Mathematical and Computer Modelling 57 (2013) 2576–2579

Contents lists available at SciVerse ScienceDirect

Mathematical and Computer Modelling

journal homepage: www.elsevier.com/locate/mcm

Application of S-box and chaotic map for image encryption

Iqtadar Hussain [*], Tariq Shah, Muhammad Asif Gondal

Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
National University of Computer and Emerging Sciences, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 27 October 2011
Received in revised form 10 January 2013
Accepted 22 January 2013

Keywords:
S-box
UACI
NPCR

ABSTRACT

In this work we propose a method for image encryption based on chaotic skew tent-map and substitution box transformation. This method provides confusion and diffusion at the same time. It is well known from literature that simple image encryption based on a total shuffling scheme is not secure against different types of attacks. We then projected an extended algorithm which works well against chosen cipher text attacks due to the substitution box operation. Furthermore we analyze the proposed technique for NPCR and UACI analysis to determine its strength.

1. Introduction

A large amount of worry has been brought up regarding the security of digital images that are transmitted over stored or open channels with the dynamic developments in the communications and multimedia industry. The unauthorized handling of digital images makes it extremely crucial for the images to be guarded against it. Data can be guarded by costumed cryptographic standards like the IDEA or AES. However it is not possible to encrypt images through these methods due to the colossal data dimensions and increased correlation between pixels in image files. For this matter, chaos-based algorithms have proved to be superior for encrypting images. Chaotic systems that fit the major requirements of confusion and diffusion are differentiated on the basis of their reactiveness to initial conditions and control parameters, pseudo-randomness, and ergodicity. This makes chaotic systems particularly catch heaps of heed for cryptology [1–5].

A few chaos-based algorithms of image encryption with a permutation–diffusion layout are defragmented. The key streams used to encrypt plain images are the same and independent of them and hence provide a mutual characteristic between these algorithms. For security betterment, an original image encryption method based on a skew tent map was brought forward by Zhang and Liu in [6]. Their schema is a depiction of the operations of permutation and diffusion to harvest the necessary confusion and diffusion effect. Such a method has numerous advantages such as abundant key space, decreased encryption time, increased key sensitivity, and a few other things. Nevertheless, the author figured that this particular method is exposed to a particular plaintext attack and put forth a successful plaintext attack. However, they have not come up with the whole random code sequence utilized in the diffusion operation, and therefore it is not easy to decipher other cipher text images encrypted through their algorithm. An attack method contrasting to the original attack method presented by the researches is presented in this paper by us. Through this attack method, the whole random code sequence $\{d_{ij} = 1, 2, \ldots\}$ and the transformation sequence $T = \{t\,(i)\,, i = 1, 2, \ldots, M \times N\}$ can be achieved, which can then be used effectively and appropriately to decipher any other cipher text images encrypted by Zhang and Liu's algorithm.

The layout of the paper is as follows: Section 2 presents Zhang and Liu's algorithm. Section 3 consists of the algebraic expression of chaotic substitution box. Section 4 presents cryptanalysis and chosen plaintext together with cipher text attack on their algorithm schema. Section 5 presents a better and more efficient algorithm. Section 6 consists of experimental

[*] Corresponding author at: Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan.
E-mail address: iqtadarqau@gmail.com (I. Hussain).

0895-7177/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
doi:10.1016/j.mcm.2013.01.009

results and analyses of security issues of the more efficient algorithm proposed in Section 5. The last part is the conclusion and future work.

2. Proposed cryptosystem

The algebraic expression of skew tent map [6] is as follows:

$$X_{n+1} = f\left(X_n, p\right) = \begin{cases} \dfrac{X_n}{p}, & \textit{if } X_n \in [0, p] \\ \dfrac{(1 - X_n)}{(1 - p)}, & \textit{if } X_n \in (p, 1] \end{cases} \tag{1}$$

is accepted. $xn \in [0, 1]$ is the state of the system, and $p \in (0, 1)$ is the control parameter. The encryption scheme consists of two processes namely pixel permutation and diffusion.

Consider a gray image of size $M \times N$; transform the two-dimensional image into one-dimensional vector $V = \{p_1, p_2, \ldots, p_{M\times N}\}$, where the value of pixels in the plain image is denoted by p_i in the row $\textit{floor}\,(i/N)$ and column mod (i, N). If x_0 and p given, we can iterate the skew tent map of Eq. (1) for L number of times to eliminate the transient effect, where L is any constant number. We can then continuously repeat this process to iterate the skew tent map for $M \times N$ times to get the chaotic sequence $X = \{x_i, i = L + 1, L + 2, \ldots, L + M \times N\}$. The positions of pixels in the image are shuffled with the help of a permutation method and we then sort them according to chaotic sequence. Now assume that the sorted chaotic sequence is $Y = \{y_i, i = L + 1, L + 2, \ldots, L + M \times N\}$. Now we have to get the transformation sequence $T = \{t\,(i)\,, i = 1, 2, \ldots, M \times N\}$ such that the value of y_{L+i} and $x_{L+t(i)}$ exactly coincide with each other. Now, shift the $t(i)$th pixel $p_t(i)$ in the original image to the place of the ith pixel $p_i{}'$ in the cipher text image, so we have, $p_i{}' = p_t\,(i)$ where $(i = 1, 2, \ldots, M \times N)$. The total number of iterations of chaotic map in the permutation step is denoted by r, and $r = L + M \times N$. Furthermore we transform the chaotic cipher image with the help of chaotic substitution boxes [7] to improve the confusion capability of the proposed encryption scheme.

3. Permutation and substitution

In the diffusion process, we will find these steps:
1. Suppose $I \leftarrow 1$.
2. Produce the preliminary condition value X and control parameter Q of the skew tent map by using the formula given below respectively:

$$X = (P_0' + \alpha)/(255 + \alpha + \beta) \tag{2}$$

$$Q = (T\,(1) + \alpha)/(M \times N + \alpha + \beta) \tag{3}$$

where $P_0' \in [1, 255]$, $T(1)$ is the initial value of the string $\boldsymbol{T}$ produced in the permutation process, $\alpha, \beta \in \{1, 2, 3, \ldots, M\times N\}$. Consequently $X \in (0, 1), Q \in (0, 1)$.
3. Iterate the chaotic map (1) once to obtain the new value X.
4. We can get a random code d with the help of the formula below:

$$D = \text{mod}(\textit{floor}\left(X \times 2^{48}\right), 256). \tag{4}$$

5. Encipher the first pixel with the help of the formula below:

$$C_1 = D \oplus \text{mod}(P_1' + P_0' + D + \alpha, 256). \tag{5}$$

6. Suppose $I = I + 1$.
7. Produce the preliminary condition value X and control parameter Q of the skew tent map by using the formula given below respectively:

$$X = (C_{I-1} + \alpha)/(255 + \alpha + \beta) \tag{6}$$

$$Q = (T\,(I) + \alpha)/(M \times N + \alpha + \beta) \tag{7}$$

where $T\,(I)$ is the Ith value of the $\boldsymbol{T}$ sequence produced in the permutation process; $X \in (0, 1)\,, Q \in (0, 1)\,.$
8. Iterate the chaotic map (1) once to obtain the new value X.
9. D is determined by using X with the help of Eq. (4).
10. Encipher the first pixel with the help of the formula below:

$$C_I = D \oplus \text{mod}(P_I' + C_{I-1} + D + \alpha, 256). \tag{8}$$

11. Repeat steps 6–10 in anticipation of I reaching $M \times N$.
Now for the confusion process we perform the following steps.

12. After the permutation process find the inverse of each pixel x of C with the help of the formula given below:

$$y = I(x) = \begin{cases} x^{-1} & \textit{if } x \neq 0 \\ 0 & \textit{if } x = 0 \end{cases} \tag{9}$$

where $x \in GF(2^8)$ (Galois field of order 256).

13. Now transform each pixel y with the help of affine transformation given below:

$$AT(y) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}. \tag{10}$$

Now for the decryption process move in the reverse order. Some steps which are not trivial are explained below:

$$AT^{-1}(y) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \tag{11}$$

where AT and AT^{-1} are the affine transformation and its inverse while the vector y is the multiplicative inverse of the input byte x.

Decryption of the diffusion step of Ith pixel is done using the following formulas:

$$C_I = \text{mod}(D \oplus C_I - C_{I-1} - D - \beta, 256) \tag{12}$$

where $I = M \times N, M \times N - 1, \ldots, 2$.

$$C_I = \text{mod}(D \oplus C_I - C_{N-1} - D - \beta, 256) \tag{13}$$

for $I = 1$.

With this decryption procedure we will get the plain image corresponding to the cipher image C.

4. Sensitivity analysis

The average density between two images can be measured by UACI [8] i.e. unified average changing intensity. Two plain images different that are different in only one pixel can be encrypted and combined to obtain cipher images CA and CB. In this case UACI can be represented as:

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M \times N} \frac{|ca_i - cb_i|}{255}. \tag{14}$$

In the above mentioned equation ca_i and cb_i are the ith pixels of the cipher image. If we take an 8-bit, the value of UACI comes out to be 0.3446. For experimental purposes we have chosen a set of 8 different pixels, one at a time, changing their value slightly by 1. As shown in Table 1, all values of UACI in the second row are very close to the ideal value.

NPCR [9] is a relatively better indicator of sensitivity of the algorithm corresponding to image encryption i.e. the change in the pixels of the cipher image if one of the pixels from the plain image is changed. We can calculate NPCR by:

$$\text{NPCR} = \frac{\#\{i | ca_i \neq cb_i\}}{M \times N}. \tag{15}$$

For an ideal image encryption algorithm NPCR is usually expected to turn out as $1\text{–}2^{-8}$ (about 0.9961). During experimentation, we randomly chose around eight unique pixels (one by one, including the first and last pixels of the image) in each plain image and slightly altered their value (change the lowest bit of gray-scale value). In Table 1, the values of NPCR are presented in the third row, all of which are close to 0.9961.

Table 1
Value of UACI and NPCR for ciphered Baboon image.

Position	1	256	512	32 767	32 768	64 769	65 281	65 536
UACI	0.3261	0.3261	0.3264	0.3259	0.3253	0.3261	0.3255	0.3262
NPCR	0.9866	0.9881	0.9864	0.9873	0.9899	0.9893	0.9899	0.9868

5. Conclusions

We have therefore a good image encryption algorithm. The value of NPCR and UACI analysis of the anticipated algorithm are very close to the optimal value. Furthermore, this algorithm provides extra confusion due to chaotic substitution box transformation. Basically this algorithm directly hits the S–P network idea of Shanon due to the permutation and substitution operation.

References

[1] X. Tong, M. Cui, Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation, Sci. China Inf. Sci. 53 (2010) 191–202.

[2] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, Opt. Commun. 285 (2012) 29–37.

[3] O. Mirzaei, M. Yaghoobi, H. Irani, A new image encryption method: parallel sub-image encryption with hyperchaos, Nonlinear Dyn. 67 (2011) 557–566.

[4] X. Huang, Image encryption algorithm using chaotic Chebyshev generator, Nonlinear Dyn. 67 (2011) 2411–2417.

[5] I. Hussain, T. Shah, M.A. Gondal, Image encryption algorithm based on PGL(2, GF(2^8)) S-boxes and TD-ERCS chaotic sequence, Nonlinear Dyn. 70 (1) (2012) 181–187.

[6] G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Opt. Commun. 284 (2011) 2775–2780.

[7] M. Khan, T. Shah, H. Mahmood, M.A. Gondal, I. Hussain, A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems, Nonlinear Dyn. 70 (2012) 2303–2311.

[8] I. Shatheesh Sam, P. Devaraj, R.S. Bhuvaneswaran, An intertwining chaotic maps based image encryption scheme, Nonlinear Dyn. 69 (2012) 1995–2007.

[9] Q. Zhou, X. Liao, Collision-based flexible image encryption algorithm, J. Syst. Softw. 85 (2012) 400–407.