Defence Science Journal, Vol. 71, No. 2, March 2021, pp. 209-221, DOI : 10.14429/dsj.71.15643

Security Analysis of Bit-plane Level Image Encryption Schemes

Ram Ratan[*] and Arvind Yadav[#]

[*]*DRDO-Scientific Analysis Group, Delhi - 110 054, India*
[#]*Hansraj College, University of Delhi, Delhi - 110 007, India*
[*]*E-mail: ramratan_sag@hotmail.com*

ABSTRACT

A selective bit-plane encryption scheme was proposed for securing the transmission of image data in mobile environments with a claim that it provides a high security viz. the encryption of the four most significant bit-planes is sufficient for a high image data security. This paper presents the security analysis of the said encryption scheme and reports new important results. We perform the security analysis of the bit-level encryption by considering the normal images and their histogram equalised enhanced images. We consider different bit-plane aspects to analyse the security of the image encryption, and show that the encryption of the four most significant bit-planes is not adequate. The contents of the images can be obtained even when all the bit-planes except one least significant bit-plane are encrypted in the histogram equalised images as shown in the results. The bit-plane level security analysis seems very useful for the analysis of the bit-plane level image encryption schemes.

Keywords: Image encryption; Bit-plane level encryption; Cryptanalysis; Bit-plane measures; Security analysis

1. INTRODUCTION

The use of visual data in the form of image, video, and audio is rapidly growing in every aspect of life such as distant learning, finance, medical, sport, defence applications and even in entertainment industries. Nowadays, we can say that the use of visual data has become a necessity of modern society. There are some unavoidable and unfavourable conditions where we capture very poor quality images/videos due to the instant and rarely occurred events as well as the poor weather and recording conditions. Such unavoidable conditions can be compensated by the image processing methods which improve the quality of poor images so that the processed images can be visualised, interpreted and understood appropriately. There are various image enhancement techniques and the histogram equalisation (HE) is one of the important technique which is commonly used for the contrast enhancement of poor quality images[1-6]. In this paper, we consider the HE technique which equalises the gray level distribution based on the cumulative probability density function, to discuss the bit-plane characteristics and bit-plane encryption of images. The quality of the images can be observed qualitatively and quantitatively[7-11]. We consider both the qualitative and quantitative measures to study the security of the image encryption scheme.

In the image security applications, the safeguarding of visual data is a major task while its communication over open and insecure networks to avoid the misuse of vital by an adversary. To meet the task of image security requirements, a large number of image encryption schemes are reported based on pixel permutations, substitutions, or both[12-20]. The chaotic based image encryption schemes using random key sequences generated with the chaotic functions[21-25] are reported by the researchers. Some of the encryption schemes encrypt the images selectively as the region of interest (ROI) encryption[26-30]. The selective bit-plane encryption schemes[14, 30] are reported for real-time applications. An image encryption scheme is called secure if an adversary cannot apply the existing cryptanalytic attacks to decrypt the encrypted data even in distorted form, to get the key information even in partial form, and to reduce the complexity of the brute force attack. The cryptanalytic attacks are categorised as (i) known cipher image attack, (ii) known plain image attack, (iii) chosen plain image attack, and (iv) chosen cipher image attack.

In the cryptanalysis, an attacker exploits the characteristics of data such as the occurrence of gray levels, patterns, and the neighbourhood similarity characteristics of image pixels; key characteristics such as the related keys, weak keys, and equivalent keys; and the vulnerabilities if any in the encryption algorithm. The cryptanalysis of some of the image ciphers is reported[31-41] where it was shown that the reported security solutions were not secure as claimed and the attackers can obtain the meaningful image details, key information from the encrypted images. The cryptanalysis of the image encryption schemes was reported under the known and chosen plain data attacks[31-36] and the known cipher data attack[37-41]. A review on the design and cryptanalysis of recent chaotic image encryption schemes is carried out where some design aspects and weak parameters are discussed for the design of image ciphers[33]. Two attack replacement and reconstruction are reported to reconstruct the images[14, 42-43] for the bit-plane encryption.

Received : 29 March 2020, Revised : 02 November 2020
Accepted : 04 January 2021, Online published : 10 March 2021

In this paper, we present the bit-plane level security analysis of a selective bit-plane image encryption scheme in which we segment an encrypted image into different bit-planes as per the divide-and-conquer approach to arrive at meaningful findings. It was claimed that the selective bit-plane encryption provides the high security when the four most significant bit (MSB) planes of the images were encrypted and the two MSB planes encrypted for the considerable security[42-43]. We analyse the bit-plane image characteristics for normal images as well as the HE images and find that the bit-plane characteristics change drastically in the HE images from its normal images. This finding is very important and useful. The encryption of the four MSB planes is not enough, and the intelligible information can be obtained from the encrypted images even encrypting all the bit-planes except a least significant bit (LSB) plane of the HE images. We observe that the number of bit-planes to be encrypted for achieving the high security depends on the kind of an image as normal or HE image. The findings indicate that we require to encrypt at least the five MSB planes of normal images and six bit-planes (four MSB planes and two LSB planes) of the HE images. The bit-plane measures can be used to identify such images as normal images or the HE images and also to identify the unencrypted bit-planes that have some meaningful information. These can be applied in various other applications of image classification and pattern recognition[39-40].

2. HISTOGRAM EQUALISATION AND BIT-PLANE EENCRYPTION

An image is the projection on a two-dimensional (2-D) plane of the real-world objects. It is known as digital image when represented in numbers. Mathematically, a digital image is a function $f(x,y)$ or a matrix $[f(x,y]_{M\times N}, 1\le x\le M, 1\le y\le N$, where (x,y) represents the position and $f(x,y)$ represents the value of an image element. The $M\times N$ is the size of an image where M and N indicate the number of rows and columns respectively. An image element is also called a pixel and its value is called pixel value or gray level value. For a L-bit gray level image, the value of $f(x,y)$ lies between 0 *to* 2^{L-1}. For 8-bit gray level image, the $f(x,y)$ takes any value from 0 to 255. An image is called a binary image when $L=1$, and it is called a gray level image or panchromatic image when $L>1$. An image recorded in different colour bands is called a multispectral image. Normally, a colour image is represented in different colour bands red (R), green (G), and blue (B) viz. $f_C(x,y)=(f_R(x,y), f_G(x,y), f_B(x,y))$. A pixel value is represented with 24 bits (8 bit for each colour band). For more detail on images, one may refer[1,2,39,40].

An image exhibits neighbourhood similarity characteristics. The pixel values vary smoothly in the image region, highly correlated with near pixels and less correlated with farther neighbouring pixels. Such characteristics vary from image to image depending on different types of images. The neighbourhood characteristics are utilised in several image processing applications like image sharpening, smoothing, registration, and classification.

2.1 Histogram Equalisation (HE)

The HE technique is a contrast enhancement technique that improves the quality of a poor image by equalising its gray level histogram using probability density function. A HE image is the enhanced form of normal poor quality image[1-8]. The rescaling of pixel values is performed using the cumulative density function of the original image and a specified uniform distributed function in such a manner that the pixel values follow uniform distribution in a HE enhanced image. For an image, $f(x,y)$, the probability density function (PDF) is given by (1).

$$P(G)=n_g/(M\times N) \tag{1}$$

where, n_g is the value of the occurrence of gray level g. A transformation function is given by (2).

$$s_k=T(g_k)=\sum_{i=0}^{k}p(g_i), k=1\ to\ 255 \tag{2}$$

The transformation function is based on cumulative density function, $0\le T(g_k)\le 1$. The function s_k maps uniformly the gray level of poor image over the entire available range of gray values (0 to 255) to obtain an enhanced image. The HE technique is also known as the global histogram equalisation technique. As an example, a Lena image and its HE image along with their histograms are shown in Fig. 1. The histogram of the Lena image shows that the lower gray levels are not appearing in the image but the histogram of the HE Lena image shows that almost all the gray levels are appearing in the HE Lena image with approximately the equal distributions. We consider the Lena image to present the results on the image characteristics and discuss the findings on the security of bit-plane image encryption.

2.2 Bit-plane Encryption

The bit-plane level-encryption scheme segments a given image in different bit-planes and encrypts the bit-planes by an encryption algorithm. An 8-bit gray level image is decomposed into eight different bit-planes and encrypted with a suitable encryption scheme. In partial or selective encryption, some of the bit-planes are chosen to encrypt them. If we encrypt all the bit-planes of an image than encryption is called full encryption otherwise it is called partial encryption or selective encryption.

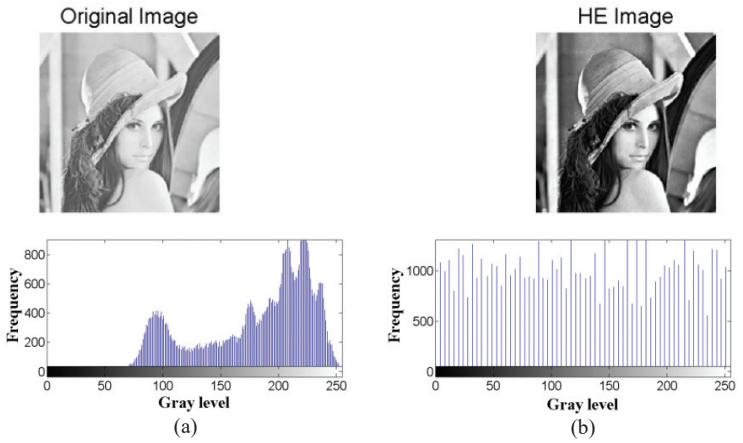


Figure 1. (a) Lena image and its histogram (b) HE image of Lena and its histogram.

In selective bit-plane level encryption, one can choose even a single bit-plane or some bit-planes selected suitably to encrypt them. In bit-plane level encryption, LSB planes of an image are used to XOR with specific MSB planes[14] and an AES block cipher is used to encrypt chosen bit-planes[39]. In single bit-plane encryption 12.5%, in double bit-plane encryption 25%, and so on, and in encrypting all the bit-planes 100% image data is encrypted. The effect of bit-plane encryption is shown in Fig. 2 for the Lena image.

3. METHODOLOGY

A methodology to analyse the strength of the bit-level encryption scheme consists the following processes.

3.1 Extraction of Bit-planes

Bit-planes are the decomposed form of a gray level image, each bit-plane is a binary image with pixel values zero or one[1,2].

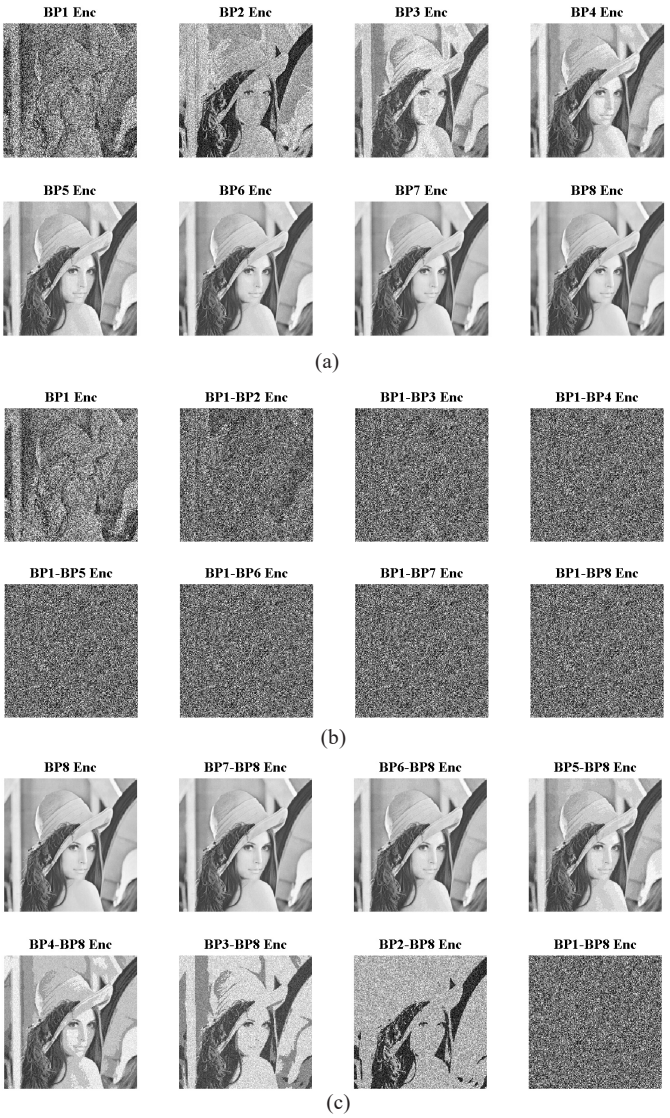


Figure 2. Bit-plane encryption for the Lena image (a) Single bit-plane encryption from MSB to LSB plane (b) Combined effect of bit-plane encryption from MSB to LSB plane (c) Combined effect of bit-plane encryption from MSB to LSB plane.

A plane containing the least significant bits of pixels is called the LSB plane and a bit-plane containing the most significant bits of pixels is called the MSB plane. These bit-planes have the neighbourhood similarity characteristics viz. pixel-to-pixel, block-to-block, line-to-line correlation, and smooth variations in gray level of an image. For an 8-bit gray level image, there are eight different bit-planes. If $f(x,y)$ be an image then the bit-planes are $f_1(x,y), f_2(x,y)...f_7(x,y)f_8(x,y)$ where $f_1(x,y)$ is the MSB plane and $f_8(x,y)$ is the LSB plane. We represent these bit-planes as BP1, BP2, ..., BP7, BP8 for demonstrating the analysis results.

3.2 Extraction of Edges

Edges are the features of an image that are used in the image analysis and pattern recognition problems. These edges are formed in an image where there are the sharp changes in the pixel values. For extracting the edges of an image, the gradient edge detection techniques are reported[1,2,44]. We consider a Canny edge detector[44] to obtain the edge details of an image. It detects the edge points with lesser error. We apply the canny edge detector in all the bit-planes and extract the edges in all the bit-planes of the images.

3.3 Computation of Bit-plane Measures

Image measures help to analyse the image characteristics. We consider the bit-plane measures for studying the image characteristics[11] for the HE images and the bit-plane encryption scheme. These bit-plane measures are briefly mentioned as follows[11].

(i) Bit-plane row(column) frequencies of ones are taken as $rf(k,i)$ and $cf(k,j)$ for row i, column j and bit-plane k, $i = 1\ to\ M$, $j = 1\ to\ N$, and $k = 1\ to\ 8$.

(ii) Bit-plane row(column) maximum run length are taken as $rr(k,i)$ and $cr(k,j)$ for row i, column j and bit-plane k, $i = 1\ to\ M$, $j = 1\ to\ N$, and $k = 1\ to\ 8$.

(iii) Bit-plane row(column) adjacent correlation between two rows, i and $i+1$, or two columns, j and $j+1$, are taken as $rc(k,i)$ and $cc(k,j)$, for $i = 1\ to\ M$, $j = 1\ to\ N$, and $k = 1\ to\ 8$.

3.4 Computation of Bit-plane Entropy Measures

Entropy is a measure of the information which gives an indication about the redundancy and randomness of data[45-46]. It is associated with the random variables variable say, X and is computed by (3).

$$H(X) = H(p_1, p_2, \ ..., \ p_n) = -\sum_{i=0}^{n} p_i \log_2 p_i \qquad (3)$$

where, $p_i = prob(X = x_i)$ in which x_i is the i^{th} possible value of X out of n symbols. The $H(X)$ lies in the range $0\ to\ \log_2 n$. For the gray level image of the L-symbols (256 for 8-bit/pixel) in which each symbol occurs equally, $(p_0 = p_1 = p_2 = ... = p_{L-1} = 1/L)$, the $H(X)$ is given by $\log_2 L$ which is approximately equal to 8. The entropy computed for an image f is called the global entropy. The entropy for a bit-plane is computed as similar to the global entropy for the two symbols 0 and 1 and called the local entropy or the bit-plane entropy.

3.5 Computation of Bit-plane Similarity Measures

A bit-plane to bit-plane similarity measure between successive bit-planes of an image $f(i,j)$, $1 \le i \le M$, $1 \le j \le N$ is computed by (4)

$$S(BP_k f(i,j), BP_{k+1} f(i,j)) = 100 \times (number\ of\ bits\ match / M \times N), \quad k = 1\ to\ 7\ and$$
$$S(BP_8 f(i,j), BP_1 f(i,j)) = 100 \times (number\ of\ bits\ match / M \times N), \quad k = 8 \tag{4}$$

Similarly, a bit-plane to bit-plane similarity measure between two images $f(i,j)$ and $g(i,j)$ is computed by (5)

$$S(BP_k f(i,j), BP_k g(i,j)) = 100 \times (number\ of\ bits\ matches / M \times N), \quad k = 1\ to\ 8 \tag{5}$$

4. RESULTS AND OBSERVATIONS

We apply the above methodology on several images for analysis of the bit-plane level characteristics. We consider different images of size 256×256 from Matlab and Google databases and some own collected images. The detailed results are presented for a standard image of Lena as an illustration. First, we processed some images and computed the bit-plane measures for the normal images and their HE images, then we perform encryption of the normal images and their HE images. The results for the bit-planes extracted, edges obtained, and the plots of bit-plane measures for the normal images and their HE image are shown in Figs. 3-5 respectively. The values of the bit-plane measures and the bit-plane entropy measures for normal images and their HE images are given in Tables 1 and 2. The bit-plane similarity measures within the images and between the images are given in Tables 3 and 4.

Here, we observed some new findings on the characteristics of the images at the bit-plane level based on the bit-plane patterns, edges, and the bit-plane measures.

4.1 Bit-plane Characteristics of HE Images

It is well known that the HE technique enhances the contrast of given gray level images, and changes the gray level distributions of the HE images to follow approximately the uniform distribution. The bit-plane characteristics are found drastically different in the bit-planes BP7 and BP8 for normal images and the HE images. We can see from Figs. 3 and 4 that many of the bit-planes have visible intelligible information and edge details. The plots of bit-plane measures exhibit larger variations and there are the drastic changes in some of the bit-planes as shown in Fig. 5. Table 1 shows that the MSB plane of normal images and the MSB and LSB planes of the HE images exhibit larger variations in the bit-plane measures. Table 2 shows that the values of entropy of normal images are higher but are lesser for their HE images. The bit-plane entropy values for the first four MBS planes of normal images are lesser and these values are higher for the four LSB planes. All the bit-planes of the HE images exhibit high entropy values of approximately 1. Table 3 shows that the bit-plane to bit-plane similarity for the MSB planes of normal images and for the MSB planes as well as the LSB planes of the HE images. These bit-plane similarity values are higher or lower than 50%. Also,

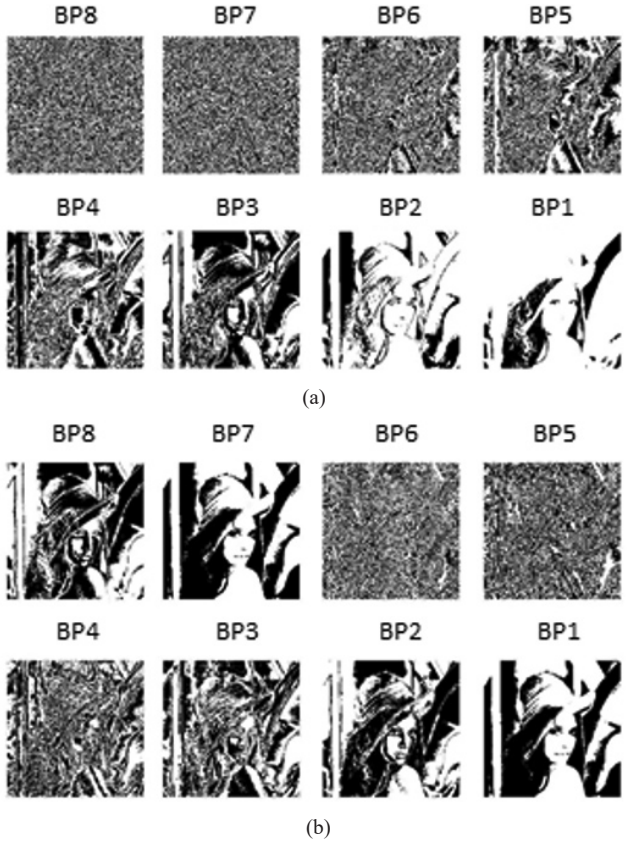


Figure 3. Bit-planes of the Lena image (a) Normal image (b) HE image.

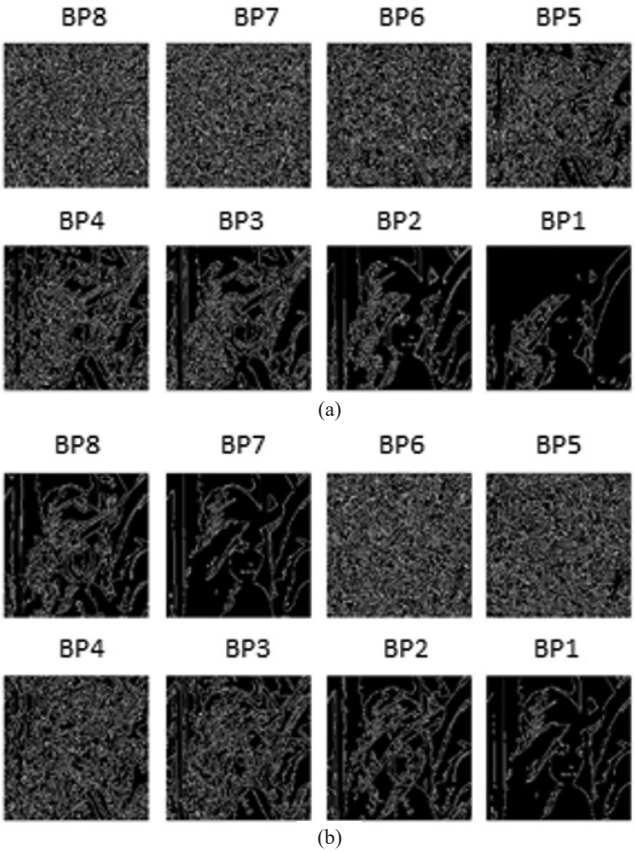


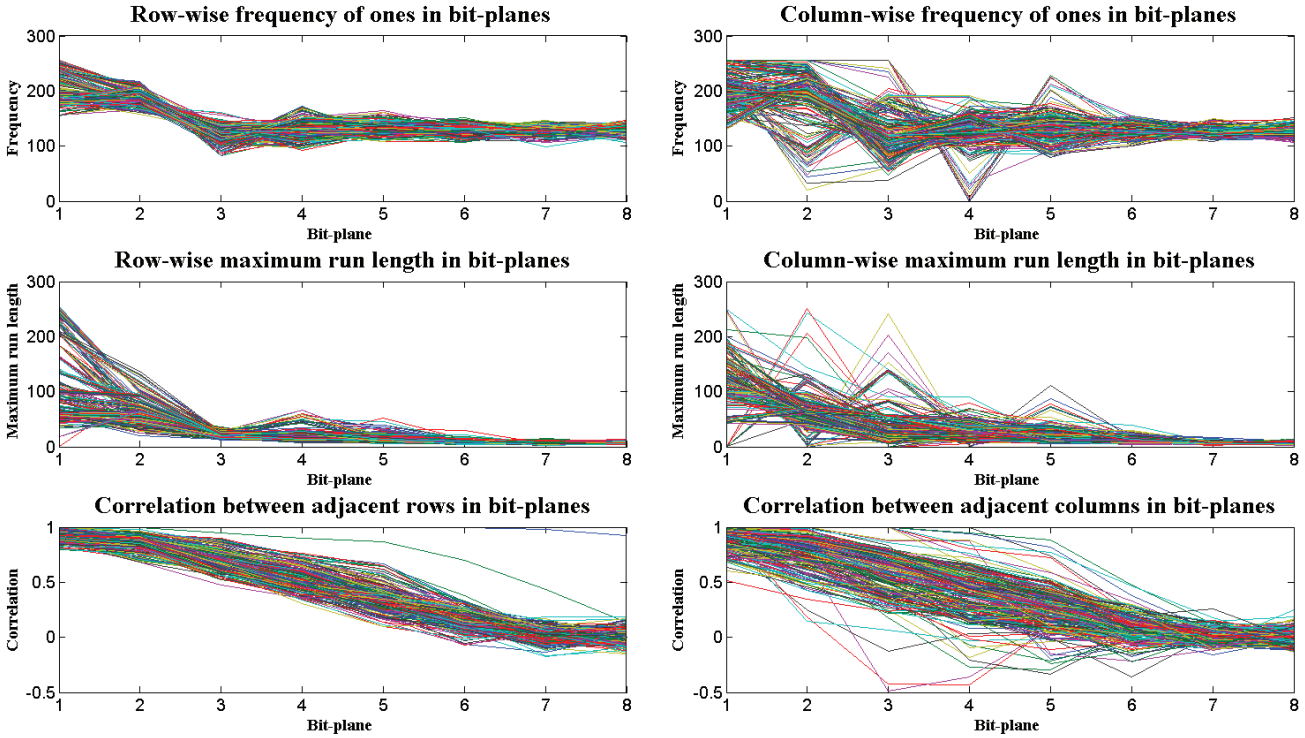
Figure 4. Edges extracted in the bit-planes of the Lena image (a) For normal image (b) For HE image.

Table 1. Maximum and minimum values of bit-plane measures

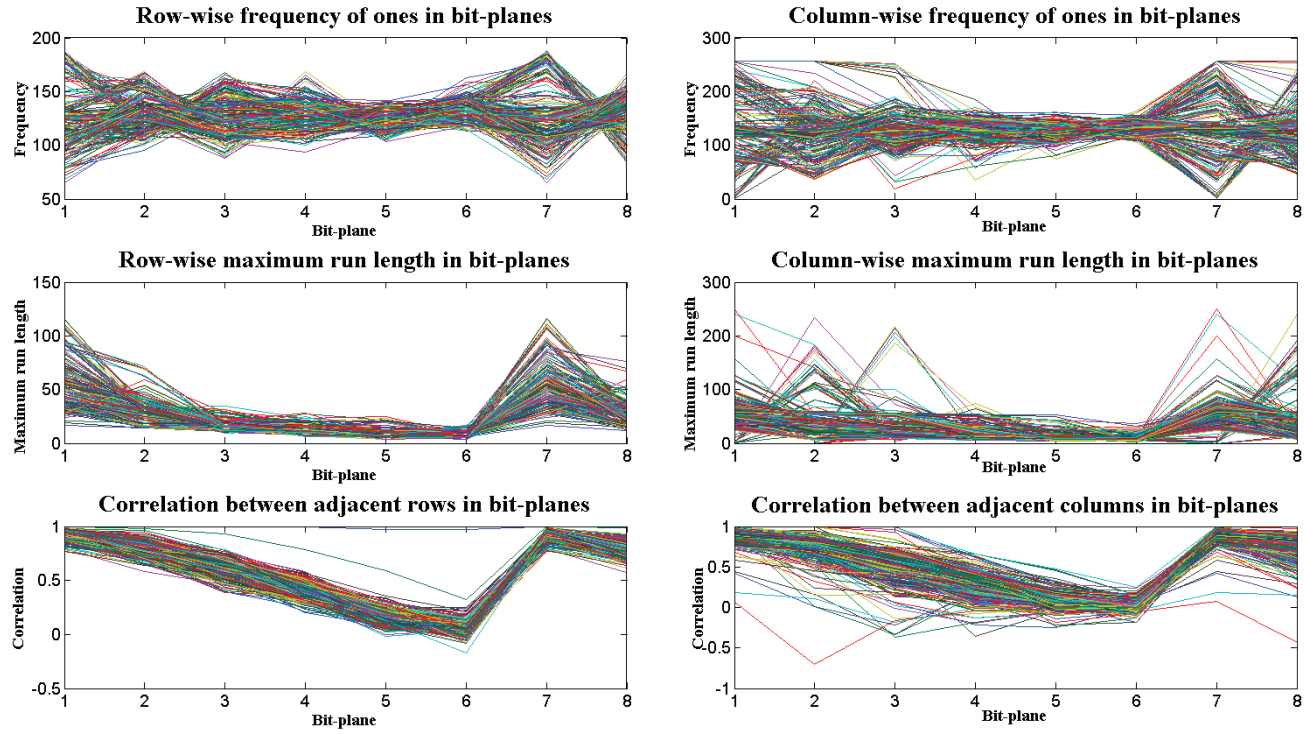
Image	Bit-plane Measures	Range of measures in bit-planes (BP_1 (MSB) - BP_8 (LSB))							
		BP_1	BP_2	BP_3	BP_4	BP_5	BP_6	BP_7	BP_8
Lena Image	Frequency of Ones (Row-wise)	170 0	189 49	199 81	173 62	174 80	153 102	152 102	159 102
	Frequency of Ones (Column-wise)	220 0	226 18	205 89	202 87	182 103	190 99	182 101	159 96
	Maximum Run Length (Row-wise)	67 0	65 2	73 4	43 4	94 4	25 3	27 3	22 3
	Maximum Run Length (Column-wise)	140 0	114 3	113 6	116 4	114 4	96 3	104 3	63 3
	Correlation (Adjacent Rows)	1.000 0.625	0.992 0.383	0.891 0.125	0.820 0.000	0.734 -0.148	0.500 -0.133	0.250 -0.149	0.227 -0.148
	Correlation (Adjacent Columns)	1.000 0.375	0.977 0.234	0.797 0.102	0.664 -0.040	0.570 -0.086	0.508 -0.117	0.461 -0.133	0.406 -0.148
Lena HE Image	Frequency of Ones (Row-wise)	188 65	169 95	168 88	169 94	142 103	163 113	188 65	166 85
	Frequency of Ones (Column-wise)	256 1	256 36	252 18	185 35	163 75	164 107	256 1	256 46
	Maximum Run Length (Row-wise)	116 17	71 14	35 9	28 6	25 4	17 4	116 17	76 12
	Maximum Run Length (Column-wise)	250 0	234 0	217 4	74 6	53 4	36 3	250 0	241 0
	Correlation (Adjacent Rows)	1.000 0.766	1.000 0.586	1.000 0.391	0.992 0.203	0.969 -0.016	0.969 -0.172	1.000 0.766	1.000 0.570
	Correlation (Adjacent Columns)	1.000 0.070	1.000 -0.703	0.992 -0.359	0.664 -0.250	0.477 -0.180	0.250 -0.156	1.000 0.070	1.000 -0.438
Lena (Encrypted)	Frequency of Ones (Row-wise)	146 104	145 105	148 106	146 109	145 102	150 106	147 108	151 106
	Frequency of Ones (Column-wise)	151 107	152 107	148 107	148 108	152 99	150 97	147 109	152 104
	Maximum Run Length (Row-wise)	14 3	17 3	15 4	15 4	15 3	15 3	16 4	19 4
	Maximum Run Length (Column-wise)	15 3	14 4	16 4	13 3	15 3	15 4	14 3	14 3
	Correlation (Adjacent Rows)	0.164 -0.211	0.180 -0.172	0.258 -0.172	0.156 -0.156	0.188 -0.188	0.164 -0.164	0.148 -0.180	0.156 -0.195
	Correlation (Adjacent Columns)	0.180 -0.203	0.188 -0.141	0.164 -0.156	0.180 -0.156	0.149 -0.188	0.164 -0.148	0.125 -0.156	0.188 -0.156

Table 2. Values of the entropy measures for different images and their bit-planes

Image	Type	Global Entropy	Bit-plane Entropy							
			BP1	BP2	BP3	BP4	BP5	BP6	BP7	BP8
Lena	Normal	7.2486	0.7250	0.8314	0.9985	1.0000	0.9992	1.0000	1.0000	1.0000
	Hist. Equal	5.9684	1.0000	0.9998	1.0000	1.0000	0.9989	0.9986	1.0000	0.9999
Cameraman	Normal	7.0097	0.9732	0.6741	0.9994	0.9844	0/9957	1.0000	1.0000	1.0000
	Hist. Equal	5.9106	1.0000	0.9999	0.9998	0.9980	0.9994	0.9997	1.0000	0.9999
Monalisa	Normal	7.6916	0.9584	0.9285	1.0000	0.9909	0.9987	0.9998	1.0000	1.0000
	Hist. Equal	5.9777	1.0000	1.0000	0.9998	1.0000	0.9998	0.9985	1.0000	1.0000
Street	Normal	7.2317	0.8794	0.9922	0.9974	1.0000	1.0000	0.9999	0.9999	1.0000
	Hist. Equal	5.8969	0.9995	0.9999	0.9850	0.9983	0.9998	0.9981	0.9995	0.9977
Baboon	Normal	6.6962	0.9999	0.9968	0.9961	0.9999	1.0000	0.9999	0.9999	0.9999
	Hist. Equal	5.9379	0.9999	0.9994	0.9998	1.0000	0.9995	0.9907	0.9999	0.9999



(a)



(b)

Figure 5. Plots of the bit-plane measures for the Lena image (a) Normal image (b) HE image.

from Table 4, the values of bit-plane similarity between the bit-planes of normal images and the HE images exhibit higher and lower than 50%. The MSB planes have the higher variations in similarity values.

Findings observed for the bit-planes of normal images and their HE images are presented in Table 5.

A slight variation in the bit-plane characteristics of the images may occur due to their gray level variations in different image acquisition conditions.

4.2 Effect of Bit-Plane Encryption

The effect of the selective encryption is studied by performing the bit-plane encryption of the images. We encrypt the bit-planes by performing the XOR operation bit-by-bit with

Table 3. Values of the bit-plane similarity measures between bit-planes of different images

Image	Type	Bit-plane similarity (%)							
		BP1-BP2	BP2-BP3	BP3-BP4	BP4-BP5	BP5-BP6	BP6-BP7	BP7-BP8	BP8-BP1
Lena	Normal	53.6118	40.0299	37.2955	49.9237	54.4342	50.1740	50.0565	49.7009
	Hist. Equal	50.7050	49.2142	48.9334	48.6923	49.1699	51.6830	35.0403	35.0403
Cameraman	Normal	26.2527	57.3151	49.3225	42.1234	50.7477	50.0839	48.9304	49.5590
	Hist. Equal	49.4507	51.4374	50.8713	49.8627	51.1154	48.6969	33.9432	33.9432
Monalisa	Normal	49.1867	46.5820	43.0130	49.6750	49.9603	50.6516	50.0366	49.6674
	Hist. Equal	49.9023	49.8947	49.8520	49.8260	49.5590	52.9129	34.5215	34.5215
Street	Normal	47.1619	46.3547	52.1927	52.1790	52.6215	51.7624	50.7782	50.3464
	Hist. Equal	81.1707	66.7343	66.5558	42.5949	60.7269	59.8755	52.4124	51.5503
Baboon	Normal	49.3912	26.7181	49.4675	49.5956	47.8622	50.9094	49.8795	49.4125
	Hist. Equal	49.6552	50.2792	49.5560	49.8810	51.8539	52.4185	34.1568	34.1568

Table 4. Values of the bit-plane similarity measures between different normal images and their HE images

Image	Bit-plane similarity (%)							
	BP1	BP2	BP3	BP4	BP5	BP6	BP7	BP8
Lena	69.9890	34.3277	60.4797	36.8820	50.5981	43.4723	50.1144	50.0793
Cameraman	90.4770	67.2791	58.9081	48.2346	47.0657	44.5587	49.9039	51.3657
Monalisa	87.9578	60.6400	31.4636	65.8752	54.6555	50.6104	50.2289	49.5087
Street	74.7208	52.4597	39.6637	51.5030	49.3164	50.6592	58.1680	58.1680
Baboon	50.6088	50.8728	65.9286	54.0665	48.1689	54.4373	50.2426	49.8917

Table 5. Findings on the bit-planes for normal images and their HE images

No.	For the Normal Images	For the HE Images
1.	MSB planes (BP1-BP5) are intelligible where BP1 is more intelligible and BP5 is less intelligible. Also, the LSB planes (BP6-BP8) are random, unintelligible, and their intelligibility is decreasing as we move from MSB to LSB bit-planes.	For the HE images, the LSB planes (BP7-BP8) are also intelligible in addition to the MSB planes (BP1-BP4). It means, we can infer information from the MSB planes (BP1-BP4) and the LSB planes (BP7 and BP8) of the HE images.
2.	Edges can be extracted in the bit-planes (BP1-BP4) which have visible intelligible information. Edges cannot be extracted in the bit-planes which have no intelligible information and appear random.	Edges can be extracted in the bit-planes (BP1-BP4 and BP7-BP8) which have visible intelligible information. Edges cannot be extracted in the bit-planes which have no intelligible information and appear random.
3.	Plots of the bit-plane measures show that the MSB planes have higher variations (larger dynamic range) and the LSB planes have lesser variations for the bit-plane measures. The frequency of ones is nearly the half of number of bits in columns(rows) and the maximum run length and correlation values are very less in LSB planes (BP6-BP8).	Plots of the bit-plane measures show that in addition to MBS planes (BP1-BP4), the LSB bit-planes (BP7-BP8) also have higher variations (larger dynamic range) for the bit-plane measures (frequency, maximum run length, and correlation). The frequency of ones is nearly the half of number of bits in columns(rows), and the maximum run length and correlation values are very less in bit-planes (BP5-BP6).
4.	Values of the bit-plane entropy measures for the most significant bit-planes are lesser compared to the least significant bit-planes.	Values of the bit-plane entropy measures for the most significant bit-planes as well as the least significant bit-planes are higher.
5.	MSB planes have larger variations in the bit-plane similarity values.	MSB and LSB planes have larger variations in the bit-plane similarity values.

the random binary sequences. The results of the selective bit-plane encryption for the Lena image are shown in Fig. 2 where Figs. 2(a) and 2(b) show the encryption for the single bit-plane encryption. In the single bit-plane encryption, the image details do not disappear completely even in encrypting the MSB plane. When we encrypt some of the bit-planes together starting from the MSB plane up to the LSB plane then the unintelligibility of an image increases and it appears highest for encryption of all the bit-planes as shown in Fig. 2(b). Encryption of more than the two MSB planes visually wipe-out the visible intelligibility of the images but the unencrypted bit-planes may contain a lot of intelligible information. When we encrypt the bit-planes together starting from the LSB plane to the MSB plane then the effect of encryption appears negligible in encryption of

the LSB planes as shown in Fig. 2(c). The images appear intelligible even when all the bit-planes except the MSB plane are encrypted. From Figs. 2(b) and 2(c), we can see that the encryption of all the bit-planes attain the maximum security strength and the same effect of encryption appeared either starting encryption from the MSB to the LSB plane or the LSB to the MSB plane. The effect of bit-plane encryption in the HE images is not similar as in the bit-plane encryption of the normal images and it varies in the bit-planes according to changes in the bit-planes of the HE images. The encryption of the MSB planes in the normal images wipe-out the intelligibility of the bit-planes but encryption of both the MSB and the LSB planes are needed to wipe out the intelligibility of the bit-planes for the HE images.

The plots of measures for encryption of all the bit-planes of the Lena image are shown in Fig. 6. It shows that the bit-plane measures appear uniformly flattened for all the bit-planes encrypted. It is seen that similar plots are appeared for normal images and their encrypted HE images.

4.3 Security Analysis

It was claimed for the selective bit-plane encryption[42-43] that the encryption of the two MSB planes is sufficient to secure the images but the encryption of the four MSB planes provides a high security of the images. The security analysis aims to obtain the image information from encrypted images even when more than the four bit-planes are encrypted in normal or in the HE images. The security of the bit-level image encryption scheme is the highest when all the bit-planes are encrypted with the unique and non-repeating random sequences. Hence, if an adequate number of specified bit-planes are not encrypted then the detail of a plain image can be obtained from such encrypted images. We have carried out the analysis of the bit-plane level encryption and shown the results for encrypting all the bit-planes except a single bit-plane left unencrypted for normal image and histogram equalised image of Lena as given in Fig. 7. Figure 7(a) shows an encrypted image and its histogram obtained by encrypting all the bit-planes except BP4 and Fig. 7(b) shows an encrypted HE image and its histogram by encrypting all the bit-planes except BP8. We see from Figs. 7(a) and 7(b) that both the encrypted images appear visually random and their histograms appear uniformly distributed[11]. From the appearance of these encrypted images, it seems that one cannot get any intelligible information but the presented bit-plane security analysis exhibits that we can observe the intelligible information of such encrypted images.

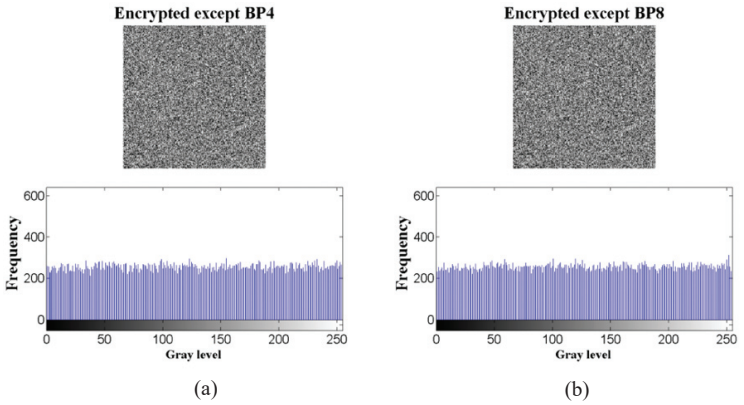


Figure 7. Encrypted images of the Lena and its histograms (a) Encryption of all the bit-planes except BP4 of normal image, (b) Encryption of all the bit-planes except BP8 of HE image.

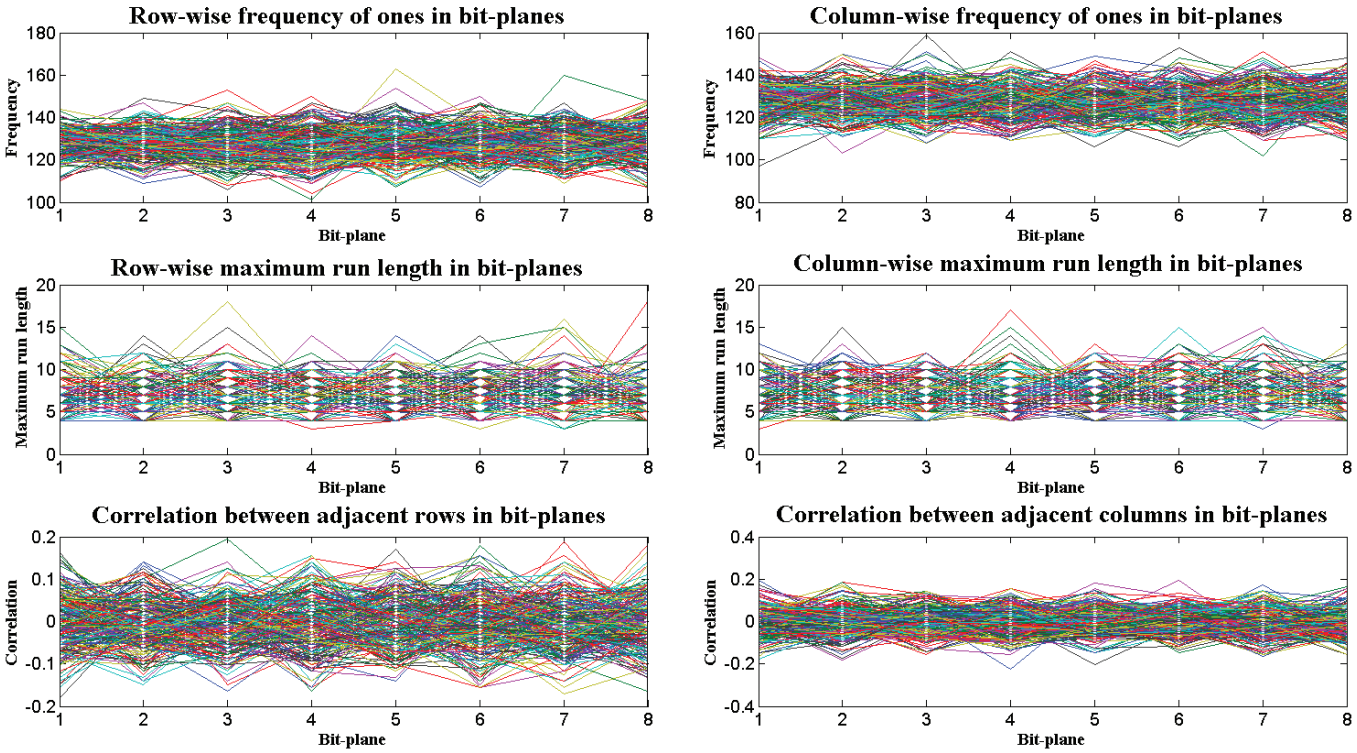


Figure 6. Plots of the bit-plane measures for the Lena image after encryption of all the bit-planes.

Analysis of the bit-plane encryption indicates that an image in which some chosen bit-planes encrypted appears visually random and unintelligible but some of its bit-planes which left unencrypted remain intelligible and contain enough detail to obtain image information. Specifically, if any bit-plane BP1 - BP5 is left unencrypted in normal images or any bit-plane BP1 - BP4 or BP7 - BP8 in the HE images is left unencrypted then the image information can be obtained from such unencrypted bit-planes. As an example, Figs. 8 and 9 show the details of the bit-plane left unencrypted in the encrypted image of the Lena image or its HE image. Plots of the bit-planes measures, Figs. 8(a) and 9(a) indicates that the unencrypted bit-planes have the similar bit-plane patterns as of the bit-plane of unencrypted image and the random pattern for the encrypted bit-planes. These plots show that the unencrypted bit-plane can be identified because the bit-plane measures of unencrypted bit-planes have non-flattened and non-random behaviour. The visual perception of encrypted/ unencrypted bit-planes are shown in Figs. 8(b) and 9(b) for the encrypted normal and the HE images. Visually, all the encrypted bit-planes looks random and unintelligible. The randomness of bit-planes for normal image, HE image and their encrypted images can be analysed by performing randomness tests[47-49]. Bit-planes encrypted with cryptographically strong binary sequences will pass the randomness tests and the unencrypted bit-planes will fail the randomness tests. The edges extracted in the unencrypted bit-planes of encrypted the normal image and the HE image are shown in Figs. 8(c) and 9(c) which exhibit the edges clearly in the unencrypted bit-planes but not in the encrypted bit-planes.

The above analysis of the bit-plane level encryption shows that the bit-plane encryption scheme is not able to provide the adequate security of the images by encrypting only the four MSB planes. For achieving the high security for all kinds of images either the normal or the HE images, we have to encrypt the specified and specific number of bit-planes or to perform the bit-plane level full encryption with strong encryption schemes that resist to cryptanalytic attacks.

4.4 Identification of HE Images and Unencrypted Bit-planes

For analysis of encrypted communications of the bit-plane level encryption schemes, an identification methodology for segregation of the normal/HE images and encrypted/unencrypted bit-planes of encrypted images is required before processing further for interpretation in the image processing applications. Many image classification schemes are reported in the literature but we can consider a bit-plane specific methodology[39] suited to the problem for the bit-plane level analysis and identification of specific images and bit-planes. The values of different measures given in Table 1-4 exhibits that the bit-plane measures are the suitable measures to form features for the classification of the images and the bit-planes.

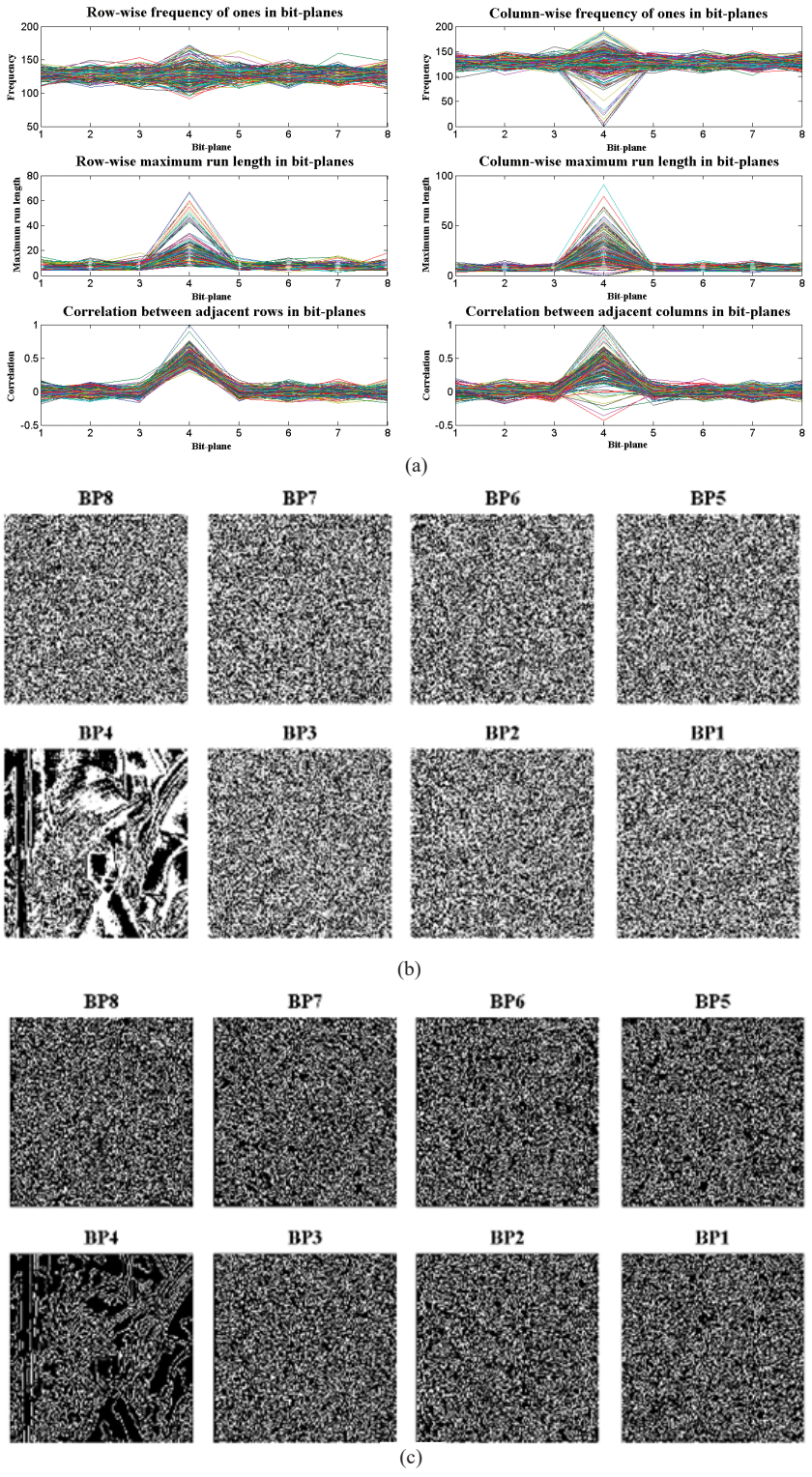
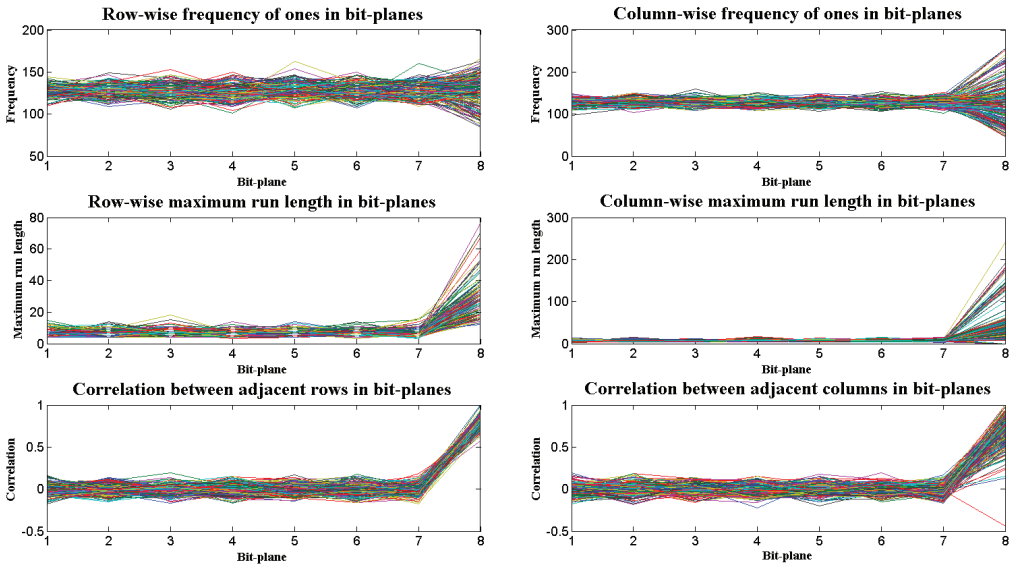
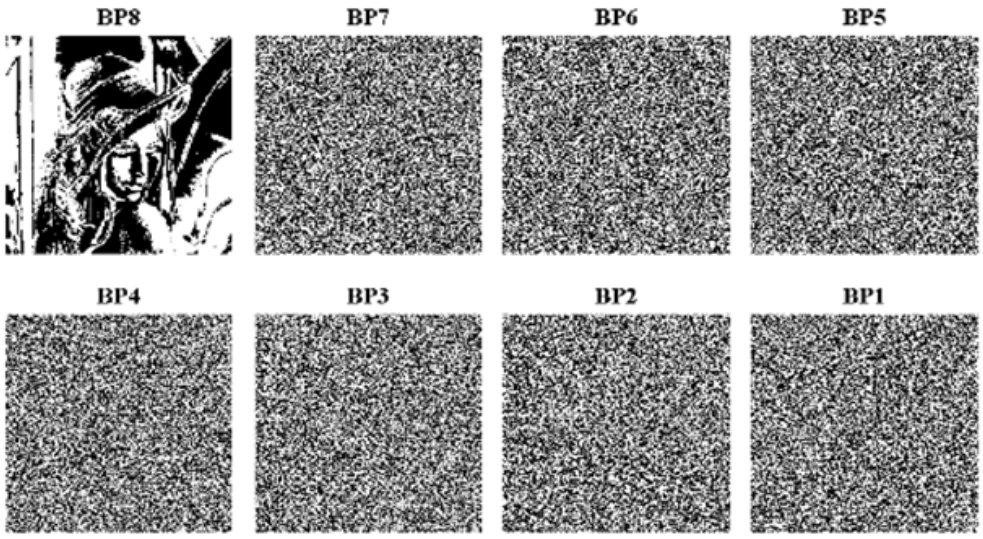


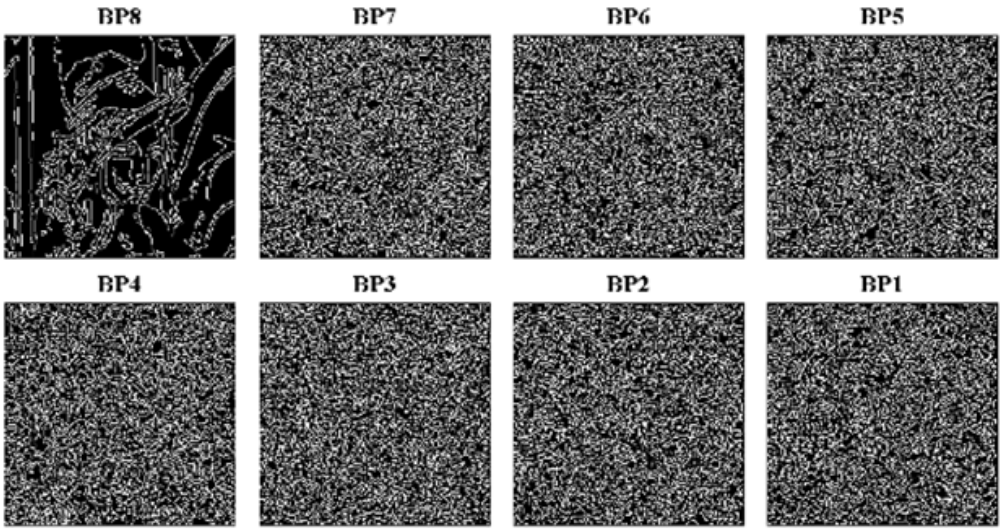
Figure 8. Plot of the bit-plane measures and the bit-plane detail for all bit-plane encryption except BP4 for the Lena image (a) Plots of the bit-plane measures, (b) Visual perception, and (c) Edges of bit-planes.



(a)



(b)



(c)

Figure 9. Plot of the bit-plane measures and the bit-plane detail for all bit-plane encryption except BP8 for the Lena image (a) Plots of the bit-plane measures, (b) Visual perception, and (c) Edges of the bit-planes.

We compute the bit-plane measures and obtain the maximum/minimum frequency row-wise $rfm(k), rfl(k)\ from\ rf(k,i)$, column-wise $cfm(k), cfl(k)\ from\ cf(k,i)$; maximum/minimum length of maximum run length row-wise $rrm(k), rrl(k)\ from\ rr(k,i)$, column-wise $crm(k), crl(k)\ from\ cr(k,i)$; maximum/minimum correlation row-wise $rcm(k), rcl(k)\ from\ rc(k,i)$, column-wise $ccm(k), ccl(k)\ from\ cc(k,i)$ [11].

Based on the variations in the above measures for bit-planes of the normal images, histogram equalised images and encrypted images, the values of $rrl(k)$ and $crl(k)$ are discarded, and we consider the features $(f_1^k, f_2^k, ..., f_9^k f_{10}^k)$ for each bit-plane $k = 1\ to\ 8$. These features are given by (6)

$$\begin{aligned} &f_1^k = abs(N/2 - rfm(k)), f_2^k = abs(N/2 - rfl(k)), \\ &f_3^k = abs(N/2 - cfl(k)), f_4^k = abs(N/2 - cfl(k)), \\ &f_5^k = rrm(k), f_6^k = crm(k), f_7^k = rcm(k), f_8^k = rcl(k), \\ &f_9^k = ccm(k), f_{10}^k = ccl(k) \end{aligned} \quad (6)$$

From these features, the membership values are computed for a given pattern based on the value of features for the reference pattern and membership function[39-40].

Let $T_{i_{r_c}}^k$ be the value of i^{th} feature and k^{th} bit-plane for c^{th} reference pattern r_c and let $Th1_{i_{r_c}}^k$ and $Th2_{i_{r_c}}^k$ be the thresholds for i^{th} feature and k^{th} bit-plane for c^{th} reference pattern r_c. Also, let $\mu(P_i^k)$ is the membership values of i^{th} element and k^{th} bit-plane of given unknown pattern which is obtained as $\mu(P_{i_{r_c}}^k)$ using a fuzzy membership function. The values of $Th1_{i_{r_c}}^k$ and $Th2_{i_{r-c}}^k$ in the fuzzy membership function are to be fixed carefully depending upon the variation of feature values of the reference pattern. An unknown image is identified as a normal image or HE image and a bit-plane as an encrypted or unencrypted bit-plane based on the average similarity score S_{r_c} computed for the n number of features as given by Eqn (7)

$$S_{r_c} = (1/n)\sum_{i=1}^{n} \mu(P_{i_{r_c}}^k) \quad (7)$$

An image belongs to a class rc for which the similarity score S_{rc} for feature vector of unknown image concerning the feature vector of the reference image is maximum[40]. In this manner, a given image can be identified as a histogram equalised image or normal image and a bit-plane encrypted or unencrypted in an image.

The bit-plane based identification can be used for the analysis of the traffic of cryptographic communications to segregate the images as the normal/HE images and the encrypted/unencrypted bit-planes of the encrypted images.

5. CONCLUSIONS

Methodology consisting of the extraction of bit-plane, detection of edges, and computation of bit-plane measures, entropy and bit-plane similarity has been presented for the security analysis of the bit-plane level encryption scheme. The bit-plane analysis of the images and their histogram equalised enhanced images has reported important new results and findings on the bit-plane characteristics of the images and their bit-plane level encryption. It has been shown that the characteristics of the images and their histogram equalised enhanced images show a drastically different behaviour at the bit-plane level. The least significant bit-planes appear random and unintelligible in normal images but these appear non-random and intelligible in the histogram equalised enhanced images. Further, the security of the bit-plane level encryption scheme encrypting the four most significant bit-planes claimed for a high security has been found insecure even encrypting a more number of bit-planes. It has also been shown that the details of images can be obtained when all the bit-planes except any bit-plane form BP1 to BP5 of normal images, and any bit-plane from BP1 to BP4 or BP7 to BP8 of the histogram equalised enhanced images are encrypted. The unencrypted bit-planes can be identified by observing the plots of bit-plane measures and the details of the images and their edges can be found from the unencrypted bit-planes. The bit-plane analysis of bit-plane level encryption infers that one has to encrypt the specified five most significant bit-planes of normal images and six planes of the histogram equalised enhanced images for achieving a higher security of visual data. The security analysis presented seems very useful and the methodology presented can be applied for evaluating the bit-plane level encryption schemes and the interpretation of communications of encrypted image data.

REFERENCES

1. Jain, A.K. Fundamentals of Digital Image Processing. Prentice Hall, USA, 1995.
2. Russ, J.C. The Image Processing Handbook. Sixth Edition, CRC Press, Boca Raton, 2011.
3. Ting, C.C.; Wu, B.F.; Chung, M.L.; Chiu, C.C. & Wu, Y.C. Visual contrast enhancement algorithm based on histogram equalization. *Sensors*, 2015, **15**(7), 16981-16999. doi: 10.3390/s150716981
4. Kaur, M.; Kaur, Jasdeep & Kaur, J. Survey of contrast enhancement techniques based on histogram equalization. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2011 **2**(7), 137-141. doi: 10.14569/IJACSA.2011.020721
5. Agarwal, R. Bit planes histogram equalization for tone mapping of high contrast images. *In* IEEE Eighth International Conference on Computer Graphics, Imaging and Visualization, 2011, 13-18. doi: 10.1109/CGIV.2011.18
6. Arvind & Ratan, R. Bit-plane specific selective histogram equalization for image enhancement and representation. *In* Recent Trends in image Processing and Pattern Recognition, CCIS, Springer, 2019, **1035**, 678-687. doi: 10.1007/978-981-13-9181-1_58
7. Sheikh, H.R. & Bovik, A.C. Image information and visual quality. *IEEE Trans. Image Process.*, 2000, **15**(2), 430-444.
8. Janssen, T.J.W.M. & Blommaert, F.J. Computational approach to image quality. *Displays*, 2000, **21**(4), 129-142. doi: 10.1016/S0141-9382(00)00056-1

9. Avcibas, I.; Sankur, B. & Sayood, K. Statistical evaluation of image quality measures. *J. Electron. Imag.*, 2002, **11**(2), 206-223. doi: 10.1117/1.1455011
10. Xin, Z. & Fu, S. User centric QUE model of visual perception for mobile videos. *Vis Comput*. 2019, **35**(9), 1245-1254. doi: 10.1007/s00371-018-1590-y
11. Ratan, R. & Arvind. Bit-plane specific measures and its applications in analysis of image ciphers. *In* Signal Processing and Intelligent Recognition Systems. CCIS, Springer, 2019, **968**, 282-297. doi: 10.1007/978-981-13-5758-9_24
12. Bourbakis, N.G. & Alexopoulos. C. Picture data encryption using scan patterns. *Pattern Recognition*, 1992, **25**(6), 567-581. doi: 10.1016/0031-3203(92)90074-S
13. Maniccam, S.S. & Bourbakis, N.G. Image and video encryption using scan patterns. *Pattern Recognition*, 2004, **37**(4), 725-737. doi: 10.1016/j.patcog.2003.08.011
14. Furht, B. & Kirovski, D. Multimedia Security Handbook. CRC Press; 2004.
15. Maitra, A.; Rao, Y.V.S. & Prasanna, S.R.M. A new image encryption approach using combinational permutation techniques. *Int. J. Comput. Sci.*, 2006, **19**(2), 127-131.
16. Mohammed Abbas Fadhil Al-Husainy A novel encryption method for image security. *Int. J. Security Its Applications*, 2012, **6**(1), 1-8.
17. Yen, J.C. & Guo, J.I. Design of a new signal security system. *In* IEEE International Symposium Circuits and Systems, 2002, **4**, 121-124.
18. Schwartz, C. A new graphical method for encryption of computer data. *Journal of Cryptologia*, 1991, **15**(1), 43-46. doi: 10.1080/0161-119191865777
19. Chang, C.C.; Hwang, M.S. & Chen, T.S. A new encryption algorithm for image cryptosystems. *J. Syst. Software*, 2001, **58**, 83-91. doi:10.1016/S0164-1212(01)00029-2
20. Ahmed Bashir Abugharsa, A.B. & Almangush, H. A new image encryption approach using block-based on shifted algorithm. *Int. J. Comput. Sci. Network Security*, 2011, **11**(12), 123-130.
21. Ratan, R. Image encryption using inversion and shifting. *In* Soft Computing for Problem Solving, AISC, Springer, 2012, **131**, 401-412. doi: 10.1007/978-81-322-0491-6_38
22. Mondal, B.; Behera, P.K. & Gangopadhyay, S. A secure image encryption scheme based on a novel 2D sine-cosine cross chaotic (SC3) map. *J. Real Time Image Proces.*, 2020. doi: 10.1007/s11554-019-00940-4
23. Fu, C. & Zhu, Z. A chaotic encryption scheme based on circular bit shift method. *In* International Conference for Young Computer Scientists, *IEEE Computer Society*, 2008, 3057-3061. doi: 10.1109/ICYCS.2008.522
24. Liu, L.; Hao, S., Lin, J. & Wang, Z. Image block encryption algorithm based on chaotic maps. *IET Signal Proces.*, 2017, **12**, 22-30. doi: 10.1049/iet-spr.2016.0584
25. Tong, X. & Cui, M. Image encryption with compound chaotic sequence cipher shifting dynamically. *Journal of Image and Vision Computing*, 2008, **26**(6), 843-850. doi: 10.1016/j.imavis.2007.09.005
26. Kumar, M.; Aggarwal, A. & Garg, A. A review on various digital image encryption techniques and security criteria. *International Journal of Computer Applications*, 2014, **96**(13), 19-26. doi: 10.5120/16854-6720
27. Ravishankar, K.C. & Venkateshmurthy, M.G. Region based selective image encryption. *In* International Conference Computing and Informatics, 2006, 6-8.
28. Kumar, N.; Panduranga, S.K. & Kiran, H. Partial image encryption for smart camera. *In* International Conference Recent Trends in Information Technology, 2013, 126-132. doi: 10.1109/ICRTIT.2013.6844192
29. Ozturk, I. & Sogukpinar, I. Analysis and comparison of image encryption algorithms. *International Journal of Information Technology*, 2005, **1**(2), 64-67.
30. Uhl, A. & Pommer, A. Image and Video Encryption from Digital Rights Management to Secured Personal Communication. Springer, USA, 2005.
31. Li, C.; Li, S.; Chen, G.; Chen, G. & Hu, L. Cryptanalysis of new signal security system for multimedia data transmission. *EURASIP J. Applied Signal Proces.*, 2005, **8**, 1277-1288.
32. Li, C. & Lin, D. Cryptanalysing an image scrambling encryption algorithm of pixel bits. *IEEE Multimedia*, 2017, **24**(3), 64-71. doi: 10.1109/MMUL.2017.3051512
33. Li, C.; Zhang, Y. &Xie, E.Y. When an attacker meets a cipher-image in 2018: A year in review. *J. Inf. Secur. Appl.*, 2019, arXiv:1903.11764. doi: 10:1016:.j.jisa.2019.102361
34. Ma, Y.; Li, C. & Ou, B. Cryptanalysis of an image block encryption algorithm based on chaotic maps. *J. Inf. Secur. Appl.*, 2020, arXiv:1912.12915 doi: 10.1016/j.jisa.2020.102566
35. Preishuber, M.; Huetter, T.; Katzenbeisser, S. & Uhl A. Deciphering motivation and empirical security analysis of chaos based image and video encryption. *IEEE T. Information Forensics and Security*, 2018, **13**(9), 2137-2150. doi: 10.1109/TIFS.2018.2812080
36. Chin, Y.C.; Wang, P.C. & Hwang, J.J. Cryptanalysis on Schwartz graphical encryption method. *Journal of Cryptologia*, 1993, **17**(3), 301-304. doi: 10.1080/0161-119391867962
37. Ratan, R. Key independent retrieval of chaotic encrypted images. *In* Advanced in Pattern Recognition and Machine Intelligence, LNCS, Springer, 2009, **5909**, 483-488. doi: 10.1007/978-3-642-11164-8_78
38. Ratan, R. Key independent decryption of graphically

encrypted images. *In* Intelligence and Security Informatics, LNCS, Springer, 2010, **6122**, 88-97.
doi: 10.1007/978-3-642-13601-6_11

39. Arvind & Ratan, R. Identifying traffic of same keys in cryptographic communications using fuzzy decision criteria and bit-plane measures. *Int. J. Syst. Assur. Eng. Manag.*, 2020, **11**(2), 466-480.
doi: 10.1007/s13198-019-00878-7
40. Ratan, R. & Yadav, A. Cryptanalysis of an image cipher using multi-entropy measures and the countermeasures. *Def. Sci. J.*, 2020, **70**(4), 425-439.
doi: 10.14429/dsj.70.15467
41. Ratan, R. & Yadav, A. Key independent image deciphering using neighbourhood similarity characteristics and divide-and-conquer attack. *Recent Patents Eng.*, 2020.
doi: 10.2174/1872212114999200719144548
42. Podesser, M.; Schmidt, H.P. & Uhl, A. Selective bitplane encryption for secure transmission of image data in mobile environments. https://pdfs.semanticscholar.org/8484/7bb66aacb487a6aaa1f4798cd0ff6258737c.pdf
43. Nazneen, M.G.; Sufia, B.; Zahira, T.; Khamer, F. & Arshia Shariff, S. Selective bitplane encryption for secure transmission of image data in mobile environments. *Int. J. Sci. Technol. Res.*, 2013, **2**(6), 92-96.
44. Canny, J. A computational approach to edge detection. *IEEE Trans. Patt. Rec. Mach. Intel.*, 1986, **8**(6), 679-698.
doi: 10.1109/TPAMI.1986.4767851
45. Shannon, C.E. Communication theory of secrecy systems. *Bell System Tech. J.*, 1949, **28**(4), 656-715.
doi: 10.1002/j.1538-7305.1949.tb00928.x
46. Wu, Y.; Zhou, Y.; Saveriades, G.; Agaian, S.; Noonan, J.P. & Natarajan, P. Local Shannon entropy measure with statistical tests for image randomness. *Inform Sciences*, 2013, **222**, 323-342.
doi: 10.1016/j.ins.2012.07.049
47. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A. & Dray, J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication, 2010, SP 800–22, Revision-1a, http://www.nist.gov (Accessed on 25 July 2021).
48. Ratan, R.; Jangid, B.L. & Arvind. Bit-plane specific randomness testing for statistical analysis of ciphers. *In* Soft Computing for Problem Solving 2018, AISC, 2020, **1138**, 199-213.
doi: 10.1080/0161-119391867962
49. Jangid, B.L. & Ratan, R. A New bit plane specific longest repeating pattern test for statistical analysis of bit sequences. *In* Soft Computing: Theories and Applications, 2019, AISC, Springer, 2020, **1154**, 943-954.
doi: 10.1007/978-981-15-4032-5_85

CONTRIBUTORS

Mr Ram Ratan is a Scientist in Defence Research Development Organisation (DRDO) and currently working at Scientific Analysis Group (SAG), Delhi. Currently, he is working in the area of information security. His research area includes cryptography, mathematics, image processing, information security and pattern recognition.
In the current study, he has proposed a methodology for security analysis of bit-plane level image encryption scheme by considering different bit-plane level aspects and reported important new findings. He has improved the manuscript by incorporating meaningful suggestions of the reviewers.

Dr Arvind Yadav is working as an Assistant Professor in Hansraj College, University of Delhi. He also worked as Scientist in Defence Research Development Organisation (DRDO) at Scientific Analysis Group (SAG), Delhi. He is teaching the mathematics and has more than 12 years of experience in teaching and research. His research area includes mathematics, cryptography, information security and image processing.
In the current study, he has surveyed relevant research and consolidated important results for bit-plane level encryption and analysis of images. He also contributed in improving the manuscript.