Substitution-diffusion based Image Cipher

Narendra K Pareek[1], Vinod Patidar [2] and Krishan K Sud [2]

[1] University Computer Centre, Vigyan Bhawan,
M L Sukhadia University, Udaipur-313 002, India.
npareek@yahoo.com

[2] Department of Physics, School of Engineering
Sir Padampat Singhania University, Bhatewar, Udaipur- 313 601, India.
vinod.patidar@spsu.ac.in, kksud@yahoo.com

ABSTRACT

In this paper, a new image encryption scheme using a secret key of 128-bit size is proposed. In the algorithm, image is partitioned into several key based dynamic blocks and further, each block passes through the eight rounds of diffusion as well as substitution process. In diffusion process, sequences of block pixels are rearranged within the block by a zigzag approach whereas block pixels are replaced with another by using difference calculation of row and column in substitution process. Due to high order of substitution and diffusion, common attacks like linear and differential cryptanalysis are infeasible. The experimental results show that the proposed technique is efficient and has high security features.

KEYWORDS

Image encryption, Image Processing, Diffusion, Substitution, Secret key, Information security.

1. INTRODUCTION

Security of images has become very important for many applications like video conferencing, secure facsimile, medical, military applications etc. It is hard to prevent unauthorized user from eavesdropping in any communication system including internet. To protect information from unauthorized user, mainly two different technologies are used. These are - digital watermarking and cryptography. These two technologies could be used complementary to each other. In secured communications using cryptography, which is the main focus of the present work, the information under consideration is converted from the intelligible form to an unintelligible form at sender end. Encryption process scrambles the content of data such as text, image, audio, and video to make the data unreadable or incomprehensible during transmission. The encrypted form of the information is then transmitted through the insecure channel to the desired recipient. At the recipient end, the information is again converted back to an understandable form using decryption process. When same key is used in encryption and decryption process, such algorithms are grouped under symmetric key cryptography. Numerous symmetric image encryption schemes based on different approaches are available in literature. Among them, chaotic dynamical systems have been exploited extensively to develop the secure cryptographic schemes both for text and image data. A few chaos based image encryption schemes suggested recently are [1-6]. Most of the chaotic encryption scheme have been cryptanalysed successfully [7-10] due to the finite computing precision used to represent the floating point output of chaotic systems as it introduces cycles in the behaviour of chaotic systems and hence become vulnerable to attacks.

In this paper, a non-chaos based image encryption scheme using secret key of 128-bit size is proposed. In the proposed scheme, image is divided into several dynamic blocks and each block passes through the eight rounds of diffusion process. In each round, block size is kept different

DOI : 10.5121/ijnsa.2011.3212

which depends on the secret key used in the algorithm. In diffusion process, sequences of block pixels are rearranged within the same block by a zigzag approach as shown in the Figure 2. Further, blocks are resized and pass through the eight rounds of substitution process. In each round of substitution process, size of each block is secret key dependent and may be entirely different from block size used in diffusion process. In substitution process, block pixels are replaced with another by using difference computation of rows and column pixels. The rest of the paper is organized as follows. In Section 2, details of different components used in the proposed scheme as well as complete encryption algorithm are introduced. Security analysis and simulation results of the proposed image encryption scheme are presented in Section 3. Finally, Section 4 concludes the paper.

2. PROPOSED CRYPTOGRAPHIC ALGORITHM

Image data have high correlations among adjacent pixels forming intelligible information. To encrypt the image, this intelligible information needs to be reduced by decreasing the correlation among the pixels. The proposed scheme does this by scrambling the pixels of the image as well as changing the pixel values of the resultant image. In the following paragraph, we discuss in detail the functions of different units used in the proposed algorithm.

2.1. Plain image block size

In each round of diffusion and substitution process, image pixels are divided into several non-overlapping squared dynamic blocks and their size (B_r) depends on the secret key used in the algorithm. Both Equation (1) and (2) are used to decide the plain image block size in diffusion and substitution process respectively.

$$B_r = \sum_{p=1}^{4} K_{(4*(r-1)+p)} \quad \text{(Diffusion process)} \tag{1}$$

$$B_r = \sum_{p=1}^{4} K_{(4*(8-r)+p)} \quad \text{(Substitution process)} \tag{2}$$

where K_i and B_r are the i^{th} subkey and block size in r^{th} round respectively.

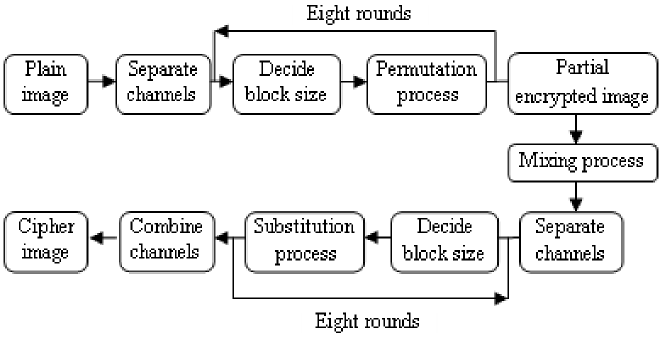


Figure 1. Schematic diagram of the proposed image encryption scheme.

2.2. Diffusion process

In the diffusion process, pixels of each dynamic block are rearranged within the same block by a zigzag path. For example, a path shown in Figure 2 is used to rearrange the pixels of a block of 8x8 size. In Figure 2, if we start traversing the path from the pixel location (7,6), then stop traversing at the pixel location which is previous to the start one i.e. (6,7). During traversing process, the pixels, encounter in the path, are arranged sequentially row by row and column by column in the same block. Each channel (red, green and blue) of pixels passes through eight rounds of diffusion. In each round, image pixels are divided into several non-overlapping squared dynamic blocks as discussed in Sub section 2.1. Location of pixel (X_r,Y_r) to start traversing the path in blocks of r^{th} round is made completely secret key dependent and computed by Equation (3).

$$X_r = \sum_{p=1}^{3} K_{(4*(r-1)+p)}\ ,\quad Y_r = \sum_{p=2}^{4} K_{(4*(r-1)+p)} \qquad (3)$$

where K_i is the i^{th} subkey.

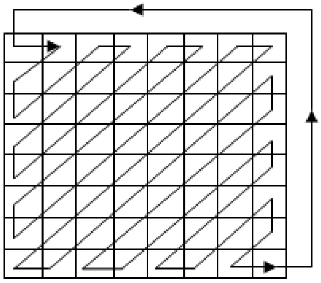


Figure 2. A zigzag approach to scramble pixels of a block.

2.3. Mixing process

To reduce correlation between adjacent pixels in image, three different layers of pixels corresponding to red, green and blue channel of plain image are separated out and the properties of each pixel are modified using exclusive-OR operation with its previous pixel in the following way:

```
i=1
for x = 1 to $H$
 for y = 1 to $W$
   $R_{x,y} = R_{x,y} \oplus G_{x,y-1} \oplus B_{x,y-1}$                (4)
   $G_{x,y} = G_{x,y} \oplus R_{x,y-1} \oplus B_{x,y-1}$
   $B_{x,y} = B_{x,y} \oplus R_{x,y-1} \oplus G_{x,y-1}$
 endfor
endfor
```

where $R_{x,0} / G_{x,0} / B_{x,0} = \begin{cases} 0 & x = 1 \\ R_{x-1,w} / G_{x-1,w} / B_{x-1,w} & x > 1 \end{cases}$. H and W represent height and width of plain image respectively.

2.4. Substitution process

In the substitution process, a simple computation is performed on pixels to change their properties. Each channel (red, green and blue) of pixels passes through the eight rounds. In each round, pixels are divided into several non-overlapping dynamic squared blocks as discussed earlier in Sub section 2.1. After deciding the block size, each block is passed through row and column transformation. For example, a row pixel of a 15x15 size block is shown in Table 1. In a row transformation process, we first find largest pixel value (PV) among a row pixel which is 216 in our example and then, subtract all those pixel values of a row form PV whose pixel value is smaller to PV.

When transformation of all the rows of a block is over, a similar operation is performed on pixels of each column of a block obtained after row transformation. In Table 2, we have shown the pixel values for an 8x8 block before and after the complete substitution process (i.e. row transformation + column transformation).

Table 1. Procedure of a row transformation.

Row pixels	90	200	138	56	21	81	152	216	202	140	8	98	45	115	22
Resultant row pixels	126	16	78	160	195	135	64	216	14	76	208	118	171	101	194

Table 2. Pixel values before and after row and column transformations.

56	45	57	60	48		13	50	11	2	43
48	65	54	44	61		17	65	3	41	51
56	51	48	62	49	→	11	54	14	62	42
46	49	51	55	54		8	59	10	7	54
49	51	49	47	55		11	61	8	54	55

2.5. The complete encryption process

The block diagram of the proposed encryption algorithm is shown in Figure 1. In the proposed encryption scheme, diffusion and substitution processes are completely secret key dependent and a feedback mechanism is also applied in the mixing process to avoid the differential attack. We discuss the steps of algorithm in following paragraph:

1) Proposed encryption scheme uses a secret key of 128-bits size. Further, the secret key is divided into blocks of 4-bits each referred as subkeys.

$$K=K1K2K3 \quad \ldots\ldots \; K32, \tag{5}$$

here, Ki 's are digits from 0 to 15.

2) Colour image is separated out into red, green and blue channels and each channel passes through following steps.

```
For round = 1 to 8 do following
   a. Decide block size (B) for current round as discussed in Sub section 2.1.
   b. Divided each color channel into non-overlapping squared blocks (B).
   c. Each block passes through the diffusion process as discussed in Sub section 2.2.
 Endfor
```

3) Channels are combined resulting in partial encrypted image. The resulting image passes through the mixing process. Further, resulting image is separated out into channels (Red, Green and Blue) and each channel passes through following step.

```
For round = 1 to 8 do following
   a. Decide block size (B) for current round as discussed in Sub section 2.1.
   b. Divided each channel into non-overlapping squared blocks (B).
   c. Each block passes through the substitution process as discussed in Sub section 2.4.
Endfor
```

4) Resulting image is written in a file.

3. SECURITY AND PERFORMANCE ANALYSIS

In this section, we evaluate the performance and discuss the security analysis of the proposed image encryption scheme such as statistical analysis, key space analysis, sensitivity analysis etc to prove that the proposed algorithm is efficient 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 Mathematica application tool.

3.1. 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 encrypted image, information entropy and the correlation between the original and encrypted images.

3.1.1. Distribution of pixels

Histogram analysis is employed to illustrate the superior confusion and diffusion properties of the encryption algorithm. We have analyzed the histograms of about hundred encrypted images and their corresponding plain images having widely different contents and sizes. One example of histogram analysis for well known popular image 'Lena' is shown in Figure 3. Histograms of red, blue and green channels of image (Figure 3(a)) are shown in Frames (b), (c) and (d) respectively. In Frames (f), (g) and (h) respectively, the histograms of red, blue and green channels of the encrypted image (Figure 3(e)) are shown. Comparing the histograms of plain images and encrypted images, we find that histograms of encrypted images are very close to uniform distribution, significantly different from that of the original image and contain no resemblance to the original image. Hence, the encrypted image does not provide any clue to employ any statistical attack on the proposed image encryption scheme, which makes statistical attacks difficult. This is consistent with the perfect security defined by Shannon [11] and the proposed encryption scheme resists against the known-plaintext attack.

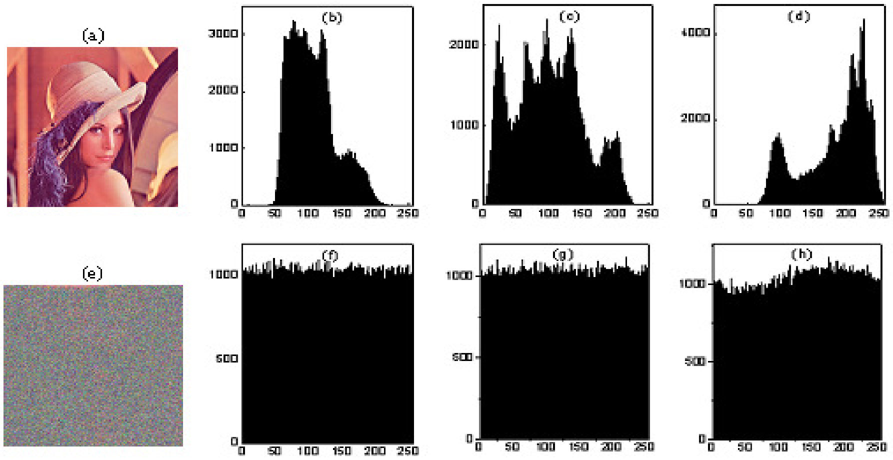


Figure 3. Histograms of plain image *'Lena'* and its corresponding encrypted image.

3.1.2. Correlation between original and encrypted images

We have also done extensive study of the correlation between pairs of plain image and their corresponding encrypted image produced using the proposed encryption scheme by computing correlation coefficient between various colour channels of the original and corresponding encrypted images. Results for a few images are shown in Table 3. Since the correlation coefficients shown in the Table 3 are very low ($C \approx 0$), which shows that the plain images are nearly independent from the encrypted images. This is consistent with the perfect security defined by Shannon[11].

Table 3. Correlation coefficient between plain images and their corresponding encrypted images.

Image Size	C_{RR}	C_{RB}	C_{RG}	C_{GR}	C_{GG}	C_{GB}	C_{BR}	C_{BG}	C_{BB}
200 x 137	0.0055	-0.0130	0.0111	0.0072	-0.0212	0.0092	0.0069	-0.0235	0.0021
200 x 200	0.0130	0.0170	0.0187	0.0086	0.0163	0.0170	0.0059	0.0177	0.0148
200 x 200	-0.0132	-0.0120	0.0036	-0.0043	-0.0017	0.0101	-0.0039	0.0024	0.0046
200 x 132	-0.0219	-0.0154	-0.0166	-0.0089	-0.0120	-0.0192	-0.0124	-0.0121	-0.0206
640 x 480	-0.0067	0.0019	0.0115	0.0001	-0.0003	0.0054	0.0070	-0.0022	-0.0012
800 x 600	-0.0614	0.0630	-0.0365	-0.0621	0.0647	-0.0377	-0.0622	0.0644	-0.0272
640 x 480	-0.0067	-0.0036	-0.0081	-0.0065	-0.0046	-0.0102	-0.0089	-0.0055	-0.0117
200 x 200	-0.0001	-0.0099	-0.0037	-0.0031	-0.0106	-0.0057	0.0029	0.0040	0.0032
900 x 600	0.0007	0.0212	0.0123	0.0959	0.0119	0.0080	0.0932	0.0054	0.0050
200 x 133	0.0004	-0.0313	-0.0252	-0.0008	-0.0236	-0.0287	-0.0030	-0.0277	-0.0235
200 x 150	-0.0080	0.0034	-0.0052	-0.0026	0.0052	-0.0002	-0.0090	0.0030	0.0004

3.1.3. Correlation analysis of adjacent pixels

In addition to the correlation analysis of images, we have also analyzed the correlation between two horizontally, vertically and diagonal adjacent pixels in several plain images and their corresponding encrypted images. In Figure 4, we have shown the distributions of horizontally adjacent pixels of red, green and blue channels in the image 'Lena' and their corresponding encrypted image. Particularly, in Frames (a), (b) and (c), we have depicted the distributions of two horizontally adjacent pixels of red, green and blue channels respectively in the plain image (Figure 3(a)). Similarly in Frames (d), (e) and (f) respectively, the distributions of two horizontally adjacent pixels in its corresponding encrypted image (Figure 3(e)) have been depicted. Similarly, in Figure5, we have shown the distributions of vertically adjacent pixels of red, green and blue channels in the plain image 'Lena' and its corresponding encrypted image. We observe from correlation graph and Table 4 that there is a negligible correlation between the two adjacent pixels in the encrypted image. However, the two adjacent pixels in the original image are highly correlated. Correlation in the encrypted images is very small or negligible when the proposed encryption scheme is used. Hence the proposed scheme has good diffusion and substitution properties.

Table 4. Correlation coefficient for two adjacent pixels.

	Original image (Figure 3a)	Encrypted image (Figure 3e)
Horizont	0.8710	0.0083
Vertical	0.4668	-0.0162
Diagonal	0.6737	0.0078

3.1.4. Information entropy

Illegibility and indeterminateness are the main goals of image encryption. This indeterminateness can be reflected by one of the most commonly used theoretical measure - information entropy. Information entropy expresses the degree of uncertainties in the system and express by Equation (6).

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\log_2[P(m_i)] \tag{6}$$

where $P(m_i)$ is the emergence probability of m_i. If every symbol has an equal probability, i.e., $m=\{m_0,m_1,m_2,\ldots m_{2^8-1}\}$ and $P(m_i)=1/2^8(i=0,1,\ldots 255)$, then the entropy is $H(m)=8$ which corresponds to an ideal case. Practically, the information entropies of encrypted images are less compared to the ideal case. To design a good image encryption scheme, the entropy of encrypted image close to the ideal case is expected. For the proposed image encryption scheme, the information entropy is $H(m)=7.99$, which is very close to the ideal value. This means a high diffusion and substitution is achieved by the proposed algorithm. Proposed algorithm has a robust performance against the entropy attack.

Table 5. Entropy values for different images.

Images	Entropy of plain images	Entropy of encrypted images
Lena	7.7502	7.9996
Baboon	7.6430	7.9979
Peppers	7.7150	7.9984
Tiger	7.8261	7.9991
Bear	7.5870	7.9973

3.2. Key sensitivity analysis

An ideal image cipher should be extremely sensitive with respect to the secret key used in the algorithm. Even flipping of a single bit in the secret key, it should produce a widely different encrypted 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 'Lena' is discussed below:

a. Plain image (Figure 3(a)) is encrypted by using the key 'D6DA750B4C1F78D328 EA25E6B15CF9E4' and the resultant encrypted image is referred as image Figure 6(a).
b. The encrypted image (Figure 6(a)) is decrypted by making a slight modification in the original key '**E**6DA750B4C1F78D328EA25E6B15CF9E4' and the resultant decrypted image is referred as image Figure 6(b).
c. The encrypted image (Figure 6(a)) is decrypted by making a slight modification in the original key 'D6DA750B4C1F78D328EA25E6B15CF9E**3**' and the resultant decrypted image is referred as image Figure 6(c).
d. The encrypted image (Figure 6(a)) is decrypted by making a slight modification in the original key 'D6DA750B4C1F78D**4**28EA25E6B15CF9E4' and the resultant decrypted image is referred as image Figure 6(d).

With a small change in the key at any position, one is unable to recover the original image. It is hard to compare decrypted images with naked eyes. To compare decrypted images, we have calculated the correlation coefficient between encrypted images and various decrypted images and results are shown in Table 6. 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 key does not reveal any information to an unauthorized user.

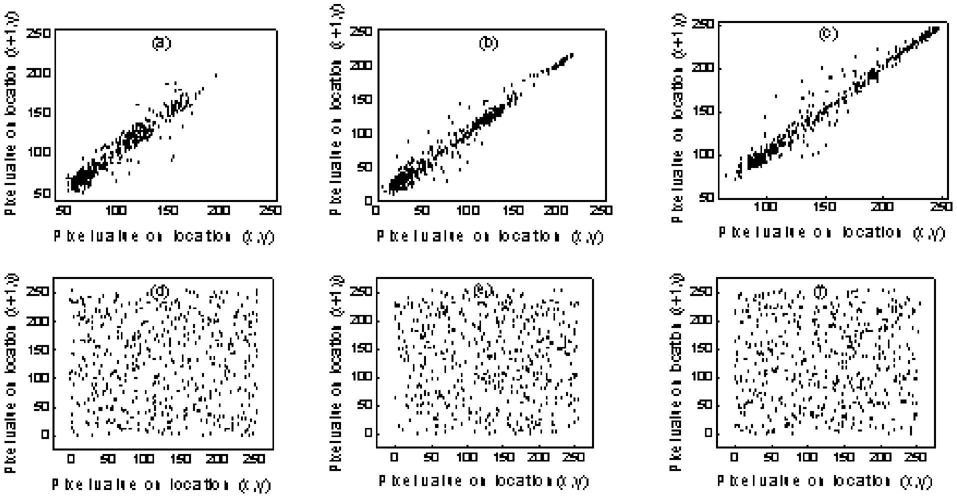


Figure 4. Distributions of horizontally adjacent pixels of RGB channels in the plain image '*Lena*' and its encrypted image.

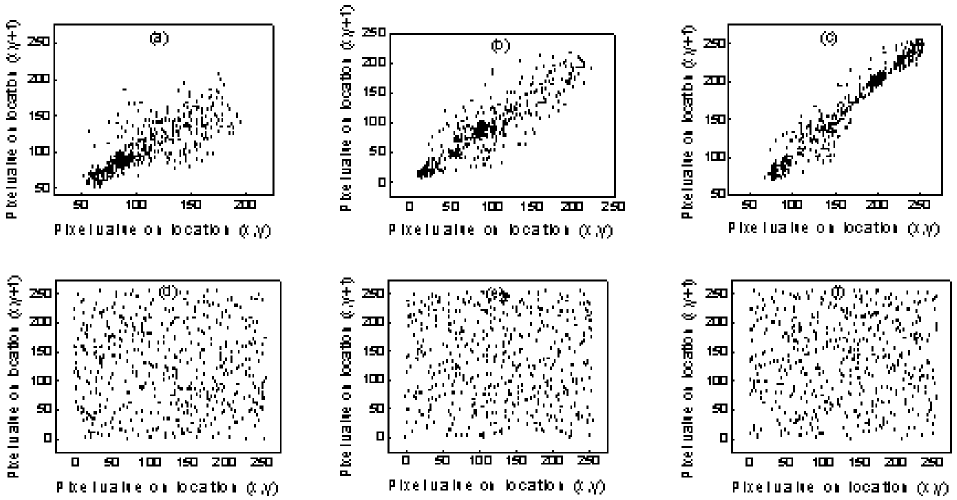
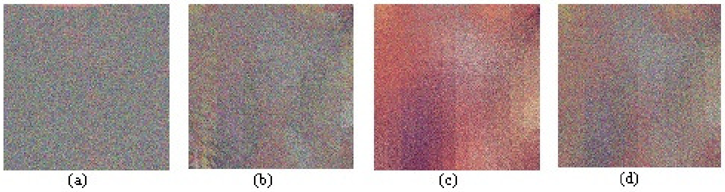


Figure 5. Distributions of vertically adjacent pixels of RGB channels in the plain image '*Lena*' and its encrypted image.



(a) (b) (c) (d)

Figure 6. Decrypted images corresponding to image 'Lena' with slightly different secret keys.

Table 6. Correlation coefficient between RGB channels of different decrypted images.

Images	Correlation coefficient
Figure6(a) and Figure 6(b)	C_{RR}=0.0182, C_{GG}=0.0290, C_{BB}=0.0162
Figure 6(a) and Figure 6(c)	C_{RR}=0.0105, C_{GG}=0.0089, C_{BB}=0.0103
Figure 6(a) and Figure 6(d)	C_{RR}=0.0284, C_{GG}=0.0414, C_{BB}=0.0255

3.3. Plain image sensitivity

If one minor change in the plain image causes large changes in the encrypted image then differential analysis may become useless. Thus, much difference between encrypted forms is expected in order to keep high security. Plain image sensitivity is mostly analyzed by the number of pixel change rate (NPCR). NPCR means the number of pixels changed in the encrypted image when only one pixel value is changed in plain image. For a larger value of NPCR, plain image has the higher sensitivity. In our plain image sensitivity test, we changed pixel at position (1,4) from (62,32,96) to (255,255,255) in plain image 'Lena'. Table 7 shows the values of NPCR for each rounds of diffusion and substitution process which is over 98%. Hence the proposed encryption scheme is resistant against differential attacks.

Table 7. Number of pixel change rate (NPCR)

NPCR		Rounds in diffusion process							
		1	2	3	4	5	6	7	8
Rounds in substitution process	1	97.71	97.87	98.12	98.89	98.79	99.12	99.23	99.20
	2	97.80	97.82	98.35	98.84	98.97	99.16	99.34	99.30
	3	97.89	97.85	97.99	98.66	98.89	99.04	99.38	99.42
	4	98.20	98.28	98.65	98.66	98.73	98.82	99.20	99.39
	5	98.67	98.71	98.69	98.72	98.78	98.94	98.99	99.33
	6	98.98	98.95	98.96	98.90	99.02	99.10	99.12	99.20
	7	99.23	99.20	99.24	99.20	99.11	99.16	99.20	99.42
	8	99.29	99.20	99.15	99.30	99.31	99.33	99.26	99.46

3.4. Image quality criterion

A very useful measure of the performance of the decryption procedure is the mean square error (MSE). The smaller MSE value, the better the image quality recovered. On the contrary, the greater the MSE value, the worse the image quality recovered. For P and P' being a plain image and the decrypted image respectively, the MSE for the each color component (RGB) is defined as

$$MSE = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} [P(m,n) - P'(m,n)]^2}{MxN} \tag{7}$$

where (m,n) are the pixel coordinates, *MxN* is the number of pixels of the images considered. *P(m,n)* and $P^{'}(m,n)$ are the original and decrypted image recovered respectively. We have calculated MSEs for the red, green and blue components of the decrypted images with respect to their original for around fifty images. In all test cases, it was found to be approximately zero. Hence, proposed image cipher comes under the category of lossless image cipher.

3.5. Key space analysis

The key space of the proposed encryption scheme is large enough to resist all kinds of brute-force attacks. The experimental results also demonstrate that our scheme is very sensitive to the secret key. If the decryption key changes slightly, the decrypted image will be greatly different from the original plain image as shown in Figure 6. Secret key used in the image cipher should be neither too long nor too short. A larger secret key decreases the encryption speed and is not preferred for real time image transmission whereas a choice of smaller secret key results in an easy cryptanalysis. In the proposed encryption scheme, a secret key of 128-bits long is used. Thus, it has 2^{128} different combinations ($3.40x10^{38}$). An image cipher with such a large key space is sufficient for resisting various brute-force attacks. With respect to the speed of the today's computers, it is recommended that key space should be more than 2^{100} in order to avoid brute-force attacks [12].

3.6. Time analysis

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 1.5GB RAM. The results are summarized in Table 8, which clearly predicts an average encryption rate of proposed scheme is 380KB/second.

Table 8. Encryption rate of proposed image cipher.

Image	Image	Average time
512x512	768 KB	2.26s
200x200	117 KB	0.27s
200x305	178 KB	0.44s
800x600	1.37 MB	4.17s

4. CONCLUSIONS

We propose a new non-chaos based image encryption scheme using a key of 128-bit size. In the algorithm, image is partitioned into several key based dynamic blocks and each block is passed through the eight rounds of diffusion as well as substitution process. In diffusion process, sequences of block pixels are rearranged within itself by a zigzag approach whereas block pixels are replaced with another by using difference transformation in substitution process. We have carried out an extensive security and performance analysis of the proposed image encryption technique using various statistical analysis, key sensitivity analysis, differential analysis, key space 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.

ACKNOWLEDGEMENTS

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).

REFERENCES

[1] Vinod Patidar, N.K. Pareek, G. Purohit and K.K. Sud, (2010) “Modified substitution–diffusion image cipher using chaotic standard and logistic maps”, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, No. 10, pp 2755-2765.

[2] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, (2011) “A chaos-based symmetric image encryption scheme using a bit-level permutation”, Information Sciences, Vol. 181, No. 6, pp 1171-1186.

[3] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan and Z. Hassan, (2010) “A novel scheme for image encryption based on 2D piecewise chaotic maps”, Optics Communications, Vol. 283, No. 17, pp 3259-3266.

[4] Huaqian Yang, Kwok-Wo Wong, Xiaofeng Liao, Wei Zhang and Pengcheng Wei, (2010) “A fast image encryption and authentication scheme based on chaotic maps “, Communications in Nonlinear Science and Numerical Simulation, Vol. 15, No. 11, pp 3507-3517.

[5] Anil Kumar and M. K. Ghose, (2010) “Substitution-Diffusion Based Image Cipher Using Chaotic Standard Map and 3D Cat Map”, Communications in Computer and Information Science, Vol. 70, pp 34-38.

[6] Yupu Dong, Jiasheng Liu, Canyan Zhu and Yiming Wang, (2010), Image encryption algorithm based on chaotic mapping”, Third IEEE International Conference on Computer Science and Information Technology (ICCSIT), July 2010 , pp 289-291.

[7] S. Li, C. Li, G. Chen and K.-T. Lo, (2008) “Cryptanalysis of the RCES/RSES image encryption scheme”, Journal of Systems and Software, Vol. 82, No.7, pp. 1130-1143.

[8] D. Arroyo, C. Li, S. Li, G. Alvarez and W.A. Halang, (2009) “Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm”, Chaos, Solitons and Fractals, Vol. 41, No. 5, pp. 2613-2616.

[9] G. Alvarez and S. Li, (2009) “Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption”, Communications in Nonlinear Science and Numerical Simulations, Vol. 14, No. 11, pp. 3743-3749.

[10] C. Li, S. Li, G. Chen and W.A. Halang, (2009), “Cryptanalysis of an Image Encryption Scheme based on a compound chaotic sequence”, Image and Vision Computing, Vol. 27, No. 8, pp 1035-1039.

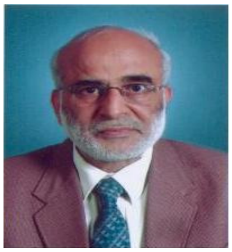
[11] C. E. Shannon, (1940) “Communication theory of secrecy systems”, Bell Systems Technical Journal, Vol. 28, pp 656–715.

[12] Yun, Li, Feng-Ying, Han, (2009) “New image encryption algorithm based on combined high – dimension chaotic system”, Computer Engineering and Applications, Vol. 45, No. 1, pp. 103–107.

Authors

Narendra K Pareek received his M.Sc. from University of Rajasthan, Jaipur, India in 1986 and Ph.D. degree in Computer Science from M L Sukhadia University, Udaipur, India in 2005. He has worked as lecturer in the Department of Computer Science, Banasthali University, Banasthali, India for a period of two years. Presently, he is working as a Programmer at the University Computer Centre of the M L Sukhadia University, Udaipur since 1991 and has been teaching various courses of computer science to undergraduate and post graduate students. His research interests are in information security, chaotic cryptology, data compression, and information retrieval systems. He has published one book and more than fifteen papers on chaotic cryptography and image encryption in referred international journals/conferences. His research work has received more than 300 citations and one of his papers has also received MOST CITED PAPER AWARD for Image and Vision Computing journal.

Vinod Patidar is working as Assistant Professor of Physics at Sir Padampat Singhania University (SPSU), Udaipur, India since August, 2008. He is also Principal Investigator in a Fast Track Young Scientist research project on the "Application of chaotic dynamical systems in developing secure cryptosystems and their cryptanalysis" funded by the Department of Science and Technology, Government of India (2009-2012). Prior to joining SPSU, he served as Lecturer and Senior Lecturer in the Department of Physics, Banasthali University, Banasthali, India. He received his M.Sc. (Physics) degree with the University Gold Medal in 1999 and completed the Doctoral Research (Ph.D.) in the field of Nonlinear Dynamics with a National Level Fellowship in 2004 from M. L. S. University, Udaipur, India. He was Visiting Guest Scientist at the Helmholtz Institute for Supercomputational Physics, University of Potsdam, Germany and International Centre for Theoretical Physics (ICTP), Trieste, Italy in 2003 and 2005 respectively. He has published one research monograph and more than 35 research papers in various refereed international & national journals and conference proceedings. His research work has received more than 350 citations and one of his papers has also received MOST CITED PAPER AWARD for Image and Vision Computing journal. His present research interests include bifurcation & chaos in classical systems, control & synchronization of chaos, dynamical behaviour of q-deformed nonlinear dynamical systems, applications of chaotic dynamical systems in the development of secure cryptosystems & their crypt-analysis and theoretical studies of electron atom/ion collisions. More details are available at http://www.vinod-patidar.webs.com



Krishan K Sud received M.Sc. in Physics from the University of Jodhpur, Jodhpur,India in 1965 and M.S. and Ph.D. from Ohio University, Ohio USA in 1973 and1976 respectively. He is at present Dean, School of Engineering at Sir Padampat Singhania University Udaipur. He taught physics and computer science at the University of Jodhpur (1966- 1993) and M.L.S. University Udaipur (1994-2005). He was Director, University Computer Centre and the MCA programme (Master's degree in computer applications) (1994-2005) and Chairman, Faculty of Science (2004-05) of the M.L.S. University. He was Director of the Acharya Nanesh College of Information Technology, Danta (2006-2007). He also held short term visiting research positions at the International Centre for Theoretical Physics, Trieste, Italy, University of Pittsburgh and Ohio University. He was visiting Research Professor at the Universidad de Costa Rica, San Jose Costa Rica (May86-Dec-86). He has supervised 10 Ph.D. dissertations, published two books and more than 100 papers in refereed national and international journals and conference proceedings in the field of external key based chaotic cryptosystems, cryptanalysis of the chaotic cryptosystems, image encryption, radiation physics and electron-atom collision problems. He was President (2001-03) of the Indian Society of Atomic and Molecular Physics and Chairman Computer Society of India, Udaipur Chapter (2001-03). He is also a senior member of the Computer Society of India.