Defeating Steganography with Multibit Sterilization using Pixel Eccentricity

Imon, Mukherjee; Goutam, Paul, and Jawahar, Altrin Jarvis

Abstract: ***Image sterilization is a technique to remove any secret data concealed within an image. Eccentricity of an image is estimated by the ratio between the maximum and the minimum distances between the centroid and the boundary of the image. Analogously, we define the eccentricity of each pixel using central moments within a 3×3 window centered around that pixel. We propose a blind sterilization technique by finding the eccentricity of each stego pixel that can annihilate utmost four least significant bits of the stego images formed using steganography algorithm, irrespective of how the algorithm embeds information inside the images. We ran simulations over three kinds of stego images (viz. cartoon, nature and busy nature) created by different state-of-the-art algorithms and our technique succeeded in sterilizing around 50% to 90% stego bits on average (depending on a particular algorithm).***

Index Terms: ***Data Hiding, Eccentric Pixels, Spatial Domain, Steganalysis, Steganography, Sterilization***

1. INTRODUCTION AND MOTIVATION

WITH the emergence of Internet as a widely preferred mode of communication, there has been an increasing need for security in communication between a sender and a receiver. Secret messages which are being transferred between them can easily be intercepted and copied or duplicated by an unauthorized person. Hence secure transmission of data via Internet is of utmost importance. The process of encrypting and sending information in such a way that no person, other than the intended recipients, can decipher the information sent by the sender is known as *cryptography*. The main aim of cryptography is to achieve confidentiality. It also provides other added advantages like authentication, data integrity and non-repudiation [13]. On the other hand, the art of hiding secret message in various media such as textual media, image files, audio files and video files without any suspicion is known as *steganography* [1], while the art and science of uncovering the existence of steganography in a particular media is known as Steganalysis [5].

The most common steganographic method is the LSB (Least Significant Bit) based technique, which modifies the LSB of the pixels of the cover image to embed the secret message. LSB modification is the easiest method available and is computationally least intensive [3]. Multi-bit Steganography can also be employed which helps us in achieving greater efficiency in embedding secret data in the LSBs (more than one position) of the pixels of the cover image. Care is taken to ensure that the final stego image formed is visually very similar to the cover image used [6], [7], [9], [14]. Bit Plane Complexity Segmentation (BPCS) [11] is also a steganographic technique which can be implemented to hide messages in an image. High embedding rates can be achieved using this technique with low distortion. Low distortion is due to the fact that noisy area in a cover image are replaced by noisy like secret data which results in minimal loss in image quality of the stego image. In method [9], an occurrence of an edge is used to embed greater number of bits in the pixels, while in smoother areas; less number of bits are embedded. In method [7], four-pixel differencing and modified LSB substitution method is used. Using this, four pixel's average difference is calculated. This difference helps us to determine the value of k in the k-bit LSB substitution method for embedding hidden data into the image. The authors [14] describe a single digit sum function based steganographic technique which can withstand statistical attacks.

After the well-known tragic incidents of 11th September, 2001, both steganography and steganalysis have become very important discipline to the researchers. According to the report of ``*Federal Plan for Cyber Security and Information Assurance Research and Development*" [2], the statement ``…immediate concerns also include the use of cyber-space for covert communications, particularly by terrorists but also by foreign intelligence services…" and ``International interest in R&D for steganographic technologies and their commercialization and application has exploded in recent years…" prove that the plan considers steganography as a potential risk. The report also mentioned the importance of identification of secret message.

To defeat steganography, *steganalysis* may play an important role. Most of the state-of-the-art steganalysis techniques [5], [15] detect whether information is embedded in the media or not. The more secret data embedded in an image the easier it is for steganalytic methods to detect them [18]. Extracting the actual hidden message is very difficult and is rarely the target of practical steganalysis. Moreover, most of the steganalytic attacks

Manuscript received June 11, 2014.
Imon Mukherjee is with St. Thomas' College of Engineering and Technology, Kolkata, India (email: mukherjee.imon@gmail.com)
Goutam Paul is with Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India (email: goutam.paul@isi.ac.in)
Jarvis Altrin Jawahar is with Life Science Business Unit, Cognizant Technology Solutions, Chennai, India (email: jarvisaltrin@gmail.com).

are algorithms-specific. In this scenario, disturbing the message without altering the image features could be a viable option to defeat malicious use of steganography.

The concept of image sterilization for preventing steganographic communication was introduced for the first time in [10]. The goal of such technique is not to recover the secret information, rather to annihilate stego information transmission without the occurrence of any perceptible distortion in the image. While the method of [10] can sterilize only the LSB of each pixel intensity of the stego image, a later work [8] extended the method for sterilizing up to two bits.

One obvious method of performing LSB sterilization may be to replace the LSBs of all the pixel intensities by zero (or one). But this immediately gives a clue to the recipient that the image might have been modified in transit. On the other hand, randomly sterilizing each LSB to 0 or 1 would achieve an average efficiency of 50% only. Thus, designing a sterilization algorithm that does not leave any signature and preserves the pseudo-randomness of the sequence of the LSBs in an image is a challenging task.

In our current work, we propose a new algorithm for sterilizing at most 4 bits. Our method uses pixel eccentricities that depend on determining the two-dimensional moment invariants for planar geometric figures [4]. It is to be noted that mostly the eccentric pixels having higher values (i.e., the pixels in the edge area of the image) contain higher number of stego bits, hence in our method we determine the number of bits for sterilization based on the eccentricity of each image pixel. Section 2 shows how the eccentricity value is calculated in terms of central moment and Section 3 describes our proposed algorithm. We present detailed performance analysis in Section 4.

2. *FUNCTION TO DEFINE THE* eccentricity *OF PIXELS*

All circular objects have a centre. For an irregular polygon, which is a complex object, the center is indicated by the centroid or the centre of gravity of that object as shown in Figure 1.

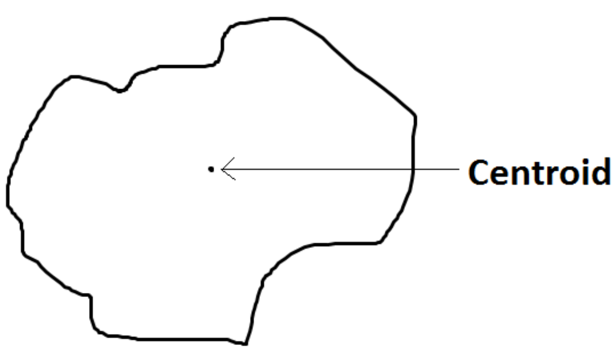


Fig. 1. Centroid of an object.

The centre of gravity or centroid of a two-dimensional object can be determined as follows.

$$X_c = \frac{1}{\sum_{x=1}^{M}\sum_{y=1}^{N} f(x,y)} \cdot \sum_{x=1}^{M}\sum_{y=1}^{N} x \cdot f(x,y), \quad (1)$$

$$Y_c = \frac{1}{\sum_{x=1}^{M}\sum_{y=1}^{N} f(x,y)} \cdot \sum_{x=1}^{M}\sum_{y=1}^{N} y \cdot f(x,y), \quad (2)$$

where $f(x, y)$ denotes the density distribution function at location (x, y) of an object.

Hu et al. [4] have estimated the two-dimensional $\{(p+q) : p, q \in \mathbb{R}\}^{th}$ order moments of a density distribution function $f(x, y)$ in terms of Riemann integrals as:

$$m_{p,q} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^p \cdot y^q \cdot f(x,y)dx\ dy \quad (3)$$

It is assumed that moment of all order exist when $f(x, y)$ is a piecewise continuous or bounded function with non-zero values in the finite part of the XY-plane. The Uniqueness Theorem shows that $m_{p,q}$ is uniquely determined by $f(x, y)$ and conversely, $f(x, y)$ is uniquely determined by $m_{p,q}$.

Modifying Equation (3) for discrete grayscale image of size $M \times N$ with $\gamma(x, y)$ representing the image pixel intensities, we can determine image moments of order $(p + q)$ after padding `0' at the surroundings of the image intensity matrix as follows:

$$m_{p,q} = \sum_{x=1}^{M}\sum_{y=1}^{N} x^p \cdot y^q \cdot \gamma(x,y) \quad (4)$$

The zero-order moment $m_{0,0}$, the first order moments $\{m_{p,q} : p+q = 1\}$ and the second order moments $\{m_{p,q} : p + q = 2\}$ are as follows (Equation (5) to (10)).

$$m_{0,0} = \sum_{x=1}^{M}\sum_{y=1}^{N} \gamma(x,y), \quad (5)$$

$$m_{1,0} = \sum_{x=1}^{M}\sum_{y=1}^{N} x \cdot \gamma(x,y), \quad (6)$$

$$m_{0,1} = \sum_{x=1}^{M}\sum_{y=1}^{N} y \cdot \gamma(x,y), \quad (7)$$

$$m_{1,1} = \sum_{x=1}^{M}\sum_{y=1}^{N} x \cdot y \cdot \gamma(x,y), \quad (8)$$

$$m_{2,0} = \sum_{x=1}^{M}\sum_{y=1}^{N} x^2 \cdot \gamma(x,y), \quad (9)$$

$$m_{0,2} = \sum_{x=1}^{M}\sum_{y=1}^{N} y^2 \cdot \gamma(x,y). \quad (10)$$

The centroid of an image can be calculated using the aforesaid image moments as follows.

$$X_c = \frac{m_{1,0}}{m_{0,0}}, \quad (11)$$

$$Y_c = \frac{m_{0,1}}{m_{0,0}}. \quad (12)$$

The central moments of the image are defined as

$$\mu_{p,q}^{(c)} = \sum_{x=1}^{M}\sum_{y=1}^{N}(x - X_c)^p \cdot (y - Y_c)^q \cdot \gamma(x, y). \quad (13)$$

The ratio between the maximum and the minimum distance between the centroid and the boundary of the image is called the eccentricity of the image. It can be shown that the eccentricity of the image can be expressed in terms of the central moments as follows [12].

$$\varepsilon_{image}^{(c)} = \frac{\left(\mu_{2,0}^{(c)} - \mu_{0,2}^{(c)}\right)^2 + 4 \cdot {\mu_{1,1}^{(c)}}^2}{\mu_{0,0}^{(c)}}. \quad (14)$$

All the above definitions apply to the entire image. We divide the image into 3×3 overlapping blocks in row major order and define the central moment of the central pixel of each block as

$$\Omega_{p,q}^{(c)} = \sum_{i=x-1}^{x+1}\sum_{j=y-1}^{y+1}(i - X_c)^p \cdot (j - Y_c)^q \cdot \gamma(i, j). \quad (15)$$

where (i, j) represents the co-ordinates of the pixels of each block.

Analogous to Equation (14), we define the *eccentricity of the central pixel* as

$$\varepsilon_{pixel}^{(c)} = \frac{\left(\Omega_{2,0}^{(c)} - \Omega_{0,2}^{(c)}\right)^2 + 4 \cdot {\Omega_{1,1}^{(c)}}^2}{\Omega_{0,0}^{(c)}}. \quad (16)$$

3. *PROPOSED METHOD*

The set of pixels having higher eccentric values ($\varepsilon_{pixel}^{(c)}$) can be considered as potential candidate for message bearer. Such pixels lie in the busy area of the image where there is a great change in color/intensity.

Using Equation (16), we find the *eccentricity* ($\varepsilon^{(c)}$) values of each individual pixel of the stego images obtained by applying methods [7], [9], [14]. Then the intensity values of each pixel component is sorted in descending order according to their eccentricities. The maximum and minimum eccentricity value (say, $\varepsilon_{max}^{(c)}$ and $\varepsilon_{min}^{(c)}$ respectively) are determined.

The probability of embedding bits into higher bitplanes increases in busy part of the image where the eccentricity of the image pixel is very high. In other words, we can say that the pixels having lower eccentricity contain stego information at its lower bitplanes. Hence based on the above assumption our algorithm sterilizes varying number of bits for the pixels of the stego image as shown in Step 6 of Algorithm 1. Note that we divide here the range of $\varepsilon_{max}^{(c)} - \varepsilon_{min}^{(c)}$ into four non-overlapping parts for sterilizing different number of bits (say, $\mathfrak{N}^{steri}$) for determining this number.

$\Pi_{x-1,y-1}$	$\Pi_{x-1,y}$	$\Pi_{x-1,y+1}$
$\Pi_{x,y-1}$	$\Pi_{x,y}$	$\Pi_{x,y+1}$
$\Pi_{x+1,y-1}$	$\Pi_{x+1,y}$	$\Pi_{x+1,y+1}$

Fig. 2. 3×3 window.

Let $\gamma(x, y)$ be the intensity value of the pixel $\Pi_{x,y}$. Based on the value of $\mathfrak{N}^{steri}$, we calculate the likelihood of getting a 0 or 1, considering the $\mathfrak{N}^{steri}$ LSBs of all the pixels of that block.

A 3×3 window, as shown in Figure 2, is taken with the pixel in consideration being the central pixel. The $\mathfrak{N}^{steri}$ LSBs are found for all the pixels falling in this window. The central pixels' LSBs are substituted with a 0 or 1 based on the maximum occurrence of 0's or 1's in their respective bitplanes. In other words, we find the majority bit among $\mathfrak{N}^{steri}$ bitplanes of the neighboring pixels and the center pixel. Then replace the bit of the corresponding bitplane of the central pixel in that window with majority bit. We present the step-by-step procedure in Algorithm 1.

Example: Calculate the eccentricity of first pixel (i.e., intensity 50) of the following sample image (as shown in Figure 3).

50	56	201	5
42	195	200	10
200	75	150	143
200	80	147	173

Fig. 3. Sample pixel intensity matrix.

Solution: We pad the sample image with 0's along the boundary as shown in Figure 4. Considering the whole image we calculate the zero, first and second order moments as follows.

$$m_{0,0} = \sum_{x=1}^{M}\sum_{y=1}^{N}\gamma(x, y) = 1927,$$

$$m_{1,0} = \sum_{x=1}^{M}\sum_{y=1}^{N}x \cdot \gamma(x, y) = 7237,$$

$$m_{0,1} = \sum_{x=1}^{M}\sum_{y=1}^{N}y \cdot \gamma(x, y) = 6649,$$

$$m_{1,1} = \sum_{x=1}^{M}\sum_{y=1}^{N}x \cdot y \cdot \gamma(x, y) = 24976,$$

$$m_{2,0} = \sum_{x=1}^{M}\sum_{y=1}^{N}x^2 \cdot \gamma(x, y) = 9359,$$

$$m_{0,2} = \sum_{x=1}^{M}\sum_{y=1}^{N}y^2 \cdot \gamma(x, y) = 25065.$$

Input: A stego image.
Output: The sterilized version of the input stego image.

Read the intensity values from the the stego image;
for *each image component* **do**
    Determine the $\varepsilon^{(c)}_{pixel}$ of each pixel using Equation (16);
    Sort the image pixels in decreasing order according to their eccentricity values (break tie in the row-major order);
    Find the maximum and minimum eccentricity (say, $\varepsilon^{(c)}_{max}$ and $\varepsilon^{(c)}_{min}$ respectively) amongst all the pixels;
    Determine the number of bits $\mathfrak{N}^{steri}$ to be sterilized as follows:

$$\mathfrak{N}^{steri} = \begin{cases} 4 & \text{if } \varepsilon^{(c)}_{max} \geq \varepsilon^{(c)}_{pixel} > \frac{3}{4} \cdot (\varepsilon^{(c)}_{max} - \varepsilon^{(c)}_{min}), \\ 3 & \text{if } \frac{3}{4}(\varepsilon^{(c)}_{max} - \varepsilon^{(c)}_{min}) \geq \varepsilon^{(c)}_{pixel} > \frac{1}{2} \cdot (\varepsilon^{(c)}_{max} - \varepsilon(c)_{min}), \\ 2 & \text{if } \frac{1}{2}(\varepsilon^{(c)}_{max} - \varepsilon^{(c)}_{min}) \geq \varepsilon^{(c)}_{pixel} > \frac{1}{4} \cdot (\varepsilon^{(c)}_{max} - \varepsilon^{(c)}_{min}), \\ 1 & \text{if } \frac{1}{4}(\varepsilon^{(c)}_{max} - \varepsilon^{(c)}_{min}) \geq \varepsilon^{(c)}_{pixel} \geq \varepsilon^{(c)}_{min}. \end{cases}$$

    Divide the image into 3×3 blocks (overlapping);
    for *each block* **do**
        for $i = 1$ *to* $\mathfrak{N}^{steri}$ **do**
            Find the majority bit among the $\mathfrak{N}^{steri}$ bitplanes of neighbouring pixels (including center pixel);
            if *majority bit* $= 1$ **then**
                Replace the i-th bitplane of the central pixel with 1;
            end
            else
                Replace the i-th bitplane of the central pixel with 0;
            end
        end
    end
end
Output the transformed image;

Algorithm 1: Sterilization of Stego images.

50	56	201	5
42	195	200	10
200	75	150	143
200	80	147	173

$\xrightarrow{\text{Padding the boundary with zeros}}$

0	0	0	0	0	0
0	50	56	201	5	0
0	42	195	200	10	0
0	200	75	150	143	0
0	200	80	147	173	0
0	0	0	0	0	0

Fig. 4. Sample image intensity matrix before (at left) and after (at right) padding.

The centroid of the image can be calculated as

$$X_c = \frac{m_{1,0}}{m_{0,0}} = 3.7556$$
$$Y_c = \frac{m_{0,1}}{m_{0,0}} = 3.4504.$$

Now considering a 3×3 block (as shown in Figure 5), we calculate the central moments and eccentricity value:

$$\Omega^{(c)}_{1,1} = \sum_{i=1}^{3}\sum_{j=1}^{3}(i - X_c)^1 \cdot (j - Y_c)^1 \cdot f(i,j) = 283.9979$$

0	**0**	**0**	0	0	0
0	**50**	**56**	201	5	0
0	**42**	**195**	200	10	0
0	200	75	150	143	0
0	200	80	147	173	0
0	0	0	0	0	0

Fig. 5. Selection of 3×3 block from the intensity matrix.

$$\Omega^{(c)}_{0,2} = \sum_{i=1}^{3}\sum_{j=1}^{3}(i - X_c)^0 \cdot (j - Y_c)^2 \cdot f(i,j) = 244.4749$$

$$\Omega_{2,0}^{(c)} = \sum_{i=1}^{3}\sum_{j=1}^{3}(i - X_c)^2 \cdot (j - Y_c)^0 \cdot f(i,j) = 462.0010$$

From Equation (16), we calculate the eccentricity value from the central moments as

$$\varepsilon_{pixel}^{(c)} = \frac{\left(\Omega_{2,0}^{(c)} - \Omega_{0,2}^{(c)}\right)^2 + 4 \cdot \Omega_{1,1}^{(c)\,2}}{\Omega_{0,0}^{(c)}} = 191.9755.$$

4. PERFORMANCE ANALYSIS

The performance of our algorithm can be analyzed by observing the perceptible visual quality of the images as well as checking for their structural changes. We have tested our technique on images obtained by applying methods [7], [9], [14] on 100 of each type of bitmap images, viz., cartoon, nature and busy nature.

4.1. Accuracy Measurement

To determine the accuracy of our technique, we need to take some sample stego images as inputs for which we know which pixel bits are actually changed due to the embedding. Let

S := the number of stego bits,
S' := the number of stego bits (out of S) having different intensity value from their cover counterpart,
S'' := the number of recovered stego bits (out of the S') due to the sterilization process.

Then the accuracy of sterilization for this image is defined as :

$$ACC_{steri}(I) = \frac{S''}{S'} \tag{17}$$

Table 1 and 2 show the accuracy of 24 bit color image and grayscale image of three different types viz. cartoon, nature and busy nature respectively.

4.2. Structural Analysis

The structure of the image file format may get changed when we apply steganographic or sterilization techniques on the image. Care should be taken for different file formats, especially in such cases where we are reconstructing the image after manipulating the pixel intensities, that there are no perceptible visual changes in the reconstructed image. For example, for an image of the GIF file format undergoing a similar algorithm, changes may occur at all the bit layers to some extent since 256 values are used to represent 2^{24} colors [17]. In our algorithm, we have worked with bitmap images and have noticed that the structure of bitmap images do not change before or after the steganographic and sterilization process. We come to the conclusion that our proposed method can withstand structural analysis without any ensuing discernible errors.

4.3. Visual Quality Analysis

The visual quality of the analyzed images can be examined by looking at them (before and after processing) with naked eyes and also checking their histograms and bitplanes obtained before and after applying sterilization algorithm.

1) **Visual Perceptibility and their Histogram Analysis**
As said before, we have tested our algorithm considering stego images obtained using methods [7], [9], [14] and we have not found any perceptible difference between the stego and sterilized images. Figure 6 shows both stego and sterilized version of three types (viz. cartoon, nature, busy nature) of sample images. The histograms are shown in Figure 7.
2) **Bitplane Analysis**
The bitplanes of the stego and sterilized images are analysed in this section. Table 3 shows the bitplanes of both the stego (obtained using method [7], [9], [14]) and sterilized version of the stego image. Wayner [16], and Westfeld [17] have suggested that every bitplane (including the least significant bitplane) is non-random. Suppose the i-th bitplane of an image is denoted by B_i' and the expected value of the corresponding bitplane for a suspect image is denoted by $E(B_i)$. It should then be a relatively simple task to spot arbitrary modifications on any bitplane when analysing the suspicious bitplane B_i' against $E(B_i)$. There are two possibilities:
$$E(B_i) = B_i', \tag{18}$$
$$E(B_i) \neq B_i'. \tag{19}$$
If Equation (18) is satisfied, then there is no difference between the bitplanes of the two examined versions of the image, i.e., the image has not been altered; but if Equation (19) works well, then the two bitplanes are inconsistent, and the examined image is suspicious. Using our method we do not find any differences in bitplanes of stego and sterilized version of analyzed image.
3) **Analysis through MSE and PSNR**
Let $\{A(x,y)\colon x = 1,2,3,\ldots,M$ and $y = 1,2,3,\ldots,N\}$ denote the intensity values of the sterilized image of dimension $M \times N$ and $\{B(x,y)\colon x = 1,2,3,\ldots,M$ and $y = 1,2,3,\ldots,N\}$ denote that of the cover image of same dimension (considered as referenced image) in the spatial domain. The imperceptibility of the image is measured in terms of Mean Squared Error (MSE) and Peak-Signal-to-Noise-Ratio (PSNR) as below.
$$MSE = \frac{1}{MN}\sum_{M,N}\left((A(x,y) - B(x,y)\right)^2, \tag{20}$$
$$PSNR = 10\log_{10}\left(\frac{T^2}{MSE}\right), \tag{21}$$

TABLE 1. Accuracy (minimum, average and maximum) of sterilization over three hundred 24-bit color images for three different algorithms A [7], B [9], C [14].

			No. of Bits	Sterilization Performance (%)								
				Minimum			Average			Maximum		
				A	B	C	A	B	C	A	B	C
Image Type	Cartoon	R	LSB	49.59	50.46	50.06	49.84	54.30	51.24	59.64	55.64	53.37
			2-LSB	50.30	76.35	79.67	51.05	79.23	80.48	53.87	86.06	81.02
			3-LSB	50.42	82.13	64.96	51.86	85.23	69.74	55.13	90.33	75.32
			4-LSB	63.78	88.25	83.35	67.06	89.38	85.01	73.02	93.15	87.50
			Average	53.64	73.75	70.60	55.46	76.76	71.59	60.29	78.19	73.30
		G	LSB	47.05	50.78	49.20	49.59	53.80	49.83	50.26	55.65	50.28
			2-LSB	48.94	74.54	72.98	50.72	80.01	76.82	54.05	85.45	79.85
			3-LSB	50.35	82.02	65.13	51.13	86.86	68.82	53.33	92.94	72.59
			4-LSB	63.68	87.60	83.67	67.56	90.13	84.12	71.55	94.62	84.85
			Average	53.66	74.10	67.83	54.70	78.04	69.82	56.08	80.61	71.12
		B	LSB	47.18	48.46	49.77	50.19	54.62	53.17	53.67	57.57	54.93
			2-LSB	49.79	76.17	77.00	50.60	80.05	84.09	51.54	85.20	89.08
			3-LSB	50.56	81.80	74.30	52.09	86.10	79.75	56.09	92.96	87.19
			4-LSB	62.88	85.93	87.55	68.17	91.26	89.97	75.77	95.06	93.91
			Average	53.58	74.20	71.01	55.10	77.10	75.17	58.24	82.71	79.96
	Nature	R	LSB	49.71	50.76	49.74	50.07	53.16	50.00	50.73	55.08	50.11
			2-LSB	50.06	71.63	73.55	50.59	74.57	78.47	51.77	77.98	80.76
			3-LSB	50.08	75.06	67.55	50.75	79.09	68.30	52.24	83.39	69.14
			4-LSB	53.22	80.81	83.46	57.71	84.55	84.00	63.64	89.85	84.43
			Average	51.03	70.52	69.15	52.24	74.21	70.09	53.54	76.11	70.67
		G	LSB	49.85	49.82	49.91	50.1	53.21	50.09	51.19	56.52	50.32
			2-LSB	49.92	70.53	76.08	50.59	74.51	78.72	51.48	78.65	79.91
			3-LSB	50.17	75.05	67.39	50.82	79.07	68.02	52.50	82.76	68.98
			4-LSB	52.69	80.09	83.37	59.10	84.80	84.12	64.29	88.95	84.70
			Average	50.93	70.61	69.92	52.56	74.31	70.18	53.63	78.01	70.67
		B	LSB	49.73	49.59	50.07	49.96	53.18	50.34	51.29	56.97	50.85
			2-LSB	50.22	71.43	78.61	50.48	74.33	79.63	51.50	78.96	80.78
			3-LSB	50.20	74.09	68.00	50.98	80.34	69.02	52.33	85.44	70.34
			4-LSB	53.83	79.26	82.96	62.19	85.47	83.83	67.75	92.47	85.14
			Average	51.38	69.01	69.73	53.22	74.01	70.33	54.64	78.06	71.00
	Busy Nature	R	LSB	49.80	49.72	50.20	49.96	53.82	50.34	50.17	55.09	50.58
			2-LSB	49.76	72.92	75.19	50.48	80.83	79.97	54.02	89.64	84.17
			3-LSB	50.04	75.16	58.77	50.98	85.71	67.53	55.55	94.61	75.48
			4-LSB	54.85	78.50	82.16	62.19	89.05	85.37	71.53	96.24	89.98
			Average	51.47	68.91	65.84	53.22	74.77	69.64	55.55	82.77	72.55
		G	LSB	49.90	50.47	50.07	50.11	54.17	50.21	50.63	56.65	50.45
			2-LSB	50.00	73.23	75.26	50.64	80.08	81.07	54.11	87.99	88.50
			3-LSB	50.02	79.02	58.80	50.76	86.04	68.71	55.30	94.77	80.06
			4-LSB	57.13	82.52	82.35	62.96	89.66	84.71	72.67	97.96	87.97
			Average	52.00	71.85	65.88	53.42	75.94	70.10	56.12	84.54	74.34
		B	LSB	48.64	49.65	50.73	50.09	53.95	50.18	51.73	56.03	50.30
			2-LSB	49.99	74.00	75.24	50.89	79.38	83.28	54.12	87.15	94.05
			3-LSB	50.05	78.36	58.80	51.44	86.12	71.56	56.26	93.13	87.60
			4-LSB	58.24	82.63	82.19	63.93	87.09	83.81	72.34	96.88	85.18
			Average	52.26	71.72	65.83	53.88	77.09	71.04	57.50	82.16	76.80

TABLE 2. Accuracy (minimum, average and maximum) of sterilization over hundred grayscale images for three different algorithms A [7], B [9], C [14].

		No. of Bits	Sterilization Performance (%)								
			Minimum			Average			Maximum		
			A	B	C	A	B	C	A	B	C
Image Type	Cartoon	LSB	49.42	48.91	57.51	50.13	49.87	60.17	51.31	50.43	62.38
		2-LSB	47.35	72.98	77.17	50.35	76.81	78.18	53.80	81.89	79.67
		3-LSB	49.89	76.66	68.27	50.83	82.11	69.85	55.27	86.92	74.28
		4-LSB	57.13	80.95	83.30	68.05	86.01	84.81	75.55	90.61	87.67
		Average	51.87	70.09	72.15	54.77	73.64	73.92	57.49	77.17	76.43
	Nature	LSB	49.91	49.78	57.65	50.78	50.76	57.85	57.74	57.90	58.01
		2-LSB	49.98	71.01	76.85	50.68	76.91	78.63	53.37	91.00	79.55
		3-LSB	50.07	72.63	67.60	50.78	80.32	69.63	53.61	96.25	70.81
		4-LSB	52.77	74.94	83.92	58.53	82.95	84.18	72.74	97.43	84.40
		Average	50.83	67.07	71.73	52.72	72.48	72.03	55.71	83.63	72.27
	Busy Nature	LSB	49.82	49.80	57.84	49.98	50.08	58.39	50.11	50.57	59.23
		2-LSB	49.67	73.89	75.42	50.33	81.61	78.48	52.57	96.53	81.85
		3-LSB	49.97	76.47	68.49	51.13	86.22	70.05	54.16	97.27	71.86
		4-LSB	53.75	78.78	84.22	65.81	89.24	84.98	78.66	97.25	85.87
		Average	50.94	69.94	71.49	54.00	76.55	72.45	56.16	84.21	73.20

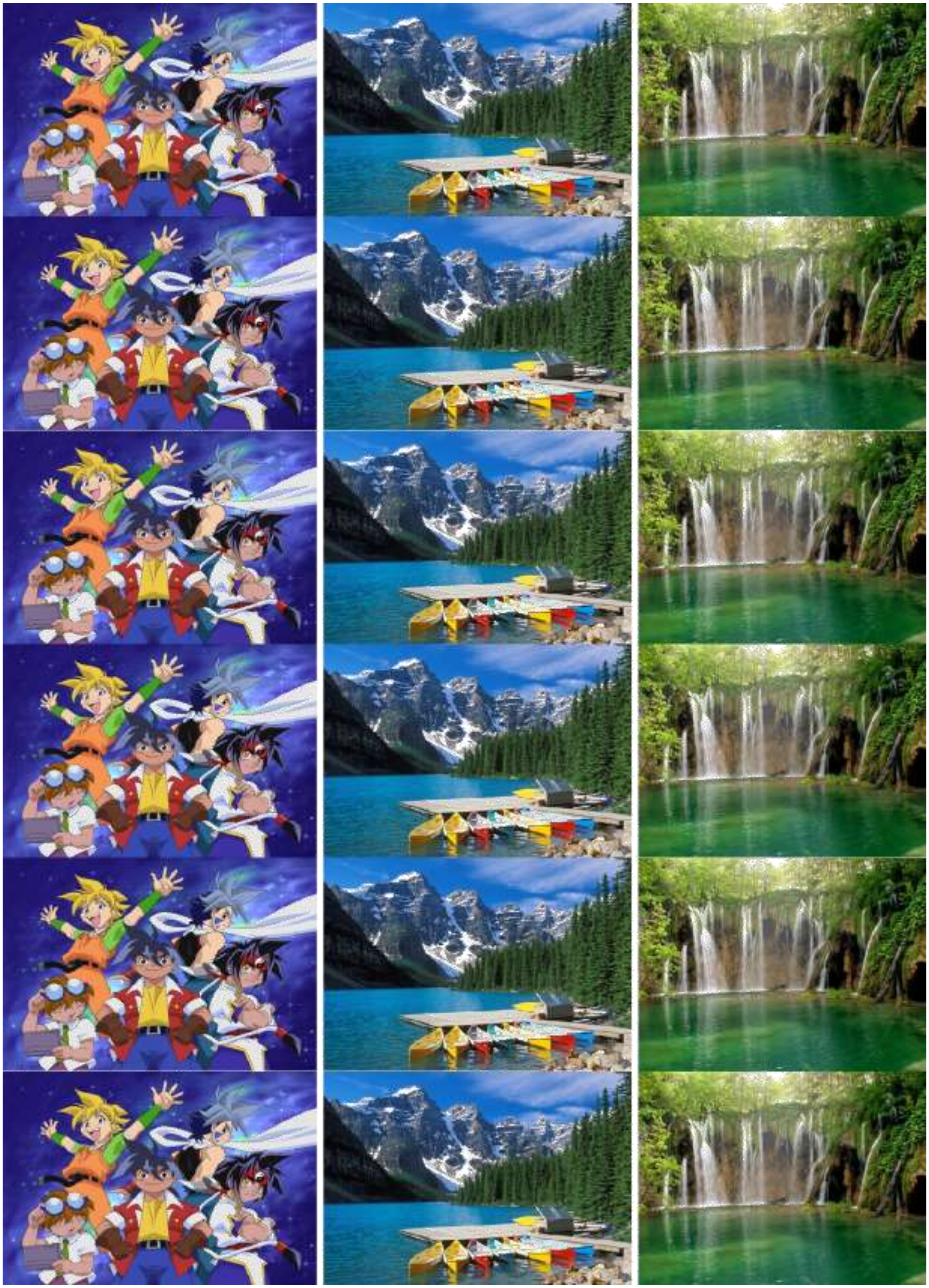


Fig. 6. Sample stego images (cartoon, nature and busy nature respectively) using methods [7], [9] and [14] (Rows 1, 3 and 5 respectively) and their sterilized versions (Rows 4, 5 and 6 respectively).

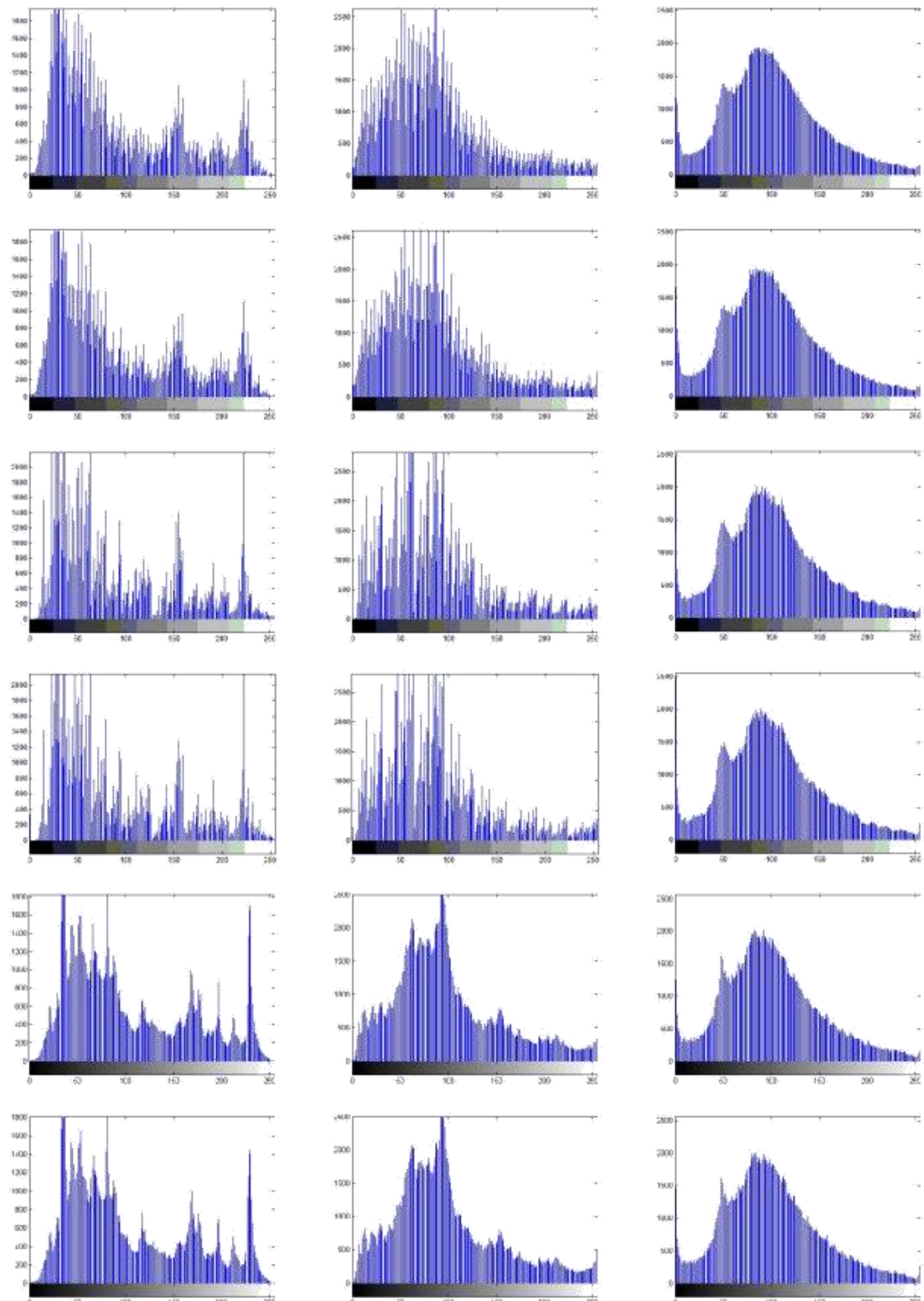
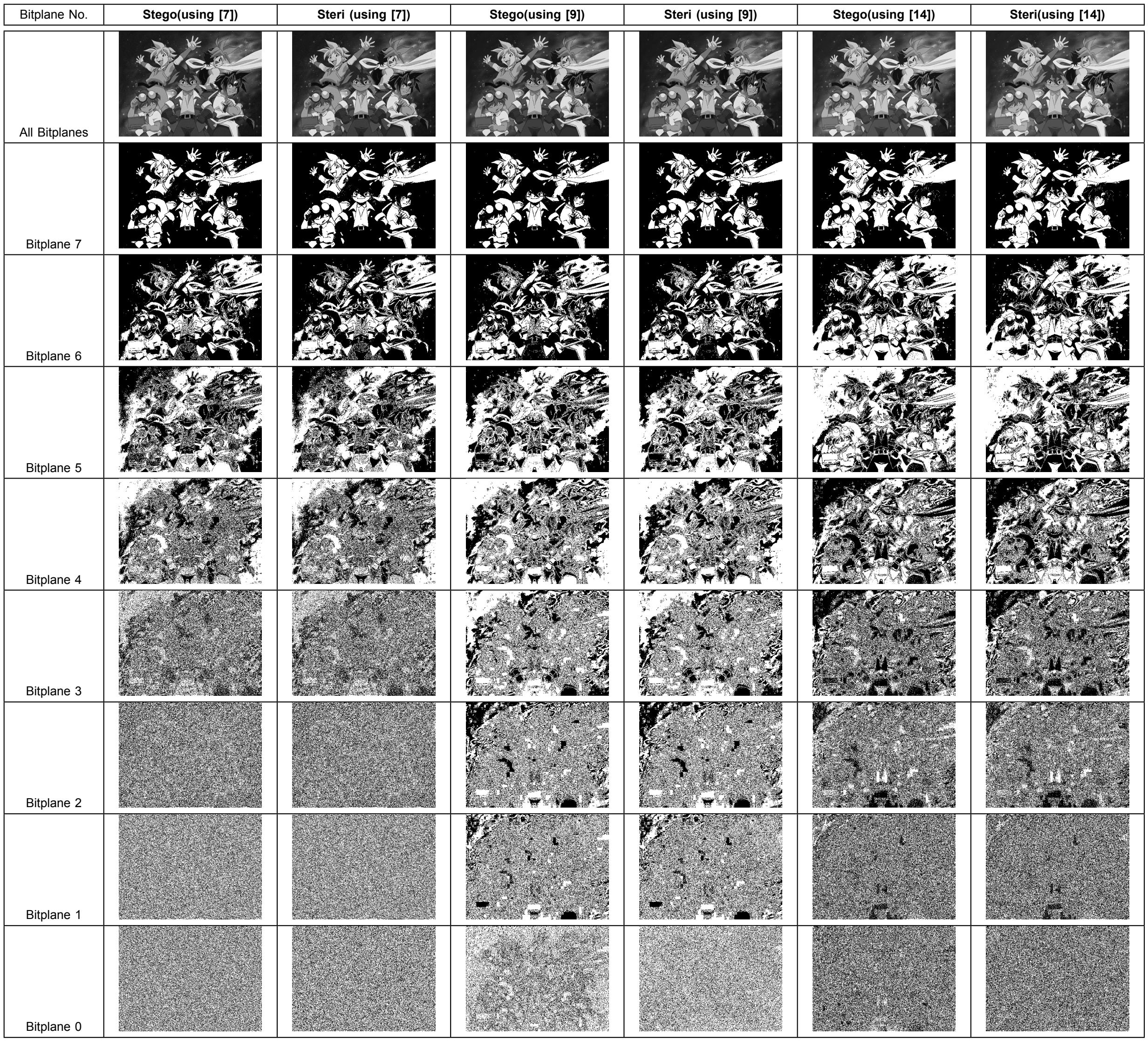


Fig. 7. Histograms of sample stego images of Fig. 6.

TABLE 3. Bitplane analysis of stego and sterilized version of beyblade.bmp obtained using [7], [9], [14].



where T denotes the maximum possible intensity value in an image.

The MSE represents the cumulative squared error between the two analyzed images. The estimation of MSE is very popular as it can correlate reasonably with subjective visual analysis and also is mathematically tractable. Small distortion between the cover and sterilized image provides a low MSE value and high PSNR value. We experimentally find satisfactory MSE and PSNR value as shown in Table 4. Figure 8 shows the comparative analysis of PSNR calculated from the analyzed images obtained from the methods [7], [9], [14].

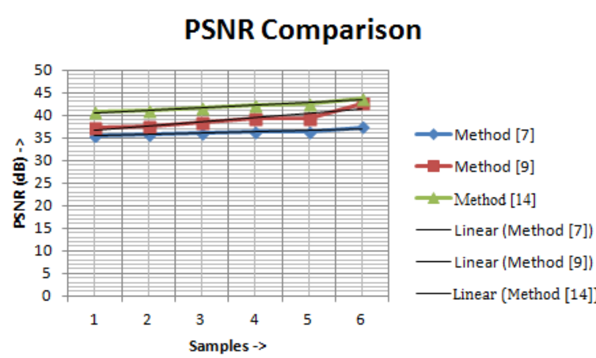


Fig. 8. PSNR comparison for methods [7], [9] and [14] with respect to some sample images.

TABLE 4. MSE values and PSNR values of tested images obtained from methods [7], [9] and [14].

	MSE		PSNR (dB)	
	Grey Image	Color Image	Grey Image	Color Image
Method [7]	11.7883	11.8390	37.42	37.40
Method [9]	3.6342	3.5067	42.53	42.68
Method [14]	3.9872	3.5856	42.12	42.58

5. CONCLUSIONS AND FUTURE WORK

Robust steganographic methods are being used with malicious intent to cause harm frequently on a regular basis. Our proposed method is a blind sterilization technique that gives good results against several leading steganographic methods. We have demonstrated, with substantial data, that our method can render embedded information unreadable in almost all cases.

With the need of security in data transfer increasing every day, advanced methods of Steganography are being looked into as the future protocols for communication. As a result, such techniques are also being used by people with harmful intentions. Hence, our first and foremost future objective is to keep looking into the upgrading of the proposed method to keep it at par with the leading steganography techniques.

We would like to increase the ability of our method to sterilize more than four bits of the stego image. We intend to extend our method to the frequency domain as well.

REFERENCES

[1] Chanu, Y.J., Singh, M., Tuithung, T., ``Image Steganography and Steganalysis - A Survey", In International Journal of Computer Applications, 52(2), 2012, pp. 1-11.

[2] Federal Plan. 2006. Federal Plan for Cyber Security and Information Assurance Research and Development, Interagency Working Group on Cyber Security and Information Assurance.

[3] Gupta, H., Kumar, R., Changlani, S., ``Steganography using LSB Bit Substitution for Data Mining", In International Journal of Advanced Research in Computer Science and Electronics Engineering, 2(10), 2013, pp. 676-680.

[4] Hu, M.K., ``Visual Pattern Recognition by Moment Invariants", In IRE Transactions on Information Theory, 8(2), 1962, pp. 179-187.

[5] Johnson, N.F., Jajodia, S., ``Steganalysis of Images Created using Current Steganographic Software", Information Hiding, 1525, 1998, pp. 273-289.

[6] Kumar, R., Khushil, K., Chand, S., ``A New Steganography Technique using Snake Scan Ordering Strategy", International Journal of Image, Graphics and Signal Processing, 5(6), 2013, pp. 25-32.

[7] Liao, X., Wen, Q.Y., Zhang, J., "A Steganographic Method for Digital Images with Four-Pixel Differencing and Modified LSB Substitution", Journal of Visual Communication and Image Representation, 22, 2011, pp. 1-8.

[8] Mukherjee, I., Paul, G., ``Double Bit Sterilization of Stego-images", In Proceedings of the 10th International Conference on Security and Management (SAM), July 18-21, 2011, Las Vegas, U.S.A., pp 743-746.

[9] Park, Y.R., Kang, H.H., Shin, S.U., Kwon, K.R., ``An Image Steganography using Pixel Characteristics", Computational Intelligence and Security, 3802, 2005, pp. 581-588.

[10] Paul, G., Mukherjee, I., ``Image Sterilization to Prevent LSB-based Steganographic Transmission", CoRR abs/1012.5573 (2010). Later appeared in Proceedings of the 11-th International Conference on Security and Management (SAM), July 16-19, 2012, Las Vegas, U.S.A., pp. 448-454 under the title ``Sterilization of Stego-images through Histogram Normalization".

[11] Spaulding, J., Noda, H., Shirazi, M.N., Kawaguchi, E., ``BPCS Steganography using EZW Lossy Compressed Images", Pattern Recognition Letters, 23(13), 2002, pp. 1579-1587.

[12] Sridhar, S., ``Digital Image Processing", Oxford University Press, India, ISBN: 978-0-19-807078-8.

[13] Stinson, D.R., Cryptography: Theory and Practice, Third Edition, CRC Press, 2005.

[14] Sur, A., Goel, P., and Mukhopadhyay, J., ``A Novel Spatial Domain Scheme for Multiple Bitplane Steganography", Proceedings, NCVPRIPG 2008, Jan 11 – 13, Gandhinagar, Gujarat, India.

[15] Wang, H., Wang, S., ``Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, 47(10), 2004, pp. 76-82.

[16] Wayner, P., 2002, ``Disappearing Cryptography - Information Hiding", In Steganography & Watermarking (Second Edition)", A volume in The Morgan Kaufmann Series in Software Engineering and Programming. Morgan Kaufmann, Elsevier. http://www.sciencedirect.com/science/book/9781558607699

[17] Westfeld, A., Pfitzmann, A., ``Attacks on Steganographic Systems, Information Hiding", Lecture Notes in Computer Science, Vol. 1768. Springer, 1999, pp. 61-76.

[18] Zhang, X., Wang, S., ``Dynamical running coding in digital steganography", IEEE Signal Processing Letters, 13(3), 2006, pp. 165-168.

Imon Mukherjee is presently working as an Assistant Professor in the Dept. of Computer Science & Engineering, St. Thomas' College of Engineering and Technology, Kolkata, India.

Goutam Paul is presently working as an Assistant Professor in the Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India.

Jarvis Altrin Jawahar is presently working as Programmer Analyst Trainee in Life Science Business Unit, Cognizant Technology Solutions, Chennai, India.