Modern Applied Science; Vol. 7, No. 12; 2013
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Improving a New Logistic Map as a New Chaotic Algorithm for Image Encryption

Omar A. Saraereh[1], Qais Alsafasfeh[2] & Aodeh Arfoa[2]

[1] Electrical Engineering Department, Hashemite University, Jordan

[2] Electrical Engineering Department, Tafila Technical University, Jordan

Correspondence: Omar A. Saraereh, Electrical Engineering Department, Hashemite University. E-mail: eloas2@hu.edu.jo

Received: October 15, 2013 Accepted: November 3, 2013 Online Published: November 11, 2013

doi:10.5539/mas.v7n12p24 URL: http://dx.doi.org/10.5539/mas.v7n12p24

Abstract

Image encryption is not a new field, but the techniques used to encrypt images are constantly being re-evaluated. As computer processing power grows, the need for better encryption algorithms grows with it. In this paper, the attention was focused on the encryption of still images. In particular, a precise look at encryption using chaotic techniques was subjected. In this paper we present improving existing chaotic algorithm (NCA) for image encryption proposed in 2005. The analysis of the four existing encryption algorithms directed the work to conclude that it is possible to do this encryption much quicker, without much loss in the way of obscurity, robustness, correlation, or security. Therefore, we propose a new encryption algorithm that is essentially a modification of the NCA. The improving method created an encryption method for images that does not allow masks to be of any use in the cryptanalysis.

Keywords: encryption, chaotic, logistic map, chaotic system, correlation coefficient

1. Introduction

Almost unimaginable amounts of information are stored on digital media and transmitted over various networks these days. One method of organizing certain digital information is in image form. An extension of the static image form is the sequence of still images that when run at a fast enough speed can provides digital video. More and more, image and video files are sent around the world through the Internet, exchanged within intranets, stored on removable media, archived in vast storage facilities, and so on.

Some businesses are moving towards a paperless office environment by going digital so as to avoid the need for storage of hardcopy records and to provide the ability to easily archive and back up their most sensitive information. In order to shift to a paperless workplace, paper documents must all be converted by various means to digital documents. Additionally, in a world where video security cameras seem ubiquitous, the storage needs for the video feeds are increasing daily.

Often, representations of visual data contain private or confidential information that should only be seen by people who have the proper authority. As a consequence, techniques are required to provide security features such as watermarking to prove a document is the property of the expected entity, encryption to obscure data for various purposes, and authentication to verify the integrity of the recipient of digital media. These and other features are part of a relatively new area of study called Multimedia Security (Delp, 2003; Alsafasfeh & Alshabatat, 2011)

In this paper, the attention was focused toward the encryption of still images. In particular, the encryption was investigated thoroughly using chaotic techniques. The focus was going to be on one new chaotic algorithm (NCA) for image encryption proposed in 2005 in an effort to answer the question, “Does this chaotic encryption algorithm really provide the data security that is required?” During the course of examining four previously-published chaotic encryption techniques (Lorenz, Rossler, Logistic Map, and NCA), many attempts were done to determine which was best suited for image encryption and decryption while maintaining the desired security. In order to do so for each, it was a good idea to look at the speed of the algorithm, the ability of the algorithm to obscure the original image data, the robustness of the algorithm with respect to changes in initial conditions and parameters (the key) affecting decrypting, the lack of correlation of the encrypted image pixels,

and the overall security of the algorithm.

The analysis through this work of the four existing encryption algorithms led to the fact that it was possible to do this encryption much quicker, without much loss in the way of obscurity, robustness, correlation, or security. Therefore, a new encryption algorithm that is essentially a modification of the NCA was proposed in this article.

The paper is organized as follows. Section one presents the current stage of chaos based image encryption work in literature. Section two discusses the step by step the procedure of image encryption. Section three includes the experimental analysis for the proposed algorithm. Section four illustrates the security analysis of the image encryption scheme such as statistical analysis, key and plaintext sensitivity analysis, key space analysis etc. to prove its security against the most common attacks. Finally, section five gives the conclusions of the paper.

2. Background

Image encryption is not a new field, but the techniques used to encrypt images are constantly being re-evaluated. As computer processing power grows, the need for better encryption algorithms grows with it. Depending on the application, a user may require only that portions of an image be obscured, and sometimes this selective encryption is only enough to hide the portion of original image information, not completely obscure it. For example, think of a video broadcast of an interview where the person being interviewed wants to remain anonymous. You may have seen this done by hiding the face behind encrypted blocks. As the person moves, the blocks move with him since each frame of video is being encrypted separately. You can still tell there is a person's head there, but you cannot make out facial features (Alsafasfeh & Alshabatat, 2011; Hua, 2009).

Other applications may require encryption that completely obscures the original image in a way that nothing from the original image can be determined from the encrypted image. This whole-image encryption is what examined here. Surprisingly, not all of these algorithms completely obscured the test images, as the proposed research here seemed to indicate would happen.

Prior to the use of chaotic encryption techniques, the industry-wide standard was the DES algorithm, or Data Encryption Standard. DES was developed and widely-adopted in the 1970s, but is being used less and less now due to its 56-bit key being deemed too small, thus inviting attacks to break the encryption (Alsafasfeh & Arfoa, 2011).

The successor to the DES algorithm is the AES algorithm, or Advanced Encryption Standard. The AES was developed and adopted around the turn of the century and is still very much in use. Its key size is as high as 256 bits and the encryption is done on blocks of data. However, even with its significantly larger key size, there are still concerns that AES is not secured enough (Droogenbroeck & Benedett, 2002). These types of concerns have lead researchers to explore the idea of chaotic encryption to help foil would-be attackers by increasing the security of algorithms.

There are many chaos based image encryption schemes developed in literature. In 1992, Bourbakis and Alexopoulos (1992) have proposed an image encryption scheme which utilizes the SCAN language to encrypt and compress an image simultaneously. Zhang et al. (2011) proposed an image encryption method based on skew tent map diffusion architecture. Zhu et al. (2011) have proposed a new permutation method at the bit-level, which can confuse and diffuse the image at the same time. Muttoo et al. (2010) has proposed data hiding in JPEG images, which has been one of the well known embedding method of stenography based on Transform domain. Puech (2004) have explained and reviewed the security, performance and reliability issues, in respect to the combination of various chaos based symmetric key cryptosystems. Logistic, Henon, Tent, Cubic and Cheyshev mappings have been used for the enhancement of the key space.

2.1 Lorenz Encryption

The first chaotic encryption method which has been looked at was the Lorenz method (a three-dimensional chaotic system). This algorithm generates its chaotic matrix elements by first performing a number of differential equation calculations based on certain input parameters (σ, ρ andβ) (Alsafasfeh & Alarni, 2011) as given by Equations (1), (2) and (3):

$$\frac{dx}{dt} = \sigma(y - x) \tag{1}$$

$$\frac{dy}{dt} = \rho x - y - xz \tag{2}$$

$$\frac{dz}{dt} = xy - \beta z \tag{3}$$

2.2 Rossler Encryption

The second chaotic encryption method was the Rossler method (another three-dimensional chaotic system). This algorithm is similar to the Lorenz method in that it too generates its chaotic matrix elements via differential equations with parameters a, b, and c as described in (Gao, Zhang, & Liang, 2006) by the Equations (4), (5) and (6):

$$\frac{dx}{dt} = -y - z \tag{4}$$

$$\frac{dy}{dt} = x + ay \tag{5}$$

$$\frac{dz}{dt} = b + z(x - c) \tag{6}$$

It has been quickly abandoned both of these methods based on speed alone. Encryption took interminably longer using the differential equation method of generating chaotic elements than in the other methods that follow.

2.3 Logistic Map Encryption

Thirdly, it has been decided to look at the Logistic Map method for generating the chaotic matrix. The Logistic Map is a simpler one-dimensional chaotic system based on the logistic Equation (7),

$$x_{n+1} = \lambda x_n(1 - x_n) \tag{7}$$

where x_0 is the initial condition and λ is the parameter, together comprises the key. This algorithm is much quicker. It simply iterates recursively until there are as many values of x_n as there are pixels in the original image. The values of x_n are scaled to be in [0, 255] and the XOR is performed, as expected in (Gao, Zhang, & Liang, 2006).

The Logistic Map algorithm has been widely used due to its simplicity and efficiency, but can only accept values of $\lambda \in (0, 4)$. This limitation to λ is detrimental to the successful usage of the Logistic Map as a high-security algorithm. This is especially true when you consider the fact that for $\lambda \in (0, 3.6)$, the iterations of x_n bounce back and forth between handful of values, or converge on only one value, making all λ in that interval unusable for encryption purposes. Thus, $\lambda \in (3.6, 4)$ as described by (Gao, Zhang, & Liang, 2006).

2.4 NCA Encryption

Limitations of the Logistic Map lead a few researchers to develop their own algorithm. They decided to use a nonlinear chaotic algorithm (NCA) in an effort to improve security. The nonlinear aspect of the algorithm is provided by the use of a power function and a tangent function in the recursive generation of the x_n. The formulas used to generate the chaotic matrix are as follows in Equation (8):

$$x_{n+1} = \lambda \cdot \tan(\alpha x_n) \cdot (1 - x_n)^{\beta} \tag{8}$$

where $x_n \in (0, 1)$ and $n = 0, 1, 2, \ldots$, and

$$\lambda = \mu \cdot \cot\left(\frac{\alpha}{1+\beta}\right) \cdot \left(1 + \frac{1}{\beta}\right)^{\beta} \tag{8.a}$$

where $\mu = 1 - \beta^{-4} > 0$. Through experimentation, the researchers determined that there were three sets of parameter combinations that would eventually lead to a proper chaotic-matrix:

(1) $x_n \in (0, 1)$, $\alpha \in [0, 1.4]$, $\beta \in [5, 43]$;

(2) $x_n \in (0, 1)$, $\alpha \in [1.4, 1.5]$, $\beta \in [9, 38]$;

(3) $x_n \in (0, 1)$, $\alpha \in [1.5, 1.57]$, $\beta \in [3, 15]$.

where it has been found that changing the initial condition and parameters could have a noticeable effect on the encrypted image (Gao, Zhang, & Liang, 2006). The question may arise, "why are the iterated values of x_n thrown away at various times throughout this process?". The researchers claim that it is to "avoid the harmful effect of transitional procedure" and to increase security by selecting the "pseudo-random numbers discontinuously" (Gao,

Zhang, & Liang, 2006).

All of the algorithms that studied during this work were slower than expected, or in some cases, slower than reported in the literature where they were run on less-capable computers. One reason behind this could be the Matlab software used for the analysis of these encryption techniques might not be the ideal software to work with. Another reason could be that there are elements to the encrypting techniques that are left out of the research papers; the authors may be trying to hold back some essential part of the encryption algorithm for future financial gain. A third reason could be that even though the encryption/decryption steps have been followed correctly for each algorithm, the researchers might have coded the analysis in an inefficient way in Matlab. Regardless, a decision was taken to try and develop a new nonlinear chaotic algorithm which would maintain the robustness, obscuring, security, and correlation features of the NCA, but would be significantly faster.

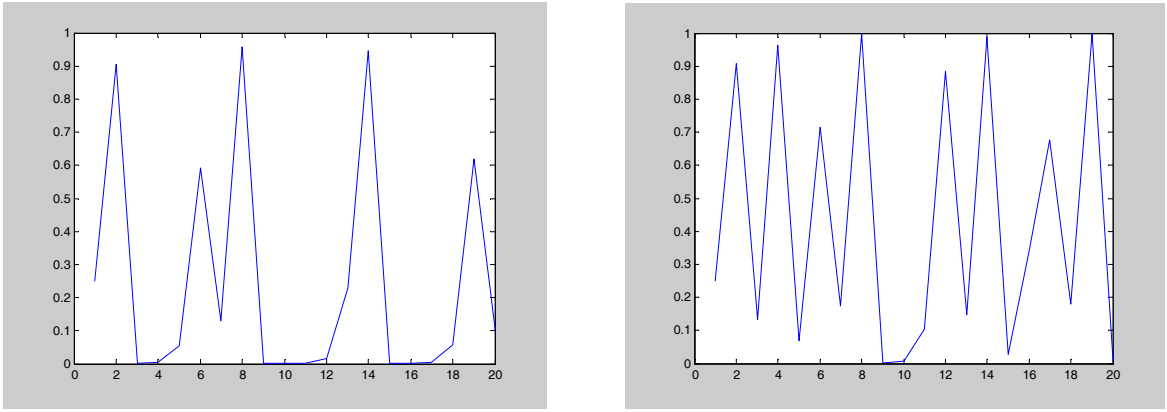
3. Proposed Scheme Improving a New Logistic Map (INCA)

The proposed scheme is a modification of the one suggested of a new chaotic algorithm for image encryption (NCA) (Gao, Zhang, & Liang, 2006). In this paper we modified the logistic map $\lambda \times x_n(1-x_n)$ by adding two keys such that fixed point should not less than 1 so we define new factor $\lambda_1 x_n^{\tau-1}$ then by multiplying new factor with logistic map $\lambda \times x_n(1-x_n) \times (\lambda_1 x_n^{\tau-1}) = \gamma \times x_n^{\tau}(1-x_n)$ new algorithm will be constructing and keep the chaotic properties, a new NCA shown in Equation (9.a) and (9.b):

$$x_{n+1} = (1-\beta^{-4}) \cdot \cot\left(\frac{\alpha}{1+\beta}\right) \cdot \left(1+\frac{1}{\beta}\right)^{\beta} \tag{9.a}$$

$$\tan(\alpha x_n) \cdot (1-x_n)^{\beta} + \gamma \cdot x_n^{\tau}(1-x_n) = 0 \tag{9.b}$$

Where $x_n \in (0,1)$, $\alpha \in (0, 1.47]$, $\beta \in [1.8, 9]$, $\gamma \in [4.2, \infty)$, $\tau \in (0, 2.3]$ and Figure 1 shows the iteration curve of the improving map (INCA) when $x_o = 0.5, \alpha = 1.4, \beta = 5, \gamma = 4.4$ and $\tau = 2.2$ from these statistical data, we can see that the new chaotic algorithm spreads the initial region over the entire phase space.



(a) (b)

Figure 1. (a) Iteration of NCA Map (b) Iteration of Improving Map INCA

4. Encryption Based Improving INCA Map

The entire encryption process can be split up into three main sections: initial setup, mask generator process, and the dynamic XORing process. Generated elements have been stored within the chaotic matrix of size the same as the original image's size. As with the other algorithms that made use of the XOR operation to encrypt, decryption is a simple matter of recreating the matrix of chaotic elements and XORing it with the encrypted image matrix. The actual procedure for encryption below shows in Figure 2 a flowchart for the entire setup, encryption, and decryption:

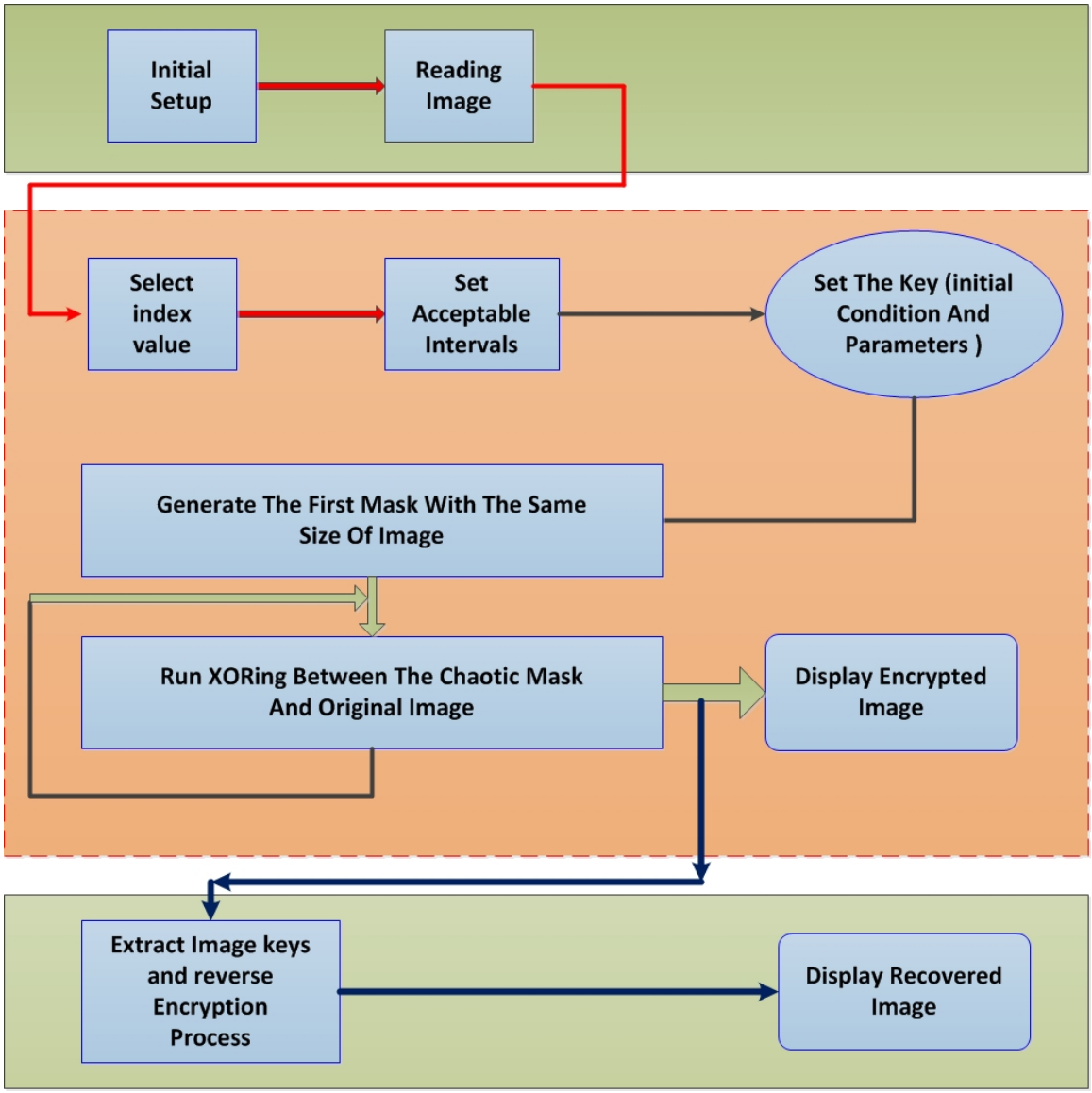


Figure 2. Flowchart for the entire setup, encryption, and decryption process

5. Results Analysis and Discussion

Simulation results and experimental performance analyses of the proposed image encryption scheme are provided in this section. A 256 × 256 size 8 bits Lena image has been considered as an example as depicted in Figure 3(a) and Figure 3(b) shown encrypted image with initial parameters are $(\alpha,\beta,\gamma,\tau,\chi_0)=(1.47,5,4.876545676545671,2.3)$ also we divided initial condition for each generated mask $(\chi_{10},\chi_{20},\chi_{30})=(0.987654321012345,0.345645477457451,0.34564547745745)$ after applying INCA the encrypted image is rough-and-tumble, mysterious and 100% obscure of the image as shown in Figure 3(b) also Figure 3(c) shown the decrypted image by use the same encryption key, it can be seen that the decrypted image is clear and correct without any distortion also as shown in Figure 3(f) there is no error between original image and decrypted image.

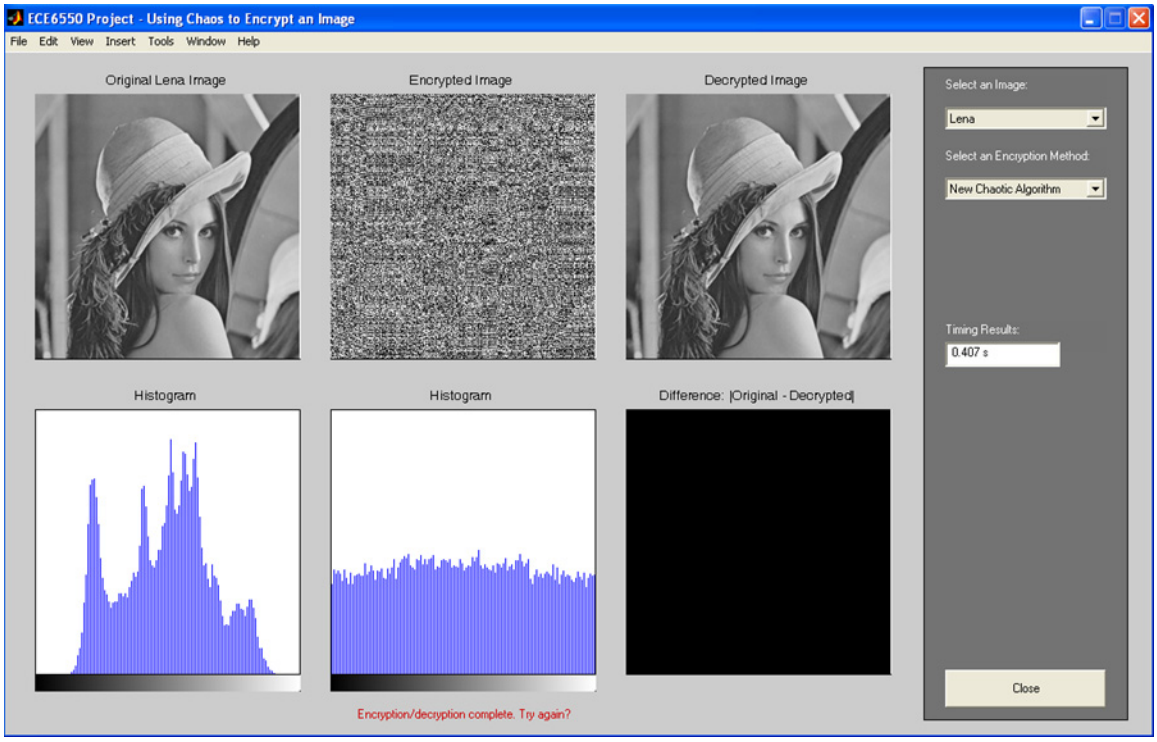
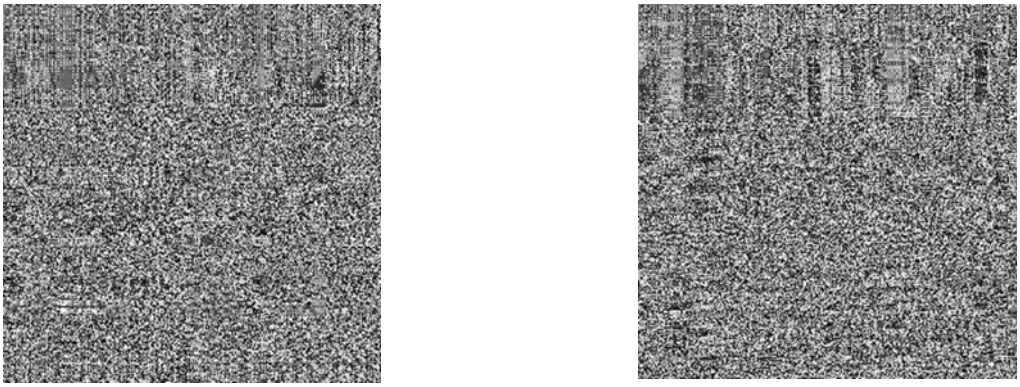


Figure 3 (a) Original image (b) encrypted image (c) decrypted image (d) histogram of original image (e) histogram of decrypted image (f) error between original and encrypted image

The secret key should produce a completely different encrypted image. For testing the key sensitivity of the proposed image encryption procedure, we use the wrong key, initial parameters are $(\alpha,\beta,\gamma,\tau,\chi_0) = (1.47,5,4.876545676545672,2.3)$ and initial condition $(\chi_{10},\chi_{20},\chi_{30}) = (0.987654321012345,0.345645477457451,0.34564547745745)$ we note the decrypted image still rough-and-tumble and unknowable see Figure 3(a) and if we chose another key initial parameters are $(\alpha,\beta,\gamma,\tau,\chi_0) = (1.47,5,4.876545676545670,2.3)$ and initial condition $(\chi_{10},\chi_{20},\chi_{30}) = (0.987654321012345,0.345645477457451,0.34564547745745)$ we can note that image still unknowable see Figure 4(b).



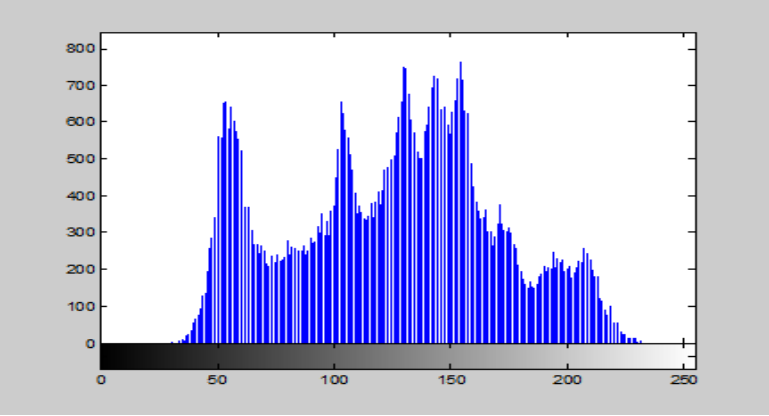
(a) (b)

Figure 4. Decrypted using wrong key

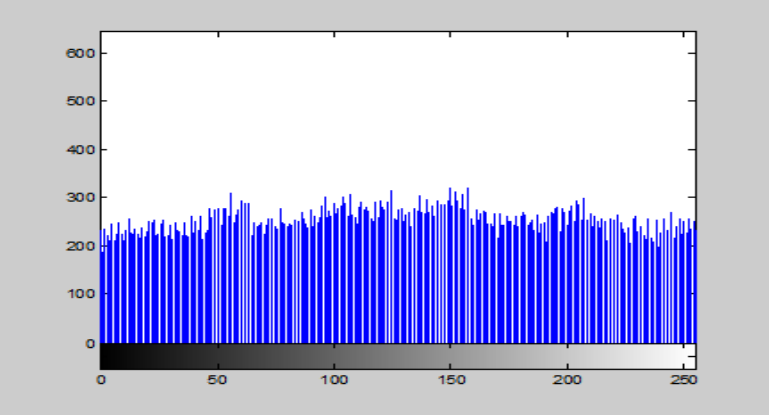
5.1 Statatistical Analysis

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 a test on the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

(1) Histograms of encrypted images. One typical example among them is shown in Figure 5. From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image.



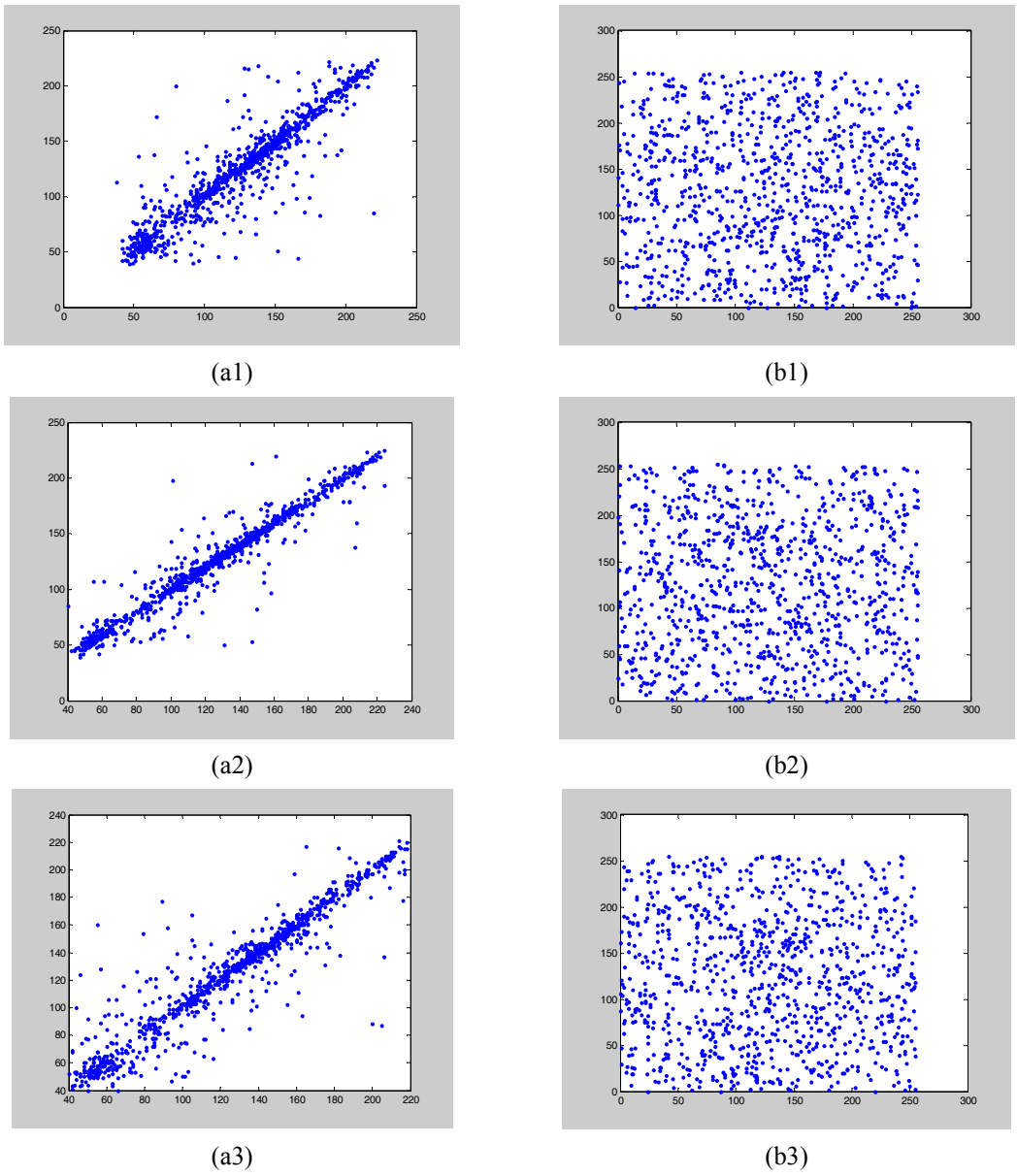
(a)



(b)

Figure 5. Histogram of (a) Original Image and (b) Encrypted

(2) The extensive study of the correlation between image and its corresponding encrypted image by using the proposed encryption algorithm. The correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, as expressed by Figure 6 and Table 1.



(a1) (b1)

(a2) (b2)

(a3) (b3)

Figure 6. Correlations of two diagonal, horizontally and vertical adjacent pixels in the plain image and in the cipher-image

Table 1. Correlation coefficients of two adjacent pixels in two images

	Plain image	*Ciphered image*
Horizontal	0.9681	-0.0066
Vertical	0.9434	0.0153
Diagonal	0.9238	-0.0104

5.2 Key Space Analysis

For a secure image cipher, the key space should be large enough to make the brute force attack infeasible. The key of the new algorithm consists of three floating-point numbers. If we use the first 15 digits of a floating-point number, then there are:

$$15 + 15 + 15 + 15 + 15 = 75 \text{ uncertain digits}$$

So the possible key number is 10^{75}. An image cipher with such a long key space is sufficient for reliable practical use.

5.3 Time Analysis

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. We measured the encryption/decryption rate based on 256 grey-scale images of size 256 x 256 by using the proposed image encryption scheme. The time analysis has been done on Pentium-4 with 512 MB RAM computer. The average encryption/decryption time is 0.4 s which is less than the speed of the algorithm proposed NCA moreover the time is very close to the algorithm proposed in (Delp, 2003; Alsafasfeh & Alshabatat, 2011). Table 2 shows the comparison between INCA and the other chaotic encryption methods.

Table-2. Comparison between INCA and the other chaotic encryption methods

	Lorenz (Chong, Chuan, & Ying, 2007)	Rossler (Elkouny, Zakaria, & Sobhy, 2002)	Logistic Map (Pareek, Patidar, & Sud, 2006)	New Logistic Map (Gao, Zhang, & Liang, 2006)	The 3D cat map Chen, Mao, & Chui, 2004	One D based (Chon,Chuan, & Ying, 2007)	Improving New logistic Map
Key Space	2^{158}	10^{16}	$1.2x10^{24}$	10^{45}	2^{36}	2^{53}	10^{75}
Time	10.84 s		0.33 s	0.5 s	0.4 s	12.27 s	0.4 s
Obscure	100%	100%	< 100%	< 100%	100%	100%	100%

5.4 Obscuring Analysis

The Logistic Map and the NCA encryption methods both chaotically modify every pixel in the original image, but they still leave "shadows" of the original image visible especially in text image or high edge image see Figure 7 so the INCA has a full obscuring.

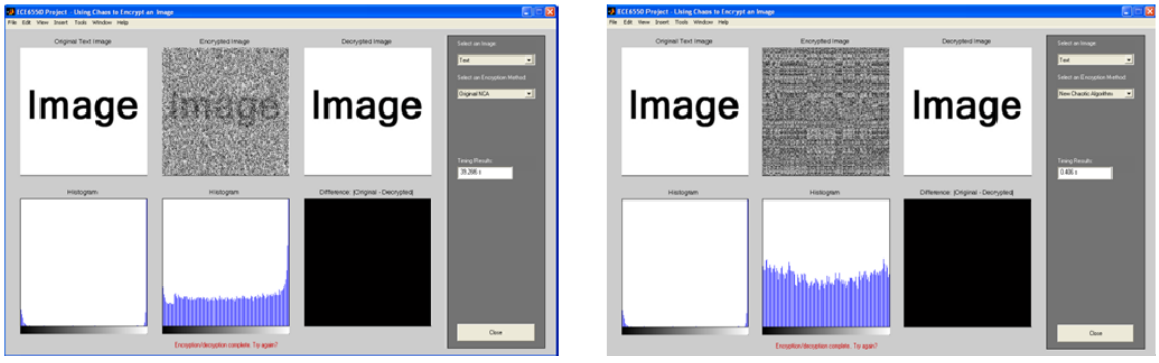


Figure 7. Obscuring analysis

6. Conclusion

This paper presents a new nonlinear chaotic algorithm. A new way of image encryption scheme has been proposed which utilizes two chaotic logistic maps. To overcome the drawbacks of small key space and weak obscure in the widely used NCA, its structural parameters and initial value can all be used as encryption key in chaotic. Experimental analysis demonstrates that the image encryption algorithm based on INCA shows advantages of large key space and high-level security, high obscure level and high speed. Finally, experimental and analytic results show that our scheme is efficient, the adopted examples show the highly confidential encrypted images and demonstrate a good potential in the application of the digital-color image encryption.

References

Alsafasfeh, Q., & Alshabatat, A. (2011). Image Encryption Based on Synchronized Communication Chaotic Circuit. *Journal of Applied Sciences Research, 7*(4), 392-399.

Alsafasfeh, Q., & Arfoa, A. (2011). Image Encryption Based on the General Approach for Multiple Chaotic System. *Journal of Signal and Information Processing, 2*(3), 238-244. http://dx.doi.org/10.4236/jsip.2011.23033

Alsafasfeh, Q. H., & Al-Arni, M. S. (2011). A New Chaotic Behavior from Lorenz and Rossler Systems and Its Electronic Circuit Implementation. *Circuits and Systems, 2*(2), 101-105. http://dx.doi.org/10.4236/cs.2011.22015

Bourbakis, N., & Alexopoulos, C. (1992). Picture data encryption using SCAN pattern. *Pattern Recogn, 25*, 567-581. http://dx.doi.org/10.1016/0031-3203(92)90074-S

Chen, G., Mao, Y., & Chui, C. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals, 21*, 749-761. http://dx.doi.org/10.1016/j.chaos.2003.12.022

Chong, F., Zhen-chuan, Z., & Ying-yu, C. (2007). An Improved Image Encryption Algorithm Based on Chaotic Maps. *Third International Conference on Natural Computation, ICNC 2007*, August, 2007 (pp. 189-193). http://dx.doi.org/10.1109/TENCON.2007.4429127

Delp, E. (2003). Multimedia Security: So What's the Big Deal? *Purdue University School of Electrical and Computer Engineering Video and Image Processing Laboratory* (VIPER).

Elkouny, A., Zakaria, N., & Sobhy, M. (2002). Communication Security Using Chaotic Generator, 2002. MWSCAS-2002. *The 2002 45th Midwest Symposium on Circuits and Systems*.

Gao, H., Zhang, Y., Liang, S., & Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons & Fractals, 29*, 393-399. http://dx.doi.org/10.1016/j.chaos.2005.08.110

Hua, J. (2009). The Network Identity Authentication System. *Modern Applied Science, 3*(5), 127-130.

Muttoo1, S. K., & Sushil, K. (2009). Data Hiding in JPEG Images. *BVICAM'S International Journal of Information Technology*.

Pareek, N., Patidar, V., & Sud, K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing, 24*, 926-934. http://dx.doi.org/10.1016/j.imavis.2006.02.021

Puech, W., & Rodrigues, J. M. (2004). A New Crypto- Watermarking Method for Medical Images Safe Transfer. In *The 12th European Signal Processing Conference* (pp. 1481-1484).

VanDroogenbroeck, M., & Benedett, R. (2002). Techniques for a Selective Encryption of Uncompressed and Compressed Images. *Proceedings of Advanced Concepts for Intelligent Vision Systems* (pp. 90-97).

Zhang, L., & Zhang, Y. (2005, May). Research on Lorenz chaotic stream cipher. In *VLSI Design and Video Technology, 2005. Proceedings of 2005 IEEE International Workshop on* (pp. 431-434). IEEE.

Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communications, 284*(12), 2775-2780. http://dx.doi.org/10.1016/j.optcom.2011.02.039

Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences, 181*(6), 1171-1186. http://dx.doi.org/10.1016/j.ins.2010.11.009

Copyrights