Journal of King Saud University – Computer and Information Sciences (2017) 29, 499–504

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

# A light weight secure image encryption scheme based on chaos & DNA computing

**Bhaskar Mondal** [a,*], **Tarni Mandal** [b]

[a] *Department of Computer Science and Engineering, National Institute of Technology Jamshedpur, Jamshedpur, Jharkhand 831014, India*
[b] *Department of Mathematics, National Institute of Technology Jamshedpur, Jamshedpur, Jharkhand 831014, India*

Received 21 July 2015; revised 3 February 2016; accepted 11 February 2016
Available online 30 March 2016

**KEYWORDS**

Confusion diffusion;
DNA computation;
Encryption;
Logistic map

**Abstract** This paper proposed a new light weight secure cryptographic scheme for secure image communication. In this scheme the plain image is permuted first using a sequence of pseudo random number (PRN) and encrypted by DeoxyriboNucleic Acid (DNA) computation. Two PRN sequences are generated by a Pseudo Random Number Generator (PRNG) based on cross coupled chaotic logistic map using two sets of keys. The first PRN sequence is used for permuting the plain image whereas the second PRN sequence is used for generating random DNA sequence. The number of rounds of permutation and encryption may be variable to increase security. The scheme is proposed for gray label images but the scheme may be extended for color images and text data. Simulation results exhibit that the proposed scheme can defy any kind of attack.

## 1. Introduction

We are living in the age of digital information. Images, audio visual documents (music, speech and video) are digitized at a cheap cost so as to store on a memory device or send through the public (communication) media. Any kind of unauthorized access of secret data may cause financial or political loss. Therefor new research in security is the need of the hour. Data encryption is one of most secure ways to protect data. In encryption the data to be transmitted, is converted to an unrecognizable content using some secret keys. This makes the data secure but also makes it a matter of attraction for the intruders, those are intending to decrypt it by employing various cryptographic attacks.

A variety of encryption algorithms are being proposed to meet the demand. In the last three years a series of encryption algorithms have been published based on DNA sequence addition and complimentary rules mixed with chaotic maps (ur Rehman et al., 2015).

In this paper Hermassi et al. (2014) made cryptanalysis of an image encryption algorithm based on DNA addition by combining with chaotic maps and realized the weakness. In the proposed scheme the strength has been enhanced. The proposed scheme may be easily modified and used for color images. In the last few years researchers proposed a huge

[*] Corresponding author.
E-mail addresses: bhaskar.cse@nitjsr.ac.in (B. Mondal), tmandal.math@nitjsr.ac.in (T. Mandal).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2016.02.003

number of cryptographic schemes based on confusion and diffusion (Wang and Gu, 2014; xin Chen et al., 2014; Zhang et al., 2009; Acharya, 2011; Lian et al., 2005; Liu, 2012). The confusion and diffusion based cryptography Wong et al., 2008 algorithms consist of two basic steps. The first step is confusion in which the pixel positions are permuted to reduce inter-pixel correlation and the second step is diffusion which consists of some reversible computations that change the pixel values. Confusion and diffusion may be of $m$ or $n$ rounds. A typical pictorial representation of modern confusion and diffusion based cryptosystem is shown in Fig. 1. Confusion and diffusion are done by using PRN sequences which are generated by chaotic maps (Wang and Gu, 2014; xin Chen et al., 2014; Mondal et al., 2013). In Wang and Wang (2014) an effort has been made to improve the diffusion process.

In Bhatnagar and Wu (2014) has proposed a scheme for biometric image encryption which uses fractional wavelet packet transform (FrWPT), chaotic map and Heisenberg decomposition due to which the algorithm has very high computational overhead and is not suitable for large image encryption. In Li et al. (2012) has shown weakness of a chaotic map based color image encryption algorithm by successful chosen-plain text attack and chosen-cipher text attack. In Hermassi et al. (2011) the author proposed an improvement of image encryption algorithm based on hyper-chaos. In Wang and Wang (2014) a dynamic s-box based image encryption scheme is presented but performance and security of s-boxes for stream cipher has to be compared with other schemes. In Biswas et al. (2015) they used Elliptic Curve Cryptography (ECC) and Chaotic Map and Genetic operations, The algorithm has high Memory overhead which is greater than Advanced Encryption Standard (AES). In Cho and Miyano (2015) chaotic cryptography using augmented Lorenz equations aided by quantum key distribution. In most of the schemes the authors considered the statistical tests like key-space analysis, histogram analysis, correlation of two adjacent pixels, differential attack analysis, information entropy analysis, known plain-text and cipher-text only attack etc. and over all complexity but they have not given enough emphasis on memory uses and energy consumption, throughput of the algorithms.

In the proposed scheme chaotic logistic map (Wang and Wang, 2014; Jakimoski et al., 2001) is used which will generate a highly randomized number sequence. The chaotic logistic map runs on low computational overhead, so it becomes an light weight PRNG. In the diffusion part, the scheme uses DNA computation as it is reversible. The DNA computation is like the bit wise operations hence the encryption process becomes the first. Therefor the whole algorithm becomes a light weight and first process as well as is resistive to any kind of known attack.

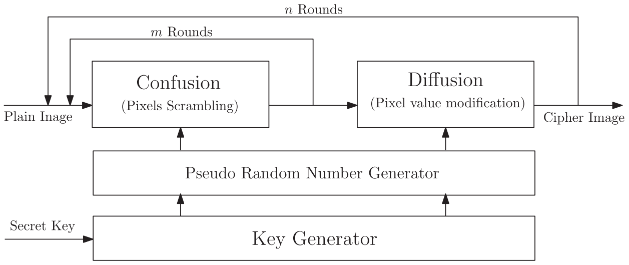

**Fig. 1** A typical model of modern symmetric key crypto-systems.

In the next section the logistic chaos map is discussed first followed by DNA sequencing. In Section 3 the proposed scheme is discussed and then the experimental results and security analysis are presented in Section 4. Finally the conclusion and future scope are discussed.

## 2. Preliminaries

### 2.1. Chaotic logistic map

Chaos is a deterministic, random-like process found in nonlinear, dynamical system, which is non-period, non-converging and bounded. Moreover, it has a very sensitive dependence upon its initial condition and parameter (Schuster and Just, 2006). A chaotic map is a discrete-time dynamical system, defined as the following Eq. 1:

$$x_{k+1} = \tau(x_k), \;\; x \in (0,1), \;\; k = 0,1,2,3 \tag{1}$$

The chaotic sequences $x_k : k = 1,2,3$ are uncorrelated when their initial values are different and spread over the entire space (Wang et al., 2006). Logistic map is one of the simplest chaotic maps, described by Eq. 2:

$$x_{k+1} = f(x) = \mu x_k(1 - x_k)$$
$$\mu \in (0,4), \quad x_k \in (0,1) \tag{2}$$

When $\mu \in (3.5699456, 4)$ the map is in chaotic state. It has some identical statistical characteristics with the white noise, thus, chaotic signals can be used in communication (Ismail et al., 2010; Wang et al., 2006).

### 2.2. Encryption using DNA sequencing

A DNA sequence contains four nucleic acid bases A(adenine), C(cytosine), G(guanine), T(thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases A, C, G and T to encode 00, 01, 10 and 11, there are 24 kinds of coding schemes. But there are only 8 kinds of coding schemes that satisfy the Watsonrick complement rule, which are shown in Table 1 (Zhang et al., 2009; ur Rehman et al., 2015).

Addition and subtraction operations for DNA sequences are performed according to traditional addition and subtraction in the binary. There exist 8 kinds of DNA addition rules and 8 kinds of DNA subtraction rules corresponding to 8 kinds of DNA encoding schemes as shown in Table 1. Taking two DNA sequences [AGCT] and [CTGA] for example, we adopt one type of addition operation shown in Table 2 to add them and we get a sequence [CATT]. Similarly, we can also get the sequence [AGCT] by subtracting the sequence [CTGA] from [CATT]. The addition and subtraction operation of the DNA sequence is shown in Table 2. Seen from

**Table 1** DNA sequence encoding table.

| + | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| A | 00 | 00 | 01 | 01 | 10 | 10 | 11 | 11 |
| T | 11 | 11 | 10 | 10 | 01 | 01 | 00 | 00 |
| G | 01 | 10 | 00 | 11 | 00 | 11 | 01 | 10 |
| C | 10 | 01 | 11 | 00 | 11 | 00 | 10 | 01 |

Tables, the results of addition operation and subtraction operation are unique (Wei et al., 2012).

## 3. The proposed scheme

### 3.1. Chaos based Pseudo Random Bits Generation (PRBG)

Using simple chaotic maps, large numbers of random numbers can be generated. A large number of chaotic maps are available and many of them have already been used in the field of Cryptography, Physics, Medical Science, etc. For generating Pseudo Random Bits (PRB) two Chaotic maps are used parallely, which are cross connected to each other as shown in Fig. 2. Each of the map generates one random number per iteration say $x_{k+1}$ *and* $y_{k+1}$. One PRB is generated using the condition in Eq. 3 shown below:

$$f(x_{k+1}, y_{k+1}) = \begin{cases} 1 & : x_{k+1} > y_{k+1} \\ 0 & : x_{k+1} \leqslant y_{k+1} \end{cases} \tag{3}$$

The PRNG used in the encryption scheme is based on the proposed PRBG.

### 3.2. The proposed encryption scheme

The paper proposes an image encryption scheme making it robust, imperceptible and safe. The step by step proposed encryption procedure is as presented in the following chart of Fig. 3:

#### 3.2.1. The permutation phase

- The PRNG is used to generate a random sequence. The initial conditions are chosen such that $\mu$ belongs to the range $(3.65, 3.95)$ and $x_0$ belongs to the range $(0, 1)$. The values are chosen with a precision of 10 digits.
- The sequence generated by the above step is used to permute the pixels of plain image.

#### 3.2.2. The substitution phase

- The permuted data are converted to DNA sequence ($C$).
- Same PRNG is again used to generate a random bit sequence. For this purpose, this binary sequence is also converted to its DNA sequence ($D$).
- The DNA sequences $C$ and $D$ are added together using Galva Field which results in a new DNA sequence $E$. $E$ is again converted back to sequence of 8 bit (integer) $F$ form.
- XORing of each element of the sequence is done with the elements previous to that index on $F$ which gives the final encrypted image.

**Table 2** Addition and subtraction operations for DNA sequence.

| Addition | | | | | Subtraction | | | | |
|---|---|---|---|---|---|---|---|---|---|
| + | A | G | C | T | − | A | G | C | T |
| A | A | G | C | T | A | A | T | C | G |
| G | G | C | T | A | G | G | A | T | C |
| C | C | T | A | G | C | C | G | A | T |
| T | T | A | G | C | T | T | C | G | A |

## 4. Experimental results and cryptanalysis

The proposed algorithm was experimented against various tests to check its robustness, imperceptibility and quality. The watermark encryption tests were done on three standard gray scale images, Lena, airplane and baboon.

### 4.1. Cryptanalysis of encryption

#### 4.1.1. Key space analysis

We are using Logistic map equation which involves two real numbers as their initial condition. Also we use this equation twice, once for permutation and other for substitution. Because the precision of the parameters are $10^{-10}$, the key space is $10^{40}$ which is roughly equal to $2^{133}$. This large key space eliminates all brute force and exhaustive attacks.

#### 4.1.2. Key sensitivity

The system is very sensitive to the initial conditions which forms the cipher key for the encryption/decryption process. Certain tests were done to examine the sensitivity of the key. If we increase the value of $x_0$ by $-1e10$ in the decryption process, we get the decrypted image and histogram as shown in Fig. 4(d), Fig. 5(d), and Fig. 6(d) which clearly shows the dependence of the images on the initial conditions. The decrypted image is completely changed and is unrecognizable.

#### 4.1.3. Differential attacks

Differential attacks is the study of how differences in an input can affect the resultant difference at the output. Attackers take a pair of images which differ in small magnitude and then generate their cipher images from the same algorithm. Then they compare the two encrypted images, hoping to detect statistical patterns in their distribution. There are two methods used to find performance against differential attacks:

*NPCR*. Number of Pixel Change Rate, it measures the percentage of different pixels between two cipher images whose plane images have only one pixel difference. Larger value is better.

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

$$NPCR : N(C^1, C^2) = \sum_{i,j} \frac{C^1(i,j) - C^2(i,j)}{F\dot{T}} \times 100\% \tag{4}$$

$$UACI : U(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \tag{5}$$

*UACI*. Unified Average Changing Intensity, it measures the average intensity of differences between two cipher images. Smaller value is better. They are calculated as in Table 3 randomly selected 5 pixels randomly and changed the pixel value by 1. The average values are tabulated as in Table 3.

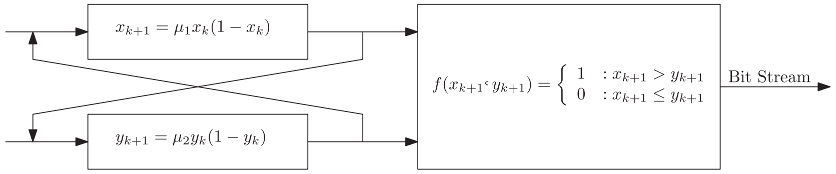
$x_{k+1} = \mu_1 x_k(1 - x_k)$
$y_{k+1} = \mu_2 y_k(1 - y_k)$
$f(x_{k+1}‘ y_{k+1}) = \begin{cases} 1 & : x_{k+1} > y_{k+1} \\ 0 & : x_{k+1} \leq y_{k+1} \end{cases}$
Bit Stream

**Fig. 2** PRBG based on cross coupled logistic map.

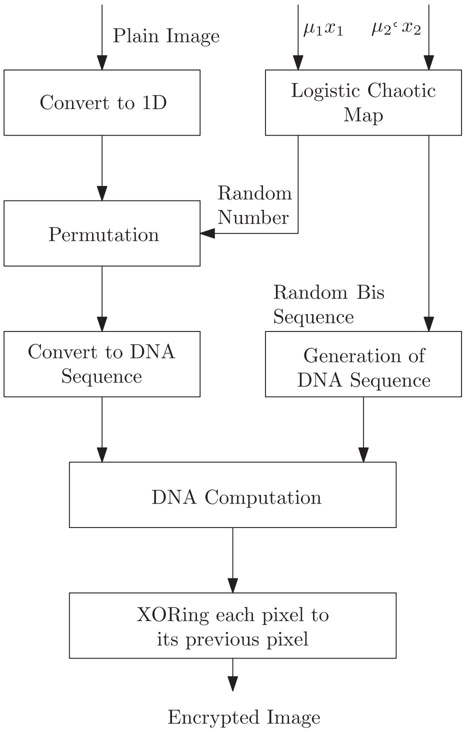

**Fig. 3** Schematic layout diagram of the proposed scheme.

### 4.1.4. Statistical attacks

*Histogram analysis*. The histogram of the encrypted images are plotted below. It shows that the histogram of the encrypted image is uniform which makes statistical attacks difficult. The original test images Figs. 4(a), 5(a), 6(a) and their corresponding histogram shown in Figs. 4(b), 5(b), 6(b) and corresponding histogram after encryption are shown in Figs. 4(c), 5(c), 6(c).

*Information entropy*. The information entropy is defined as the degree of uncertainties in the system. The greater the entropy, the more is the randomness in the image, or the image is more uniform. Thus statistical attacks become difficult. Entropy is defined as in Eq. 6

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2\left[\frac{1}{p(m_i)}\right] \tag{6}$$

where $p$ is the histogram counts returned from the histogram. For an ideal random image, the entropy is calculated to be 8. So closer to 8, better is the randomness in the image. The entropy of the image was calculated and is plotted in the Table 3.

*Correlation coefficient*. It tells us how much there is relation between the same pixels of the original and the encrypted image. It is calculated from the formula below Eq. 3:

$$r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\left((A_{mn} - \overline{A})^2\right)\left((B_{mn} - \overline{B})^2\right)}} \tag{7}$$

where A and B are the original and the encrypted image respectively, and are their means. The lower the value of the correlation coefficient, the better it is. The values were found to be as shown in Table 3.

### 4.2. Complexity

In an image $A$ of size $M \times N$ is encrypted using the proposed algorithm, the algorithm needs to generate $M \times N$ number of random numbers $R_1$ using the chaotic map, So the complexity to generate $M \times N$ numbers of random number is $O(n)$. Again the algorithm needs to generate a random $DNA$ sequence of $M \times N$ bits using the same chaotic map, so again the complexity to generate $M \times N \times 8$ numbers of random bits is $O(n)$. Thereafter it makes a series $(M \times N2)$ of DNA additions or

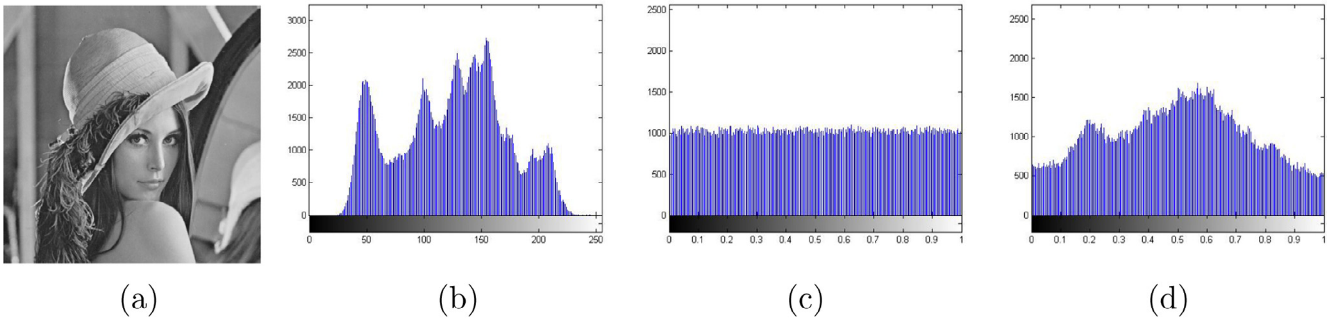

**Fig. 4** Test 1. (a) Test image 1, (b) histogram of test image 1, (c) histogram after encryption, (d) histogram of extracted test image 1 to test key sensitivity.

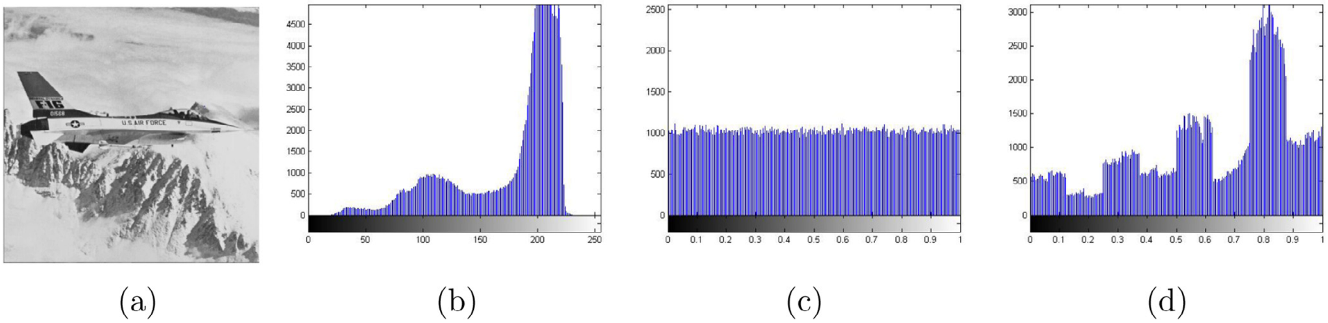

**Fig. 5** Test 2. (a) Test image 2, (b) histogram of test image 2, (c) histogram after encryption, (d) histogram of extracted test image 2 to test key sensitivity.

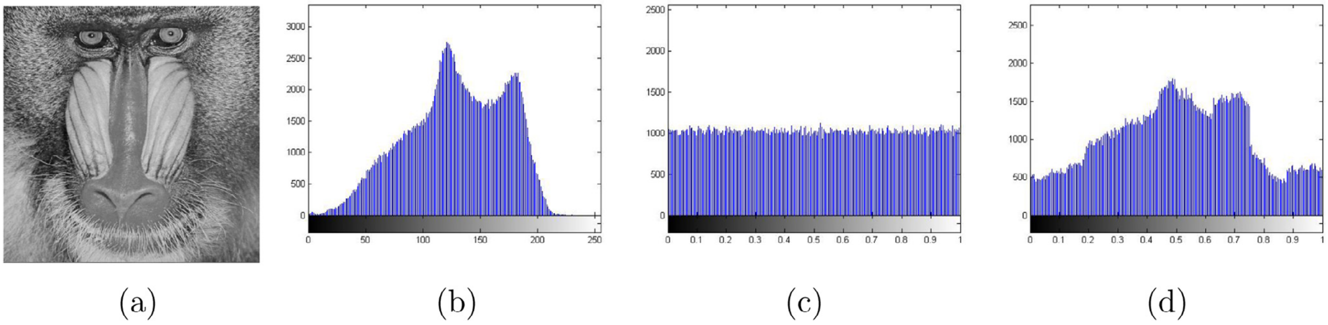

**Fig. 6** Test 3. (a) Test image 3, (b) histogram of test image 3, (c) histogram after encryption, (d) histogram of extracted test image 3 to test key sensitivity.

**Table 3** Results of different statistical test.

| Image | Entropy | Correlation | NPCR (%) | UACI (%) |
|---|---|---|---|---|
| Lena | 7.99925692 | 0.001178542895092 | 99.7570 | 0.3912 |
| Baboon | 7.99930193 | 0.001576673227643 | 98.0961 | 0.7702 |
| Airplane | 7.99923814 | 0.00007263856137 | 99.1405 | 1.5548 |

subtractions, which has a complexity of $O(n)$. Finally it makes a chain $XOR$ of operations which is of $O(n)$. So the overall complexity of the algorithm is $O(n)$.

## 5. Conclusions

The proposed algorithms use logistic map and DNA sequencing and is used in the substitution phase of the encryption process which makes it light weight and resistant against statistical attacks. Permutation is also done on a plain image which gives better performance and quality. We have also shown that a slight change in the key value yields a highly uncorrelated image as compared to the plain image.

The experimental results show that the proposed algorithm is robust, imperceptible, and safe against various attacks like statistical and differential attacks, noise, etc. The results were found to be satisfactory and in most cases better than the existing algorithms referred to in this paper. However, there is scope for further improvements of the encryption techniques so as to make it applicable to Internet of things.

## References

Acharya, A., 2011. Image encryption using a new chaos based encryption algorithm. In: Proceedings of International Conference on ICCCST11, pp. 1–5, http://dl.acm.org/citation.cfm?id=1948060.

Bhatnagar, G., Wu, Q., 2014. Enhancing the transmission security of biometric images using chaotic encryption. Multimedia Syst. 20 (2), 203–214. http://dx.doi.org/10.1007/s00530-013-0323-3.

Biswas, K., Muthukkumarasamy, V., Singh, K., 2015. An encryption scheme using chaotic map and genetic operations for wireless sensor networks. Sens. J., IEEE 15 (5), 2801–2809. http://dx.doi.org/10.1109/JSEN.2014.2380816.

Chen, J. xin, Zhu, Z. liang, Yu, H., 2014. A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme. Optik – Int. J. Light Electron Opt. 125 (11), 2472–2478. http://dx.doi.org/10.1016/j.ijleo.2013.12.001, URL: http://www.sciencedirect.com/science/article/pii/S0030402613014770.

Cho, K., Miyano, T., 2015. Chaotic cryptography using augmented lorenz equations aided by quantum key distribution. IEEE Trans. Circuits Syst. I: Regular Papers 62 (2), 478–487. http://dx.doi.org/10.1109/TCSI.2014.2365767.

Hermassi, H., Rhouma, R., Belghith, S., 2011. Improvement of an image encryption algorithm based on hyper-chaos. Telecommun. Syst., 539–549 http://dx.doi.org/10.1007/s11235-011-9459-7, URL: http://link.springer.com/10.1007/s11235-011-9459-7.

Hermassi, H., Belazi, A., Rhouma, R., Belghith, S., 2014. Security analysis of an image encryption algorithm based on a dna addition combining with chaotic maps. Multimedia Tools Appl. 72 (3), 2211–2224. http://dx.doi.org/10.1007/s11042-013-1533-6.

Ismail, I., Amin, M., Diab, H., 2010. A digital image encryption algorithm based a composition of two chaotic logistic maps. IJ Network Secur. 11 (1), 1–10, URL: http://core.kmi.open.ac.uk/download/pdf/793123.pdf.

Jakimoski, G., Kocarev, L., Member, S., 2001. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst.-I: Fundam. Theory Appl., 163–169

Lian, S., Sun, J., Wang, Z., 2005. A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons Fractals 26 (1), 117–129. http://dx.doi.org/10.1016/j.chaos.2004.11.096, URL: http://www.sciencedirect.com/science/article/pii/S0960077905000378.

Li, C., Zhang, L., Ou, R., Wong, K., Shu, S., 2012. Breaking a novel colour image encryption algorithm based on chaos. Nonlinear Dyn., 2383–2388 http://dx.doi.org/10.1007/s11071-012-0626-5, URL: http://link.springer.com/article/10.1007/s11071-012-0626-5.

Liu, R., 2012. Chaos-based fingerprint images encryption using symmetric cryptography. In: 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 2153–2156. http://dx.doi.org/10.1109/FSKD.2012.6234120.

Mondal, B., Priyadarshi, A., Hariharan, D., 2013. An improved cryptography scheme for secure image communication. Int. J. Comput. Appl. 67 (18), 23–27. http://dx.doi.org/10.5120/11496-7206, URL: http://research.ijcaonline.org/volume67/number18/pxc3887206.pdf.

Schuster, H., Just, W., 2006. Deterministic Chaos: An Introduction. Wiley, URL: http://books.google.co.in/books?id=-14Y2WPfYgsC.

ur Rehman, A., Liao, X., Kulsoom, A., Abbas, S., 2015. Selective encryption for gray images based on chaos and dna complementary rules. Multimedia Tools Appl. http://dx.doi.org/10.1007/s11042-013-1828-7.

Wang, X.-Y., Gu, S.-X., 2014. New chaotic encryption algorithm based on chaotic sequence and plain text. Inf. Secur., IET 8 (3), 213–216. http://dx.doi.org/10.1049/iet-ifs.2012.0279.

Wang, X., Wang, Q., 2014. A novel image encryption algorithm based on dynamic s-boxes constructed by chaos. Nonlinear Dyn. http://dx.doi.org/10.1007/s11071-013-1086-2.

Wang, R., Li, Q., Yan, D., 2006. A high robust audio watermarking algorithm. In: The Sixth World Congress on Intelligent Control and Automation, WCICA 2006, vol. 1, pp. 4171–4174. http://dx.doi.org/10.1109/WCICA.2006.1713160.

Wei, X., Guo, L., Zhang, Q., Zhang, J., Lian, S., 2012. A novel color image encryption algorithm based on {DNA} sequence operation and hyper-chaotic system. J. Syst. Softw. 85 (2), 290–299. http://dx.doi.org/10.1016/j.jss.2011.08.017, special issue with selected papers from the 23rd Brazilian Symposium on Software Engineering, URL: http://www.sciencedirect.com/science/article/pii/S0164121211002147.

Wong, K.-W., Kwok, B.S.-H., Law, W.-S., 2008. A fast image encryption scheme based on chaotic standard map. Phys. Lett. A 372 (15), 2645–2652. http://dx.doi.org/10.1016/j.physleta.2007.12.026, URL: http://linkinghub.elsevier.com/retrieve/pii/S0375960107017768.

Zhang, Q., Guo, L., Xue, X., Wei, X., 2009. An image encryption algorithm based on dna sequence addition operation. In: Fourth International Conference on Bio-Inspired Computing, 2009, BIC-TA ’09, pp. 1–5. http://dx.doi.org/10.1109/BICTA.2009.5338151.