k \times 2^k \times 2^k$ 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

$$\text{bpp}_{\text{PMM(4-bit)}} = \frac{MN \times N \times 3}{2^k \times 2^k \times 2^k} \approx \frac{n}{6}$$  \hspace{0.5cm} (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 while as 1179648 bits or 147456 characters can be embedded using PMM (2 bit). 

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.

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.

![Figure 13 Embedding capacity for different test images](image1)

![Figure 14 Comparison of embedding capacity in terms of Byte](image2)

![Figure 15 Comparison of embedding capacity in terms of BPP](image3)

**B. Imperceptibility Test**

How to preserve the details of the cover carrier when the secret message is being embedded in such 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):

\[
\text{MSE} = \frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N [C(i,j) - S(i,j)]^2
\]

(7)

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

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \text{db}
\]

(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.

<table>
<thead>
<tr>
<th>Cover Image</th>
<th>LSB</th>
<th>PVD</th>
<th>SIDE MATCH</th>
<th>OPAP</th>
<th>GLM</th>
<th>N-PVD</th>
<th>DE ((k=1))</th>
<th>PMM(B) in Bit Plane (RGB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>49.3</td>
<td>46.3</td>
<td>46.2</td>
<td>50.1</td>
<td>35.5</td>
<td>49.6</td>
<td>52.1</td>
<td>58.7</td>
</tr>
<tr>
<td>Baboon</td>
<td>49.5</td>
<td>46.1</td>
<td>43.4</td>
<td>50.1</td>
<td>35.5</td>
<td>49.4</td>
<td>52.0</td>
<td>60.1</td>
</tr>
<tr>
<td>Pepper</td>
<td>49.5</td>
<td>46.2</td>
<td>46.6</td>
<td>50.1</td>
<td>35.5</td>
<td>49.6</td>
<td>52.0</td>
<td>56.2</td>
</tr>
<tr>
<td>Airplane</td>
<td>49.5</td>
<td>46.1</td>
<td>46.5</td>
<td>50.0</td>
<td>35.5</td>
<td>49.5</td>
<td>52.0</td>
<td>61.3</td>
</tr>
<tr>
<td>Boat</td>
<td>49.5</td>
<td>46.1</td>
<td>45.4</td>
<td>50.1</td>
<td>35.5</td>
<td>49.4</td>
<td>52.1</td>
<td>58.4</td>
</tr>
<tr>
<td>Barbara</td>
<td>49.5</td>
<td>46.1</td>
<td>49.5</td>
<td>50.1</td>
<td>35.5</td>
<td>49.5</td>
<td>52.1</td>
<td>58.7</td>
</tr>
<tr>
<td>Tiffany</td>
<td>49.4</td>
<td>46.1</td>
<td>46.7</td>
<td>50.0</td>
<td>35.5</td>
<td>49.7</td>
<td>52.1</td>
<td>62.6</td>
</tr>
<tr>
<td>Zelda</td>
<td>49.4</td>
<td>46.2</td>
<td>46.5</td>
<td>50.1</td>
<td>35.5</td>
<td>49.5</td>
<td>52.1</td>
<td>57.7</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Cover Image</th>
<th>LSB</th>
<th>PVD</th>
<th>SIDE MATCH</th>
<th>OPAP</th>
<th>GLM</th>
<th>N-PVD</th>
<th>DE ((k=1))</th>
<th>PMM(B) in Bit Plane (RGB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>42.3</td>
<td>37.5</td>
<td>46.2</td>
<td>45.7</td>
<td>NA</td>
<td>40.6</td>
<td>46.3</td>
<td>49.9</td>
</tr>
<tr>
<td>Baboon</td>
<td>42.3</td>
<td>37.1</td>
<td>43.4</td>
<td>45.3</td>
<td>NA</td>
<td>40.3</td>
<td>46.3</td>
<td>50.3</td>
</tr>
<tr>
<td>Pepper</td>
<td>42.3</td>
<td>37.8</td>
<td>46.6</td>
<td>45.4</td>
<td>NA</td>
<td>40.2</td>
<td>46.4</td>
<td>48.2</td>
</tr>
<tr>
<td>Airplane</td>
<td>42.3</td>
<td>37.4</td>
<td>46.5</td>
<td>45.3</td>
<td>NA</td>
<td>40.4</td>
<td>46.7</td>
<td>51.9</td>
</tr>
<tr>
<td>Boat</td>
<td>42.3</td>
<td>37.0</td>
<td>45.4</td>
<td>45.4</td>
<td>NA</td>
<td>40.2</td>
<td>46.3</td>
<td>48.6</td>
</tr>
<tr>
<td>Barbara</td>
<td>42.4</td>
<td>37.7</td>
<td>49.5</td>
<td>45.6</td>
<td>NA</td>
<td>40.5</td>
<td>46.2</td>
<td>49.1</td>
</tr>
<tr>
<td>Tiffany</td>
<td>42.5</td>
<td>37.2</td>
<td>46.7</td>
<td>45.6</td>
<td>NA</td>
<td>40.3</td>
<td>46.6</td>
<td>51.9</td>
</tr>
<tr>
<td>Zelda</td>
<td>42.4</td>
<td>37.1</td>
<td>46.5</td>
<td>45.4</td>
<td>NA</td>
<td>40.5</td>
<td>46.2</td>
<td>47.2</td>
</tr>
</tbody>
</table>

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:

\[
\text{SSIM} (x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}
\]

(9)

where \( \mu_x \) is the average of \( x \) and \( \mu_y \) is the average of \( y \); 2. \( \sigma_x^2 \) is the variance of \( x \); 3. \( \sigma_y^2 \) is the variance of \( y \); 4. \( \sigma_{xy} \) is the covariance of \( x \) and \( y \); 5. \( c_1 = (k_1L)^2 \) and \( c_2 = (k_2L)^2 \) 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.
between the probabilities $P$ and $Q$, where the average is taken based on $Q$, rather than using a code based on $P$. Typically $P$ 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

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

(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 $0 \log 0$ 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

$$D_{KL}(P \parallel Q) = \int_{x} P(x) \ln \frac{P(x)}{Q(x)}$$  

(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 Kullback-Leibler divergence from $P$ to $Q$ is defined as

$$D_{KL}(P \parallel Q) = \int \frac{dP}{dQ} dP \ln \frac{dP}{dQ}$$  

(12)

where $\frac{dP}{dQ}$ 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

$$D_{KL}(P \parallel Q) = -\int \ln \frac{dQ}{dP} dP$$  

(13)

which we recognize as the entropy of $P$ relative to $Q$. Continuing in this case, if $\mu$ 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

$$D_{KL}(P \parallel Q) = \int p \ln \frac{p}{q} d\mu$$  

(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 $C \times M \times K \rightarrow C$ that assigns a new (stego) object, $s \in C$, to each triple $(c,M,K)$, where $M \subseteq M$ is a secret message selected from the set of communicable messages, $M$, and $K \in K$ 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 or relative entropy,

$$D_{KL}(P \parallel Q) = \sum_{c \in C} P(c) \ln \frac{P(c)}{Q(c)}$$  

(15)

When $D_{KL}(P \parallel Q) < \epsilon$, the stego system is called $\epsilon$ secure. Fig. 20 shows the values of relative entropy of different stego images at embedding rate of 0.3 bpp.
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 \( x^{(i)} \) represent the cover object and \( y^{(i)} \) be the stego object. If \( x^{(i)} \) is the stego object with embedding rate \( p \). Then estimated embedding rate \( \hat{p} \) can be given by,

\[
\hat{p} = \text{Detect}_{\text{Quant}}(x^{(p)})
\]

In this section all the stego images produced by PPM Bit Plane (RGB) algorithms have 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 \( \leftrightarrow \) 1, 2 \( \leftrightarrow \) 3, 4 \( \leftrightarrow \) 5... 252 \( \leftrightarrow \) 253, 254 \( \leftrightarrow \) 255. This will affect the histogram \( Y_k \) of the images pixel value \( k \), while the sum of \( Y_k + Y_{k+1} \) will remain unchanged. Thus the expected distribution of the sum of adjacent values given in (18) and the \( \chi^2 \) value for the difference between distributions with v-1 degrees of freedom is in (19). From (18) and (19) \( \chi^2 \) statistic can be obtained for the PoVs as given in (20).

\[
E(Y_{2i}) = \frac{1}{2}(Y_{2i} + Y_{2i+1})
\]

\[
X^2 = \sum_{i=1}^{V} \left( \frac{F_i - E_i}{E_i} \right)^2
\]

\[
X^2_{\text{PoV}} = \sum_{i=1}^{128} \left( Y_{2i}-\frac{1}{2}(Y_{2i}+Y_{2i+1}) \right)^2
\]

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) ∈ 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

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

Furthermore, let F_i be a flipping invertible function F_i: 0 ↔ 1, 2 ↔ 3, ..., 254 ↔ 255, and F_i be a shifting function denoted as F_i: -1 ↔ 0, 1 ↔ 2, ..., 255 ↔ 256 over P. For completeness, let F_0 be the identity function such as F_0(x) = x ∀ x ∈ P. Define a mask M that represents which function to apply to each element of a group G. The mask M is an n×1 vector with values in 0, 1. The value -1 stands for the application of the function F, 1 stands for the function F_1 and 0 stands 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 ∈ R_M ⇔ f (F_i (G)) > f (G)
- Singular groups: G ∈ S_M ⇔ f (F_i (G)) < f (G)
- Unusable groups: G ∈ U_M ⇔ f (F_i (G)) = f (G)

In similar manner R_{-1, 0, 1}, S_{-1, 0, 1} and U_{-1, 0, 1} can be defined for -M such that |R_M + S_M| ≤ T and |R_M + S_M| ≤ T, where T is the total number of G groups. RS Analysis method describes that, for typical images R_M ≈ S_M and S_M ≈ |U_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.

<table>
<thead>
<tr>
<th>Insertion Rate (in bpp)</th>
<th>F_i Flipping</th>
<th>F_{-1} Flipping</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>32716</td>
<td>21079</td>
</tr>
<tr>
<td>0.1</td>
<td>32717</td>
<td>21081</td>
</tr>
<tr>
<td>0.2</td>
<td>32719</td>
<td>21081</td>
</tr>
<tr>
<td>0.3</td>
<td>32720</td>
<td>21081</td>
</tr>
<tr>
<td>0.4</td>
<td>32720</td>
<td>21081</td>
</tr>
<tr>
<td>0.5</td>
<td>32720</td>
<td>21081</td>
</tr>
</tbody>
</table>

Fig. 24 RS Parameter 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 the 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 \( (s_i, s_j) \), \( 1 \leq i, j \leq N \). 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, \( 0 \leq u \leq 2^n - 1 \), \( 0 \leq v \leq 2^n - 1 \), and \( b \) is the number of bits to represent each sample value. Denote by \( D_b \) 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, \( 0 \leq n \leq 2b - 1 \). 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 \( (x_i, x_j) \) to a trace set \( C_i \), so that

\[
C_i = \{(x_i, x_j) \in \mathbb{R}^2 | x_j = x_i + \epsilon \}, \text{ where } |\epsilon| \leq (\max x - \min x)/2(22)
\]

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

- Pairs \( (x_i, x_j) \) whose values differ by \( i = x_j - x_i \) and whose first elements \( x_i \) are even belong to \( C_i \).
- Pairs \( (x_i, x_j) \) whose values differ by \( i = x_j - x_i \) and whose first elements \( x_j \) are odd belong to \( C_i \).

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

This definition of trace sets and subsets ensures that the LSB replacement embedding operation never changes a sample pair’s trace set, i.e., \( C_i^{(0)} = C_i^{(p)} = C_i \), but may move sample pairs between trace subsets that constitute the same trace set. So cardinalities \( |C_i| \) are invariant to LSB replacement, where \( |C_i| \) and \( |C_i| \) 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):

\[
\begin{bmatrix}
|\mathcal{C}_{2i+1}| \\
|\mathcal{C}_{2i}| \\
|\mathcal{C}_{2i-1}|
\end{bmatrix} =
\begin{bmatrix}
(1 - \frac{\epsilon^2}{4}) & \frac{\epsilon}{2} & \frac{\epsilon}{2} \\
\frac{\epsilon}{2} & (1 - \frac{\epsilon^2}{4}) & \frac{\epsilon}{2} \\
\frac{\epsilon}{2} & \frac{\epsilon}{2} & (1 - \frac{\epsilon^2}{4})
\end{bmatrix}
\begin{bmatrix}
|\mathcal{C}_{2i+1}|^{(0)} \\
|\mathcal{C}_{2i}|^{(0)} \\
|\mathcal{C}_{2i-1}|^{(0)}
\end{bmatrix}
(22.1)
\]

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

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

\[
\begin{bmatrix}
|\mathcal{C}_{2i+1}|^{(p)} \\
|\mathcal{C}_{2i}|^{(p)} \\
|\mathcal{C}_{2i-1}|^{(p)}
\end{bmatrix} =
\begin{bmatrix}
|\mathcal{C}_{2i+1}|^{(0)} \\
|\mathcal{C}_{2i}|^{(0)} \\
|\mathcal{C}_{2i-1}|^{(0)}
\end{bmatrix}
(22.2)
\]
With one additional cover assumption, namely \( \beta_{i+1}^{(0)} = E_{i+1}^{(0)} \), the first equation of this system for \( i \) can be combined with the fourth equation for \( i + 1 \) to obtain a quadratic estimator \( \hat{\beta} \) for \( p \).

\[
\sum_{i=1}^{m} E_{i+1}^{(0)} = \sum_{i=1}^{m} E_{i+1}^{(0)} \tag{23}
\]

\[
O = \frac{(2-p)^2}{2-p} \left( E_{i+1}^{(0)} - \beta_{i+1}^{(0)} \right) + \frac{(p^2 - p)}{2-p} \left( |E_{i+1}^{(0)}| - |\beta_{i+1}^{(0)}| \right) + \frac{(p^2 - p)}{2-p} \left( |E_{i+1}^{(0)}| - |\beta_{i+1}^{(0)}| \right) \tag{24}
\]

\[
O = p^2 (|E_{i+1}^{(0)}| - |\beta_{i+1}^{(0)}|) + 4 (|E_{i+1}^{(0)}| - |\beta_{i+1}^{(0)}|) + 2p (|E_{i+1}^{(0)}| - |\beta_{i+1}^{(0)}|) - |E_{i+1}^{(0)}| - |\beta_{i+1}^{(0)}|) \tag{25}
\]

The smaller root of (25) is a secret message length estimate \( \hat{\beta} \) based on the information of pairs in trace set \( C \). Standard SPA sums up the family of estimation equation (25) for a fixed interval around \( C_m \), such as \(-30 < m = 30\), and calculates a single root \( \hat{\beta} \) from the aggregated quadratic coefficients. Fig. 28 shows percentage of deviation in estimated embedding rate from the actual embedding rate \( \hat{\beta} \) 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 \( \hat{\beta} \).

**D.Triples Analysis**

Triples analysis [36] considers 3-tuples of sample values. First step is to fix a trace set \( C_m \) 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.

The smaller root of (25) is a secret message length estimate \( \hat{\beta} \) based on the information of pairs in trace set \( C \). Standard SPA sums up the family of estimation equation (25) for a fixed interval around \( C_m \), such as \(-30 < m = 30\), and calculates a single root \( \hat{\beta} \) from the aggregated quadratic coefficients. Fig. 28 shows percentage of deviation in estimated embedding rate from the actual embedding rate \( \hat{\beta} \) 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 \( \hat{\beta} \).

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

\[
T_i^{-1} = \begin{pmatrix}
(1-q) & (1-q)(1+q) & (1-q)(1+q)(1+e) \\
(1-q)(1+q) & (1-q)(1+q) & (1-q)(1+q)(1+e) \\
(1-q)(1+q)(1+e) & (1-q)(1+q)(1+e) & (1-q)(1+q)(1+e)(1+e)
\end{pmatrix}
\]

For a given stego image, considering each trace set \( C_{m,n} \) and counting the trace subsets to form a vector \( \tilde{X} \). 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).

\[
\tilde{X} = T_i^{-1} \tilde{X} \tag{26}
\]

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

\[
\epsilon_{m,n} = \xi_{2m+1,2n+1} - \theta_{2m+1,2n+1} \tag{27}
\]

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.

\[ P_E = \min(P_{FA}) \left[ \frac{P_{FA} \cdot P_{MD}}{2} \right] \]

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.

**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**


Aparajita Khan has received her B.E. in Computer Science and Engineering from University of Burdwan, Burdwan, India and is currently pursuing 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.

Indradyut 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, Durgarpur, 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.