A Bit Level Image Encryption Algorithm using Generated Binary Key Matrices

Neha Verma

Department of Computer Science and Engineering, Inderprastha Engineering College, Ghaziabad, UP

---***---

Abstract: In this paper, the authors have suggested an effective gray scale image encryption scheme at bit level to protect and to ensure the confidentiality of the image data both at pixel as well as at bit level. The proposed cryptosystem is involved in different phases where in first phase, the secret image is decomposed into eight bit planes using the bit plane decomposition and subsequently, in the second phase each bit planes are considered for enciphering process using eight different binary key matrices of size equivalent to the given image size. Practically, it is not feasible to share large size of eight different binary key matrices using any key exchange protocol. So here, the authors have suggested a key expansion mechanism for formation of eight binary key matrices from a small key of size 256 bits where the secret key is initially transformed into a binary matrix of size equivalent to the given image size using Arnold cat map. Then, eight binary shares are generated by the Ou, Sun and Wu's visual cryptographic scheme. The generated eight binary shares are considered as binary key matrices to encrypt each bit planes independently. The experimental results shows that the proposed scheme can effectively encipher the secret image data both at pixel and bit level. It also provides satisfactory results in terms of Histogram analysis, PSNR, Correlation coefficients, entropy and key space analysis. Overall, the proposed scheme is suitable for transmission of the secret image data in secure way even using a key of size 256 bits.

***Keywords*: *Arnolds Cat Map (ACM), Bit-plane decomposition, Image Cryptosystem, Bit Level Image Encryption, Visual Cryptography Scheme (VCS*)**

1. INTRODUCTION

The digital information sharing and transmission through the Internet has become the easiest mode among the sender and the receiver. The data transmission rate is rapidly increasing due the advancement of Internet technology and computer devices. Every second a huge number of confidential data is being generated, transferred and stored. Internet inherently doesn't provide any security mechanism to protect the confidentiality, integrity and authenticity of the digital data. The security issues of digital data are protected in various forms like using cryptography/ steganography techniques [1], fragile watermarking [2] and robust watermarking [3] respectively. To maintain the confidentiality of textual data, several standard encryption algorithms such as DES, AES, RSA, ECC etc. [4] are used in various instances. These standard encryption algorithms are not suitable to apply directly for enciphering the multimedia data like image or video successfully. Since pixel elements of the multimedia data are highly correlated and their size is comparatively huge. So in literature, several image/ video cryptosystem [5-6] can be found to protect their confidentiality property during transmission. The image data are widely used in various internet based applications and their security is essential during transmission over the internet.

In general, the image data can be encrypted either in pixel level [7] or in bit plane level [8]. The bit plane level encryption algorithms has shown excellent encryption performance and is easily implemented on hardware. It is also possible to implement in parallel architecture. The bit plane decomposition based image encryption scheme first decomposes the image into binary bit planes using any decomposition method, such as traditional binary decomposition, gray code decomposition and Fibonacci p-code decomposition. These bit planes are encrypted through some encryption algorithm and then all the encrypted bit planes are combined together to obtain the final encrypted image. Based on this technique, many image encryption algorithms have been proposed in literature. J.W. Han et al. [9] proposed an image encryption technique that includes XOR operation to encrypt binary bit planes of optical images. Later, for image encryption various bit plane encryption schemes have been developed to achieve low computational complexity [10] and [11]. But, due to limited key spaces and predictable decomposition results, these algorithms have low security level. Y. Zhou et al. [12] proposed an image encryption based on the parametric decomposition methods including the (n, k, p)-Gray code decomposition and Fibonacci p-code decomposition. But due to low security level, there still exists a chance for security enhancement. Later, in [13-14] introduces an image encryption methodology to improve the security of the bit plane decomposition encryption scheme by decomposing the source image into bit planes. L. Xu et al. [15] proposed a novel bit level image encryption algorithm that is based on piecewise linear chaotic maps (PWLCM). Later, P Praveenkumar et al. [16] proposed a scheme in which a rapid key encryption procedure is used by employing a symmetric key. Fu et al. [17] proposes a novel chaos-based bit-level permutation scheme for secure and efficient image cipher. Significant diffusion effect in permutation procedure through a two-stage bit-level shuffling algorithm is introduced to overcome the drawback of conventional permutation-only type cipher image. The two stage permutation operations are realized by chaotic sequence sorting algorithm and Arnold Cat map. Z. Tang [18] proposed efficient encryption algorithm for multiple gray scale images where input images are decomposed into bit planes and bit blocks are swapped randomly among the different bit planes and finally XOR operation is performed between the scrambled bit planes and the secret key to obtain the encrypted image. Later, W. Zhang et al. [19] proposes a cryptosystem to address the drawbacks of bit level and pixel level encryption. G.D. Ye and K.W. Wong [20] proposed image encryption algorithm using generalized Arnold's Cat Map(ACM) and is composed of two stages: permutation and diffusion. In permutation stage, correlation coefficients between adjacent pixels are reduced and in diffusion stage key stream is generated using double diffusion function. Therefore, it can resist known and chosen plaintext attacks. You et al. [21] proposed 3-D image encryption scheme based on micro lens array, which can be reconstructed using digital refocusing algorithm. The Arnold transform and gravity model based encryption algorithm is used to improve the security of the image cryptosystem. D. Xiao [22] proposed a novel image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Initially plain image is divided into 8×8 non-overlapped pixel blocks with random matrix and then each blocks into 8×8×8 3 dimensional binary matrixes which is similar as cube. Then, use block diffusion to further change the statistical characteristics of the image after confusion. Li, Peng, et al. [23] introduces a general gray visual cryptographic scheme (VCS), which can share more information, called Sharing More Information Gray Visual Cryptography Scheme (SMIGVCS). All the shadow pixels of VCS embed additional information to generate gray shadows of SMIGVCS, and the embedded information comes from the shadows of a polynomial-based secret sharing scheme (PSSS). S. Zhou et al. [24] proposed a key generation process on the basis of operations of AC and DC value in YUV space to improve the security of color image encryption.

In recent, there is a demand for light weighted encryption algorithm with comparatively small size of secret key for processing them in some low processing computer devices. In this paper each bit plane is encrypted using straightforward XOR operation with a binary key matrix of size equivalent to the original image size. This approach is simple and provide satisfactory results when the key matrix is random in nature. Now, it is not feasible to share different eight binary key matrices of size equivalent to the original image size between the sender and the receiver for enciphering/deciphering process. Here, we have considered a small size key of length 256 bits and that one was shared between the sender and the receiver using any standard key agreement protocol [4]. The key is used for formation of different eight binary key matrices using the proposed key expansion algorithm. Then, each bit plane of the original image is encrypted using the above generated binary key matrices using the XOR operation. All the encrypted bit planes are combined to obtain the preferred encrypted image. The main contribution of this paper is to derive different eight binary matrices in randomly from a secret key of length 256 bits.

The rest of this paper is organized as follows. In section 2, the basic theory of bit plane decomposition, the Arnold's Cat Map (ACM) and Ou et al. Visual cryptography scheme [25] are presented briefly. In section 3, the proposed algorithm is described in detail. The experimental results and security analysis are presented in section 4. Finally, the conclusions are given in section 5.

2. *Preliminaries*

In this section, we have briefly described Bit-plane decomposition procedure, Arnold's Cat Map (ACM) and Ou et al. Visual cryptography scheme [27] algorithm for share generation.

2.1. *Bit plane Decomposition*

The image data can be visualized in a sequence of bits by using the bit plane decomposition where the set of MSB's provides more information compared to the set of LSB's. A non-negative decimal number N can be represented in a binary sequence $(b_0, b_1, \cdots, b_{n-1})$ based on the following equation:

$$N = \sum_{i=0}^{n-1} b_i \times 2^i = b_0 \times 2^0 + b_1 \times 2^1 + \cdots + b_{n-1} \times 2^{n-1} \qquad (1)$$

As the pixel values of the gray scale image are decimal numbers between 0 and 255. So, each pixel can be represented by 8 bit binary sequence. Therefore, bit plane decomposition decomposes the gray scale image into 8 binary bit planes. Among these bit planes, higher bit planes in image data conveys more information than the lower bit planes of image data. The bit plane images of the Baboon image are shown in Fig 1 which depicts that first four MSB bit planes carries more information than first LSB bit planes.

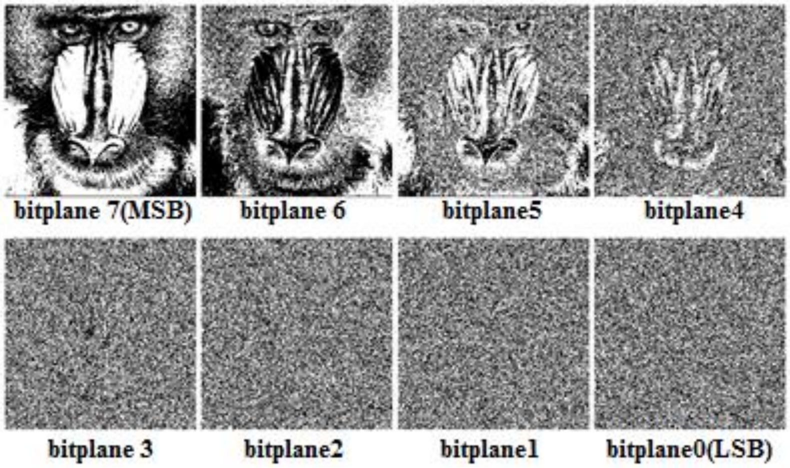


Fig.1. Bit plane decomposition of Baboon image

2.2. Arnold's Cat Map (ACM)

Arnold cat map (ACM) is a technique for shuffling the pixels position across the square matrix in such a way that the correlation of pixels elements will get reduced as the number of iterations will get increased up to the mid of its periodicity. This method is generally used to destroy the original orientation of the image for secure image cryptosystem. It can be expressed for a matrix of size N×N as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \mod N$$

Where, $A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$, (x,y) ε[1,N] and det(A)=1. (x,y) and (x',y') represent the position vector of the image before and after the shifting operation, and mod denotes the modulus after division.

Since, it is a reversible process. Therefore, the original image matrix can be found by using the inverse ACM. The inverse ACM of a matrix can be expressed as follows:

$$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \mod N$$

Where $A^{-1} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$.

2.3.Algorithm 1

This algorithm is proposed by Ou et al. [25] to construct n number of meaningful shares by adopting basic idea of Visual Cryptographic scheme (VCS) [26]. So, to generate 8 different binary key matrices of size N×N this algorithm is advised and can be obtained with the following steps:

Input: A binary matrix of size N×N
Output: 8 binary shares of size N×N

Step1. Construct a matrix M_8 of size 2^8×8

```
    for i=1 to2^8
    M_8(i)=decimal_to_binary(i-1,8)
    end for
```

Step2. Construct *8*different binary matrices using secret image *S* and M_8

a.)Divide the matrix M_8 into two sub matrices M_8^{odd} and M_8^{even} where $M_8^{odd} \cup M_8^{even}$ and $M_8^{odd} \cap M_8^{even}=\phi$. First, let $M_8^{odd}=\phi$ and $M_8^{even}=\phi$. For each row vector M_8 (i,1:8) in $M_{8,}$ if the hamming weight *hw* (M_8(i,1:8) is an odd numbers, then add the row vector M_8 (i,1:8) into the matrix M_8^{odd}, otherwise add the row vector M_8 (i,1:8) into the matrix M_8^{even}. When all the row vectors in M_8 are processed completely, two sub matrices M_8^{odd} and $M_8^{even}$are generated, each of which is 2^{8-1}×8 in size.

b) For each position (i,j) in the matrix S, M_8^{odd} or M_8^{even} is adopted to construct n shares pixels R_1(i,j),...,R_8(i,j) according to the pixel S(i,j).

c) If S(i,j)=0,construct n share pixels R_1(i,j),...,R_8(i,j) by adopting matrix M_8^{even}. Sequentially choose a row vector M_8^{even} (r,1:8) from M_8^{even}. Subsequently, the corresponding 8 share pixels R_1(i,j),...,R_8(i,j) can be constructed by

$$R_1(i,j)=M_8^{even}(r,1)$$
$$\vdots$$
$$R_8(i,j)=M_8^{even}(r,8)$$

d) If S(i,j)=1, construct 8 share pixels R_1(i,j),...,R_8(i,j) by adopting the matrix M_8^{odd}. Sequentially choose a row vector M_8^{odd}(r,1:n)from M_8^{odd}. Subsequently the corresponding 8 share pixels R_1(i,j),...,R_8(i,j) can be constructed by

$$R_1(i,j)=M_8^{odd}(r,1)$$
$$\vdots$$
$$R_8(i,j)=M_8^{odd}(r,8)$$

e) Repeat steps 2.3.2.2-2.3.2.4 until all the secret pixels are processed, the output *8* binary key matrices each of which has the same size as the original image.

3. Proposed Method

In this paper, we can encrypt large size of image with small key size by manipulating the key to the size of the original image. As large size keys are not feasible to transmit. So, here three major phases are designed *Key generation phase, Encryption phase* and *Decryption phase* respectively.

3.1 *Key Generation Phase*

In this phase, 8 binary key matrices of size equivalent to the size of the original image i.e. N×N is generated with the help of a small key of size 256 bits. The key generation phase is shown in Figure 2. Following steps depicts the key generation phase in details:

Input: A small key of size 256 bits
Output: 8 binary different key matrices of size N×N

Step1. Input a small key of size 256 bits.
Step2. Reshape the binary bits of keys into a binary matrix(I) of size 16×16.
Step3. Construct a matrix (L) of same size as original image by appending the matrix I several times through raster scan order.
Step4. Apply ACM to shuffle the pixel positions of matrix L to obtain matrix L'
Step5. Using **algorithm 1**, construct 8 binary matrix by considering L' as S.by considering rows sequentially in cyclic order from M_8^{odd} and M_8^{even} respectively.

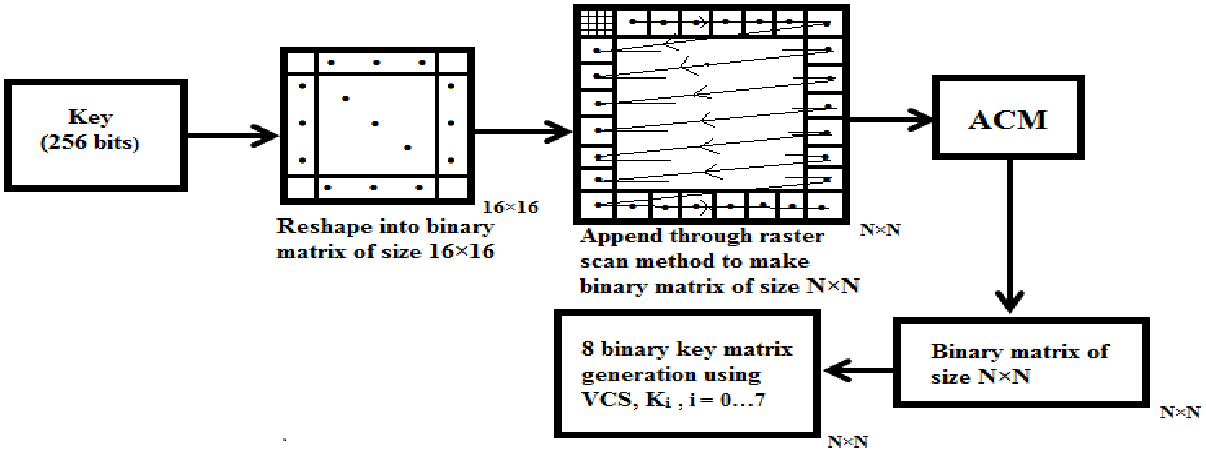

Key
(256 bits)
16×16
Reshape into binary matrix of size 16×16
Append through raster scan method to make binary matrix of size N×N
N×N
ACM
Binary matrix of size N×N
N×N
8 binary key matrix generation using VCS, Ki , i = 0…7
N×N

Fig 2: Key generation process

3.2 *Encryption Phase*

For secure transmission of any data, encryption is the most effective way to achieve data security. Therefore in this phase, an image is encrypted using 8 different binary key matrices randomly to protect and provide secure transmission of the data. The key matrices are generated from a small size of 256 bits key and this small size of key is feasible to transmit through any suitable key exchange protocols. The schematic diagram of the proposed scheme is shown in figure 3.The major steps of encryption process is described as follows:

Input: An image of size N×N
Output: An encrypted image of size N×N

Step1. Decompose the original image into 8 binary bit Planes $P_{i=0to7}$ using the Bit Plane decomposition.

Step2. Encrypt each binary bit planes by XORing with Different keys, generated in *key generation phase* .

$C_i = P_i \oplus K_i$ where, P_i = original image plane
K_i= i-th binary key matrix
C_i = i-th Encrypted image plane

Step3. Finally, all the encrypted bit planes $C_{i=0\text{to}7}$ are combined to obtain the encrypted image.

3.3 *Decryption Phase*

Decryption is the reverse process of encryption and can be obtained with the following steps:

Input: An encrypted image of size N×N
Output: An original image of size N×N

Step1. Similarly, decompose the encrypted image into 8 binary bit planes $C_{i=0\text{to}7}$ using Bit Plane decomposition.
Step2. Receiver receives key of 256 bits and generate the eight key matrices as described in *Key generation phase.*
Step3. Decrypt each binary bit planes by XORing with the key matrices generated in step 2.

$$P_i = C_i \oplus K_i$$

Step4. Finally, all the decrypted bit planes are combined to obtain the original image.

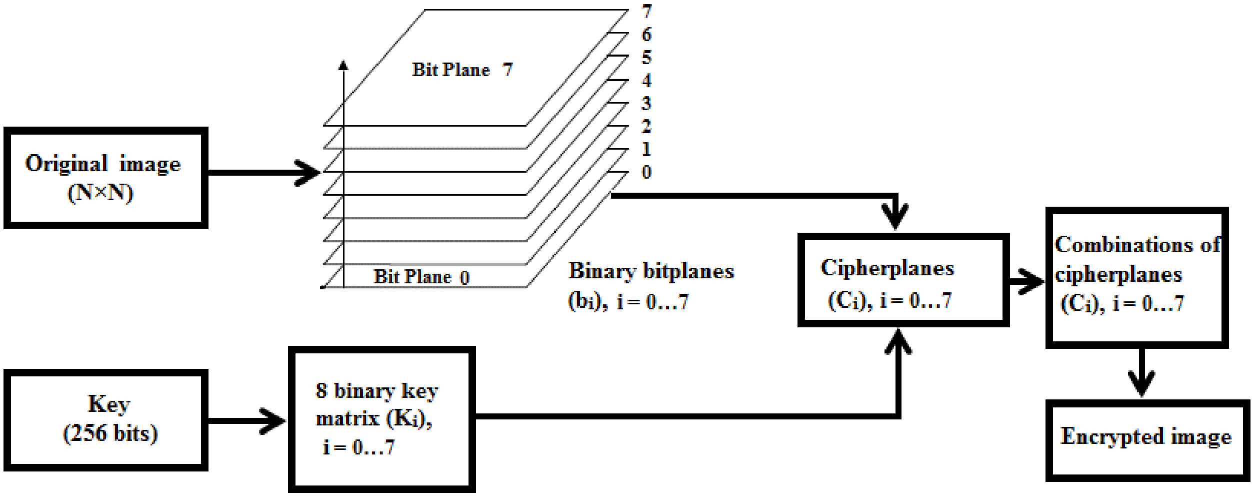
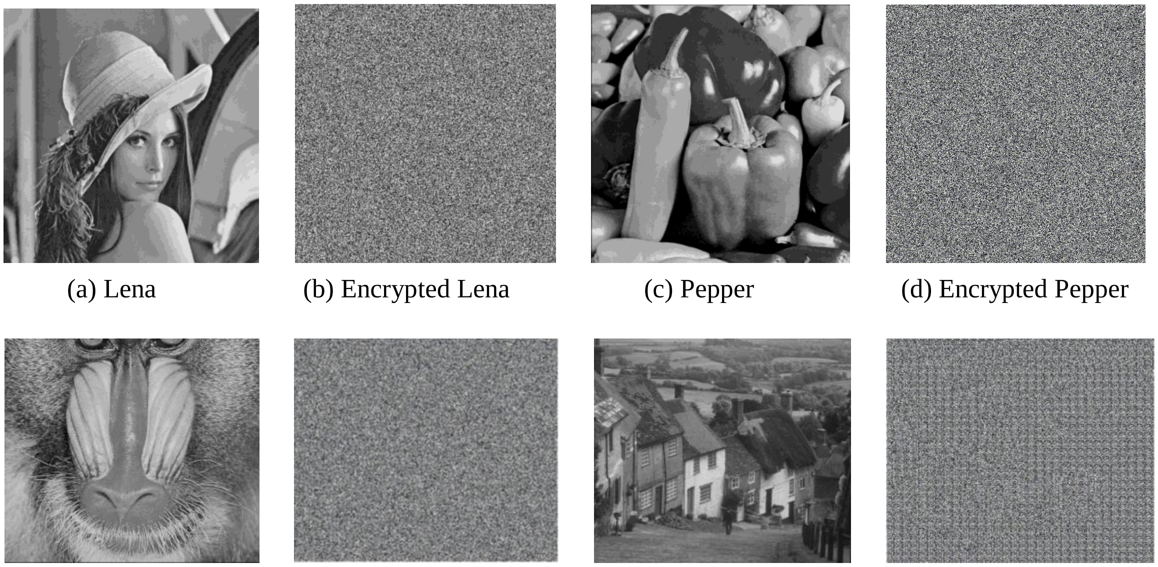

Original image (N×N)
Bit Plane 7
Bit Plane 0
7
6
5
4
3
2
1
0
Binary bitplanes (bi), i = 0…7
Cipherplanes (Ci), i = 0…7
Combinations of cipherplanes (Ci), i = 0…7
Encrypted image
Key (256 bits)
8 binary key matrix (Ki), i = 0…7

Fig.3 The schematic diagram of the Encryption algorithm

4. *Experimental Results and Analysis*

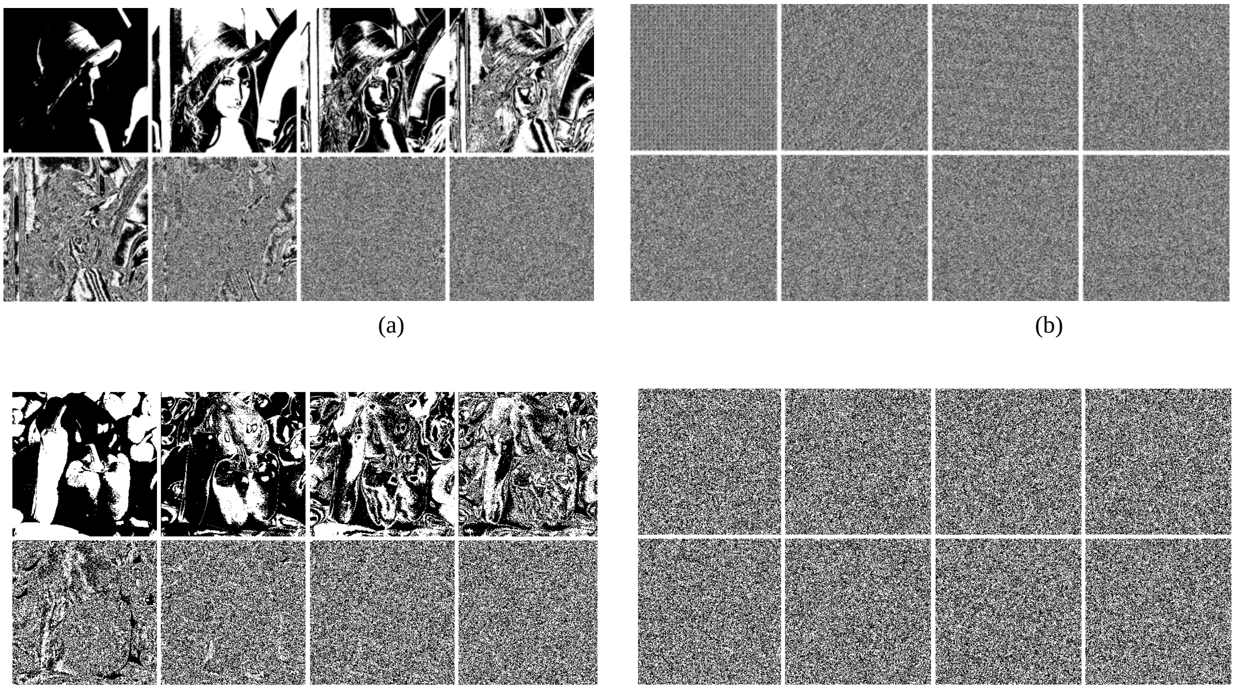
The proposed scheme is simulated with MATLAB and tested with a set of standard images. But as a representative only the results for two standard images (i.e. Lena and Pepper) are presented. All the test images are of typical size of 512×512. Initial 256 bits binary key is reshaped into a matrix of size 16×16. Subsequently, the block of size 16×16 are appended one after another in raster scan order to form a matrix of size 512×512. This binary matrix of size 512×512 preserve the some symmetric patterns which was removed by ACM. This ACM operation will confuse the matrix and from this shuffled matrix, another eight random key matrices will be generated using the algorithm 1. The visual presence after the encryption process is shown in Figure 4. The encrypted images are appeared randomly and they do not provide any visual information to the human perception. This random appearance is also preserved even in bit levels of the encrypted images. Figure 5 shows that the bit plane images of encrypted images are completely appeared in random manner. We have further analyzed the effectiveness of the proposed image cryptosystem in terms of analysis of perceptual security, histograms, correlation coefficients, entropy and the key space.



(a) Lena (b) Encrypted Lena (c) Pepper (d) Encrypted Pepper

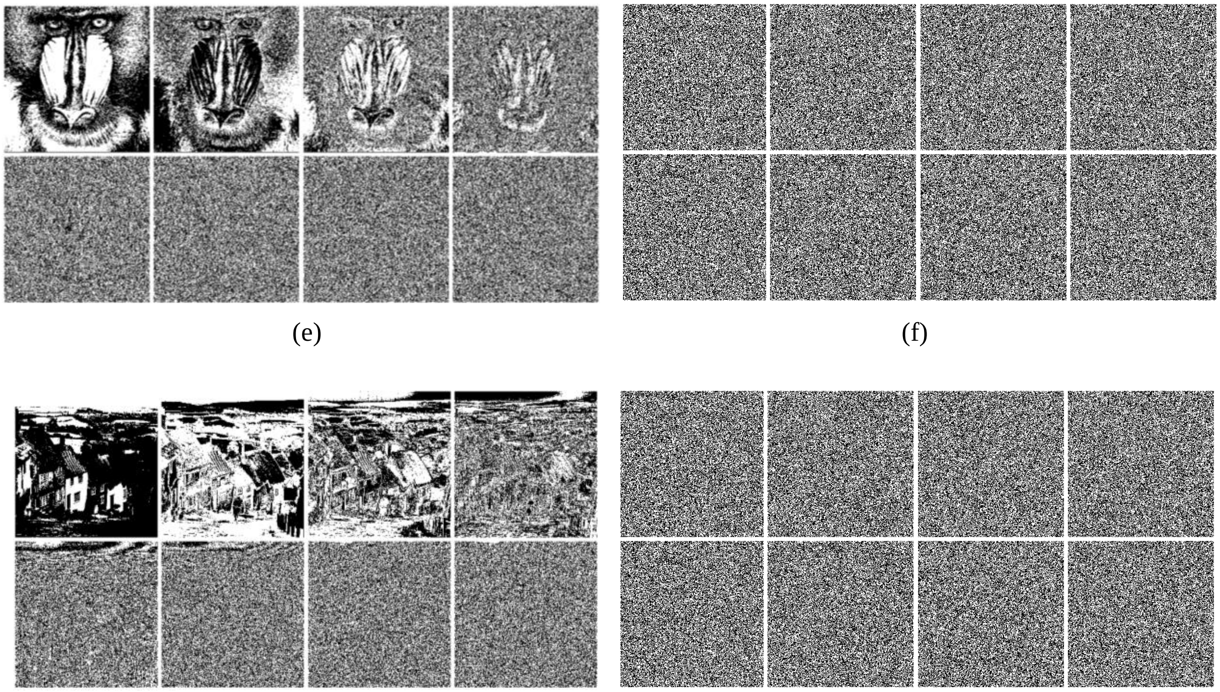
(e) Baboon (f) Encrypted Baboon (g) Goldhill (h) Encrypted Goldhill

Fig.4 The original images and the corresponding encrypted images



(a) (b)

(c) (d)



(e) (f)

(g) (h)

Fig.5 The bit-plane decomposition of original and corresponding encrypted (a) Lena (b) Pepper (c) Baboon (d) Goldhill

4.1 Perceptual Security Analysis

PSNR is the ratio between the maximum possible power and the noise corrupted power that affects the quality of representation. It checks the changes in the pixel value between the original and the enciphered image. Mathematically, it can be expressed as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}$$

and $$MSE = \frac{\sum_{i-1}^{W}\sum_{j-1}^{H} x_{i,j} - y_{i,j}}{W \times H}$$

Where *x* and y denote the original and encrypted image respectively. The obtained low PSNR (less than 10dB) of the encrypted images indicate the effectiveness of the proposed cryptosystem. Table 1 shows PSNR performance for different encrypted images.

Table 1: PSNR performance

Images	Lena	Pepper	Baboon	Goldhill
PSNR Value	8.4326	8.4424	9.6180	9.6180

4.2 Statistical Analysis

Statistical analysis is fundamental to all experiments that use statistics. Here, different statistical methods have been used to compare the results between original and the encrypted image such as histogram, correlation coefficient, entropy and PSNR.

4.2.1 Histogram Analysis

Histogram shows the pixel distribution of the image and it can be easily determined by seeing original image and encrypted image that there are no similarities between the pixel distributions. Figure 6 represents the histogram analysis of different original image as well as their corresponding encrypted image. An effective cryptosystem provides the uniform distribution of cipher elements. In the proposed scheme, we have obtained roughly uniformly distributed histogram so it prevents the statistical based cryptographic attacks.

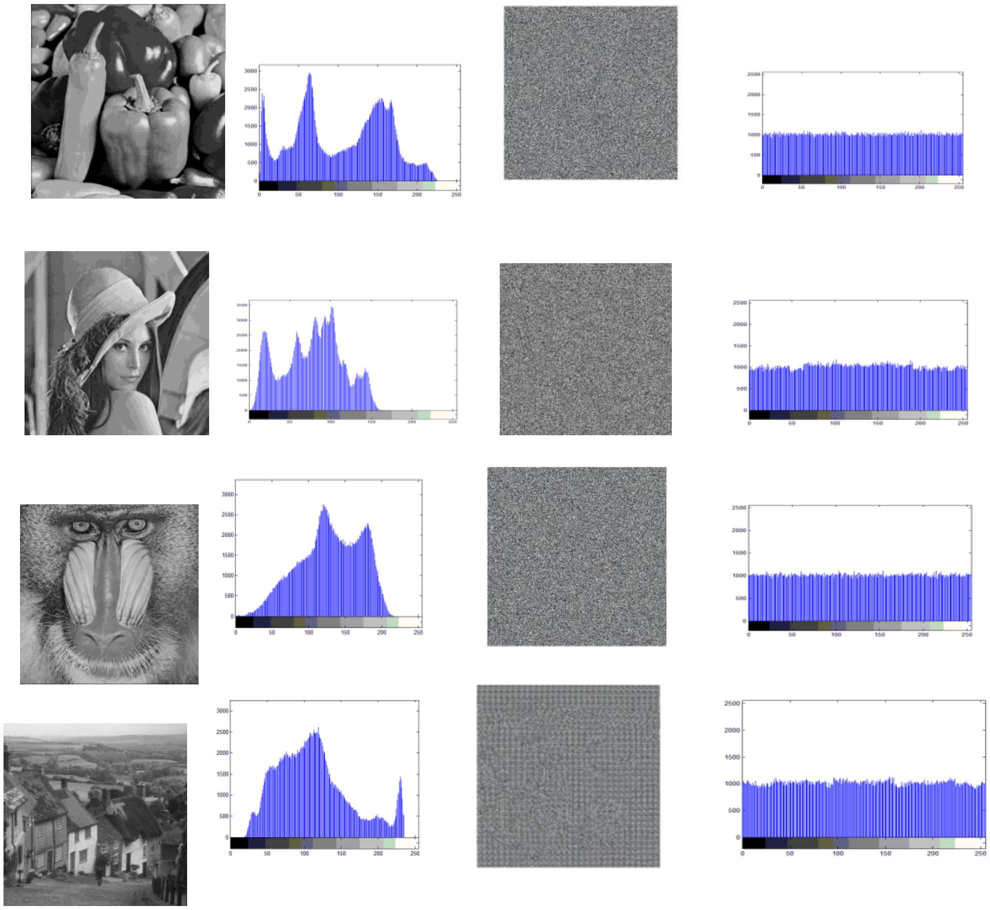


Fig. 6 Histogram of original image and corresponding encrypted image

4.2.2. Correlation Analysis

The correlation analysis is also another kind of statistical measurement tools to shown the effectiveness of the image encryption process. In digital image, each pixel is not independent of other pixels, but has some significant correlation. A standard image algorithm provides correlation coefficient close to zero for encrypted image. The correlation coefficient, horizontal coefficient (HC), vertical coefficient (VC) and diagonal coefficient (DC) are given by:

$$r_{x,y} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where,

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j\right)\left(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j\right)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j\right)^2$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j\right)^2$$

The horizontal, vertical and diagonal distribution of original pepper image, original Lena image, original Baboon, original Goldhill image and their corresponding encrypted image are presented in figures 7-30. The correlation coefficients relation as shown for the plots of encrypted images are found competently destroyed. We have also compared the obtained correlation coefficients for Lena and Pepper with some existing related schemes. The proposed scheme provides superior results for most of the cases.

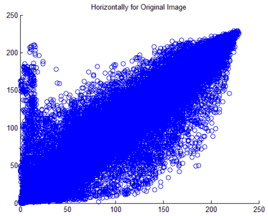


Fig.7 Horizontal _original Pepper image

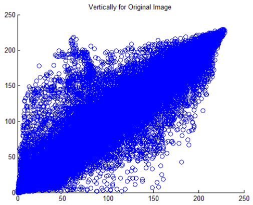


Fig.8 Vertical _original Pepper image

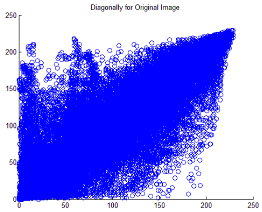


Fig.9 Diagonal_original Pepper image

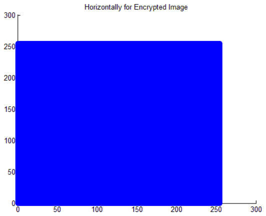


Fig.10 Horizontal_ encrypted Pepper image

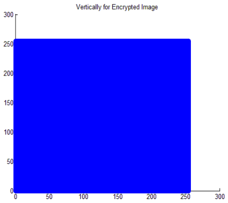


Fig.11 Vertical_encrypted Pepper ir

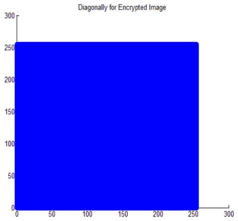


Fig.12 Diagonal _encrypted Pepper image

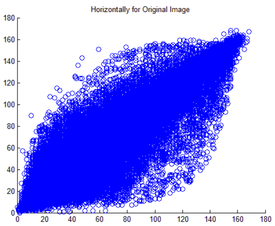


Fig.13 Horizontal_original Lena image

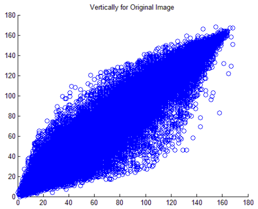


Fig.14 Vertical_original Lena image

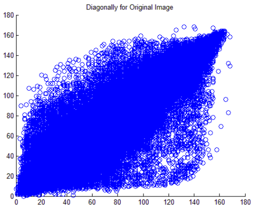


Fig.15 Diagonal_original Lena image

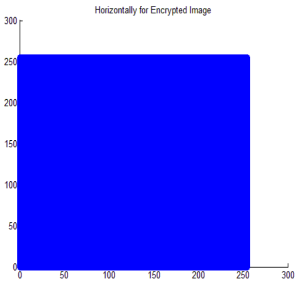


Fig.16 Horizontal _ encrypted Lena image

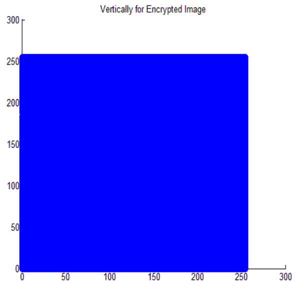


Fig.17 Vertical_encrypted Lena image

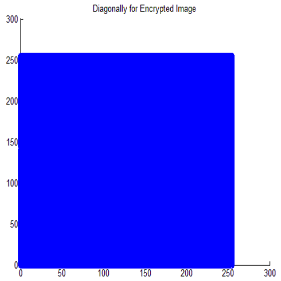


Fig.18 Diagonal_encrypted Lena image

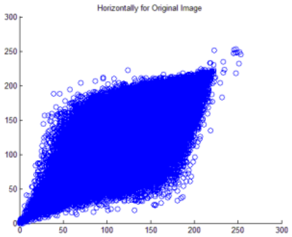


Fig.19 Horizontal_original Baboon image

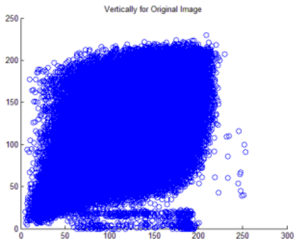


Fig.20 Vertical_original Baboon image

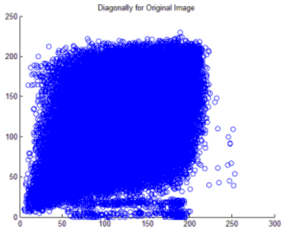


Fig.21 Diagonal_original Baboon image

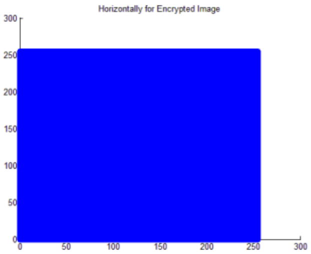


Fig.22 Horizontal_encrypted Baboon image

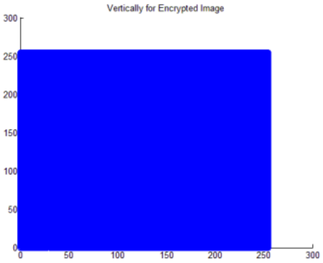


Fig.23 Vertical_encrypted Baboon image

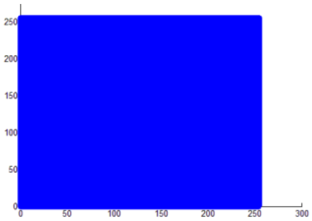


Fig.24 Diagonal_encrypted Baboon image

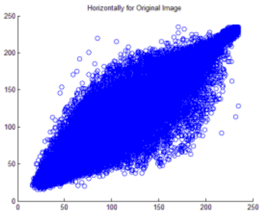


Fig.25 Horizontal_original Goldhill image

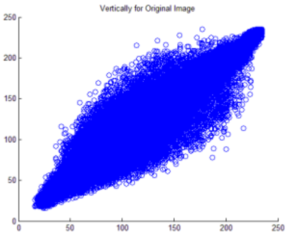


Fig.26 Vertical_original Goldhill image

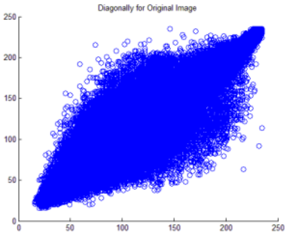


Fig.27 Diagonal_original Goldhill image

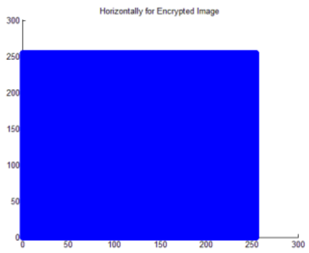


Fig.28 Horizontal_encrypted Goldhill image

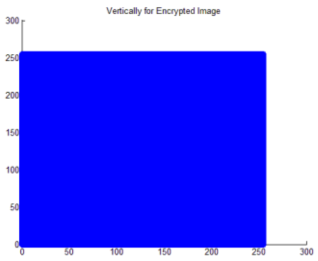


Fig.29 Vertical_encrypted Goldhill image

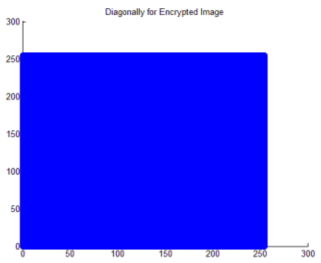


Fig.30 Diagonal_encrypted Goldhill image

Table 2: Correlation Coefficient performance image

Image	Metrics	Proposed Method	P.Praveenkumar et al. [16]	Xu et al. [15]	Paul et al. [29]
Lena	Horizontal	-0.0017	0.0072	-0.0230	0.0056
	Vertical	1.1207e-004	0.0007	0.0019	0.0920
	Diagonal	0.0026	0.0052	-0.0034	0.0749
	Average	0.0003	0.0043	-0.0081	0.0824
Pepper	Horizontal	6.4744e-004	0.0021	---	---
	Vertical	-8.8351e-005	0.0082	---	---
	Diagonal	-8.3164e-004	0.0038	---	---
	Average	4.9333e-004	0.0047	---	---

4.2.3. Entropy Analysis

Entropy is used to measure the randomness of an encrypted image. It is calculated for each pixel pposition. Mathematically, It can be defined as:

$$Entropy = \sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$$

Where, n represents the gray scale values of *p(x)* holds the pixel value from the histogram. The total randomness of the encrypted image is indicated when its value to close to 8. The entropy value for the proposed scheme is 7.9993 for encrypted pepper image and 7.9992 for the encrypted Lena image. Table 3. Shows the entropy analysis of the different images and also compared to show the effectiveness of the propoesd work.

Table 3: Entropy of the proposed method with the other literature for Lena image

Metrics	Image	Proposed method	P.Praveenkumar et al. [16]	Xu et al. [15]	Loukhaoukha et al. [30]
	Lena	7.9992	7.9974	7.9974	7.9968

Entropy	Pepper	7.9992	7.9975	7.9973	---
	Baboon	7.9980	---	---	7.9974

4.4 Key Space Analysis

In security analysis, the key space is the total number of keys that can be used for encryption procedure. The brute force attacks of any cryptosystem become infeasible when the key space is large enough. In the proposed scheme, the key is taken of 256 bits, therefore total key space is of 2^{256} bits. Xu et al. [15] suggested that the key space should be at least 2^{100} for ensuring the sufficient security level against brute-force attacks. So the 256 bits binary key of the proposed scheme is sufficient to protect the cryptographic brute force attacks.

5. Conclusions

In this paper, the proposed image cryptosystem is effective in producing high quality encrypted image. As we have dicussed earlier, key of small size is manipulated and generated through VCS algorithm. Therefore, it is highly secured and prevent from various cryptographic attacks. In this scheme, the key of size 256 bits is adequate to protect the secrecy of the gray scale image. The expermental results of our proposed scheme validates the effectiveness of the encryption algorithm and the scheme is also comparebale to some related existing schemes.

References

[1] R.Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Image Processing, Proceedings International Conference on, Thessaloniki, 2001, pp. 1019-1022 vol.3.
[2] D. Caragata, S.E. Assad, and M.Luduena, "An improved fragile watermarking algorithm for JPEG images", AEU-International Journal of Electronics and Communications 69.12 (2015): 1783-1794.
[3] X. Y. Wang et al. "A Blind Robust Digital Watermarking Using Invariant Exponent Moments." AEU- International Journal of Electronics and Communications (2016).
[4] "Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.
[5] L. Chen et al. "A new optical image cryptosystem based on two-beam coherent superposition and unequal modulus decomposition", Optics & Laser Technology 78 (2016): 167-174.
[6] X. Ge et al. "Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version." Physics Letters A 375.5 (2011): 908-913.
[7] A. V. Diaconu, "Circular inter–intra pixels bit-level permutation and chaos-based image encryption."Information Sciences (2015).
[8] X. Wang and H. Zhang. "A color image encryption with heterogeneous bit-permutation and correlated chaos" Optics Communications 342 (2015): 51-60.
[9] J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim, "Optical image encryption based on XOR Operations", Opt. Eng., Vol. 38, No. 1, 1999, pp. 47–54.
[10] M. Podesser, H. Schmidt and A.Uhl ,"Selective bitplane encryption for secure transmission of image data in mobile environments", The 5th Nordic Signal Processing Symposium—NORSIG-2002, 2002, pp. 1037.
[11]D. Moon, Y. Chung, S.B. Pan, K. Moon and K. Chung, "An efficient selective encryption of fingerprint images for embedded processors", Electron. Telecommun. Res. Inst. J., Vol. 28, No. 4 , 2006, pp. 444–452.
[12] Y.Zhou, K. Panetta, S. Agaian and C.Chen,"Image encryption using p-Fibonacci transform and decomposition", Opt. Commun., Vol. 285, No. 5 ,2012, pp. 594–608.
[13] Y.Zhou, K.Panetta, S. Agaian and C.Chen,"(n, k, p)-Gray code for image systems", IEEE Trans. Cybern., Vol. 43, No. 2, 2013, pp. 515–529.
[14] Y.Zhou, W. Cao, and C.Chen, "Image encryption using binary bitplane",Signal Processing, Vol. 100, 2014, pp 197-207
[15] L. Xu, Z. Li, J. Li and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps", Optics and Lasers in Engineering, Vol. 78, 2015, pp 17-25.

[16]P. Praveenkumar, et al. “Pixel scattering matrix formalism for image encryption—A key scheduled substitution and diffusion approach”, AEU - International Journal of Electronics andCommunications, Vol. 69, No. 2, 2015, pp. 562-572.
[17]C. Fu, et al. “A novel chaos-based bit-level permutation scheme for digital image encryption.”, Optics communications ,vol.284.23, 2011,pp. 5415-5423.
[18] Z.Tang, et al. “Multiple-image encryption with bit-plane decomposition and chaotic maps”, Optics and Lasers in Engineering, vol.80, 2016, pp.1-11.
[19] W. Zhang, et al. “Image encryption based on three-dimensional bit matrix permutation.”, Signal Processing vol.118,2016,pp.36-50.
[20] G. Ye and K. Wong “An efficient chaotic image encryption algorithm based on a generalized Arnold map Nonlinear”, Dyn, vol.69 (4) ,2012, pp. 2079–2087.
[21] S.You, Y. Lu, W.Zhang, B. Yang, R. Peng, and S. Zhuang, “Micro-lens array based 3-D color image encryption using the combination of gravity model and Arnold Transform”, Optics Communications, Vol.355, No.15, 2015,pp. 419-426.
[22] Y.Zhang and D. Xiao. “An image encryption scheme based on rotation matrix bit-level permutation and block diffusion.”, Communications in Nonlinear Science and Numerical Simulation ,vol.19.1 ,2014,pp. 74-82.
[23] P. Li, et al. “Sharing more information in gray visual cryptography scheme”, Journal of Visual Communication and Image Representation ,vol.24.8 ,2013,pp.1380-1393.
[24] S. Zhou, et al. “Encryption method based on a new secret key algorithm for color images.”, AEU-International Journal of Electronics and Communications ,vol.70.1 2016,pp 1-7.
[25] D. Ou, W. Sun, and X.Wu, “Non-expansible XOR-based visual cryptography scheme with meaningful shares”, Signal Processing, Vol. 108, 2015, pp.604-621.
[26] M. Naor, and A. Shamir, “Visual cryptography, in: Advances in Cryptology”, EUROCRYPT’94, Springer, 1995, pp. 1–12.
[27] A.J. Paul, P. Mythili, and J.K. Paulose, “Matrix based cryptographic procedure for efficient encryption”, IEEE recent advances in international communication system (RAICS) ,2011, pp. 173–177.
[28]K. Loukhaoukha, J.Y. Chouinard, and Berdai A “ A secure image encryption algorithm based on Rubik's cube principle”, J Electr Comput Eng, Vol.1.,2012, pp. 3.