A Symmetric Encryption Scheme for Colour BMP Images

Narendra K Pareek
University Computer Centre,
Vigyan Bhawan, Block-A,
M. L. Sukhadia University,
Udaipur (Raj.) India.

Vinod Patidar
School of Engineering,
Sir Padampat Singhania
University, Bhatewar,
Udaipur (Raj.) India.

Krishan K Sud
School of Engineering,
Sir Padampat Singhania
University, Bhatewar,
Udaipur (Raj.) India

ABSTRACT
In this paper, a new image encryption scheme for colour BMP images using a secret key of 120-bits is proposed. Initially, image is divided into blocks subsequently into color components. Each color component is modified by performing bitwise operation which depends on secret key used in algorithm as well as a few most significant bits of its previous and next color component. Three rounds are taken to complete this process. To make cipher more robust, a feedback mechanism is applied by modifying the used secret key after encrypting each block. The propose scheme is simple, fast and sensitive to the secret key. Due to high order of substitution, common attacks like linear and differential cryptanalysis are infeasible. The experimental results show that the proposed encryption technique is efficient and has high security features.

Keywords
Encryption, Secret key, Substitution, Image cipher.

1. INTRODUCTION
Recently, with the high demand in digital signal transmission and big losses due to illegal data access, data security has become a critical and imperative issue. Encryption is being used to secure data and prevent them from unauthorized access. Due to certain characteristics of digital images- redundancy of data, strong correlation among adjacent pixel, less sensitive as compare to the text data, especially the bulk quantity of data and the requirement of real-time processing, traditional ciphers such as DES, AES, RSA etc. are not suitable for image encryption. In order to protect digital images from unauthorized users doing illegal reproduction and modifications, a variety of image encryption schemes have been proposed. The various ideas used in the existing image encryption techniques can be classified into three major types: position permutation [1,2,7,10], value transformation [3,4,8,12] and the combination form [5,6,9,11,13]. The position permutation algorithms scramble the data position within the image itself and usually have low security. On the other hand, the value transformation algorithms transform the data value of the original signal and have the potential of low computational complexity and low hardware cost. Finally, the combination forms perform both position permutation and value transformation and usually have the potential of high security. In recent years, a number of different image encryption schemes have been proposed in order to overcome image encryption problems. A few image encryption techniques suggested recently are discussed in the following paragraph in brief.

In 2010, Yoon and Kim [7] developed a chaotic image cipher in which initially a small matrix is generated with logistic map then construct a large permutation matrix from generated small matrixes. The constructed permutation matrix is used to permute plain image pixels. Further, a new chaotic image cipher was suggested by Ismail et al [8] where they used two chaotic logistic maps and an external secret key of 104-bits size. The control parameters for both the chaotic logistic maps were generated through the external secret key. They also employed a feedback mechanism in their image cipher. In 2011, Jolfaei and Mirghadri [9] suggested a chaotic image cipher based on pixel shuffling using baker map and modified version of simplified AES (S-AES), developed by Musa et al. in 2003[14]. Further, Nayak et al. [10] proposed a chaotic image cipher using logistic map in which permutation of image pixels are made on the basis of index position of generated chaotic sequence. Sathishkumar and Bagan [11] suggested a chaotic image cipher based on pixel shuffling which is a combination of block permutation, pixel permutation and value transformation. Further, chaotic image cipher using two chaotic logistic maps and a secret key of 80-bits was suggested by Chen and Chang [12]. Recently, Indrakanti and Avadhani [13] developed a non-chaotic image encryption scheme and completed the encryption in three processes. In the first process, image is divided into four blocks and each image block is permuted using random numbers. The second process is the identification process which involves the numbering of shares generated from encrypted image and finally a key is generated which keep all information about encryption process.

In the available literature, most of the developed image encryption schemes are based on chaotic system. In this paper, a non-chaos based image encryption scheme using an external key of 120-bits is suggested. The proposed encryption scheme is based on pixel substitution. In pixel substitution, image is divided into block of colour components and each colour component is modified by exclusive-OR operation which depends on a few most significant bits of its previous colour component, next colour component and secret key used in the algorithm. The proposed encryption scheme requires less computation as we uses bitwise operations and highly sensitive to small changes in the secret key used in the algorithm. The scheme is simple, fast and secured against any attack. The rest of the paper is organized in the following manner. In section 2, various processes used in the proposed algorithm as well as the

detailed encryption algorithm is discussed. Simulation results and security analysis are provided in Section 3. Finally, the conclusions are drawn in Section 4.

2. PROPOSED ENCRYPTION ALGORITHM

Two different types of key mixing processes, called as FKM and BKM, are used in the proposed algorithm. In both the processes, block is divided into sub-blocks (p_1,p_2..p_{15}) and each sub-block (p_i) is modified by using sub-key (k_i), its previous sub-block (p_{i-1}) and sub-block (p_i) itself. A similar process is used in the BKM process.

Forward key mixing (FKM) process

i=2
t=p_1, p_1= $p_1 \oplus k_1$
if (i<=15) then t1=p_i , $p_i = p_i \oplus k_i \oplus$ t, t=t1
else i=i+1
endif

Backward key mixing (BKM) process

i=14
t=p_{15}, p_{15}= $p_{15} \oplus k_{15}$
if (i >=1) then t1=p_i , $p_i = p_i \oplus k_i \oplus$ t, t=t1
else i=i-1
endif

In substitution process, simple bitwise operations are performed on pixels of sub-blocks to change their properties. Architecture of substitution process, used in the proposed system, is shown in the Fig (1) and its equivalent description is as follows:

1. Take a plain image block and divided it into fifteen equal sub-blocks named as p_1,p_2,p_3.....p_{15}.
2. set pos=5
3. set i=1, T_i=p_i
4. if (pos=5) then $p_i = p_i \oplus (k_j \bmod 15)$
5. bv=T_i >> pos
6. set i=i+1, T_i=p_i
7. perform operation on p_i as shown in Table (1)
8. if (i<=15) then go to step(5)
9. if (pos=6) then
   for (i=1;i<=15;i=i+1) k_i=$k_i \oplus p_i$
   j=j+1
   stop
   endif
10. if (pos=5) then perform BKM process
    else perform FKM process
    endif
11. pos=pos+1
12. go to step(3)

In the substitution process, image block to be modified is partitioned into fifteen equal sub-blocks (p_1,p_2..p_{15}) having 8-bits (b_1,b_2...b_8) each. Further, each sub-block passes through the following two steps. In this first step, first sub-block (p_1) is modified by xoring it with first sub-key (k_1) and remaining sub-blocks (p_2...p_{15}) are modified by applying the operation as shown in the Table (1). The operation, to be applied on each sub-block (p_i), depends on first three most significant bits ($b_1b_2b_3$) of their previous sub-block (p_{i-1}). For example, value of first two sub-blocks p_1 and p_2 are 225(11100001) and 173 (10101101) respectively. The value of sub-block (p_2), after applying operation on it corresponding to bits value 7 (111) of its previous sub-block (p_1), change to 41 (000101001). Further, BKM process, as discussed above, is applied on the resultant block. In the second step, resultant block received from the first step is processed again. In this step, first sub-block (p_1) remains unchanged and remaining sub-blocks (p_2...p_{15}) are modified by applying the operation as shown in the Table (1). The operation, to be applied on each sub-block (p_i), depends on first two most significant bits (b_1b_2) of their previous sub-block (p_{i-1}). For example, value of first two sub-blocks p_1 and p_2 are 225 (11100001) and 173 (10101101) respectively. The value of second sub-block (p_2), after applying the operation on it corresponding to bits value 3 (11) of its previous sub-block (p_1), change to 82 (01010010). Further, FKM process, as discussed above, is applied on the resultant block.

In the proposed system, the secret key is modified from the previously encrypted plain image block for processing the next block. This feedback mechanism is applied to avoid differential attack and to make the system more robust.

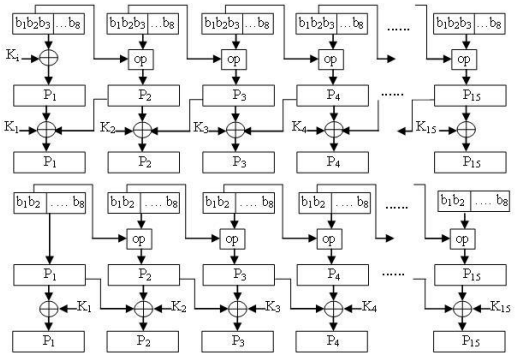

Fig 1 : Architecture of substitution process.

Table 1. Bits and their corresponding operations.

Bits value	Operation on sub block for encryption
0	p_i = Not (p_i) $\oplus$ (k_i mod 15)
1	p_i = Not ($p_i \oplus$ (k_i mod 15))
2	$p_i = p_i \oplus$ (k_i mod 15)
3	Invert all bits i.e. p_i = Not (p_i)
4	Circular left shift by one position i.e. $p_i = p_i$ <<1
5	Circular right shift by one position i.e. $p_i = p_i$ >>1
6	p_i = Not (circular left shift by one position)
7	p_i = Not (circular right shift by one position)

3. PERFORMANCE AND SECURITY ANALYSIS

An ideal image cipher should resist against all kinds of known attacks such as cryptanalytic, statistical and brute force attacks. In this section, we discuss the security analysis of the proposed image encryption scheme such as statistical analysis, sensitivity analysis etc to prove that the proposed image cipher is effective and secure against the most common attacks. The proposed algorithm has been implemented in C programming language. For the analysis of image data, we have used Matlab application tool.

3.1 Statistical analysis

In the literature, we found that most of the existing ciphers have been successfully cryptanalyzed with the help of statistical analysis. To prove the robustness of the proposed encryption scheme, statistical analysis has been performed which demonstrates its superior confusion and diffusion properties results in a strongly resisting nature against the statistical

attacks. This is done by testing the distribution of pixels of the ciphered images, study of correlation among the adjacent pixels in the ciphered image and the correlation between the plain and cipher images.

3.1.1 Distribution of pixels

We have analyzed the histograms of several cipher images and their corresponding plain images having widely different contents and sizes. One example of histogram analysis for well known image 'Baboon' is shown in Fig 2. Histograms of red, blue and green components of image (Fig 2(a)) are shown in Frames (b), (c) and (d) respectively. In Frames (f), (g) and (h) respectively, the histograms of red, blue and green components of the cipher image (Fig 2(e)) are shown. Comparing the histograms, we find that encryption process returns noisy images. Histograms of cipher images, approximated by uniform distribution, are quite different from that of the plain image and contain no statistical resemblance to the plain image. This is consistent with the perfect security defined by Shannon [15] and the proposed encryption scheme resists against the known-plaintext attack.

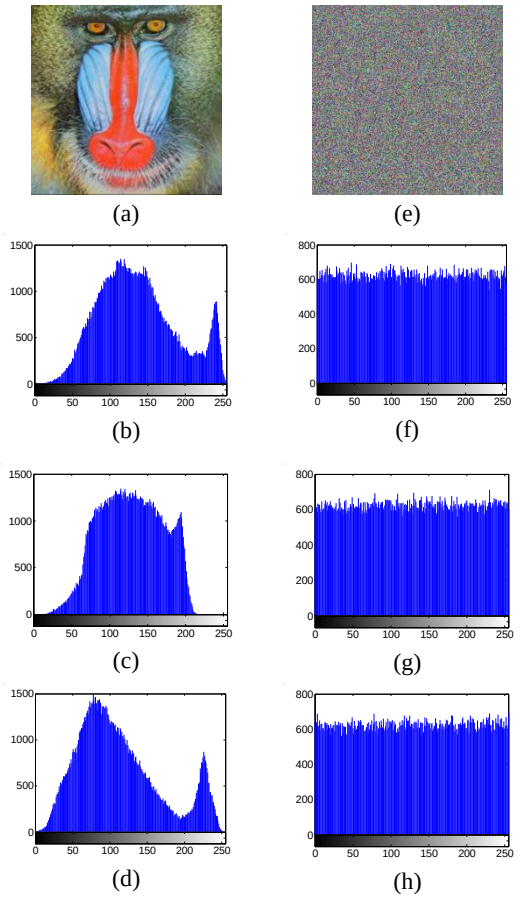

Fig 2 : Histograms corresponding to RGB components of plain image *'Baboon'* and its corresponding cipher image .

3.1.2 Correlation between plain and cipher images

We have also done extensive study of the correlation between pairs of plain image and their corresponding cipher image produced using the proposed encryption scheme by computing correlation coefficient between RGB components of the plain images and corresponding cipher images. Results for a few images are shown in Table 2. Since the correlation coefficients shown in the Table 2 are very small (C≈0), it indicates that the plain images and their corresponding cipher images are completely independent of each other.

Table 2. Correlation coefficient between plain images and their corresponding cipher images.

Image size	C_{RR}	C_{RB}	C_{RG}	C_{GR}	C_{GG}	C_{GB}	C_{BR}	C_{BG}	C_{BB}
200x200	0.012	0.032	0.019	-0.024	0.010	0.020	-0.022	0.015	0.020
512x512	0.025	0.016	-0.045	0.018	-0.011	0.026	0.022	0.026	0.026
512x768	-0.013	0.014	-0.025	0.010	0.026	0.026	-0.028	0.019	0.012
600x326	-0.020	0.029	0.016	0.029	0.018	0.027	0.024	-0.016	0.010
640x480	0.021	-0.018	0.022	-0.015	0.029	0.012	0.029	0.008	0.006
800x600	0.007	-0.017	0.019	0.003	0.008	0.019	-0.025	0.003	0.013
900x600	0.012	0.002	0.008	0.028	-0.005	0.023	0.019	0.008	-0.007

3.1.3 Correlation analysis of adjacent pixels

We have also analyzed the correlation between two vertically and horizontally adjacent pixels in various plain images and their corresponding cipher images. In Fig 3, we have shown the distributions of horizontally adjacent pixels of red, green and blue components in the image '*Baboon*' and their corresponding cipher image. Particularly, in Frames (a), (b) and (c), we have depicted the distributions of two horizontally adjacent pixels of red, green and blue components respectively in the plain image (Fig 2(a)). Similarly in Frames (d), (e) and (f) respectively, the distributions of two horizontally adjacent pixels in its corresponding cipher image (Fig 2(e)) have been depicted. Similarly, in Fig 4, we have shown the distributions of vertically adjacent pixels of red, green and blue components in the plain image '*Baboon*' and its corresponding cipher image.

Table 3. Correlation coefficient (CR) for two adjacent pixels in the plain and its cipher image.

		CR between adjacent pixels		
		Red	Green	Blue
Horizontal	Plain image	0.8908	0.9455	0.8970
	Cipher Image	0.0349	-0.0481	0.0380
Vertical	Plain image	0.8799	0.9991	0.9081
	Cipher image	0.0231	0.0180	-0.0172

We observe from correlation charts (Fig 3 and Fig 4) and Table 3 that there is a negligible correlation between the two adjacent pixels in the ciphered image. However, the two adjacent pixels in the plain image are strongly correlated. Correlation in the cipher images is very small or negligible when the proposed encryption scheme is used. Hence the proposed scheme has good permutation and substitution properties.

3.2 Key sensitivity analysis

An ideal image cipher should be extremely sensitive with respect to the secret key used in the algorithm. Flipping of a single bit in the secret key, it should produce a widely different ciphered image. This guarantees the security of a cryptosystem against brute-force attacks to some extent. We have tested the sensitivity with respect to a tiny change in the secret key for

several images. One example for plain image '*Baboon*' is discussed below:

a. Plain image (Fig 2(a)) is encrypted by using the secret key 'BB67FA03CB99FBCA2145DDE6672DAC' and the resultant encrypted image is referred as image Fig 5(a).
b. The encrypted image (Fig 5(a)) is decrypted by making a slight modification in the original key '**A**B67FA03 CB99FBCA2145DDE6672DAC' and the resultant decrypted image is referred as image Fig 5(b).
c. The encrypted image (Fig 5(a)) is decrypted by making a slight modification in the original key 'BB67FA03 CB99FB**D**A2145DDE6672DAC' and the resultant decrypted image is referred as image Fig 5(c).
d. The encrypted image (Fig 5(a)) is decrypted by making a slight modification in the original key 'BB67FA03 CB99FBCA2145DDE6672DA**D**' and the resultant decrypted image is referred as image Fig 5(d).

With a small change in the key at any position, one is not able to recover the original image. It is not easy to compare decrypted images through the visual inspection. To compare decrypted images, we have calculated the correlation coefficient between encrypted images and various decrypted images and results are given in Table 4. The correlation coefficients are negligible.

Having the right pair of secret key is an important part while decrypting the image, as a similar secret key (with one bit change) will not retrieve the exact original image. Above example shows the effectiveness of the proposed technique as the decryption with a slightly different secret key does not reveal any information to an unauthorized person.

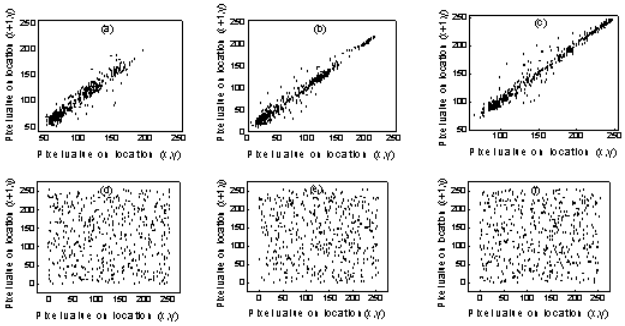

Fig 3 : Distributions of horizontally adjacent pixels of RGB components in the plain image '*Baboon*' and its cipher image.

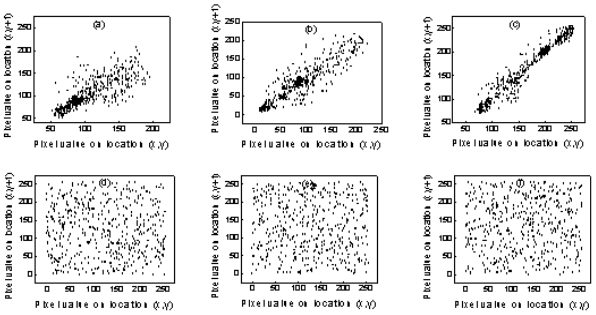

Fig 4 : Distributions of vertically adjacent pixels of RGB components in the plain image '*Baboon*' and its cipher image.

Table 4. Correlation coefficient between RGB components of different decrypted images.

Images	Correlation coefficient
Fig 5(a) and Fig 5(b)	C_{RR}= 0.016, C_{GG}= -0.011 , C_{BB}= 0.006
Fig 5(a) and Fig 5(c)	C_{RR}= 0.013, C_{GG}= -0.017 , C_{BB}= 0.010
Fig 5(a) and Fig 5(d)	C_{RR}= 0.011, C_{GG}= 0.004 , C_{BB}= 0.012

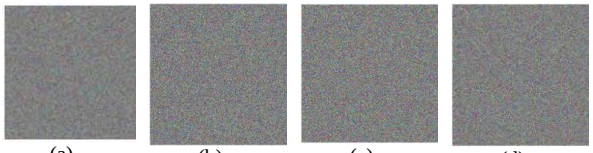

Fig 5 : Decrypted images corresponding to image 'Baboon' with slightly different secret keys.

3.3 Differential attack

One minor change in the plain image causes large changes in the cipher image then differential analysis may become useless. NPCR and UACI become two widely used security analyses in the image encryption community for differential attacks. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired cipher images [16].

Suppose cipher images before and after one pixel change in a plaintext image are c^1 and c^2 respectively. The pixel value at grid (i,j) in c^1 and c^2 are denoted as $c^1(i,j)$ and $c^2(i,j)$ and a bipolar array D is defined by Equation (3). Then the NPCR and UACI can be mathematically defined by Equation (4) and (5) respectively

$$D(i,j) = \begin{cases} 0, & if\ C^1(i,j) = C^2(i,j) \\ 1, & if\ C^1(i,j) \neq C^2(i,j) \end{cases} \quad \ldots\ldots (1)$$

$$NPCR: N(C^1, C^2) = \frac{\sum_{i,j} D(i,j)}{T} X100\% \quad \ldots\ldots (2)$$

$$UACI: U(C^1, C^2) = \frac{\sum_{i,j} |C^1(i,j) - C^2(i,j)|}{FxT} X100\% \quad \ldots\ldots (3)$$

here symbol T denotes the total number pixels in the cipher image, symbol F denotes the largest supported pixel value compatible with the cipher image format and |.| denotes the absolute value function. Table 5 shows the values of NPCR and UACI for each colour component image for four widely different nature images. Experimental results show the estimated expectations and variance of NPCR and UACI are very close to the theoretical values, which justify the validity of theoretical values. Hence the proposed encryption scheme is resistant against differential attacks.

Table 5. NPCR and UACI.

Image	Dimension	NPCR of different colour components			UACI of different components		
		Red	Green	Blue	Red	Green	Blue
Lena	512x512	98.67	98.34	98.10	32.29	32.72	32.83
Baboon	200x200	98.21	98.31	98.21	32.29	32.20	32.54
Peppers	200x200	99.01	98.07	98.37	32.87	32.61	32.18
Lion	640x466	98.79	98.33	98.36	32.43	32.15	32.35

3.4 Speed performance

Apart from the security consideration, encryption/decryption rate of the algorithm is also an important aspect for a good image cipher. We have also measured time taken by the

proposed cipher to encrypt/decrypt various different sized colour images The time analysis has been done on a personal computer with Intel core 2 duo 1.8Ghz processor and 1.5 GB RAM. The results are summarized in Table 6, which clearly predicts an average encryption rate of proposed scheme is 550 KB/second.

Table 6. Encryption rate of proposed image cipher.

Image size	Average
200x200 (117 KB)	0.17s
512x512 (768 KB)	1.19s
640x480 (900 KB)	1.89s
800x600 (1.37 MB)	2.54s

4. CONCLUSION

We have propose a new lossless image encryption scheme using a secret key of 120-bit size. In the substitution process, pixel values are modified using secret key as well as previous and next sub-block. A feedback mechanism makes the encryption scheme more robust and avoids differential attack. The propose scheme is simple, fast and sensitive to the secret key. We have carried out an extensive study of security and performance analysis of the proposed image encryption technique using various statistical analysis, key sensitivity analysis, differential analysis, speed performance, etc. Based on the results of our analysis, we conclude that the proposed image encryption technique is perfectly suitable for the secure image storing and transmission.

5. ACKNOWLEDGMENTS

One of us (VP) acknowledges to the Science and Engineering Research Council (SERC), Department of Science and Technology (DST), Government of India for the Fast Track Young Scientist Research Grant (SR/FTP/PS-17/2009).

6. REFERENCE

[1] Gao, T., & Chen, Z. (2008). Image encryption based on a new total shuffling algorithm. Chaos, Solitons and Fractals, 38, 213-220.

[2] Younes, M.A.B., & Jantan, A. (2008). An image encryption approach using a combination of permutation technique followed by encryption. International Journal of Computer Science and Network Security, 8, 191-197.

[3] Tong, X., & Cui, M. (2008). Image encryption with compound chaotic sequence cipher shifting dynamically. Image and Vision Computing, 26, 843-850.

[4] Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons and Fractals, 35, 408-419.

[5] Pareek, N.K., Patidar, Vinod, & Sud, K.K. (2006). Image encryption using chaotic logistic map. Image and Vision Computing, 24, 926-934.

[6] Patidar, Vinod, Pareek, N.K., & Sud, K.K. (2010). Modified substitution–diffusion image cipher using chaotic standard and logistic maps. Communication in Nonlinear Science and Numerical Simulation, 15, 2755-2765.

[7] Yoon, Ji Won, & Kim, Hyoungshick (2010). An image encryption scheme with a pseudorandom permutation based on chaotic maps. Communication in Nonlinear Science and Numerical Simulation, doi:10.1016/j.cnsns.2010. 01.041.

[8] Ismail, Amr Ismail, Mohammed, Amin, & Diab, Hossam (2010). A digital image encryption algorithm based a composition of two chaotic logistic map. International Journal of Network Security, 11(1), 1-10.

[9] Jolfaei, Alireza, & Mirghadri, Abdolrasoul (2011). Image encryption using chaos and block cipher. Computer and Information Science, 4(1), 172-185.

[10] Nayak, C.K., Acharya, A.K., & Das, Satyabrata (2011). Image encryption using an enhanced block based transformation algorithm. International Journal of Research and Review in Computer Science, 2(2), 275-279.

[11] Sathishkumar, G.A., & Bagan, K. Bhoopathy (2011). A novel image encryption algorithm using pixel shuffling Base 64 encoding based chaotic block cipher. WSEAS Transactions on computers, 10(6), 169-178.

[12] Chen, Dongming, & Chang, Yunpeng (2011). A novel image encryption algorithm based on logistic maps. Advances in Information Science and Service Sciences, 3(7), 364-372.

[13] Indrakanti, S.P., & Avadhani, P.S. (2011). Permutation based image encryption technique. International Journal of Computer Applications, 28(8), 45-47.

[14] Musa, M., Schaefer, E., & Wedig, S. (2003). A simplified AES algorithm and its linear and differential cryptanalysis. Cryptologia, 27, 148-177.

[15] Shannon, C.E. (1940). Communication theory of secrecy systems. Bell Systems Technical Journal, 28, 656-715.

[16] Yue, Wu, Joseph, P. Noonan, & Sos, Agaian (2011). NPCR and UACI randomness tests for image encryption. Journal of Selected Areas in Telecommunications, 31-38.