A New Image Cryptosystem Based on Chaotic Map and Continued Fractions

Atef Masmoudi, Mohamed Selim Bouhlel, William Puech

A NEW IMAGE CRYPTOSYSTEM BASED ON CHAOTIC MAP AND CONTINUED FRACTIONS

A. MASMOUDI[1,2]*, M.S. BOUHLEL*[1]*, and W. PUECH*[2]

[1]Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology, Sfax TUNISIA
[2]Laboratory LIRMM, UMR 5506 CNRS University of Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE
atef.masmoudi@lirmm.fr william.puech@lirmm.fr medsalim.bouhlel@enis.rnu.tn

ABSTRACT

Recently, a variety of chaos-based cryptosystems have been proposed. Some of these novel chaotic encryption schemes are not very suitable for image encryption due to their density function which is not uniformly distributed or due to their small key space. In this paper, we propose a new scheme for image encryption based on the use of a chaotic map with large key space and Engle Continued Fractions (ECF) map. The ECF-map is employed to generate a pseudo random sequence which satisfies uniform distribution, zero co-correlation and ideal nonlinearity to achieve higher level of security. The proposed scheme is resistant to the known attacks. Theoretic and numerical simulation analyses indicate that our scheme is efficient and satisfies high security.

1. INTRODUCTION

Recently, cryptographic algorithms based on chaos systems [11, 24, 22, 23, 25] have been proposed with good cryptographic properties. Chaos systems have many important features such ergodicity, sensitivity to initial conditions, sensitivity to control parameters and randomness [9]. These features are very important in cryptography and they have suggested some new and efficient ways to develop encryption algorithms for secure digital image transmission over the Internet and through public networks. In addition, a chaotic system would have a large key space, for resistance to brute-force attacks, and generates sequence with an uniform invariant density function for resistance to statistic attacks. The problem is not all chaotic systems can satisfy these characteristics [10, 21]. For example, the logistic map is widely used to design chaotic system. The known 1-Dimensional logistic map is defined as $x_{n+1} = \lambda x_n(1-x_n)$ where $\lambda \in [0,4]$ and $x_n \in [0,1]$. Mi *et al.* [16] proposed a new chaotic encryption scheme based on randomized arithmetic coding using the logistic map as the pseudo random bit generator. In [13], Lian *et al.* proposed a new block cipher based on the use of logistic map in the diffusion process. In [7], Kanso *et al.* proposed a new cipher based on logistic maps for generating two pseudo random binary sequences. The logistic map is weak in security because it does not satisfy uniform distribution property and it has a small key space [1, 2]. Recently, a new chaos-based image cryptosystems using piecewise linear chaotic map (PWLCM) has been proposed. The PWLCM is a chaotic map which depends on the computing precision, and its phase space includes a linear structure. Although a PWLCM has a non uniform distribution in finite computing precision and has weak security. In [12], Li *et al.* demonstrated that the chaotic encryption scheme proposed by Zhou *et al.* [27, 26], which is based on a kind of computerized PWLCM realized in finite computing precision is not secure enough from strict cryptographic viewpoint. Thus, find a secure and efficient cryptosystem motivates us to propose a new scheme which consists of using the standard map with large key space and the Engle Continued Fractions (ECF) map. The use of ECF-map increases the complexity of a cryptosystem based only on one chaotic system and thus makes difficulties in extraction of information about it [18]. In addition, ECF-map conserves the cryptography properties of the chaotic system; like sensibility to initial conditions and control parameters non periodicity and randomness; and add interesting statistical properties such uniform distribution density function and zero co-correlation.
The rest of this paper is organized as follows. In Section 2, we present the CF theory and describe the ECF-map and some important features. Section 3 details our proposed algorithm for image encryption. In Section 4, we analyze the security of the proposed algorithm and we provide experimental results to prove its performances through some well known attacks. Finally, conclusions of this paper is discussed in Section 5.

2. CONTINUED FRACTIONS

2.1 Regular Continued Fractions (RCF)

A continued fraction (CF) [14, 19, 20] refers to all expressions of the form:

$$x = b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cfrac{a_4}{\cdots}}}}, \tag{1}$$

where a_i $(i > 0)$ are the partial numerators, b_i the partial denominators, b_0 is the integer part of the CF and x is a real number. Note that the partial numerators and the partial denominators can assume arbitrary real or complex values. CF theory [8] has become used in various areas. For example, they have been used for computing rational approximations to real numbers and for solving various well known equations.

2.2 Engel Continued Fractions (ECF)

Hartono *et al.* [6] introduce a new CF expansion, called Engel continued fraction (ECF) expansion.

Let the Engel continued fraction (ECF) map $T_E : [0,1] \to [0,1)$ be given by:

$$T_E(x) = \begin{cases} \frac{1}{\lfloor \frac{1}{x} \rfloor}(\frac{1}{x} - \lfloor \frac{1}{x} \rfloor) & \text{if} \quad x \neq 0 \\ 0 & \text{if} \quad x = 0 \end{cases}. \tag{2}$$

For any $x \in [0,1)$, the ECF-map generates a new and unique CF of x of the form:

$$x = \cfrac{1}{b_1 + \cfrac{b_1}{b_2 + \cfrac{b_2}{b_3 + \ddots + \cfrac{b_{n-1}}{b_n + \ddots}}}}, \quad b_n \in \mathbb{N}, \quad b_n \leq b_{n+1}. \tag{3}$$

Let $x \in [0,1)$, and define:

$$\begin{cases} b_1 &= b_1(x) = \lfloor \frac{1}{x} \rfloor \\ b_n &= b_n(x) = b_1(T_E^{n-1}(x)), \quad n \geq 2, \quad T_E^{n-1}(x) \neq 0 \end{cases}. \tag{4}$$

From definition of T_E it follows that:

$$\begin{aligned} x &= \frac{1}{b_1 + b_1 T_E(x)} \\ &= \cfrac{1}{b_1 + \cfrac{b_1}{b_2 + \cfrac{b_2}{b_3 + \ddots + \cfrac{b_{n-1}}{b_n + b_n T_E^n(x)}}}}, \end{aligned} \tag{5}$$

where $T_E^0(x) = x$ and $T_E^n(x) = T_E(T_E^{n-1}(x))$ for $n \geq 1$.

Note that any $x \in [0,1)$ have a unique ECF representation. We paid most attention to the following sequence:

$$Z_i(x) = b_i(x) T_E^i(x),\ i \geq 1. \tag{6}$$

The sequence $\{Z_i(x)\}_{i=1}^n \in [0,1)$ and uniformly distributed for almost all values x (for a proof see [6]). The ECF-map has an underlying dynamical system which is ergodic, and their ergodic properties follow from those of the RCF-map [5]. So, the ECF-map generates a random and unpredictable sequence $\{Z_i(x)\}_{i=1}^n$ with uniform distribution. These properties which are very useful in cryptography motivate us to propose a new scheme for image encryption based on ECF-map.

3. THE PROPOSED ENCRYPTION ALGORITHM

The proposed symmetric image encryption algorithm utilizes chaotic standard map [17] and the ECF-map.

The 2-D map function known as the standard map is defined by:

$$\begin{cases} x_{1,j} &= x_{1,j} + p_0 sin(x_{2,j}) \\ x_{2,j} &= x_{2,j} + x_{1,j} \end{cases}, \tag{7}$$

where $x_{1,j}$ and $x_{2,j}$ are taken modulo 2π. The secret key in the proposed encryption technique is a set of three floating value numbers and one integer $(x_{1,0}, x_{2,0}, p_0, N_0)$, where $X_0 = \{x_{1,0}, x_{2,0}\} \in [0, 2\pi)$ is the initial value set, $P = \{p_0\}$ is the control parameters set and can have any real value greater than 18.0 as described in [17] and N_0 is the number of initial iteration times of the chaotic map. We suggest to use the standard map because it has a good chaotic properties and it has large key space which is near to 157 bits [17] with a precision of 10^{-14}, the key which is sufficient enough to resist the brute-force attack. So, for generating chaotic key stream using the chaotic standard and ECF maps, we propose to apply the following steps.

Assuming that the pixels of the plain-image are scanned from left to right and from top to down to get a set $S = \{S_1, \cdots S_N\}$. The corresponding encrypted image is represented by the set $C = \{C_1, \ldots, C_N\}$. Each element of these two set is an 8-bit value representing the gray level of pixel. N is the total number of image pixels and M is the color level and for a 256 gray-scale image $M = 256$.

Assume that $f_M(x) = i$, if $x \in I_i, i \in \{0, \cdots, M-1\}$ where $I_0, \cdots, I_{M-1}$ denote M consecutive part intervals of $I = [0,1)$. The operation procedures of the proposed chaos-based image cryptosystem are described as follows:

- **Step 1:** We propose to use the 2-D chaotic standard map with $X_0 = \{x_{i,0}\}_{i=1}^n$ and $P = \{p_i\}_{i=1}^n$ are respectively the set of the initial values and the set of the control parameters of the chosen chaotic system. We propose to iterate the chaotic map for N_0 times, where N_0 is an element of the key.
- **Step 2:** The n-Dimensional chaotic map is iterated continuously. For the j^{th} iteration, the output of the chosen chaotic map is a new set $X_j = \{x_{i,j}\}_{i=1}^n$.
- **Step 3:** Generally, most of the n-Dimensional chaotic map generates a set X_j with $|x_{i,j}| \leq 1$, $\forall i, j$. So we propose to calculate:

$$\begin{cases} A &= (\sum_{i=1}^n |x_{i,j}| + \frac{S_{j-1}}{256}) \\ y_j &= A - \lfloor A \rfloor \end{cases}, \tag{8}$$

  with S_0 is a secret value and $|x|$ returns the absolute value of x.
- **Step 4:** Finally the set S is encrypted and the encrypted image set $C = \{C_1, \ldots, C_N\}$ are calculated by the following equation:

$$C_j = S_j \oplus \left\{ f_M(\sum_{i=1}^n Z_i(y_j)) mod M \right\}, \tag{9}$$

where $\oplus$ represents the exclusive OR operation bit by bit and $Z_i(y_j)$ is calculated according to equation (6). The standard and ECF maps are iterated until all elements in the set S are encrypted to the corresponding encrypted set C. In our scheme, the keystream depends on the initial conditions set X_0, to the control parameters set P and also the plain image gray value set S. The majority of cryptosystems with keystreams independent of plaintexts are vulnerable under known plaintext attacks [21]. Thus, to enhance the security of our encryption method, we propose to use the plain-image pixels set S when producing keystreams. It should be noticed that for the decipher algorithm we use the same procedure used in the encipher process, but we should reverse the sequences S_j and C_j used in step 4.

4. SECURITY ANALYSIS

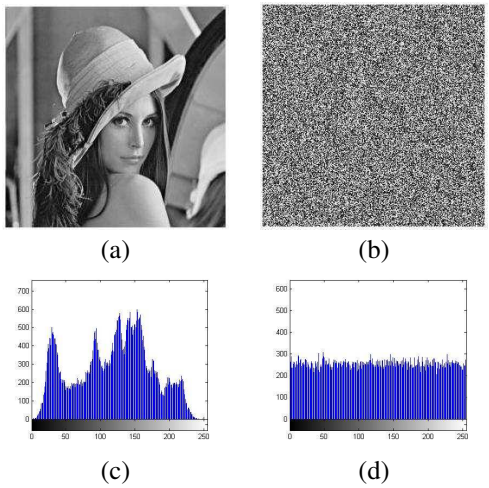
In this section, we present some security analysis of the proposed encryption algorithm, including the most important ones like key sensitivity test, statistical analysis and differential analysis. Table 1 lists four different secret keys used in the security analysis steps.

Table 1: Keys used in security analysis.

	k_0	k_1	k_2	k_3	k_4
x_0	5.87574682393162	5.87574682393161	5.87574682393162	5.87574682393162	5.87574682393162
y_0	0.20543974869398	0.20543974869398	0.20543974869399	0.20543974869398	0.20543974869398
p_0	90.41936758463719	90.41936758463719	90.41936758463719	90.41936758463720	90.41936758463719
N_0	250	250	250	250	251

4.1 Statistical analysis

a) ***Histograms of encrypted images:***
An ideal encryption algorithm should resist to statistical attacks [17]. So, we have analysed the histograms of 100 plain images and their corresponding encrypted images using different keys. The plain-image of Lena and the encrypted image by using the secret key k_0 are shown in Fig. 1.a and 1.b respectively. Fig. 1.c and 1.d show respectively the histogram of the original and the encrypted image. These two histograms are significantly different and from Fig. 1.d we can see the uniform distribution of gray-scale of the encrypted image. In all other cases of histogram analysis, we have found simular results. Hence, the proposed algorithm does not provide any clue to employ any statistical analysis attack on the encrypted images.



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

Figure 1: Histogram analysis of plain-image Lena and its encrypted image obtained using the key k_0.

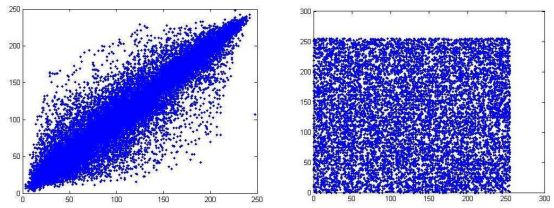
b) ***Correlation of adjacent pixels:***
For an ordinary image, each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions. However, an efficient encryption scheme should generate encrypted images with low correlation between adjacent pixels [23]. For each pixel of the image, a duplet (x_i, y_i) can be found where y_i is the adjacent pixel of x_i and then the correlation γ_{xy} is:

$$\gamma_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2}}, \tag{10}$$

where N is the total number of duplets (x_i, y_i) obtained from the image and $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ is the mean value of x. Table 2 shows the three correlation coefficients of three plain-images and those of the average values of various correlation coefficients of their corresponding cipher images founded by using 100 different keys. Fig. 2 shows the correlation distribution of two horizontally adjacent pixels in the plain-image Lena and that in it encrypted image produced by using k_0. These correlation analysis prove that our encryption algorithm satisfies zero correlation.

Table 2: Correlation coefficients of adjacent pixels in three plain images and the avarege values of various correlation coefficients of their corresponding cipher images founded by using 100 different scret keys.

	plain-image	encrypted images
Lena		
horizontal	0.9411	-0.0003
vertical	0.9702	0.0014
diagonal	0.9153	0.0001
Boat		
horizontal	0.9368	0.0012
vertical	0.9709	0.0026
diagonal	0.9293	-0.0002
House		
horizontal	0.9736	-0.0005
vertical	0.9504	0.0004
diagonal	0.9246	0.0022



(a) (b)

Figure 2: Correlations of two horizontally adjacent pixels in the plain-image Lena and in its encrypted image: a) Correlation analysis of plain-image, b) Correlation analysis of encrypted image.

4.2 Key sensitivity

According to the basic principle of cryptology, a cryptosystem should be sensitive to the key. Thus, we propose the following tests [15].

a) Assume that the encryption key used is k_0, see Table 1. First, a 256×256 Lena plain-image is encrypted by using the test key and the resultant encrypted image is shown in Fig.1.b. Next, the same plain image is encrypted with four slightly different keys described in Table 1.

We propose for each of the used secret keys, to conserve at least three parts of k_0 and to change the fourth one by 10^{-14} (if it is a floating number) or by 1 (if it is an integer). The encrypted images, produced by using different keys, are shown in Fig. 3.a, 3.c, 3.e and 3.g. Now, the encrypted images produced by slightly different keys are compared and the difference between images Fig. 1.b and 3.a, Fig. 1.b and 3.c, Fig. 1.b and 3.e and Fig. 1.b and 3.g are shown in Fig. 3.b, 3.d, 3.f and 3.h, respectively. The NPCR (Number of Pixel Change Rate) and the UACI (Unified Average Changing Intensity) [3, 4] between various encrypted images produced by using slightly different keys, are calculated and the results are given in Table 3.

Table 3: Pixel difference between image encrypted by keys with slightly difference.

test item	test results between images encrypted with tiny change in the key			
	k_1	k_2	k_3	k_4
NPCR (%)	99.60	99.56	99.57	99.60
UACI (%)	33.54	33.58	33.44	33.53

b) In addition, to test the key sensitivity of our encryption algorithm, we propose to decrypt image using key with a difference by 10^{-14} on x_0, y_0 and p_0, and with only by 1 on N_0. Fig. 4 clearly shows that an image encrypted by the key k_0 is not correctly decrypted by using a key which is changed a little 10^{-14} or which has only one difference by 1. Thus, having a perfect approximation of the encryption secret key makes decryption impossible. In addition, the histograms of the decrypted images with a little change in the secret key have a random property.

5. CONCLUSIONS

In this paper, the ECF-map has been presented and then used to design a new and secure symmetric chaos-based image encryption scheme. This new scheme utilizes the chaotic standard map and the ECF-map to generate keystreams with both good chaotic and statistical properties. The use of the ECF-map increases the resistance of the proposed scheme to various attacks and especially to statistical and differential attacks. The detailed numerical analysis demonstrates that the proposed encryption algorithm is secure and its is very suitable for image encryption.

REFERENCES

[1] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a Discrete Chaotic Cryptosystem Using External Key. *Physics Letters*, 9:319–334, 2003.

[2] G. A. Alvarez and L. B. Shujun. Cryptanalyzing a Nonlinear Chaotic Algorithm (NCA) for Image Encryption. *Communications in Nonlinear Science and Numerical Simulation*, 14(11):3743–3749, 2009.

[3] G. Chen, Y. Mao, and C. K. Chui. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps. *Chaos, Solitons and Fractals*, 21:749–761, 2004.

[4] F. Chiaraluce and L. Ciccarelli. A New Chaotic Algorithm for Video Encryption. *IEEE Transactions on Consumer Electronics*, 48(4):838–844, 2002.

[5] K. Dajani and C. Kraaikamp. The Mother of All Continued Fractions. *Colloquium Math*, 84-85:109–123, 2000.

[6] Y. Hartono, C. Kraaikamp, and F. Schweiger. Algebraic and Ergodic Properties of a New Continued Fraction Algorithm with Non-Decreasing Partial Quotients. *Journal de théorie des nombres de Bordeaux*, 14(2):497–516, 2002.

[7] A. Kanso and N. Smaoui. Logistic Chaotic Maps for Binary Numbers Generations. *Chaos, Solitons and Fractals*, 40:2557–2568, 2009.

[8] A. Y. Khintchin. Continued Fractions. *Noordhoff, Groningen*, 1963.

[9] L. Kocarev. Chaos-Based Cryptography: A Brief Overview. *IEEE Circuits and Systems*, 1(3):6–21, 2001.

[10] H. Li and J. Zhang. A Secure and Efficient Entropy Coding Based on Arithmetic Coding. *Communications in Nonlinear Science and Numerical Simulation*, 14(12):4304–4318, 2009.

[11] S. Li and X. Mou. Improving Security of a Chaotic Encryption Approach. *Physics Letters A*, 290(3-4):127–133, 2001.

[12] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang. On the Security of a Chaotic Encryption Scheme: Problems With Computerized Chaos in Finite Computing Precision. *Computer Physics Communications*, 153(1):52–58, 2003.

[13] S. G. Lian, J. Sun, and Z. Wang. A Block Cipher Based on a Suitable Use of Chaotic Standard Map. *Chaos, Solitons and Fractals*, 26(1):117–129, 2005.

[14] L. Lorentzen and H. Waadeland. Continued Fractions with Applications. *North Holland*, 1992.

[15] S. S. Maniccam and N. G. Bourbakis. Lossless Image Compression and Encryption using SCAN. *Pattern Recognition*, 34:1229–1245, 2001.

[16] B. Mi, X. Liao, and Y. Chen. A Novel Chaotic Encryption Scheme Based on Arithmetic Coding. *Chaos, Solitons and Fractals*, 38:1523–1531, 2008.

[17] V. Patidar, N. K. Parekk, and K. K. Sud. A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulation*, 14:3056–3075, 2009.

[18] V. Patidar and K. K. Sud. A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing. *Electronic Journal of Theoretical Physics*, 6(20):327–344, 2009.

[19] R. B. Seidensticker. Continued Fractions for High-Speed and High-Accuracy Computer Arithmetic. *in Proc. 6th IEEE Symp. Comput. Arithmetic*, 1983.

[20] J. Vuillemin. Exact Real Computer Arithmetic with Continued Fractions. *INRIA Report 760. Le Chesnay, France: INRIA*, NOV. 1987.

[21] J. Wei, X. F. Liao, K. W. Wong, and T. Zhout. Cryptoanalysis of Cryptosystem Using Multiple one-Dimensional Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, 12:814–22, 2007.

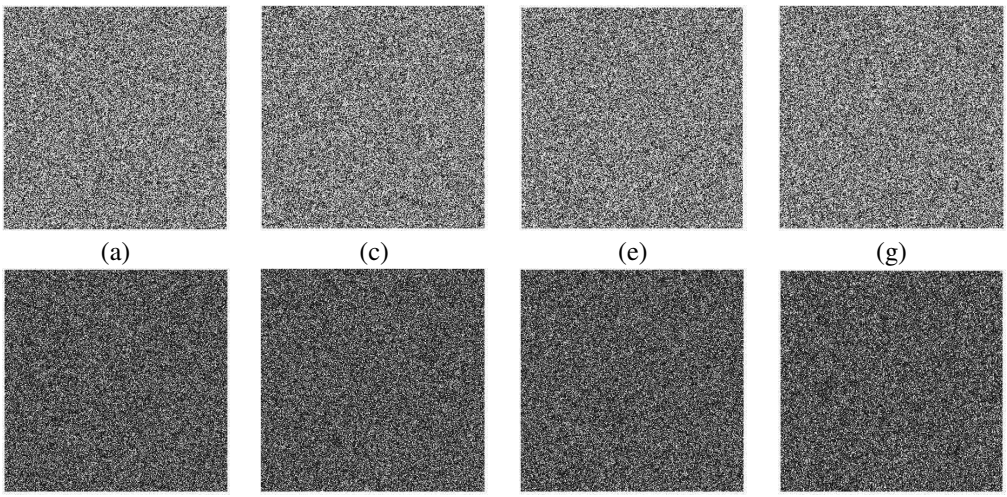


Figure 3: Key sensitivity analysis: a) Encrypted image with key k_1, b) Difference between two encrypted images using k_0 and k_1, c) Encrypted image with key k_2, d) Difference between two encrypted images using k_0 and k_2, e) Encrypted image with key k_3, (f) difference between two encrypted images using k_0 and k_3, g) Encrypted image with key k_4, h) Difference between two encrypted images using k_0 and k_4.

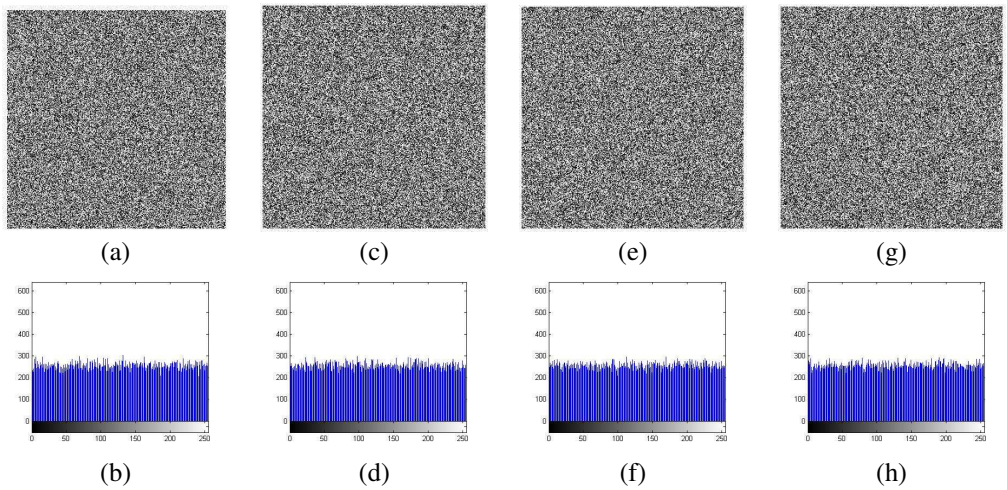


Figure 4: Key sensitivity test: a) Decrypted image with key k_1, b) Its histogram, c) Decrypted image with key k_2, d) Its histogram, e) Decrypted image with key k_3, f) Its histogram, g) Decrypted image with key k_4, h) Its histogram.

[22] K. W. Wong, B. S. H. Kwoka, and C. H. Yuena. An Afficient Diffusion Approach for Chaos-Based Image Encryption. *Chaos, Solitons and Fractals*, 41(5):2652–2663, 2008.

[23] X. G. Wu, H. P. Hu, and B. L. Zhang. Analyzing and Improving a Chaotic Encryption Method. *Chaos, Solitons and Fractals*, 22(2):367–373, 2004.

[24] T. Yang. A Survey of Chaotic Secure Communication Systems. *Journal of Computational Cognition*, 2(2):81–130, 2004.

[25] L. Zhang, X. Liao, and X. Wang. An Image Encryption Approach Based on Chaotic Maps. *Chaos, Solitons and Fractals*, 24(3):759–765, 2005.

[26] H. Zhou and X. T. Ling. Problems With the Chaotic Inverse System Encryption Approach. *IEEE Circuits and Systems*, 44(3):268–271, 1997.

[27] H. Zhou, X. T. Ling, and J. Yu. Secure Communication Via one-Dimensional Chaotic Inverse Systems. *IEEE Circuits and Systems*, 2:1029–1032, 1997.