Cryptanalysis of Image Encryption Algorithm Based on Fractional-Order Lorenz-Like Chaotic System

Musheer Ahmad[1], Imran Raza Khan[2], and Shahzad Alam[1]

[1] Department of Computer Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi-110025, India
[2] Department of Computer Science and Engineering,
Institute of Technology and Management, Aligarh-202001, India

Abstract. This paper provides break of an image encryption algorithm suggested by Xu *et al.* recently in [Commun Nonlinear Sci Numer Simulat 19 (10) 3735–3744 2014]. The authors realized a Laplace transformation based synchronization between two fractional-order chaotic systems to execute error-free encryption and decryption of digital images. The statistical analyses show the consistent encryption strength of Xu *et al.* algorithm. However, a careful probe of their algorithm uncovers underlying security shortcomings which make it vulnerable to cryptanalysis. In this paper, we analyze its security and proposed chosen plaintext-attack/known plaintext-attack to break the algorithm completely. It is shown that the plain-image can be successfully recovered without knowing secret key. The simulation of proposed cryptanalysis evidences that Xu *et al.* algorithm is not secure enough for practical utilization.

Keywords: Image encryption, security, fractional chaotic system, synchronization, chosen-plaintext attack.

1 Introduction

Due to recent advancements in information and communication technologies, the digital images have become indispensable mean of communication in the application areas of defense and military, multimedia-broadcasting, satellite-communication, tele-medicine, tele-education, weather forecasting, disaster management, etc,. The demand of secure and fast image-based communication has attracted growing attention of researchers worldwide. Consequently, enormous numbers of image-encryption proposals have been suggested using different techniques to serve the purpose. However, the underlying architecture of many proposals suffers from serious security flaws which make them susceptible to even classical cryptographic attacks. Many image encryption proposals have been successfully broken by cryptanalysts under various attacks and found insecure [1-10]. Cryptanalysis is the science of breaching cryptographic systems to recover plaintext without an access to secret key. The objective of an attacker is to find a way to recover secret key or plaintext in lesser time or storage than the brute-force attack [1]. It is practiced to find weaknesses, if any, in the security system that eventually may leads to the previous results [11, 12].

S.C. Satapathy et al. (eds.), *Emerging ICT for Bridging the Future – Volume 2,*
Advances in Intelligent Systems and Computing 338, DOI: 10.1007/978-3-319-13731-5_41

The new security systems are being designed to replace broken ones and new cryptanalytic techniques are invented to crack the improved security systems. In practice, both the cryptanalysis and cryptography are two equally significant aspects of a security system. It is recommended to design against possible cryptanalysis [13]. The four classical attacks in cryptanalysis [11], in context to image encryption, are: (1) *Ciphertext-only attack*: the attacker only has access to some ciphertext images that can be utilized to recover the plaintext image, (2) *Known-plaintext attack*: the attacker can obtain some plaintext images and corresponding ciphertext images to reveal the plaintext image, (3) *Chosen-plaintext attack*: the attacker can have temporary access to encryption machine and choose some specially designed plaintext images to generate corresponding ciphertext images, and (4) *Chosen-ciphertext attack*: the attacker can have temporary access to the decryption machine and choose some specially designed ciphertext images to obtain the corresponding plaintext images.

Very recently, Xu *et al.* [14] proposed an image encryption algorithm based on synchronization of two fractional-order chaotic systems. The dynamics of fractional-order chaotic systems has more complex behaviour than integer order systems. A Laplace transformation based synchronization of (Drive and Response) systems is realized. A 3D Lorenz-like fractional-order chaotic system is employed at the sender side to encrypt digital plain-images. The algorithm has statistical features of almost flat histograms, higher information entropy, low cross-correlation among adjacent pixels, high key-sensitivity and large key space. Our contribution includes careful security probe of algorithm to find underlying flaw of plain-image independency on the generation of decimal codes used during plain-image pixels encryption. Different plain-images yield same decimal codes if the secret key is kept unchanged. As a result, the algorithm fails to resist the proposed chosen-plaintext/known plaintext attacks which completely breaks the algorithm and recovers the plain-image.

The structure of the remaining paper is arranged as follows: Section 2 provides review of image encryption algorithm under probe. Section 3 analyzes and discusses the cryptanalysis of encryption algorithm under proposed two different attacks. The simulation of cryptanalysis is also demonstrated in the same Section. The conclusions of the work are provided in Section 4.

2 Xu *et al.* Algorithm

The Xu *et al.* image encryption algorithm is based on synchronization of fractional-order Lorenz-like chaotic systems in drive-response configuration via Pecora and Carrol (PC) control method. The fractional order chaotic system employed by Xu *et al.* in encryption algorithm is described as [15]

$$\begin{aligned} D^{\alpha_1} x &= a(x-y) \\ D^{\alpha_2} y &= bx - lxz \\ D^{\alpha_3} z &= -cz + hx^2 + ky^2 \end{aligned} \tag{1}$$

Where, α_1, α_2, α_3 are fractional derivative orders, *x, y, z* are state variables, and *a, b, c, l, h, k* are system parameters. The system (1) shows chaotic behaviour for α_1=0.97, α_2=0.98, α_3=0.99, *a*=10, *b*=40, *c*=2.5, *l*=1, *h*=2, *k*=2. The fractional-order derivative is solved using the Caputo fractional derivative method defined below [16]:

$$D^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \int_0^t \frac{f^{(n)}(\tau)}{(t-\tau)^{\alpha-n+1}} d\tau \quad for \quad n-1 < \alpha < n \tag{2}$$

Where $\Gamma(z) = \int_0^{\infty} e^{-t} t^{z-1} dt$ is the Euler's Gamma function.

Xu *et al.* build a PC drive-response configuration: a drive system constitutes fractional order Lorenz-like system with (*x, y, z*) variables denoted by subscript *m* (for master), and a response system given by the subspace containing (*y, z*) variables. The chaotic signal x_m is adopted to drive the response system. The drive (master) system is defined by

$$\begin{aligned} D^{\alpha_1} x_m &= a(x_m - y_m) \\ D^{\alpha_2} y_m &= bx_m - lx_m z_m \\ D^{\alpha_3} z_m &= -cz_m + hx_m^2 + ky_m^2 \end{aligned} \tag{3}$$

The response (slave) system is defined by

$$\begin{aligned} D^{\alpha_2} y_s &= bx_m - lx_m z_s \\ D^{\alpha_3} z_s &= -cz_s + hx_m^2 + ky_s^2 \end{aligned} \tag{4}$$

The synchronization between the systems (3) and (4) using Laplace transformation theory is realized first before an error-free encryption and decryption of images at sender and receiver sides is performed. It has been shown that the error vectors ($e_1 = y_s - y_m$, $e_2 = z_s - z_m$) converge to zero and a complete synchronization is achieved after initial synchronization time of about five seconds. The readers are advised to go through the Ref. [14] for detailed description of synchronization.

The encryption algorithm suggested by Xu *et al.* to encrypt digital images is follows as:

Algorithm #1: *Encrypt-Xu( )*

Input	:	Plain-image *P*
Output	:	Encrypted image *C*

1. Read the plain-image matrix $P_{M\times N}$ (of size M×N) and convert the 2D matrix to 1D array $P = \{p_1, p_2, \ldots\ldots, p_{MN}\}$ (of size MN)

2. Initialize all fractional derivative orders, system variables and parameters.

3. Simulate the fractional-order system (3) and (4) to achieve complete synchronization.

4. Further iterate system (3) for MN times and capture the chaotic sequence Z = $\{z_1, z_2, \ldots\ldots., z_{MN}\}$

5. Preprocess the sequence Z to obtain decimal codes $D = \{d_1, d_2, \ldots\ldots., d_{MN}\}$, $d_i \in [0, 255]$ as

$$d_i = round(mod((abs(z_i - floor(abs(z_i)))\times 10^5, 256)) \quad i = 1, 2, \ldots\ldots, \mathrm{MN}$$

6. Encrypt the pixels of plain-image p_i using d_i as

$$c_i = Bin2Dec(Dec2Bin(p_i) \oplus Dec2Bin(d_i)) \qquad i = 1, 2, \ldots\ldots, \mathrm{MN}$$

7. Convert 1D array $C = \{c_1, c_2, \ldots\ldots, c_{MN}\}$ to 2D matrix of encrypted image C.

The decryption is performed in the same way as the encryption, except that the chaotic sequence Z is obtained from fractional-order system defined in eqn (4) with same set of secret keys. The schematic diagram of Xu *et al.* image encryption-decryption algorithm based on drive-response configuration is depicted in Figure 1.

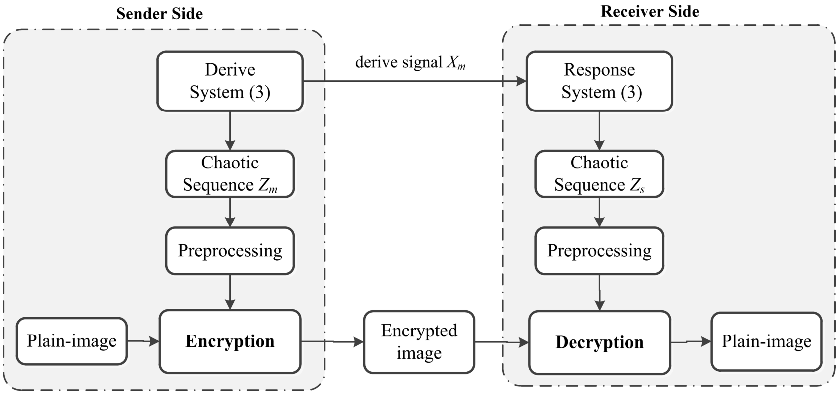


Fig. 1. Schematic diagram of Xu *et al.* image encryption-decryption algorithm

3 Cryptanalysis of Xu *et al.* Algorithm

In cryptography, there is an axiom stated by Auguste Kerckhoffs in 19-th century: "*A cryptographic system should be secure even if everything about the system, except the key, is public knowledge*" [17]. Kerckhoffs's axiom was reformulated by Claude Shannon as "*The enemy knows the system*" and acknowledged as Shannon's maxim [18]. Hence, everything about encryption algorithm including its implementation is public except the secret key which is private. In other words, the attacker has temporary access to encryption or decryption machines. Recovering the plain-image is as good as knowing the secret key.

The overall security of Xu *et al.* encryption algorithm relies on the secrecy of the initial conditions assigned to secret key components α_1, α_2, α_3, $x, y, z, a, b, c, l, h, k$. The design of their algorithm depicts that if, anyhow, attacker knows the generated decimal codes d_i, he/she can recover the plain-image from the received encrypted image. Thus, the generated decimal codes d_i are the equivalent keys of algorithm. So, instead of trying to know the actual initial conditions of key components, an attacker may design method to deduce the decimal codes. This can be achieved by exploiting the following inherent flaws of algorithm under probe.

- The decimal codes used to encrypt the plain-image always remain unchanged when different plain-images are encrypted. The generation of decimal codes is independent to the pending plain-image information.
- The algorithm has high key sensitivity which makes the brute-force attack infeasible. However, it has lack of, or practically no, plain-image sensitivity. Means, a minute change in the plain-image doesn't cause a drastic change in the encrypted content from security point of view.

The attacker utilizes above analytical information to execute attacks to reveal the plain-image. Assume that the attacker has gained temporary access to the encryption machine and encrypted image *C* which is to be decoded. Let *P* be the plain-image which is to be recovered from its received encrypted image *C*.

The chosen-plaintext (CPA) attack needs specially designed image to reveal decimal codes. A zero image *Q* (of size *C*) containing all pixels with zero gray values is designed for the purpose. The revelation of *P* from *C* under CPA attack is provided in algorithm **#2**. The method *y*=*Encrypt-Xu*(*x*) encrypts the input plain-image *x* according to Xu *et al.* algorithm and return corresponding encrypted image *y*.

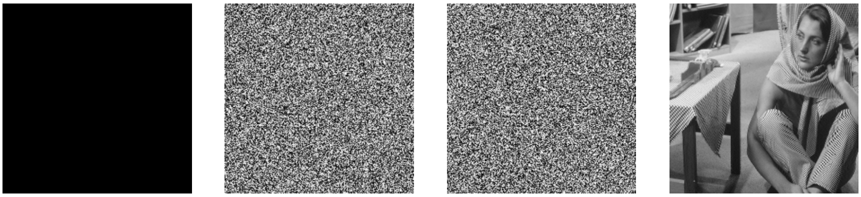
$$Q = \{q_{1,1}, q_{1,2}, \ldots\ldots, q_{1,N}, q_{2,1}, q_{2,2}, \ldots\ldots, q_{2,N}, \ldots\ldots, q_{M,N-1}, q_{M,N}\}$$

Where gray-value of pixel at (i, j) is $q_{i,j} = 0$ for all $i = 1 \sim \mathrm{M}$, $j = 1 \sim \mathrm{N}$.

Algorithm #2: *CPA-attack*( )

```
Input    :    Zero image $Q$ and received encrypted image $C$
Output   :    Recovered image $P$
begin
    $D = Encrypt\text{-}Xu(Q)$            // $Q \oplus D = 0 \oplus D = D$
    $P = Bitwise\text{-}ExOR(C, D)$       // $C \oplus D = (P \oplus D) \oplus D = P \oplus (D \oplus D) = P$
end
```

In order to illustrate the cryptanalysis under CPA attack, we give the simulation results in Figure 2.



(a) ***Q*** (b) ***D*** (c) Received **C** (d) Recovered ***P***

Fig. 2. Simulation of cryptanalysis under chosen-plaintext attack

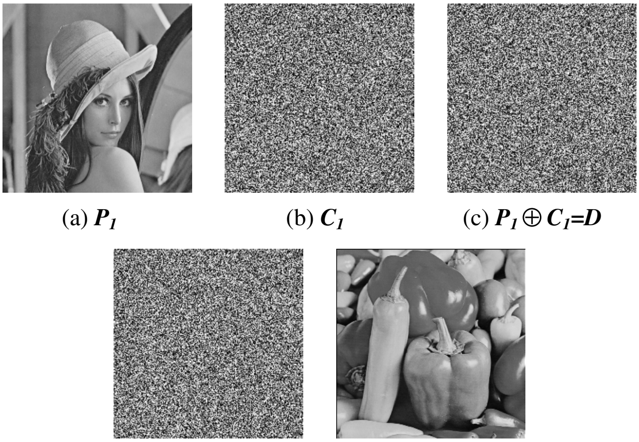
The known-plaintext (KPA) attack doesn't needs any specially designed image. Instead, it takes the access of pair of plaintext and ciphertext images and analyzes them to reveal the necessary information. Let the attacker has the access of plain-image P_1 and its encrypted image C_1. The successful revelation of P from C under KPA attack is provided in algorithm **#3**.

```
Algorithm #3: KPA-attack( )

Input     :   Pair of plain-image $P_1$ and its encrypted image $C_1$
Output    :   Recovered image $P$

begin
    $D = Bitwise\text{-}ExOR(P_1, C_1)$    // $P_1 \oplus C_1 = P_1 \oplus (P_1 \oplus D) = (P_1 \oplus P_1) \oplus D = D$
    $P = Bitwise\text{-}ExOR(D, C)$        // $D \oplus C = D \oplus (P \oplus D) = P \oplus (D \oplus D) = P$
end
```

The simulation results of cryptanalysis under KPA attack are provided in Figure 3.



(a) $\boldsymbol{P_1}$ (b) $\boldsymbol{C_1}$ (c) $\boldsymbol{P_1 \oplus C_1 = D}$

(d) Received $\boldsymbol{C}$ (e) Recovered $\boldsymbol{P}$

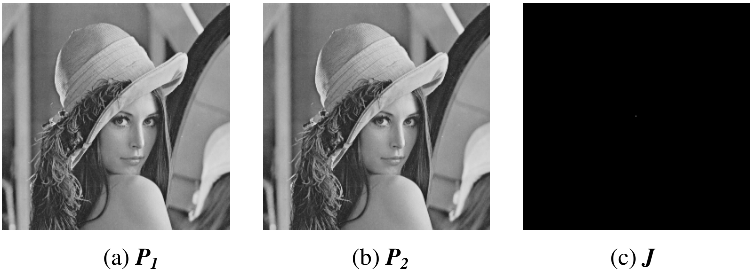
Fig. 3. Simulation of cryptanalysis under known-plaintext attack

The Shannon's properties of confusion and diffusion for a strong cryptosystem necessitate a high sensitiveness to a minute change in plain-image. A small change in plain-image should cause a drastic avalanche in the encrypted content. The Xu *et al.* algorithm has poor sensitiveness to a tiny change in plain-image. To illustrate the severity of the weakness, we take two almost similar plain-images P_1 and P_2 which have just one pixel difference and are encrypted with algorithm #1 to get C_1 and C_2 respectively. Since, the generation of decimal codes is independent to the plain-image information, the execution of algorithm #1, for P_1 and P_2, generates same decimal codes to output C_1 and C_2. As a result, the resultant encrypted images C_1 and C_2 are also identical to each other except for that one pixel difference. The difference image J of C_1 and C_2 is a black (zero) image. The poor plain-image sensitivity of Xu *et al.* algorithm is simulated in Figure 4.

Algorithm #4: *Plain-image_Sensitivity( )*

```
Input    :   Plain-images $P_1$ and $P_2$ having only one pixel difference
Output   :   Difference image $J$

begin
    $C_1 = Encrypt\text{-}Xu(P_1)$
    $C_2 = Encrypt\text{-}Xu(P_2)$
    $J = Bitwise\text{-}ExOR(C_1, C_2)$    // since $x \oplus x = 0$
end
```



(a) ***P₁***   (b) ***P₂***   (c) ***J***

Fig. 4. Simulation of poor plain-image sensitivity of Xu *et al.* algorithm

4 Conclusion

This paper presented a break of an image encryption algorithm suggested by Xu *et al.* very recently. Their algorithm exploited the features of fractional-order chaotic systems and based on the drive-response configuration. The drive system is synchronized with response system via Laplace transformation theory before the encryption/decryption process begins. The security probe of the algorithm unveils that the generation of decimal codes solely depends on secret key and independent to pending plain-image information. It yields same decimal codes sequence when different plain-images are encrypted. This flaw makes it susceptible to proposed attacks. It has been shown that plain-image can be recovered under chosen-plaintext/known-plaintext attacks without having any knowledge of secret key. It also highlighted the poor plain-image sensitivity of algorithm. Hence, the presented work demonstrated successful cryptanalysis and found that the Xu *et al.* encryption algorithm is not at all secure for practical utilization.

References

1. Hermassi, H., Rhouma, R., Belghith, S.: Security analysis of image cryptosystems only or partially based on a chaotic permutation. Journal of Systems and Software 85(9), 2133–2144 (2012)

2. Çokal, C., Solak, E.: Cryptanalysis of a chaos-based image encryption algorithm. Physics Letters A 373(15), 1357–1360 (2009)
3. Rhouma, R., Solak, E., Belghith, S.: Cryptanalysis of a new substitution-diffusion based image cipher. Communication in Nonlinear Science and Numerical Simulation 15(7), 1887–1892 (2010)
4. Li, C., Lo, K.T.: Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing 91(4), 949–954 (2011)
5. Rhouma, R., Belghith, S.: Cryptanalysis of a spatiotemporal chaotic cryptosystem. Chaos, Solitons & Fractals 41(4), 1718–1722 (2009)
6. Ahmad, M.: Cryptanalysis of chaos based secure satellite imagery cryptosystem. In: Aluru, S., Bandyopadhyay, S., Catalyurek, U.V., Dubhashi, D.P., Jones, P.H., Parashar, M., Schmidt, B. (eds.) IC3 2011. CCIS, vol. 168, pp. 81–91. Springer, Heidelberg (2011)
7. Rhouma, R., Belghith, S.: Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Physics Letters A 372(38), 5973–5978 (2008)
8. Özkaynak, F., Özer, A.B., Yavuz, S.: Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences. Optics Communications 285(2), 4946–4948 (2012)
9. Solak, E., Rhouma, R., Belghith, S.: Cryptanalysis of a multi-chaotic systems based image cryptosystem. Optics Communications 283(2), 232–236 (2010)
10. Sharma, P.K., Ahmad, M., Khan, P.M.: Cryptanalysis of image encryption algorithm based on pixel shuffling and chaotic S-box transformation. In: Mauri, J.L., Thampi, S.M., Rawat, D.B., Jin, D. (eds.) SSCC 2014. CCIS, vol. 467, pp. 173–181. Springer, Heidelberg (2014)
11. Schneier, B.: Applied Cryptography: Protocols Algorithms and Source Code in C. Wiley, New York (1996)
12. Bard, G.V.: Algebraic Cryptanalysis. Springer, Berlin (2009)
13. Military Cryptanalysis Part I- National Security Agency, `http://www.nsa.gov/public_info/_files/military_cryptanalysis/mil_crypt_I.pdf` (last access on August 30, 2014)
14. Xu, Y., Wang, H., Li, Y., Pei, B.: Image encryption based on synchronization of fractional chaotic systems. Communications in Nonlinear Science and Numerical Simulation 19(10), 3735–3744 (2014)
15. Li, R.H., Chen, W.S.: Complex dynamical behavior and chaos control in fractional-order Lorenz-like systems. Chinese Physics B 22(4), 040503 (2012)
16. Petráš, I.: Fractional-order nonlinear systems modeling, analysis and simulation. Springer, Heidelberg (2011)
17. Kerckhoffs's principle, `http://crypto-it.net/eng/theory/kerckhoffs.html` (last access on August 28, 2014)
18. Shannon, C.E.: Communication Theory of Secrecy Systems. Bell System Technical Journal 28, 662 (1949)