

Breaking a chaotic image encryption algorithm based on perceptron model

Yu Zhang · Chengqing Li · Qin Li · Dan Zhang · Shi Shu

Received: Nov 5 2011

Abstract Recently, a chaotic image encryption algorithm based on perceptron model was proposed. The present paper analyzes security of the algorithm and finds that the equivalent secret key can be reconstructed with only one pair of known-plaintext/ciphertext, which is supported by both mathematical proof and experiment results. In addition, some other security defects are also reported.

Keywords Chaos · Cryptanalysis · Known-plaintext attack · Perceptron model · Lorenz system

1 Introduction

The usage of chaos for image encryption has been received intensive attention in the past decade. This is mainly spurred by the following three points: 1) increasing importance of security of image data as it is transmitted over all kinds of networks with a more and

more higher frequency; 2) low efficiency of the traditional text encryption algorithms like DES with respect to protecting image data due to some intrinsic features of images such as bulk data capacity, high redundancy, strong correlation among adjacent pixels, etc; 3) some fundamental features of the chaotic dynamical systems such as ergodicity, mixing property, sensitivity to initial conditions/system parameter can be considered analogous to some ideal cryptographic properties such as confusion, diffusion, avalanche properties. According to the record of *Web of Science*, more than five hundreds of articles on chaos-based image encryption algorithms have been published in the past fifteen years [3]. Some other related papers consider video, audio (speech) or text as encryption objects [4, 5, 17].

Roughly speaking, the usage of chaos in designing digital symmetric encryption algorithms can be categorized as three classes: 1) creating position permutation relations directly or indirectly; 2) generating pseudo-random bit sequence (PRBS) controlling composition and combination of some basic encryption operations; 3) producing ciphertext directly by assigning plaintext as initial conditions or control parameters of a chaos system. As native opposite of cryptography, some cryptanalysis work was also developed and some chaos-based encryption algorithms are found to be not secure of different extents from the viewpoint of modern cryptology [1, 2, 8, 15, 18, 20]. Due to owning complex dynamical properties, artificial neural network was combined with chaos to design symmetric and public encryption algorithms [6, 7, 13, 14, 21]. Unfortunately, some of them are found to be equivalent to much simpler form in terms of essential structure and can be broken easily [10, 11].

In [19], a chaotic image encryption algorithm based on perceptron model, a type of artificial neural network invented in 1957, was proposed, where two PRBSs, gen-

Yu Zhang, Shi Shu
School of Mathematics and Computational Science, Xiangtan University, Xiangtan 411105, Hunan, China

Chengqing Li
College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China
Tel.: +86-731-52639779
Fax: +86-731-58292217
E-mail: chengqingli@gmail.com

Qin Li
College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China

Dan Zhang
College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, Zhejiang, China

erated from quantized orbit of Lorenz system under given secret key, is used to control the perceptron model to output cipher-image from the input of plain-image. However, we proved that the seeming complex image encryption algorithm is equivalent to a stream cipher of exclusive or (XOR) operation. So, it can be easily broken with only one pair of plain-image and cipher-image. In addition, some other security defects about secret key, insensitive of cipher-image with respect to plain-image and low randomness of the used PRBS are reported.

The rest of the paper is organized as follows. The next section briefly introduces the proposed image encryption algorithm. Section 3 presents detailed cryptanalysis on the encryption algorithm with experiment results and some other security defects. The last section concludes the paper.

2 The proposed image encryption algorithm

The plaintext encrypted by the image encryption algorithm under study is a gray-scale digital image. Without loss of generality, the plaintext can be represented as a one-dimensional 8-bit integer sequences $P = \{p_n\}_{n=0}^{N-1}$ by scanning it in a raster order. Correspondingly, the ciphertext is denoted by $P' = \{p'_n\}_{n=0}^{N-1}$. The kernel of the encryption algorithm is based on a threshold function

$$f(x) = \begin{cases} 1, & \text{if } x \geq 0, \\ 0, & \text{otherwise,} \end{cases}$$

which was considered by the proposers as simple variant of a single layer perceptron model who inputs m variables, s_0, s_1, \dots, s_{m-1} , and outputs m ones by calculating

$$g(s_i) = \begin{cases} 1, & \text{if } \left(\sum_{j=0}^{m-1} s_j w_{ij} - \theta_i \right) \geq 0, \\ 0, & \text{otherwise,} \end{cases}$$

where w_{ij} denotes the weight of the i -th input for the j -th neuron, θ_i is the threshold of the i -th neuron, and $i = 0 \sim m-1$. With these preliminary introduction, the image encryption algorithm under study can be described as follows¹.

- *The secret key*: initial state (x_0^*, y_0^*, z_0^*) and the step length h of an approximation method solving the

Lorenz system

$$\begin{cases} \dot{x} = ay - ax, \\ \dot{y} = cx - xz - y, \\ \dot{z} = xy - bz, \end{cases} \quad (1)$$

under fixed control parameters $(a, b, c) = (10, \frac{8}{3}, 28)$.

- *The initialization procedures*:

1) in double-precision floating-point arithmetic, solve the Lorenz system (1) with the fourth-order Runge-Kutta method of step h iteratively 3001 times from (x_0^*, y_0^*, z_0^*) and obtain the current approximation state (x_0, y_0, z_0) .

2) run the above solution approximation step seven more times from the current approximation state to get $\{(x_j, y_j, z_j)\}_{j=1}^7$, and set

$$w_j = \begin{cases} 1, & \text{if } (x_j - \tilde{x})/(\hat{x} - \tilde{x}) \geq 0.5, \\ -1, & \text{otherwise,} \end{cases}$$

and

$$\tilde{w}_j = \begin{cases} 1, & \text{if } (y_j - \tilde{y})/(\hat{y} - \tilde{y}) \geq 0.5, \\ -1, & \text{otherwise,} \end{cases}$$

for $j = 0 \sim 7$, where $\hat{x} = \max(\{x_j\}_{j=0}^7)$, $\tilde{x} = \min(\{x_j\}_{j=0}^7)$, $\hat{y} = \max(\{y_j\}_{j=0}^7)$, $\tilde{y} = \min(\{y_j\}_{j=0}^7)$. 3) reset the current approximation state of the Lorenz system as

$$\begin{cases} x_0 = \tilde{x} + (x_8 - \tilde{x}) \left(\sum_{j=0}^7 (w_j + 1) \cdot 2^{j-1} \oplus r \right) / 256, \\ y_0 = \tilde{y} + (y_8 - \tilde{y}) \left(\sum_{j=0}^7 (\tilde{w}_j + 1) \cdot 2^{j-1} \oplus r \right) / 256, \\ z_0 = z_8, \end{cases}$$

where $r = \lfloor (z_8 - \lfloor z_8 \rfloor) \cdot 256 \rfloor$.

4) repeat the above two steps $N-1$ times and get two sequences $\{w_k\}_{k=0}^{8N-1}$ and $\{\tilde{w}_k\}_{k=0}^{8N-1}$.

- *The encryption procedure*: for the n -th plain-byte $p_n = \sum_{i=0}^7 p_{n,i} \cdot 2^i$, obtain the corresponding cipher-byte $p'_n = \sum_{i=0}^7 p'_{n,i} \cdot 2^i$ by calculating

$$p'_{n,i} = \begin{cases} f(p_{n,i} w_k + c_k \tilde{w}_k - \theta_k), & \text{if } w_k = 1, \\ f(p_{n,i} w_k - c_k \tilde{w}_k + \theta_k), & \text{otherwise,} \end{cases} \quad (2)$$

where $c_k = -w_k/2$, $\theta_k = ((w_k + 1)/2) \oplus ((\tilde{w}_k + 1)/2)$ and $k = 8 \cdot n + i$.

- *The decryption procedure* is the same as the encryption one except that the locations of $p_{n,i}$ and $p'_{n,i}$ in the encryption function (2) are swapped.

¹ To make the presentation more concise and complete, some notations in the original paper [19] are modified, and some details about the algorithm are also amended under the condition that its security property is not influenced.

3 Cryptanalysis

3.1 Known-plaintext attack

It is well-known that any detail of an encryption algorithm, except the secret key, should be public. This is called Kerckhoffs's principle, which was reformulated by Claude Shannon as Shannon's maxim, "The enemy knows the algorithm." Under this principle, the known-plaintext attack is a cryptanalysis model where the attacker can access some samples of both the plaintext, and the corresponding ciphertext (encrypted version). The objective of the model is to reveal some (even all) information about the secret key, which is then used to decrypt other ciphertext encrypted with the same secret key. Note that feasibility of the known-plaintext attack is based on repeated usage of secret key, namely impracticability of one-time pad, which is caused by the following three problems: 1) impossibility of software source of perfectly random bits; 2) secure generation and exchange of the one-time pad material of not shorter length than that of the plaintext; 3) complex secret key management preventing the secret key is reused in whole or part.

Strength of any encryption algorithm against the known-plaintext attack is one of the most important factors evaluating its security. Unfortunately, we found that the image encryption algorithm under study can be broken with only one pair of plaintext and the corresponding ciphertext.

Theorem 1 For $n = 0 \sim N - 1$ and $i = 0 \sim 7$,

$$p'_{n,i} = \begin{cases} p_{n,i}, & \text{if } w_k = 1, \\ \overline{p_{n,i}}, & \text{otherwise,} \end{cases} \quad (3)$$

where $k = 8n + i$, $\overline{x} = (x \oplus 1)$.

Proof To proof the theorem, we study the four possible combination of $(w_k, p_{n,i})$ as follows.

– $(w_k, p_{n,i}) = (1, 1)$:

$$\begin{aligned} p'_{n,i} &= f(p_{n,i} \cdot w_k + c_k \cdot \tilde{w}_k - \theta_k) \\ &= f(1 + (-1/2) \cdot \tilde{w}_k - \theta_k) \\ &= \begin{cases} f(1 - 1/2 - 0), & \text{if } \tilde{w}_k = 1, \\ f(1 + 1/2 - 1), & \text{otherwise} \end{cases} \\ &= f(1/2) \\ &= 1. \end{aligned}$$

– $(w_k, p_{n,i}) = (1, 0)$:

$$\begin{aligned} p'_{n,i} &= f(p_{n,i} \cdot w_k + c_k \cdot \tilde{w}_k - \theta_k) \\ &= f(0 + (-1/2) \cdot \tilde{w}_k - \theta_k) \\ &= \begin{cases} f(0 - 1/2 - 0), & \text{if } \tilde{w}_k = 1, \\ f(0 + 1/2 - 1), & \text{otherwise} \end{cases} \\ &= f(-1/2) \\ &= 0. \end{aligned}$$

– $(w_k, p_{n,i}) = (-1, 1)$:

$$\begin{aligned} p'_{n,i} &= f(p_{n,i} \cdot w_k - c_k \cdot \tilde{w}_k + \theta_k) \\ &= f(-1 - 1/2 \cdot \tilde{w}_k + \theta_k) \\ &= \begin{cases} f(-1 - 1/2 + 1), & \text{if } \tilde{w}_k = 1, \\ f(-1 + 1/2 + 0), & \text{otherwise} \end{cases} \\ &= f(-1/2) \\ &= 0. \end{aligned}$$

– $(w_k, p_{n,i}) = (-1, 0)$:

$$\begin{aligned} p'_{n,i} &= f(p_{n,i} \cdot w_k - c_k \cdot \tilde{w}_k + \theta_k) \\ &= f(0 - 1/2 \cdot \tilde{w}_k + \theta_k) \\ &= \begin{cases} f(0 - 1/2 + 1), & \text{if } \tilde{w}_k = 1, \\ f(0 + 1/2 + 0), & \text{otherwise} \end{cases} \\ &= f(1/2) \\ &= 1. \end{aligned}$$

Combining the above four cases, one has

$$p'_{n,i} = \begin{cases} 1, & \text{if } p_{n,i} = 1 \text{ and } w_k = 1, \\ 0, & \text{if } p_{n,i} = 0 \text{ and } w_k = 1, \\ 0, & \text{if } p_{n,i} = 1 \text{ and } w_k = -1, \\ 1, & \text{if } p_{n,i} = 0 \text{ and } w_k = -1, \end{cases}$$

which means

$$p'_{n,i} = \begin{cases} p_{n,i}, & \text{if } w_k = 1, \\ \overline{p_{n,i}}, & \text{otherwise,} \end{cases}$$

Thus, the theorem is proved. \square

Observe Theorem 1, one has

$$p'_{n,i} = p_{n,i} \oplus \overline{w'_k}, \quad (4)$$

where $w'_k = (w_k + 1)/2$. From Eq. (4), one can get

$$(p_n \oplus p'_n) = \eta_n,$$

where $\eta_n = \sum_{i=0}^7 \overline{w'_{8n+i}} \cdot 2^i$ and $n = 0 \sim N - 1$. For any another cipher-image $Q' = \{q'_n\}_{n=0}^{N-1}$ encrypted with the same secret key, one can easily reveal the corresponding plain-image $Q = \{q_n\}_{n=0}^{N-1}$ by calculating

$$q_n = q'_n \oplus \eta_n$$

for $n = 0 \sim N - 1$, which means $H = \{\eta_n\}_{n=0}^{N-1}$ can work as equivalent secret key.

To verify performance of the above attack, some experiments were made. Figure 1 shows a plain-image “Lenna” of size 512×512 and the encryption result with the secret key $(x_0^*, y_0^*, z_0^*) = (1, 1, 0)$, and $h = 10^{-1}$. A mask image H is constructed by XORing datum of Fig. 1a) and Fig. 1b) byte by byte, and shown in Fig. 2a). The mask image is then used to decrypt another cipher-image shown in Fig. 2b) and the result is shown in Fig. 2c), which is identical with the original plain-image “Baboon”.

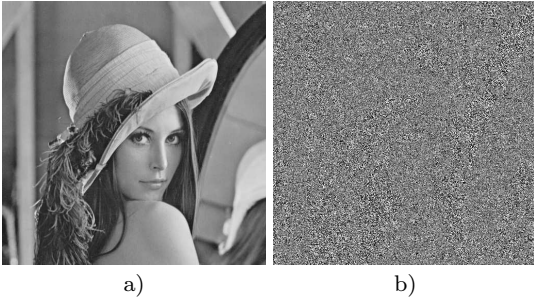


Fig. 1 One known plain-image and the corresponding cipher-image: a) known plain-image “Lenna”, b) cipher-image of Fig. 1a).

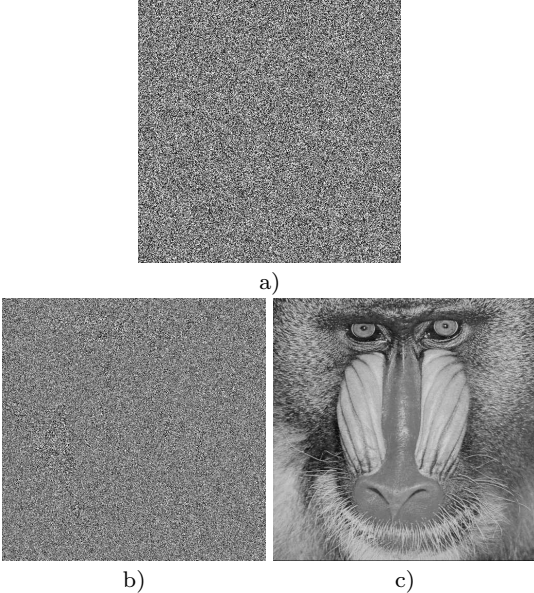


Fig. 2 Known-plaintext attack: a) the mask image H , b) cipher-image of plain-image “Baboon”, c) the recovered image of Fig. 2b).

3.2 Some other security defects

In this subsection, we further report some other security defects of the image encryption algorithm under study.

- *Low sensitivity with respect to change of plain-image*
If encryption results of an encryption algorithm are not sensitive to change of plaintext in a significant degree, the attacker can make predictions about the plaintext from the given ciphertext only. The desirable property of encryption algorithm is called avalanche effect in field of cryptography. The property is even more important for image encryption algorithms since image datum and its watermarked versions, generally slight modified versions of the original ones, are encrypted often at the same time and stored at the same place. The avalanche effect is quantitatively measured by how every bit of ciphertext is changed when only one bit of plaintext is modified. As for the image encryption algorithm under study, change of one bit of plain-image can only influent one bit of the same location in the corresponding ciphertext, which disobeys expected property of a secure encryption algorithm very far.

- *Insufficient randomness of the two used PRBSs*

The complex dynamical properties of chaos systems demonstrated in continuous domain make they are considered as good generation source of PRBS. However, chaos systems can not do the expected things in general since their dynamical properties will definitely degenerate in digital domain, where everything is stored and calculated in limited precision [12]. In addition, some chaos systems need numerical approximation, the used simulation methods and related parameters will have different influences on degradation of the dynamical properties of the chaos system also. As for the image encryption algorithm under study, trajectory of Lorenz system is continuous, which means that any two consecutive simulated states are always correlated in a high degree. As a consequence, the bits derived from neighboring states will also be correlated closely. Furthermore, the smaller the step length h is, the stronger the correlation will be [9]. Meanwhile, the value of h should be small enough since the accumulated error of the fourth-order Runge-Kutta method is $O(h^4)$. So, step length h should not be used as a sub-key since its valid scope can not be defined clearly. To verify this point, we employed the NIST statistical test suite [16] to test the randomness of 100 binary sequences of length $512 \times 512 \times 8 = 2,097,152$ bits (the number of bits in $\{\overline{w'_k}\}$ used for the encryption of 512×512 gray-scale images). Note that the 100 binary sequences are generated by randomly selected

initial conditions (x_0^*, y_0^*, z_0^*) and a given step length h . For each test, the default significance level 0.01 was adopted. The passing rates in terms of binary matrix rank test, calculating the rank of disjoint sub-matrices of the entire sequence, under different values of step length h are shown in Fig. 3, which agree with the estimation. We found that the PRBSs generated by the method used in the image encryption algorithm under study can not pass most tests in the test suite even for the step length h under which the rank test can be passed. When $h = 0.1$, the test results are shown in Table 1, from which one can see that the used pseudo-random bit generator is not a good source of PRBS.

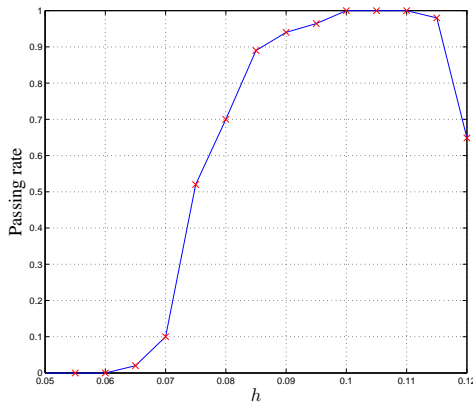


Fig. 3 Passing rate of the rank test under different values of step length h .

Table 1 The performed tests with respect to a significance level 0.01 and the number of sequences passing each test in 100 randomly generated sequences.

Name of Test	Number of Passed Sequences
Frequency	93
Block Frequency ($m = 128$)	100
Cumulative Sums-Forward	94
Runs	0
Rank	100
Serial ($m = 16$)	0
Spectral Test	0
Random Excursions($x=1$)	0
Approximate Entropy ($m = 10$)	0
Longest Runs of Ones ($m=10000$)	0
Non-overlapping Template ($m = 9, B = 000000001$)	0

4 Conclusion

In this paper, the security of a chaotic image encryption algorithm based on perceptron model has been investigated in detail. The seeming complex encryption algorithm was proved to be equivalent to a stream cipher essentially, and so it can be broken with only one pair of known-plaintext/ciphertext. In addition, some other security defects of the encryption algorithm, including insensitivity with respect to change of plain-image and low randomness of PRBS used are also reported. In all, this cryptanalysis paper shows us again that security of an encryption algorithm should be mainly built on good essential structure of the whole encryption operations instead of so-called complex theories.

Acknowledgements This research was supported by the National Natural Science Foundation of China (No. 61100216), Scientific Research Fund of Hunan Provincial Education Department (No. 11B124), and Ningbo Natural Science Foundation (No. 2011A610194).

References

1. Álvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos* **16**(8), 2129–2151 (2006)
2. Alvarez, G., Li, S.: Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption. *Communications in Nonlinear Science and Numerical Simulation* **14**(11), 3743–3749 (2009)
3. Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals* **21**(3), 749–761 (2004)
4. Chen, J., Zhou, J., Wong, K.W.: A modified chaos-based joint compression and encryption scheme. *IEEE Transactions on Circuits and Systems II* **58**(2), 110–114 (2011)
5. Chen, Z., Ip, W.H., Chan, C.Y., Yung, K.L.: Two-level chaos-based video cryptosystem on H.263 codec. *Nonlinear Dynamics* **62**(3), 647–664 (2010)
6. Guo, D.H.: A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks. *Applied Intelligence* **10**(1), 71–84 (1999)
7. Leung, K.C., Li, S.L., Cheng, L.M., Chan, C.K.: A symmetric probabilistic encryption scheme based on CHNN without data expansion. *Neural Processing Letters* **24**(2), 93–105 (2006)
8. Li, C., Chen, M.Z.Q., Lo, K.T.: Breaking an image encryption algorithm based on chaos. *International Journal of Bifurcation and Chaos* **21**(7), 2067–2076 (2011)
9. Li, C., Li, S., Álvarez, G., Chen, G., Lo, K.T.: Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. *Physics Letters A* **369**(1–2), 23–30 (2007)
10. Li, C., Li, S., Zhang, D., Chen, G.: Cryptanalysis of a chaotic neural network based multimedia encryption scheme. *Lecture Notes in Computer Science* **3333**, 418–425 (2004)
11. Li, C., Li, S., Zhang, D., Chen, G.: Chosen-plaintext cryptanalysis of a clipped-neural-network-based chaotic cipher. *Lecture Notes in Computer Science* **3497**, 630–636 (2005)

12. Li, S., Chen, G., Mou, X.: On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal of Bifurcation and Chaos* **15**(10), 3119–3151 (2005)
13. Lian, S.: A block cipher based on chaotic neural networks. *Neurocomputing* **72**(4-6), 1296–1301 (2009)
14. Mislovaty, R., Klein, E., Kanter, I., Kinzel, W.: Public channel cryptography by synchronization of neural networks and chaotic maps. *Physical Review Letters* **91**(11), art. number: 110,401 (2003)
15. Rhouma, R., Belghith, S.: Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem. *Physics Letters A* **372**(36), 5790–5794 (2008)
16. Rukhin, A., et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22rev1a (2010). Available online at http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html
17. Sheu, L.J.: A speech encryption using fractional chaotic systems. *Nonlinear Dynamics* **65**(1-2), 103–108 (2011)
18. Solak, E.: Partial identification of Lorenz system and its application to key space reduction of chaotic cryptosystems. *IEEE Transactions on Circuits and Systems-II: Express Briefs* **51**(10), 557–560 (2004)
19. Wang, X.Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron mode. *Nonlinear Dynamics* **62**(3), 615–621 (2010)
20. Zhou, J., Au, O.C.: On the security of chaotic convolutional coder. *IEEE Transactions on Circuits and Systems I* **58**(3), 595–606 (2011)
21. Zhou, T., Liao, X., Chen, Y.: A novel symmetric cryptography based on chaotic signal generator and a clipped neural network. *Lecture Notes in Computer Science* **3174**, 639–644 (2004)