ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Security for an Image using Bit-slice Rotation Method–image Encryption

R. Vijayaraghavan, S. Sathya and N. R. Raajan

Department of Electronics & Communication Engineering, School of Electrical & Electronics Communication,
SASTRA University, Thanjavur, Tamil Nadu- 613401, India; ragavtanjore@gmail.com,
sathyaa43@gmail.com, nrraajan@ece.sastra.edu

Abstract

Image encryption plays a major role in information security. It is mainly used to convert the original image into another form. In this work, we propose a bit plane slicing of digital image to provide the more security. The main aim of BPS is used to divide the digital image into 8 bit planes. The bit plane is further rotated in order to provide better encrypted image and to make hacking more difficult. It focuses on two techniques such as bit plane slicing and image rotation for efficient image encryption. The classification of bit plane is used for analyzing the importance played by each bit of an image. It is used to estimate the each pixel of an image. The proposed technique involves rotation of bit planes is employed to make highly secure image encryption. By this method scrambling of an image is based on efficient technique even it is intercepted, the information cannot be understood. It is mainly useful for image compression because it exhibits high coding efficiency. This method which makes the decryption of an image more difficult compared to other techniques.

Keywords: Bit Plane Slicing, Image Encryption, Rotation, Scrambling

1. Introduction

Cryptography is an efficient method of transferring information in a secure way. It scrambles the image before transmitting in order to change the structure of an image. Even the attacker cannot able to hack because it is difficult for him to retrieve the original image. It only provides the modified form of an image but it does not hide the image even though it is better secure method. The main intention is to provide better protection of the original image. Bit plane slicing is mainly used for splitting images into binary planes[1]. Each bit is used to represent the intensity of each pixel of an image. Image scrambling is always based on pixel values of an image. The digital image is divided into 8 bit planes because it is useful for analyzing the importance of each bit in an image. Whereas a small change in color affect bit value of an image[2]. The color image is composed of many pixels is decomposed into 8 bit planes. It is used to represent the highest order and lower order bits to specify the contribution of each bit in an image. It achieves better image encryption than the other least significant bit, perceptual masking technique. This process is done on without changing the overall image quality.

2. Survey

Many image encryption algorithms have been developed for protection of images. Salleh[3] has introduced symmetric key encryption based on chaos. It is used for any size of an image and it does not consider weak keys. It depends on three functions such as horizontal vertical transformation function, gray scale and shift function. Belkhouche[4] performs pixel value permutation for binary image encryption. The occurrence of several keys such as initial state, number of iterations and external state are used for binary image protection and it results in a fast calculation for implementation in real time. Krikor[5] introduced a new method for encryption based on specific higher frequencies of DCT coefficients. Here the 8 × 8 image block is transformed using DCT and it relates to higher frequencies of an image which are encrypted and it produces a stream cipher. It results in better security because the human eye is not sensitive to higher

**Author for correspondence*

frequencies. Gu[6] presented a method as both permutation and substitution for secure encryption algorithm. Here the image is divided into bit planes and it is encrypted individually. Each encrypted bit plane involves two processes such as first bit positions are permitted using chaotic ergodic matrices. Finally bit values are substituted using binary chaotic pseudorandom sequences. This returns in strong encryption algorithm and it is secure. Maniccam and Bourbakis[7] presented an algorithm based on SCAN methodology. It is applicable for both binary and grayscale images. This scan pattern is employed for encryption and compression schemes. Mohammad Younes and Jantan[8] proposed an image encryption using both permutation and RijinDael algorithm. This is used to reduce the correlation among the pixels of an image. By applying the above algorithm on permuted image for encryption. Indrakanti and Avadhani[9] presented an algorithm based on three phases such as image encryption, key generation and identification. Using random pixel permutation, it employs a confidentiality of an image.

3. Methods

Consider a color image which is composed of a number of pixels. Each pixel is represented in terms of bits. The image consists of 8 bit planes[10] from plane 1 to plane 8. Plane 8 contains all lowest order bits and plane 1 constitutes all higher order bits in an image.

The slices of the 8 planes contain the information of an image[11]. While we modify the positions, values and more it will result a scrambled output.

Consider 3 × 3 matrix contains image pixels as

160	162	164
166	168	170
172	172	176

The binary values for above pixel value are shown in 8 bit representation

10100000	10100010	10100100
10100110	10101000	10101010
10101010	10101110	10110000

Bit plane is used to exhibit the significant information of an image. It is composed of 8 bit planes In above example LSB bits of a binary form constitute lowest order bits and MSB bits represent high order bits of all the pixels in an image. The concept of bit plane slicing is to determine whether the image contains noise or significant information in terms of bit plane. When the replacement of MSB bit is done it causes more distortion than LSB bits[12]. It is easy to encode less significant bits and it is essential to preserve the most significant bits.

3.1 Bit Plane Slicing

Bit plane slicing is used to slice the image into different bit planes[13]. It is composed into higher order and lower order bits. MSB has the significant addition to the total image it contributes the majority of the information of an image. LSB contributes only less details of an image. It plays a major role in image processing and compression. The major influence of this method is used to furnish the essential of each bit of an image. It also ensures the

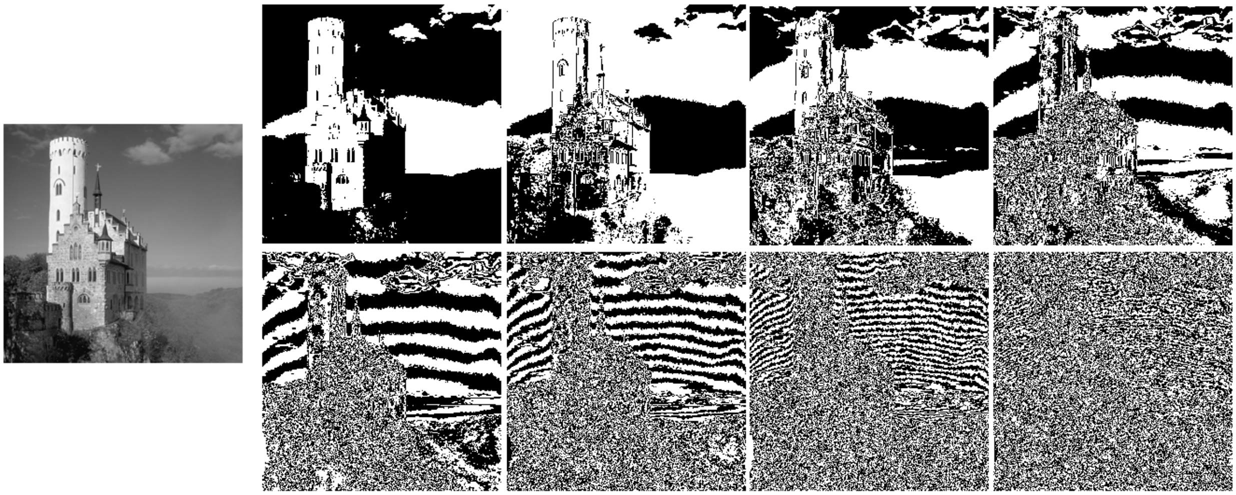

Figure 1. Information on 8 bit planes.

beneficence of specific pieces. Bit plane is mainly possessed of many layers where each layer exhibits the specific range of bit planes in an image. Level of security also depends on the number of bit planes used to decompose the image. Loss of higher order bit planes leads to much darker image therefore MSB is most essential in bit plane slicing. Encrypting the less significant bit will result in degrading the image quality slightly than encrypting in the most significant bit its cause more degradation. Encryption is done for each three individual color planes according to a bit plane slicing method.

3.2 Bit Rotation

The simple method to provide image encryption is a rotation of bit planes. It is more effective than the other method as bit shifting. After the image is decomposed into the bit plane and then applied the rotation on each of the bit planes in different angles. Rotation of bit planes is rearranged to provide the original bit plane of an image at the receiver end. The rotation of a bit plane is processed at different angles such as 90, 180, 270 in order to make image encryption to be more difficult. It is difficult for an attacker to retrieve the image without knowing what type of technique is employed. This includes the rotated form of a bit planes in order to make the transformed shape of an image. The important information of an image is extracted using bit plane slicing.

Bit rotation is applied after bit plane slicing according to a various angle in 8 bit planes. Each pixel of planes is rotated by the different angle in order to provide an encrypted image. A rotation of planes does not lose any bits. This technique is obtained by rotation of bits[14] in high dimensional space. Finally all the rotated bit planes are combined to generate an original bit plane. By using this method the original image can be retrieved without any loss of information. This work describes about the image encryption that uses both the rotation of bits combined with various degrees of rotations used as a secret key that operates on an image. This encryption is getting by providing a rotation angle for the 8 bit planes. Repeating these steps for every bit planes it gives an encrypted image. The result reveals that this encryption achieves better security than the other approaches.

4. Implementation

In this work we proposed a method for encryption and decryption based on bit plane slicing in which image is divided into bit planes. It is rotated at different angles to form the encrypted image. This enhances the robustness of the encryption of an image. The original image is retrieved by again using bit plane slicing and a rotation of bits. Combining bit plane slicing and rotation added as a layer of security to protect an image. The retrieved image will have exactly the same pixel value as the original image. By this method encrypted image is unrecognizable and scrambling is done. Increasing the different technique will result in more secure encryption method.

Consider a 2 × 2 matrix contains pixel values of an image

$$\begin{bmatrix}160 & 172\\184 & 196\end{bmatrix}$$

The above pixels of an image is represented in binary form

$$\begin{bmatrix}10100000 & 10101100\\10111000 & 11000100\end{bmatrix}$$

It is divided into individual bit plane using the slicing method in order to provide better encryption. Each bit plane represents the significant information of an image. Here we show the bit planes as a matrix.

1st bitslice – $\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$ 2nd bitslice – $\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$

3rd bitslice – $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$ 4th bitslice – $\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}$

5th bitslice – $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$ 6th bitslice – $\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$

7th bitslice – $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$ 8th bitslice – $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$

The above bit plane is further rotated at different angles to make more difficult to decrypt

1st bit plane [Rotated by 90°] – $\begin{bmatrix}1 & 1\\1 & 1\end{bmatrix}$

2nd bit plane [Rotated by 180°] – $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$

3rd bit plane [Rotated by 270°] – $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$

4th bit plane [Rotated by 90°] – $\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$

5th bit plane [Rotated by 180°] – $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$

6th bit plane [rotated by 270°] – $\begin{bmatrix}0 & 0\\1 & 1\end{bmatrix}$

7th bit plane [Rotated by 90°] – $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

8th bit plane [rotated by 180°] – $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

After a bit rotation a new pixel value is obtained that is ciphered. The cipher image is created by combining each bit from eight pixels of an image. It is further represented in decimal form of an image.

$$\begin{bmatrix} 11100000 & 10101100 \\ 10100000 & 10011100 \end{bmatrix}$$

Encrypted 2 × 2 matrix contains image pixels as

$$\begin{bmatrix} 224 & 172 \\ 160 & 156 \end{bmatrix}$$

The decryption process is done as the reverse of the above method. Pixels of an image are represented in binary form as follows

$$\begin{bmatrix} 11100000 & 10101100 \\ 10100000 & 10011100 \end{bmatrix}$$

The above cipher image is decrypted by splitting eight bits into individual bit planes in the form of 2 × 2 matrix.

1st bit plane [Rotate it by 270°] – $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

2nd bit plane [Rotate it by 180°] – $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

3rd bit plane [Rotate it by 90°] – $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

4th bit plane [Rotate it by 270°] – $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

5th bit plane [Rotate it by 180°] – $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

6th bit plane [Rotate it by 90°] – $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$

7th bit plane [Rotate it by 270°] – $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

8th bit plane [Rotate it by 90°] – $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

The process is done by taking each first bit from the every 8 bit planes which form 2 × 2 images it is repeated for the entire second to eight bits it is formed into 8 bit planes by combining every first bit of all 2 × 2 images and second bit, the third bit repeatedly up to the eighth bit from all matrices. It is exploited in binary form

$$\begin{bmatrix} 10100000 & 10101100 \\ 10111000 & 11000100 \end{bmatrix}$$

The decimal form of an above image is obtained by doing bit plane slicing and bit rotation. The original image is finally decrypted using different methods.

$$\begin{bmatrix} 160 & 172 \\ 184 & 196 \end{bmatrix}$$

5. Results

Figure 4. (a) Input image Lenna (b) R-plane histogram of the input image (c) G-plane histogram of the input image (d) B -plane histogram of the input image (e) encrypted image Lenna (f) R-plane histogram of encrypted image (g) G-plane histogram of encrypted image (h) B-channel histogram of encrypted image.

5.1 Histogram

The histogram is used to indicate the pixel representation of an image. It is represented in terms of bar charts, pie charts and line graphs and data index. Histogram results are used for statistical analysis of a cryptosystem. Generally results obtained according to higher frequencies, lower frequencies and middle frequencies in that particular frequency information is accumulated. It is also used to resist against any type of attack. In addition to histogram several measurements are available for analysis of images. A measure of image quality is required for restoration of images.

5.2 Peak Signal to Noise Ratio (PSNR)

PSNR indicates a measurement between the original and decrypted image. It reduces the correlation between the original and encrypted image. Lower PSNR indicates the decrypted image is not retrieved same as the original image. Mean Square Error is used to measure the image compression quality. It is indirectly proportional to the PSNR which is a sum of the squared value between the original and the reconstructed image divided by the total size of an image. It is used for quality assessment based on error sensitivity.

$$\mathrm{W(I,\ n)} - \mathrm{j((I,\ n))}^2$$

$$\frac{PSNR = 10\log_{10} \times \mathrm{Maximum}^2}{\mathrm{MSE}}$$

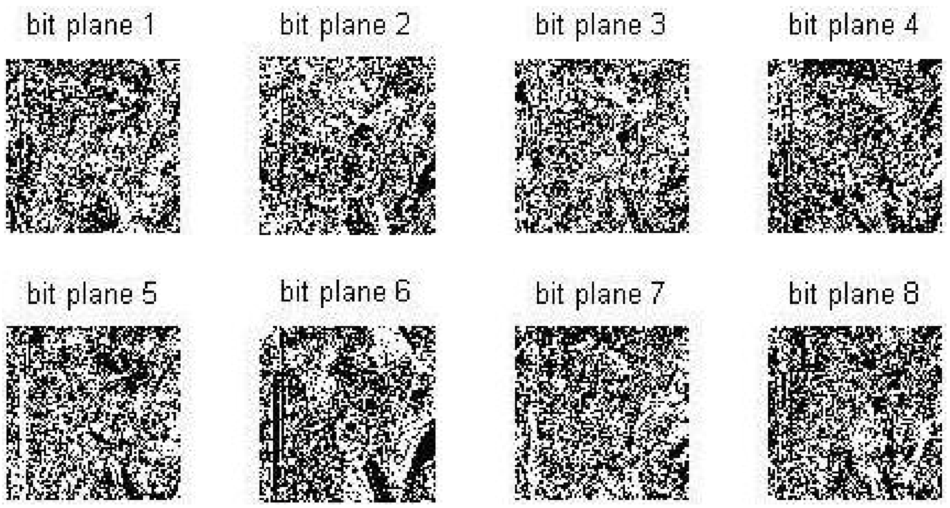

Figure 2. Bit slices of an Original Image.

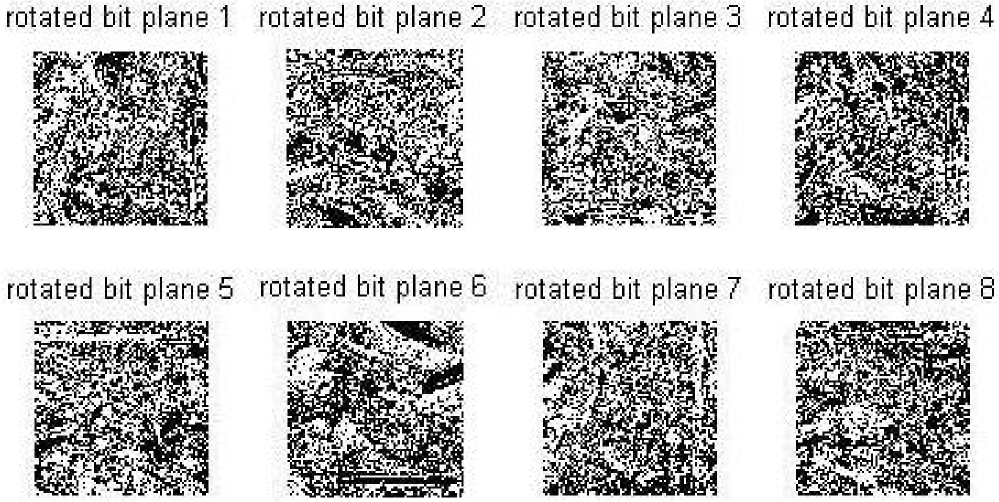

Figure 3. Images of rotated bit slices.

5.3 SSIM

Structural Similarity Index Measure is used to measure the similarity between two images. It results in correct assessments of an image compared to PSNR and MSE. It is used for the extraction of structural information from an image.

$$SSIM(w,r)=[l(w,r)]^{\alpha}[c(w,r)]^{\beta}[s(w,r)]^{\gamma}$$

$$MSSIM(w,r)=\left(\frac{1}{P}\right)\sum_{k=1}^{P}(w_k,r_k)$$

6. Comparison with Existing Methods

Encryption of color images is mostly done using bit plane methods. In lossless encryption methods, bit plane is considered as key image which is obtained from another image. The process is done as where image is converted into bit planes and XOR is carried out to invert the order of the bit planes and using BitplaneCrypt algorithm. But it does not provide much security because security key is needed to generate the key image in decryption. In another method, selective bit plane encryption is considered to encrypt an image. Each bit plane is placed in the position of pixels of an image. Only MSB or LSB subset of bit planes is chosen for Selective Encryption. It results in less processing time or power but the limitation is it provides less security than the full encryption method. In Truncated P-Fibonacci code where the image is divided into several bit planes using different P values. It results in more key space for security. Here two biplane decomposition has been

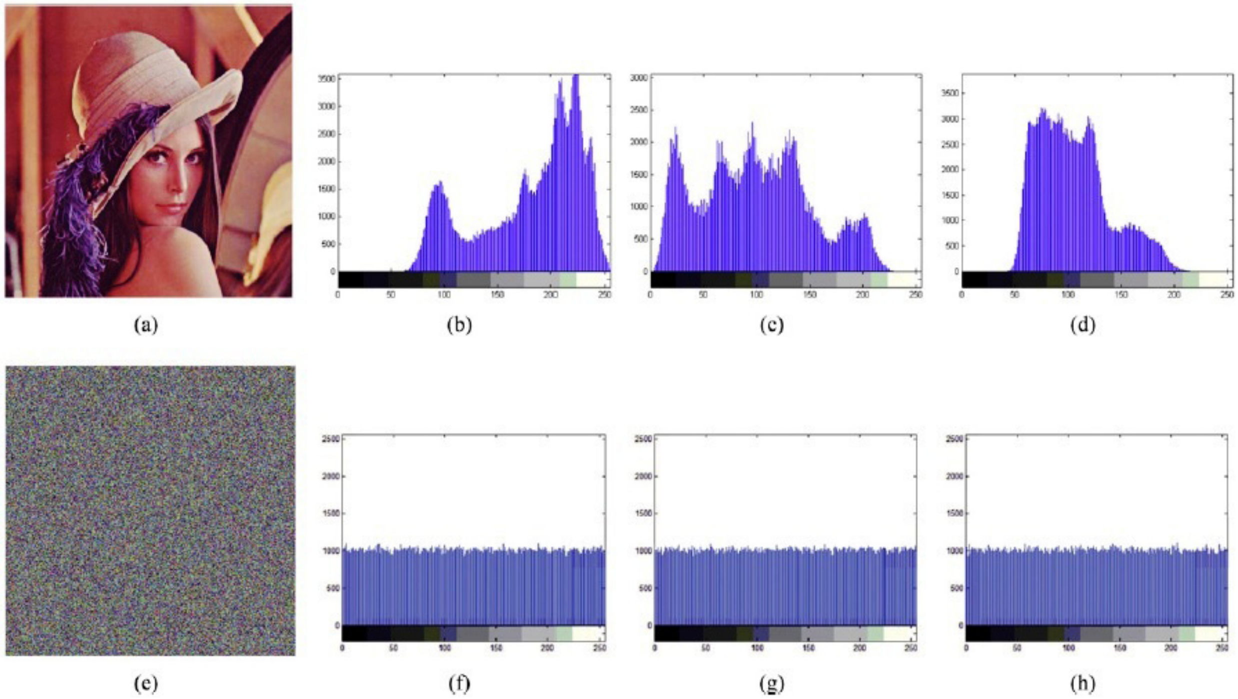

Figure 4. (a) Input image Lenna (b) R-plane histogram of the input image (c) G-plane histogram of the input image (d) B-plane histogram of the input image (e) encrypted image Lenna (f) R-plane histogram of encrypted image (g) G-plane histogram of encrypted image (h) B-channel histogram of encrypted image.

Table 1. Tabulation for Encrypted Image

Name	MSE (r)	MSE (g)	MSE (b)	PSNR (r)	PSNR (g)	PSNR (b)	MSSIM
Pears.png	1370	1342	1381	16.76	16.85	16.72	0.0132
Autumn.tif	1422	1447	1429	16.60	16.52	16.58	0.0120
Football.jpg	1478	1501	1489	16.43	16.36	16.40	0.0152

Table 2. Tabulation for Decrypted Image

Name	MSE (r)	MSE (g)	MSE (b)	PSNR (r)	PSNR (g)	PSNR (b)	MSSIM
Pears.png	0.0	0.0	0.0	.Inf	.Inf	.Inf	1
Autumn.tif	0.0	0.0	0.0	.Inf	.Inf	.Inf	1
Football.jpg	0.0	0.0	0.0	.Inf	.Inf	.Inf	1

considered as TPFB and binary bitplane decomposition for source images and original image. Scrambling algorithm is used to modify the pixel location of an image but there is a need to know the security key for decryption of an image. All these algorithms tend to result in limited key space and it decomposition result will be predictable. In our proposed concept we divide an image into bit planes and it is rotated at various angles to make an encrypted image. Our proposed method increases a security level of an image than the other approaches because of employing both bit plane slicing and rotation of an image which also increases the robustness against brute force attacks.

7. Conclusion

In this work, bit plane slicing and rotation of the bits is combined into one secure algorithm. This method may not be more secure but it is difficult to decrypt. To achieve this goal we design a scrambling method using bit plane rotation with the help of bit plane slicing. The performance of this method is measured by using MSE and PSNR values. The decryption of an image is robust because it does not lose any data. Bit plane slicing preserves the significant information of degraded image. Image encryption based on bit plane slicing and rotation can improve significantly the level of security. The results show that it provides a better level of encryption without affecting the overall image quality. Thus the mode such as bit rotation used for efficient encryption requirements it is applicable for any type of image formats. The experimental results show that the proposed scheme leads to an improved security level and its proved in terms of HISTOGRAM, MSE, PSNR and MSSIM parameters.

8. References

1. Vijayaraghavan R, Sathya S, Raajan NR. Encryption for an image using circular budge on bit-planes. Int J Appl Eng Res. 2014; 9(2):153–60.
2. Vijayaraghavan R, Sowmiya P, Manochitra G, Raajan NR. Analysis of acute lymphoblastic lukemia using cluster based image processing approach. Int J Appl Eng Res. 2014; 9(2):223–30.
3. Salleh M, Ibrahim S, Isnin IF. Image encryption algorithm based on chaotic mapping. Jurnal Teknologi. 2003;39(D):1–12.
4. Belkhouche F, Qidwai U, Gokcen I, Joachim D. Binary image transformation using two-dimensional chaotic maps. Proceedings of the 17th International Conference on Pattern Recognition, ICPR; 2004. p. 823–26 .
5. Krikor L, Baba S, Arif T. Image encryption using dct and stream cipher. Eur J Sci Res . 2009; 32(1):48–58.
6. Gu G, Han G. An image encryption scheme based on chaotic systems. Innovative Computing, Information and Control. 2006; 1:492–95.
7. Yukthi.BR, Savitha AP, Anandaraju MB, Nuthan AC. FPGA based implementation of image encryption using scan patterns and carrier images. International Journal of Science and Modern Engineering. 2013; 1(7).
8. Younes MAB, Jantan A. Image encryption using block-based transformation algorithm. IAENG International Journal of Computer Science. 35:1.
9. Indrakanti SP, Avadhani PS. Permutation based image encryption technique. Int J Comput Appl Tech. 2011; 28(8):45–7.
10. Zhang W, Wong K, Yu H, Zhu Z. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Comm Nonlinear Sci Numer Simulat. 2013; 18(3):584–600.
11. Wei Z, Kwok-Wo W, Yu H, Zhi-Liang Z. An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion. Optics Commun. 2012; 285(9): 2343–54.
12. Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recogn. 2004;37:469–74.
13. Wadhwani AK, Wadhwani S, Yadav P. Application of bit-plane slicing technique on medical image for feature extraction. Current Research in Engineering, Science and Technology (CREST) Journals. 2013; 1(4):110–16.
14. Li CQ, Li SJ, Alvarez G, Chen GR, Lo KT. Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. Physics Letters. Section A: General, Atomic and Solid State Physics. 2007; 369 (1–2):23–30.