Multimed Tools Appl (2012) 56:315–330
DOI 10.1007/s11042-010-0652-6

A novel image cipher based on mixed transformed logistic maps

I. Shatheesh Sam · P. Devaraj · Raghuvel S. Bhuvaneswaran

Published online: 7 November 2010

Abstract In this paper, a novel secure cryptosystem is proposed for direct encryption of color images, based on transformed logistic maps. The proposed cipher provides good confusion and diffusion properties that ensures extremely high security due to the mixing of colors pixels. The encryption scheme makes use of six odd secret keys and chaotic keys for each operation. The operations include initial permutation of all pixels with six odd keys, nonlinear diffusion using first chaotic key, xoring the second chaotic key with resultant values and zig-zag diffusion with third chaotic key. The proposed scheme supports key sizes ranging from 192 to 400 bits. The security and performance of the proposed image encryption technique have been analysed thoroughly using statistical analysis, key sensitivity analysis, differential analysis, key space analysis, entropy analysis and performance analysis. Results of the various types of analyses are showing that the proposed image encryption technique is more secure and fast and hence suitable for the real-time applications.

Keywords Mixed logistic map · Image encryption · Zig-Zag diffusion

I. S. Sam (✉) · R. S. Bhuvaneswaran
Ramanujan Computing Centre, College of Engineering, Guindy,
Anna University Chennai, Chennai, India
e-mail: shatheeshsam@yahoo.com

R. S. Bhuvaneswaran
e-mail: bhuvan@annauniv.edu

P. Devaraj
Department of Mathematics, College of Engineering, Guindy,
Anna University Chennai, Chennai, India
e-mail: devaraj@annauniv.edu

1 Introduction

Multimedia content security is one of the important issues in the present information age. Motivated by the rapid development of multimedia and increasing bandwidth of network technologies, images are being transmitted over networks more and more frequently. Consequently, security in storage and transmission of digital images is needed in many applications, including both public and private services such as medical imaging systems, confidential video conferencing, military image databases, online personal photograph album, satellite information systems etc. The development of various number of conventional encryption techniques such as RSA, DES, AES, IDEA, etc. [8, 13] are not reliable for the image encryption due to some intrinsic features of images such as bulk storage capacity, high redundancy, strong correlation among adjacent pixels, etc. In order to provide a better solution to image security problems, number of image encryption techniques have been suggested in the last two decades. The techniques based on chaotic dynamical systems [15] provide a good combination of speed, high security, complexity, reasonable computational overheads and computation power, etc.

Chaos-based cryptographic algorithm [7] is an efficient encryption algorithm, first proposed in 1989. It has many unique characteristics different from other algorithms such as the sensitive dependence on initial conditions [2], non-periodicity, non-convergence and control parameters. The one dimensional chaos system has the advantages of simplicity and high security [3]. Many studies [9] were proposed to adapt and improve it. Some of them use high-dimensional dynamic systems, and other studies use couple maps [4, 6, 12, 14, 17, 18]; however, all research works are mainly focused to fine tune parameters to enhance the security. An improved color image encryption scheme is proposed [5], which is based on a chaotic logistic map and OCML model. Some cryptanalysis techniques [1] are suggested to break the scheme and reduce the flaws in the algorithm design.

Patidar et al. [10] proposed a cryptosystem which utilises the chaotic 2D standard map and 1D logistic map. This is specifically designed for the color images, where the two maps are used to generate a pseudo-random number sequence (PRNS) controlling two kinds of encryption operations. The initial condition value and number of iterations together constitute as the secret key for the algorithm. The algorithm comprises four rounds: two for the substitution and two for the diffusion. The first round of substitution/confusion is achieved with the help of intermediate xoring keys calculated from the secret key. Then two rounds of diffusion namely the horizontal and vertical diffusions are completed by mixing the properties of horizontally and vertically adjacent pixels, respectively. In the fourth round, a robust substitution/confusion is accomplished by generating an intermediate chaotic key stream image in a novel manner with the help of chaotic standard and logistic maps.

Rhouma et al. [11] reported that all the steps are linear in nature and Rhouma also indicated that this cryptosystem is vulnerable to attacks by dividing the cryptosystem procedure into two majors successive steps: (1) the diffusion process and (2) the masking process. Therefore, the scheme is not secure in the sense that an equivalent key can be obtained from only one known/chosen plain-image and the corresponding cipher-image.

The cipher proposed by Patidar scheme may be described as an equivalent cryptosystem and is as follows:

1) Horizontal diffusion (HD): For each color component of the plain image P, mix the properties of horizontally adjacent pixels as done in the second step of the original description. Obtain the horizontally diffused image H as:

$$H = HD(P)$$

2) Vertical diffusion (VD): Mix the properties of vertically adjacent pixels of H and obtain the modified image V as:

$$V = VD(H)$$

3) Diffuse the key image X horizontally then vertically and obtain X_{HV} as:

$$X_{HV} = VD(HD(X))$$

4) Mix the resulting image X_{HV} from Step 3 and the CKS (Chaotic Key Stream) and obtain a new key image Y. Hence, we have

$$Y = X_{HV} \oplus CKS$$

5) Mix the new key image Y from Step 4 with the diffused image V from Step 2. Obtain the ciphered image C as:

$$C = Y \oplus V$$

Thus, we can generate the ciphered images by equivalent procedure: the method proposed by the Patidar scheme. The attack is possible because all the operations are linear in nature. The equivalent procedure is as follows:

$$\begin{aligned} C &= CKS \oplus VD(HD(P \oplus X)), \\ &= CKS \oplus VD(HD(P) \oplus HD(X)), \\ &= CKS \oplus VD(H) \oplus VD(HD(X)), \\ &= CKS \oplus V \oplus X_{HV}, \\ &= Y \oplus V. \end{aligned}$$

In order to bypass the need to know the original keys, an attacker only needs to know the equivalent keystream image key Y. Indeed, once the attacker knows Y, he can use the above procedure to reveal the plaintext image as

$$P = HD^{-1}(VD^{-1}(C \oplus Y))$$

Suppose the attacker chooses a zero image as an input to the encryption machinery. Using with $P = 0$, we have:

$$\begin{aligned} C &= Y \oplus VD(HD(0)), \\ &= Y \end{aligned}$$

Thus, the attacker obtains the secret Y as the ciphered image for his chosen plain image.

In order to alleviate this, the following scheme is suggested, mixed transformed logistic map is used. The algorithm uses significant features such as sensitivity to initial condition, permutation of odd keys and mixed transformed maps. The nonlinear diffusion using first chaotic map, xoring with second chaotic map and the zig-zag diffusion with third chaotic map are done to improve the efficiency of the encryption scheme and to improve the security against the known/chosen-plaintext attack. The nonlinearity is used to overcome the main limitation of the Patidar scheme. The rest of this paper is organized as follows. Section 2 introduces transformed maps and its unique characteristics. In Section 3, the image encryption based on mixed logistic map is proposed including new algorithm steps. In Section 4, the security of new algorithm is analysed. Finally, the conclusions are discussed in Section 5.

2 The transformed maps

In general, logistic map has security issues, like blank window, stable window, uneven distribution and weak key, we have attempted to improved it by chaotic transformation. The characteristics and the security issues are discussed in the following section.

2.1 Characteristics of logistic map

Logistic map is the most widely used classical map. It is very simple and it is deterministic, but it has very complicated dynamic behavior. The logistic map is defined as follows:

$$x_{n+1} = ax_n(1 - x_n) \tag{1}$$

where $0 < x_n < 1$ and $0 < a \leq 4$. The sequences produced by logistic map are controlled by parameter value of a and the initial value of x_n. The system has different characteristics with different values of a which is called bifurcation parameter. Figure 1 shows the different characteristics with different values of a. The horizontal axis shows the values of the parameter a and the vertical axis shows the possible long-term values of x_n.

Logistic mapping sequences also have good auto-correlation and cross-correlation properties. Because of the characteristics of logistic map, the iterative sequences which are produced by logistic map can replace traditional pseudo-random sequences produced by linear feedback shift register (LFSR) used in encryption.

The logistic map has some common problems such as stable windows, blank windows, uneven distribution of sequences and weak key [16]. The blank window is more serious problem than others. Figure 2 illustrates that the blank window which appears when $\mu = 3.828$.

Hence, to alleviate all these problems a new type of transformed logistic maps are required and proposed in the paper. The maps are mixed together so as to achieve larger key space and to attain chaotic behavior.

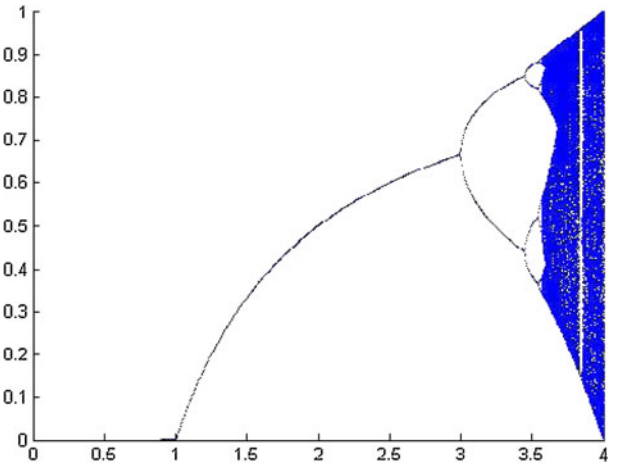


Fig. 1 Bifurcation for the logistic map

2.2 Transformed logistic map

The proposed transformed logistic maps are defined as follows:

$$x_{n+1} = \left[a \times (1 + x_n)^2 \times k_1 \times sin(1/1 + (y_n)^2)\right] \, mod \, 1$$
$$y_{n+1} = \left[a \times x_{n+1} \times k_2 \times sin(x_{n+1} \times y_n) \times (1 + (z_n)^2)\right] \, mod \, 1$$
$$z_{n+1} = \left[a \times x_{n+1} \times k_3 \times (1 + y_{n+1} \times z_n)\right] \, mod \, 1$$

where $0 < a \leq 3.999$, $| k_1 | > 37.7$, $| k_2 | > 39.7$, $| k_3 | > 37.2$ respectively. To increase the key size we can use k_1, k_2, k_3 as another set of keys. Along with the key k_i the distribution of the sequences becomes better. Figure 3, shows that the aforementioned problems of stable windows, blank windows, uneven distribution of sequences and weak key have been completely resolved.

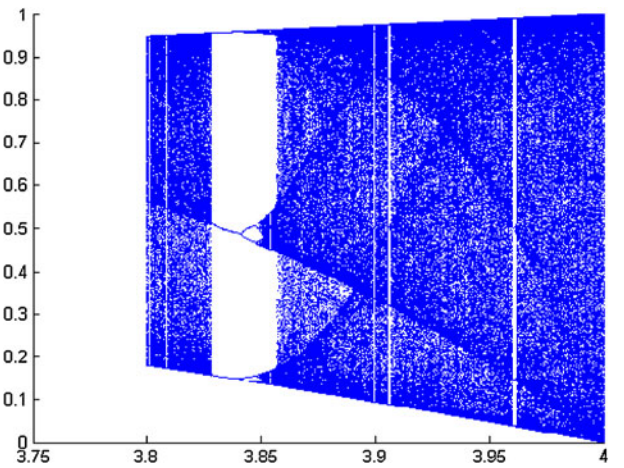


Fig. 2 Blank window for the logistic map

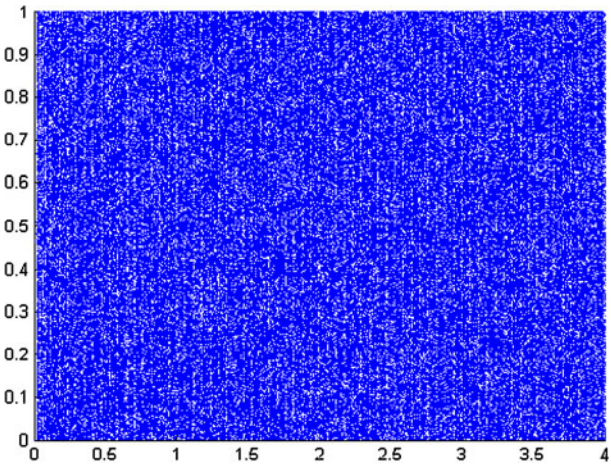


Fig. 3 Transformed logistic map of each map

Thus, the proposed transformed logistic map does not have security issues which are present in the logistic map (1). Moreover, the resulting chaotic sequences are uniformly distributed and the key size has been increased greatly.

3 The proposed encryption scheme

The plain image is stored in a two dimensional array of $\{R_{i,j}, G_{i,j}, B_{i,j}\}$ pixels. In this, $1 \leq i \leq H$ and $1 \leq j \leq W$, where H and W represent height and width of the plain image in pixels.

3.1 Key generation

With the help of proposed transformed logistic maps, the key has been generated in the following way:

$$
\begin{aligned}
&for\, i = 1\, to\, 256\\
&\quad for\, j = 1\, to\, 256\\
&\qquad x_{i,j+1} = (3.735 \times (1 + x_{i,j})^2 \times k_1 \times sin(1/1 + (y_{i,j})^2))\ mod\ 1\\
&\qquad y_{i,j+1} = (3.536 \times x_{i,j+1} \times k_2 \times sin(x_{i,j+1} \times y_{i,j}) \times (1 + (z_{i,j})^2))\ mod\ 1\\
&\qquad z_{i,j+1} = (3.828 \times x_{i,j+1} \times k_3 \times (1 + y_{i,j+1} \times z_{i,j}))\ mod\ 1\\
&\qquad X_{i,j} = \lfloor x_{i,j+1} \times 256 \rfloor\\
&\qquad Y_{i,j} = \lfloor y_{i,j+1} \times 256 \rfloor\\
&\qquad Z_{i,j} = \lfloor z_{i,j+1} \times 256 \rfloor\\
&\quad end\\
&\quad x_{i+1,1} = x_{i,j+1}\\
&\quad y_{i+1,1} = y_{i,j+1}\\
&\quad z_{i+1,1} = z_{i,j+1}\\
&end
\end{aligned}
$$

Confusion and diffusion are the two properties of the operation of a secure cipher. Confusion refers to making the relationship between the key and the cipher text as complex as possible. Generally, the confusion effect is considered by permutation stage, while the diffusion effect is found in the pixel value diffusion stage.

3.2 Initial permutation

The chaos based image encryption schemes are mainly consisting of image pixel permutation stage and pixel value diffusion stage. Our new confusion stage is composed of position permutation and simple pixel value modification. The proposed image encryption process uses the 128-bit long secret key. There are six random odd integers keys obtained in the range 0–256 from the secret key. Then, the pixels are permuted using the following operations:

$$
\begin{aligned}
&for\, i = 1\, to\, H\\
&\quad for\, j = 1\, to\, W\\
&\qquad R_{i,j} = R_{(1+(i\times oddkey(1)\times 31) mod\, 256,\ 1+(j\times oddkey(2)\times 31) mod\, 256)}\\
&\qquad G_{i,j} = G_{(1+(i\times oddkey(3)\times 31) mod\, 256,\ 1+(j\times oddkey(4)\times 31) mod\, 256)}\\
&\qquad B_{i,j} = B_{(1+(i\times oddkey(5)\times 31) mod\, 256,\ 1+(j\times oddkey(6)\times 31) mod\, 256)}\\
&\quad end\\
&end
\end{aligned}
$$

This method is used to improve the pixel scrambling of the image.

3.3 Nonlinear diffusion

Diffusion refers to the property that redundancy in the statistics of the plain text is dissipated in the statistics of the cipher text. The RGB diffusion is done by 4 bit circular shift method then, addition between shifted value and the first chaotic key. The resultant values were xoring with second chaotic key. The combination of 4 bit circular shift, secret key addition and xoring makes the encryption operation nonlinear and hence the system becomes strong against known/chosen plaintext attack. The procedure for the nonlinear diffusion is as follows:

$$
\begin{aligned}
&for\, i = 1\, to\, H\\
&\quad for\, j = 1\, to\, W\\
&\qquad R_{i,j} = ((R_{i,j} \ggg 4) + X_{i,j})\ mod\ 256\\
&\qquad R_{i,j} = R_{i,j} \oplus Y_{i,j}\\
&\qquad G_{i,j} = ((G_{i,j} \ggg 4) + X_{i,j})\ mod\ 256\\
&\qquad G_{i,j} = G_{i,j} \oplus Y_{i,j}\\
&\qquad B_{i,j} = ((B_{i,j} \ggg 4) + X_{i,j})\ mod\ 256\\
&\qquad B_{i,j} = B_{i,j} \oplus Y_{i,j}\\
&\quad end\\
&end
\end{aligned}
$$

where $X_{i,j}$ and $Y_{i,j}$ are the first and second chaotic key.

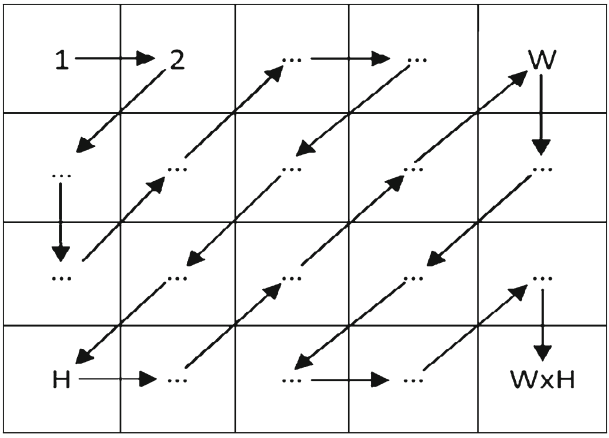


Fig. 4 Zig-Zag pixel value reading

3.4 Zig-Zag diffusion

In this, we read the values in the zig-zag (see Fig. 4) manner as follows: $R_{11}, R_{12}, R_{21}, R_{31}, R_{22}, R_{13}, R_{14}, R_{23}, R_{32}, R_{41}$ etc. However, the diffusion is obtained with the help of zig-zag xoring and xoring with third chaotic key. Therefore, these operations enhance diffusion property and hence improves the security features.

The procedure for zig-zag diffusion for the red channel is as follows:

$$
\begin{aligned}
R_{11} &= R_{11} \oplus Z_{11},\\
R_{12} &= R_{12} \oplus R_{11} \oplus Z_{12},\\
R_{21} &= R_{21} \oplus R_{12} \oplus Z_{21},\\
R_{31} &= R_{31} \oplus R_{21} \oplus Z_{31},\\
R_{22} &= R_{22} \oplus R_{31} \oplus Z_{22},\\
R_{13} &= R_{31} \oplus R_{22} \oplus Z_{13},\\
R_{14} &= R_{14} \oplus R_{13} \oplus Z_{14},\\
&\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots
\end{aligned}
$$

where Z is the third chaotic key. The above procedure is continued till the last pixel is reached. The similar procedure is applied for the other channels.

4 Security analysis

A good encryption scheme should resist all kinds of known attacks, such as known-plaintext attack, ciphertext only attack, statistical attack, differential attack, and various brute-force attacks. Some security analyses have been performed on the

proposed image encryption scheme, including the most important ones like key space analysis, statistical analysis, and differential analysis, which have demonstrated the adequate security of the new scheme, as shown in the following.

4.1 Statistical analysis

Statistical analysis has been performed on the proposed image encryption algorithm, demonstrating its superior confusion and diffusion properties which strongly resist statistical attacks. This is shown by test on the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

4.1.1 Histogram analysis

Histogram analysis is used to illustrate the confusion and diffusion properties in the encrypted data. We have chosen USC-SIPI image database (freely available at http://sipi.usc.edu/database/) for testing purposes. The histogram of the plain image 'Lena' and the histogram of the encrypted image are shown Fig. 5. Comparing the two histograms, we observed that histogram of encrypted image is fairly uniform and is significantly different from that of the original image, and that the encrypted images transmitted do not provide any suspicion to the attacker, which can strongly resist statistical attacks.

4.1.2 Correlation of two adjacent pixels

The effect of image scrambling is related to the correlation of adjacent pixels: the lager the correlation, the worse the scrambling effect, conversely, the better the scrambling effect. To test the correlation between two adjacent pixels in plain image and encrypted image, we have analysed the correlation between various pairs of plain and cipher images. We have been used the following formulae to calculate the correlation coefficients in horizontal, vertical and diagonal. The calculated results are listed in Table 1.

$$r_{\alpha\beta} = \frac{cov(\alpha, \beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}}$$

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N} \alpha_i$$

$$D(\alpha) = \frac{1}{N}\sum_{i=1}^{N} (\alpha_i - E(\alpha))^2$$

$$cov(\alpha, \beta) = \frac{1}{N}\sum_{i=1}^{N} (\alpha_i - E(\alpha))(\beta_i - E(\beta))$$

where α and β denote two adjacent pixels and N is the total number of duplets (α, β) obtained from the image.

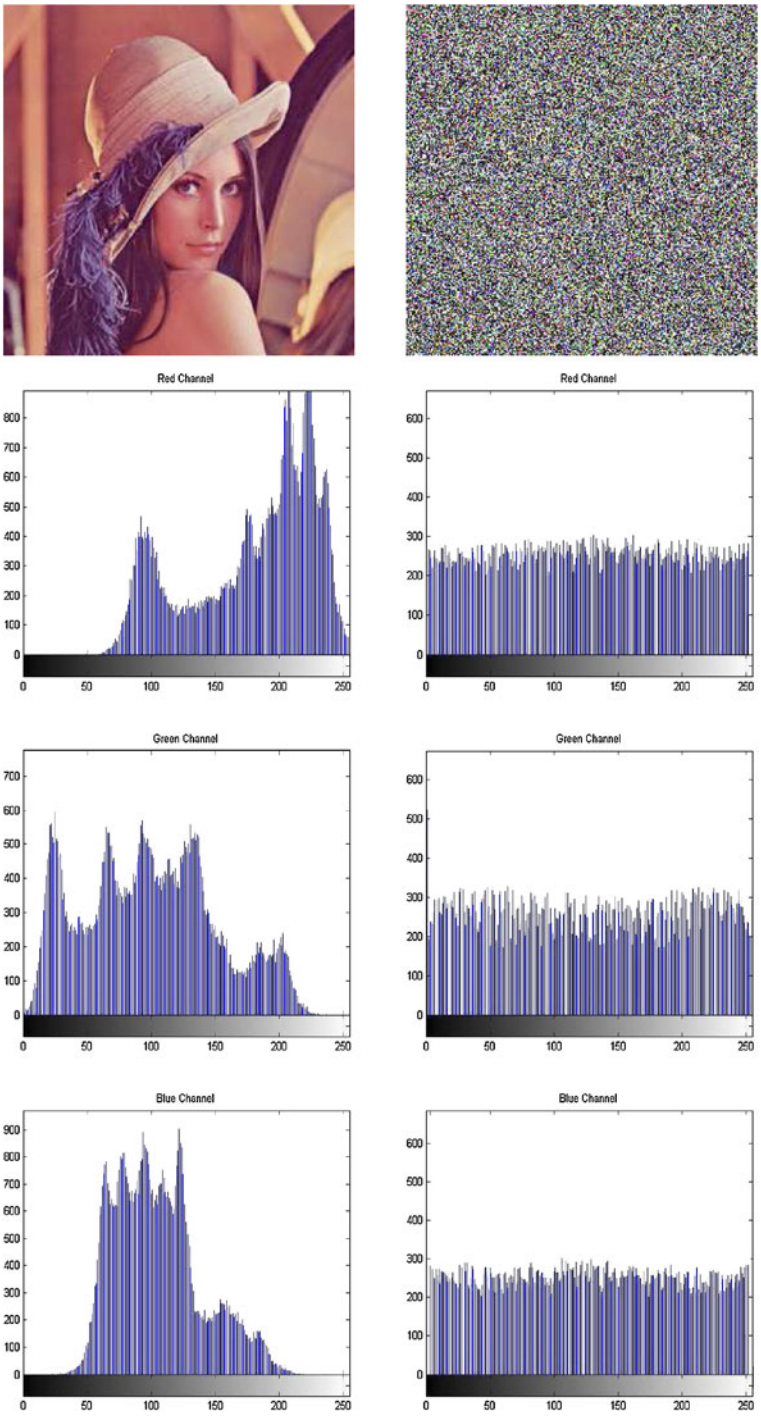


Fig. 5 Histogram of plain image Lena and its encrypted image

Table 1 Correlation coefficients of two adjacent pixels in plain-image and ciphered-image

	Plain image	Ciphered image	
		Proposed	Patidar et al. [10]
Horizontal	0.9718	0.0063	0.0117
Vertical	0.9453	0.0059	0.0102
Diagonal	0.9211	0.0073	0.0153

4.2 Key space analysis

An ideal encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. In the proposed scheme, the initial conditions and parameters of three maps are used as keys. The total number of different keys that can be used in the encryption/decryption scheme. One may see the key space is large enough to resist the attacks. The key space is approximately 2^{192}. If the multiplier k_1, k_2, k_3 used in the transformed map are also used as part of the key, then the key space increased to 2^{400} approximately.

As shown in Table 2, the proposed scheme has largest key space size than those other schemes.

4.3 Key sensitivity analysis

Key sensitivity means that the change of a single bit in the secret key should produce a completely different encrypted image. A typical key sensitivity test has been performed in the following steps:

(i) A RGB image is encrypted by using the test key "432A4E394E1CE4A0BEB9175FC9AD3674".
(ii) The key is changed slightly to "532A4E394E1CE4A0BEB9175FC9AD3674" and used to encrypt the same image.
(iii) The two cipher-images are compared pixel-by-pixel.

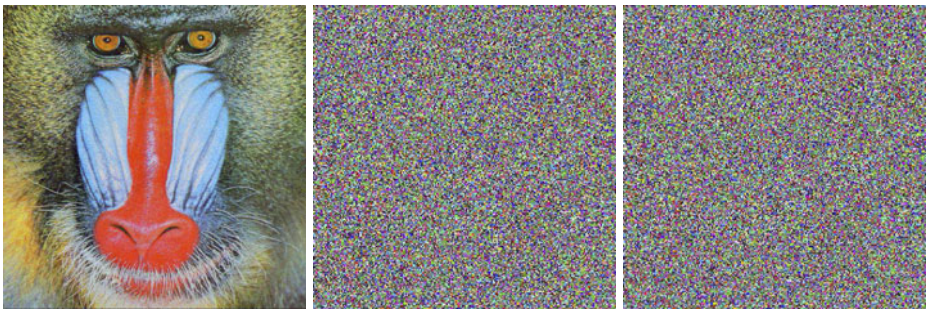
There is a 99.702% difference between the two cipher-images. It shows that this algorithm has a great sensitivity to the key. The test results are shown in Fig. 6.

4.4 Differential analysis

A desirable property for the proposed cipher is its sensitivity to small change in the plainimage (single bit change in plainimage). To test the influence of one-pixel change on the plainimage, encrypted by the proposed cipher, two common measures may be used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI).

Table 2 Key space size of the proposed scheme and different encryption scheme

Encryption scheme	Proposed	Chen et al. [3]	Pareek et al. [9]	Patidar et al. [10]
Key space size	2^{400}	2^{128}	2^{80}	2^{157}



(a) (b) (c)

Fig. 6 Key sensitivity test: **a** Plain-image; **b** cipher-image using key "432A4E394E1CE4A0BEB-9175FC9AD3674"; **c** Cipher-image using key "532A4E394E1CE4A0BEB9175FC9AD3674"

First, $NPCR_{R,G,B}$ is used to measure the number of pixels in difference of a particular color channel in two cipher images corresponding to two plain images having one pixel difference and produced using the same secret key. If $C_{R,G,B}(i,\ j)$ and $C'_{R,G,B}(i,\ j)$ (where $1 \leq i \leq H$ and $1 \leq j \leq W$, H is height and W is width and R, G and B represent red, green and blue channels) represent two cipher images whose plain images have only one pixel difference. It is defined as

$$NPCR_{R,G,B} = \frac{\sum_{i,j} D_{R,G,B}(i,\ j)}{W \times H} \times 100\%$$

where W and H are the width and height of two random images and $D_{R,G,B}(i,\ j)$ is defined as

$$D_{R,G,B}(i,\ j) = \begin{cases} 0 & C_{R,G,B}(i,\ j) = C'_{R,G,B}(i,\ j) \\ 1 & C_{R,G,B}(i,\ j) \neq C'_{R,G,B}(i,\ j) \end{cases}$$

Second, $UACI_{R,G,B}$, is used to measure the average intensity difference in a color component between two cipher images $C_{R,G,B}(i,\ j)$ and $C'_{R,G,B}(i,\ j)$. It is defined as

$$UACI_{R,G,B} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|\ C_{R,G,B}(i,\ j) - C'_{R,G,B}(i,\ j)\ |}{2^{L_{R,G,B}} - 1}\right] \times 100\%$$

Table 3 Sensitivity to ciphertext

Cipher images	NPCR %		UACI %	
	Proposed	Patidar et al. [10]	Proposed	Patidar et al. [10]
Lena	99.6092	99.0392	33.4891	33.4173
Baboon	99.6137	99.2676	33.4732	33.4292
House	99.6113	99.5865	33.4342	33.4187
Tree	99.6135	99.6084	33.4324	33.4365

Table 4 The entropy analysis of the proposed and other schemes

Cipher	Proposed	RC5	RC6	Pareek et al. [9]	Patidar et al. [10]
Lena	7.9993	7.9812	7.9829	7.9884	7.9923
Lion	7.9993	7.9863	7.9898	7.9912	7.9945

where $L_{R,G,B}$ is the number of bits used to represent the color component of red, green and blue respectively. The results of NPCR and UACI are presented in Table 3 for the different images.

In order to assess the influence of changing a single pixel in the original image on the encrypted image, the $NPCR_{R,G,B}$ and the $UACR_{R,G,B}$ is computed in the proposed scheme. It can be found that the NPCR is over 99% and the UACI is over 33%. The results show that a small change in the original image will result in a significant difference in the cipherimage, so the scheme proposed has a good ability to anti differential attack.

4.5 Performance analysis

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. The simulator for the proposed scheme was implemented using MATLAB 7.4. Performance was measured on a 3.0 GHz Pentium Core 2 Duo with 4 GB RAM running Windows Vista Business Edition. Simulation results show that the average running speed is 21.02 MB/s for encryption and 22.04 MB/s for decryption.

4.6 Information entropy analysis

Information entropy is one of the criteria to measure the strength of the cryptosystem in symmetric cryptosystem. The entropy $H(m)$ of a message m can be calculated as

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) log \frac{1}{p(m_i)}$$

where $p(m_i)$ represents the probability of occurrence of symbol m_i and log denotes the base 2 logarithm. If there are 256 possible outcomes of the message m with equal probability, it is considered as random. In this case, $H(m) = 8$, is an ideal value. In the final round of proposed scheme, it is found that the value is 7.9993.

As shown in Table 4, we notice that the values obtained of our scheme are very close to the theoretical value of 8 than other schemes. This means that information leakage in the encryption process is negligible and the encryption system is secure upon entropy attack.

5 Conclusion

In this paper, a novel secure cryptosystem for direct encryption of color images, based on transformed logistic maps has been proposed. The proposed cipher

provides good confusion and diffusion properties that ensures extremely high security. Confusion and diffusion have been achieved using permutation, nonlinear diffusion and zig-zag diffusion. We have carried out statistical analysis, key sensitivity analysis, differential analysis, entropy analysis and key space analysis to demonstrate the security of the new image encryption procedure. Based on the various analyses, it has been shown that the proposed scheme is more secure and speed and may be found suitable for real time image encryption for transmission applications.

Acknowledgements This research is partially supported by the All India Council for Technical Education, New Delhi, India.

References

1. Alvarez G, Li S (2009) Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption. Commun Nonlinear Sci Numer Simulat 14:3743–3749
2. Baptista MS (1998) Cryptography with chaos. Phys Lett A 240:50–54
3. Chen GR, Mao YB, Charles KC (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons Fractals 21:749–761
4. Gao TG, Chen ZQ (2008) Image encryption based on a new total shuffling algorithm. Chaos, Solitons Fractals 38:213–220
5. Jun H, Zheng J, Li Z-b, Qian H-f (2009) An improved color image encryption based on chaotic map and OCML model. In: IEEE international conference on networks security, wireless communications and trusted computing, pp 365–369
6. Liu S, Sun J, Xu Z, Liu J (2008) Analysis on an image encryption algorithm. In: IEEE international workshop on education technology and training & international workshop on geoscience and remote sensing, pp 803–806
7. Matthew R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia 8(1):29–42
8. Menezes AJ, Oorschot PCV, Vanstone SA (1997) Handbook of applied cryptography. CRC Press, Boca Raton, FL
9. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24:926–934
10. Patidar V, Pareek NK, Sud KK (2009) A new substitution diffusion based image cipher using chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simulat 14:3056–3075
11. Rhouma R, Solak E, Belghith S (2010) Cryptanalysis of a new substitution-diffusion based image cipher. Commun Nonlinear Sci Numer Simulat 15:1887–1892
12. Sabery MK, Yaghoobi M (2008) A new approach for image encryption using chaotic logistic map. In: IEEE international conference on advanced computer theory and engineering, pp 585–590
13. Schneier B (1996) Applied cryptography: protocols algorithms and source code in C. Wiley, New York, USA
14. ShuTang LIU, Sun FY (2009) Spatial chaos-based image encryption design. Sci China Ser G Phys Mech Astron 52(2):177–183
15. Xiao H-P, Zhang G-J (2006) An image encryption scheme based on chaotic systems. In: IEEE international conference on machine learning and cybernetics, pp 2707–2711
16. Xie J, Yang C, Tian L (2009) An encryption algorithm based on transformed logistic map. In: IEEE international conference on network security, wireless communications and truested computing, pp 111–114
17. Xu S-J, Wang Y-L, Wang J-Z, Tian M (2008) A novel image encryption scheme based on chaotic maps. In: IEEE ICSP, pp 1014–1018
18. Zhang Y, Wang Y, Shen X (2007) A chaos-based image encryption algorithm using alternate structure. Sci China Ser F Inf Sci 50(3):334-341

I. Shatheesh Sam received Master of Computer Science and Engineering from Sathyabama University, India, in 2006. Currently, he is pursuing his Ph.D. degree at Anna University Chennai, India. His research is partially supported by the All India Council for Technical Education, New Delhi, India. His research interests include multimedia security, network security and image processing. He is life member of CSI, ISTE and student member of IEEE.

P. Devaraj received Master of Science degree in Mathematics from Manonmaniam Sundaranar University in 1993 and Master of Philosophy degree in Mathematics from Department of Mathematics, Madurai Kamaraj University in 1994. He has obtained his Ph.D. degree in Harmonic Analysis from Indian Institute of Technology, Bombay in 2000. He has also worked for two years in the Research and Development laboratory of Tata Infotech Ltd., located at Department of Computer Science at Indian Institute of Technology, Bombay. He is currently working as Assistant Professor in the Department of Mathematics, College of Engineering, Guindy, Anna University Chennai, India. His recent research interests include Cryptography, Image processing, Harmonic Analysis, Reconstruction from Local Averages and Computational Number Theory.

Raghuvel S. Bhuvaneswaran received Master of Technology in Computer Science and Engineering from Pondicherry University, India, in 1996 and Ph.D. in Computer Science and Engineering from Anna University, India, in 2003. He is a post doctoral fellow (2004–2006) of JSPS, Japan. Presently, he is with Anna University as Associate Professor. His research interests include distributed systems, mobile computing, network security and fault tolerant systems.