Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090627

An Image Encryption Scheme based on Nonlinear Chaotic Algorithm and Substitution Box Transformation

Muhammad Asif Gondal[1] *and Iqtadar Hussain*[2,*]

[1] Department of Mathematics and Sciences, Dhofar University, Salalah, Oman.
[2] Department of Mathematics, King Khalid University, Abha, Saudi Arabia.

Received: 24 Feb. 2015, Revised: 24 Apr. 2015, Accepted: 25 Apr. 2015
Published online: 1 Nov. 2015

Abstract: In this paper, we have presented an image encryption algorithm based on chaotic shuffling map and S-box transformation. We test the proposed algorithm with some well-known security analysis such as correlation analysis, UACI analysis, histogram analysis, information entropy analysis and NPCR analysis and come to close that the proposed algorithm fulfils these criterion with optimal values.

Keywords: Image encryption, Block cipher, S-box, chaotic map

1 Introduction

It has always been man's desire to keep information secret and hidden from other people. Even kids use cipher to communicate with each other to keep it away from their parents or teachers. There are many examples in the past where people tried to hide information from the opponents using various methods. Emperors and Military officials passed on information to their forces with the help of basic encoding techniques to make it sure that military information is not leaked.

With the evolution of society, it is the need of the hour to use refined techniques to keep data secure. At the present time, the information era has made it imperative to make data as secure as possible. The information age has connected the word, and made it world a global village. With the increase in the demand for information and electronic services, we have become more dependent on electronic systems. Nowadays, online transactions, online banking and exchange of debit or credit card numbers have become part of our everyday life. Along with this, protection of data and electronic systems is pivotal to our living.

Cryptography is an art of protecting information. The subject of cryptography has three different titles that are 1) Cryptology, 2) Cryptography and 3) Cryptanalysis. Though these terms are used interchangeably, yet cryptology is a blanket term for the investigation over insecure channels and associated complications and problems. Cryptography is the procedure of creating systems to achieve this purpose. On the other hand, cryptanalysis is about breaking such systems. Obviously, it is not possible to do cryptanalysis or cryptography without having thorough knowledge of both disciplines.

In [1–15] different chaotic cryptographic image, encryption and S-box construction techniques are presented. Chaotic Image encryption is a branch of cryptography in which we encrypt image data with the help of cryptographic tools based on chaos theory. With the rapid development of computer technology, protection of digital images against illegal copying and distribution has become more and more important. Utilizing the merits of chaos-system to protect image security is a research hot point [16–20]. The chaos-based image encryption algorithm in Refs. [16, 19, 20] includes two phases: First, the pixel positions of the original image are permuted. Then the gray values of the permuted image are encrypted by a chaotic system. The algorithms have lots of merits, such as the sensitivity to the secret keys and the large key space. However, there are some flaws, such as never permuted (0, 0) pixel, the solely dependence of key stream on the initial conditions of chaotic system in the second phase, and the two phases are independent each other. So we can get the correct

* Corresponding author e-mail: iqtadarqau@gmail.com

histogram with the correct hyper-chaos keys in the second phase, which is easy to attack by statistical analysis.

To overcome these drawbacks, a new scheme is presented for image encryption. Shuffling the positions and S-box transformation are performed simultaneously in our approach. The rest of this study is organized as follows. Section 2 describes the proposed scheme. Section 3 presents our experiments and security analyses and finally this study is concluded in Sec. 4.

2 Shuffled by Nonlinear Chaotic Algorithm

Image data have strong correlations among adjacent pixels. In order to disturb the high correlation among pixels, we adopt NCA to shuffle the pixel positions of the plain image. Without loss of generality, we assume the dimension of the plain image is $N \times N$. The NCA is defined as [21].

$$x_{(n+1)} = (1-\beta^{(-4)})tg(\alpha((1-\beta^{(-4))}tg(\alpha x_n)(1-x_n)^{\beta})) \times(1-((1-\beta^{(-4)})tg(\alpha x_n)(1-x_n)\hat{}^{\beta}))^{\beta}. \quad (1)$$

Twhere $x_n \in (0,1), \alpha \in (0,1.4], \beta \in (5,43]$,or $x_n \in (0,1), \alpha \in (1.4,1.5], \beta \in (9,38]$,or $x_n \in (0,1), \alpha \in (1.5,1.57], \beta \in (3,15]$.

This map can apply more large key space than Logistic map. For more information about the system, please see relative Ref. [21]. The procedure of shuffling map by nonlinear chaotic algorithm is described as follows:

Step 1 From left to right and top to bottom, we transform two-dimensional image to one-dimensional set $P1(i), i = 1,2,...,N \times N$.

Step 2 Starting from certain initial condition x_0 and parameters α, β. After iterated K times, we continue to iterate the above $N \times N$ times and obtain chaotic sequence $X = \{x_1, x_2, ..., x_{(N\times N)}\}$, then order ascending, we get a new set $Y = \{y_1, y_2, ..., y_{(N\times N)}\}$.

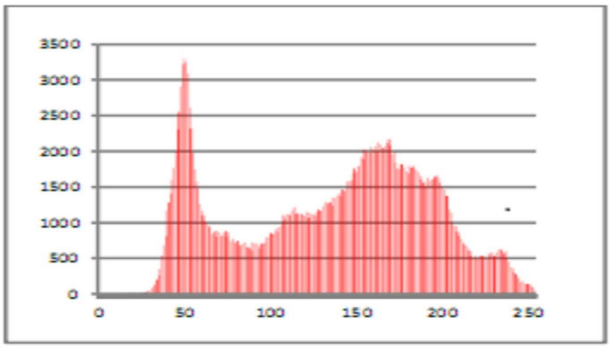
Step 3 According to the address map of to , we transform $P1(i)$ to $P2(i), i = 1,2,...,N \times N$ and record the changed chaotic values $C = \{c_1, c_2, ..., c_{(N\times N)}\}$, where $c_i = abs(y_i - x_i), abs(x)$ returns the absolute value of x.

Step 4 Transform $P2$ to shuffled image $P0$ based on the inverse processes of Step 1.

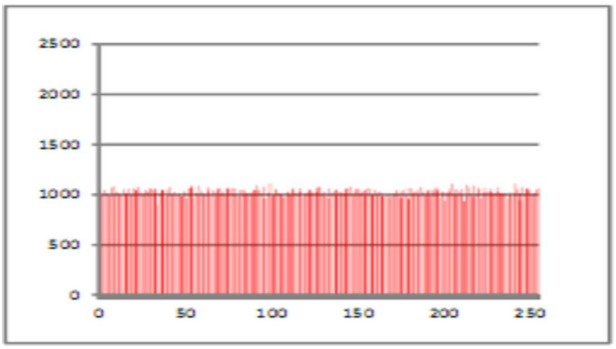
Step 5 In this step, we apply S-box transformation on plain text image. Initially we will find the inverse of each pixel x of original image with the help of formula given below

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

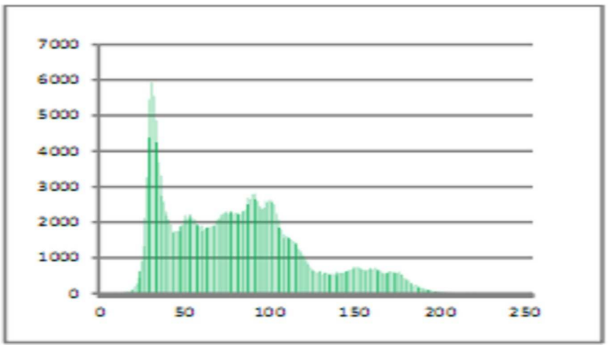
where $x \in GF(2^8)$ (Galois field of order 256). Now transform each pixel y with the help of affine transformation given below:



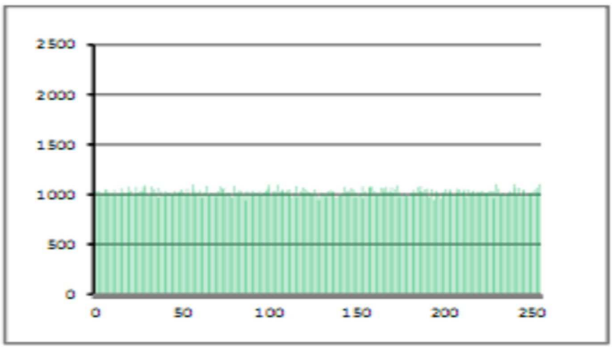
(a)



(b)

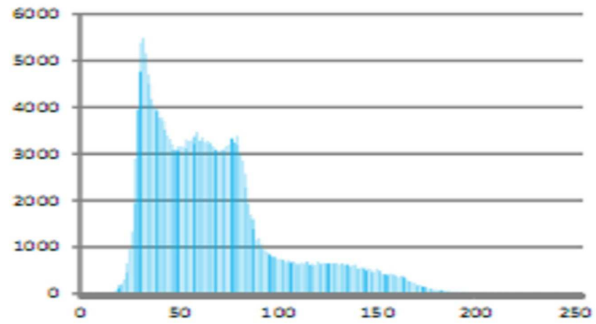


(c)

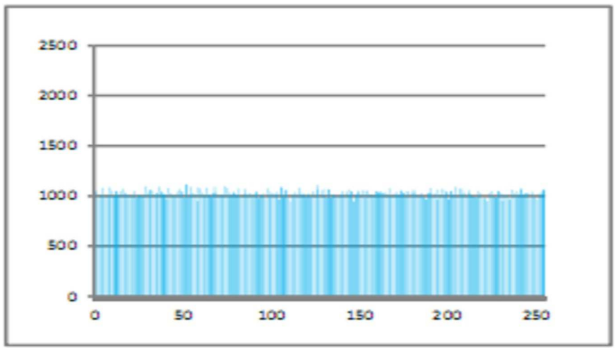


(d)

Fig. 1: Plain, Encrypted and Recovered image of Lena



(e)



(f)

Fig. 2: (a) Histogram of red channel of Lena (c) Histogram of green channel of Lena (e) Histogram of blue channel of Lena (b) Histogram of red channel of cipher (d) Histogram of green channel of cipher (f) Histogram of blue channel of cipher.

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

For the decryption process we move in the reverse order from step 5 to 1 all steps except 5 are quite trivial and easy to manage, so here we will explain the decryption process of step 5 with the help of the following mathematical expression

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

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

3 Analyses of proposed algorithm

In this section we analyze the proposed algorithm with some well known analyses such as histogram analysis, NPCR, UACI, and correlation analysis.

3.1 Histogram analysis

Histograms show the distribution of pixel values in an image. The ideal histogram of a cipher image is uniform. In Figure below, we show the histograms of RGB values of the plain image “Lena” and those of the cipher image of Figure 1.

We can find that the histograms of the cipher image are close to uniform. Thus, a frequency analysis cannot be used to break the algorithm.

3.2 Correlation of two adjacent pixels

The correlation of two adjacent pixels can be calculated according to the following formula:

Table 1: Correlation between the encrypted and the original images

		Original image		Encrypted image	
	R channel	G channel	B channel	The amplitude	The phase
Horizontal	0.7691	0.7649	0.7387	0.0674	−0.0157
Vertical	0.7398	0.7285	0.6937	0.0561	−0.0073
Diagonal	0.7186	0.7083	0.6702	0.0286	−0.0302

$$r_{xy} = \frac{cov(x,y)}{(\sqrt{(D(x))}(\sqrt{D(y)})}$$

where

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))((y_i - E(y))$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i, \text{ where } N = height \times width.$$

First, we test the correlation between various colors of "Lena" and its cipher image, and compare the results.

We can find from table 1 that the proposed algorithm have a much better statistic properties.

3.3 NPCR and UACI

Number of Pixels Change Rate (NPCR) stands for the number of pixels change rate while on pixel of plain image changed. The NPCR gets closer to 100%, the more sensitive the cryptosystem to the changing of plain image, and the more effective for the cryptosystem to resist plaintext attack. UACI (Unified Average Changing Intensity) stands for the average intensity of differences between the plain image and ciphered image. The UACI gets closer to 33.333…%, the more effective for the cryptosystem to resist differential attack.

NPCR and UACI can be calculated as follows

$$UACI = \frac{1}{Width \times Height}\sum_{i,j}\left(\frac{c_1(i,j) - c_2(i,j)}{255}\right) \times 100\%$$

$$NPCR = \frac{\sum_{i,j} D(i,j)}{Width \times Height} \times 100\%$$

Where $c_1(i,j)$ and $c_2(i,j)$ are respectively the cipher-image before and after one pixel of the plain image is changed. And if $c_1(i,j) \neq c_2(i,j)$, $D(i,j) = 1$ otherwise $D(i,j) = 0$.

The results of changing the red value of a pixel show in the table 2. below,

Table 2: Results of NPCR and UACI

Position	Red	Green	Blue
UACI	33.4745%	33.4714%	33.4676%
NPCR	99.6010%	99.6120%	99.6109%

Table 3: Information Entropy

	Red Channel	Blue Channel	Green Channel
Information entropy	7.888258	7.888188	7.888208

3.4 Information entropy

The method to calculate information entropy of an image can be expressed as below

$$H(m) = \sum_{i,=0}^{2^N-1} p(m_i)\log_2\frac{1}{p(m_i)}$$

Where $p(m_i)$ represents the probability of symbol m_i, and $\log_2$ represents the base 2 logarithm so that the entropy is expressed in bits, N represents the number of bits we use to represents a pixel, and for one color channel of a pixel, it's clear that $N = 8$. If an image is ideal random, then for each i, $p(m_i) = 1/256$, and we can easily find that $H(m) = 8$. And the results of cipher image are given in table 3.

4 Conclusions

We propose an image encryption algorithm based on chaotic shuffling map and S-box transformation. Numerical simulations from table 1, 2 and 3 illustrate that the propose Image encryption algorithm is secure. The value of information entropy, correlation analysis, NPCR and UACI analysis of anticipated algorithm are much closed to the optimal value.

References

[1] Iqtadar Hussain, Naveed Ahmed Azam, Tariq Shah, Stego optical encryption based on chaotic S-box transformation, Optics & Laser Technology, Volume 61, September 2014, Pages 50-56.

[2] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Application of S-box and chaotic map for image encryption, Mathematical and Computer Modelling, Volume 57, Issues 9–10, May 2013, Pages 2576-2579.

[3] Iqtadar Hussain, A novel approach of audio watermarking based on -box transformation, Mathematical and Computer Modelling, Volume 57, Issues 3–4, February 2013, Pages 963-969.
[4] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Hasan Mahmood, A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence, Nonlinear Dyn (2013) 73:633–637.
[5] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Hasan Mahmood, A novel image encryption algorithm based on chaotic maps and GF(2^8) exponent transformation, Nonlinear Dyn (2013) 72:399–406,
[6] Amir Anees, Adil Masood Siddiqui, Jameel Ahmed, Iqtadar Hussain, A technique for digital steganography using chaotic maps, Nonlinear Dyn (2014) 75:807–816.
[7] Sajjad Shaukat Jamal, Tariq Shah, Iqtadar Hussain, An efficient scheme for digital watermarking using chaotic map, Nonlinear Dyn (2013) 73:1469–1474.
[8] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Hasan Mahmood, An efficient approach for the construction of LFT S-boxes using chaotic logistic map, Nonlinear Dyn (2013) 71:133–140.
[9] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Hasan Mahmood, Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence, Nonlinear Dyn (2013) 74:271–275.
[10] Iqtadar Hussain, Muhammad Asif Gondal, An extended image encryption using chaotic coupled map and S-box transformation, Nonlinear Dyn, DOI 10.1007/s11071-013-1214-z.
[11] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, A group theoretic approach to construct cryptographically strong substitution boxes, Neural Comput & Applic (2013) 23:97–104.
[12] Iqtadar Hussain, Tariq Shah, Hasan Mahmood, A projective general linear group based algorithm for the construction of substitution box for block ciphers, Neural Comput & Applic (2013) 22:1085–1093.
[13] Iqtadar Hussain, Tariq Shah, Literature survey on nonlinear components and chaotic nonlinear components of block ciphers, Nonlinear Dyn (2013) 74:869–904.
[14] Amir Anees, Waqar Ahmad Khan, Muhammad Asif Gondal, and Iqtadar Hussain, Application of Mean of Absolute Deviation Method for the Selection of Best Nonlinear Component Based on Video Encryption, Z. Naturforsch. 68a, 567 – 572 (2013).
[15] Tariq Shah, Attiq Qamar, and Iqtadar Hussain, Substitution Box on Maximal Cyclic Subgroup of Units of a Galois Ring, Z. Naturforsch. 68a, 479 – 482 (2013).
[16] Z H Guan, F Huang , W Guan. Chaos-based image encryption algorithm. Phys Lett A, 346, 153-157 (2005).
[17] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan. "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps", Phys Lett A, 366-391 (2007).
[18] L H Zhang, X F Liao, X Wang, An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals, 24:759–65 (2005).
[19] T G Gao and Z Q Chen, Image encryption based on a new total shuffling map based on hyper-chaos, Phys. Lett. A, 372, 4, 394-399, (2008).
[20] T G. Gao and Z Q Chen, Image encryption based on a new total shuffling algorithm, Chaos, Solitons and Fractals, 38: 1, 213-220 (2008).
[21] H J Gao, Y S Zhang, S Y liang and D Q Li, A new chaotic algorithm for image encryption, Chaos, Solitons and Fractals, 29: 2, 393-399 (2006).

Muhammad Asif Gondal, Associate Professor, is working at the Dhofar University, Salalah, Oman. Dr Gondal received his PhD degree in Applied Mathematics in 2009 from University of Innsbruck, Austria. His name is included in the list of the most productive scientists issued by Pakistan Council for Science and Technology. He has published more than 70 research papers in recognized journals with high impact factor. He also participated in numerous International Conferences & Talks. He also has to his credit 3 books. To acclaim his one and a half decade experience of teaching and research at prestigious universities like National University of Science and Technology (NUST) and National University of Computer and Emerging Sciences, Islamabad, Pakistan, Dr. Asif Gondal was awarded the Best University Teachers Award for the year 2011 by the Higher Education Commission of Pakistan. His areas of interest include Applied Mathematics, Numerical Analysis, Numerical Methods (exponential integrators) and Financial Mathematics.

Iqtadar Hussain, Assistant Professor, is working at the King Khalid University, Abha, Saudi Arabia. Dr. Hussain received his PhD degree in Mathematics in 2014 from Quaid-i-Azam University, Pakistan. Two times he has been awarded with productive scientist of the year of the Pakistan from Pakistan council of science and technology. He has published more than 60 research papers in recognized journals with high impact factor.