Cryptanalysis of Chaos Based Secure Satellite Imagery Cryptosystem

Musheer Ahmad

Department of Computer Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi 110025, India

Abstract. Recently Usama et al. proposed a chaos-based satellite image cryptosystem, which employed multiple one-dimensional chaotic maps in novel manner to enhance the robustness, security and efficiency of sensitive satellite imagery. It is very efficient in terms of encryption time. The authors of the cryptosystem under study claimed that it has high level of security and can be applied to transmit confidential multimedia images over Internet/shared network. Unfortunately, the security analysis of the cryptosystem reveals that it has serious security flaws. Consequently, it is susceptible to a number of attacks. In this paper, the cryptanalysis of original cryptosystem is presented and it is shown that the attacker can recovers the plain-image from given cipher-image under three types of classical cryptographic attacks without knowing the secret key. The simulation results of cryptanalysis demonstrate that the cryptosystem highly lacks security and cannot be utilized for the protection of confidential/sensitive multimedia images such as the satellite imagery.

Keywords: Satellite image cryptosystem, chaotic maps, security, cryptanalysis, cryptographic attacks.

1 Introduction

Nowadays, modern multimedia and telecommunications technologies make possible to share, exchange and transmit large amount of multimedia data more frequently. This brings challenges to build faster and stronger security solutions for confidential and sensitive multimedia data to be transmitted over the public wired or wireless networks. Inadequate security can leads to unauthorized access, usage or disruption of data. Traditional cryptographic algorithms such as DES, triple-DES, AES, are considered inefficient in providing ample security to multimedia data that has bulk data capacity and high redundancy [1]. The features of chaotic systems like high sensitivity to initial conditions/parameters, non-periodicity, high randomness, mixing property etc have been highly exploited for the design of efficient security methods that suit for multimedia data. An enormous numbers of chaos-based multimedia image and video encryption proposals have been suggested [2-19] since the arrival of first such proposal given by R. Mathews in 1989 [2]. For a thorough discussion of chaos-based image and video encryption techniques, readers are referred to some review and study [20-21]. The work of assessing the security of the proposed

S. Aluru et al. (Eds.): IC3 2011, CCIS 168, pp. 81–91, 2011.

multimedia encryption techniques is equally significant; it has been performed with the intent to arrive at more robust, reliable and efficient security solutions. As a consequence, the security analyses of proposed chaos-based multimedia encryption techniques have also been performed. It has been found that some of them suffer from various security weaknesses and are incompetent to withstand even the classical and other types of cryptographic attacks, as exposed by many cryptanalysts in the literature [22-27].

Recently, Usama *et al.* [16] proposed a new chaos-based satellite imagery cryptosystem. The cryptosystem is a block cipher which employed multiple one-dimensional chaotic maps e.g. Logistic map, Henon map, Tent map, Cubic map, Sine map and Chebyshev map for enhancing the key space, robustness and security of satellite imagery in novel manner. The experimental and security analyses illustrate that the cryptosystem has high robustness and security. The cryptosystem is very fast as it incurs a very low encryption time. Moreover, the distinctive feature of the algorithm is that it uses a variable length secret key and generates a number encryption keys out of it. In spite of this, the security analysis of the proposed satellite image cryptosystem exposes its serious security flaws from cryptographic viewpoint. Consequently, it is susceptible to the classical cryptographic attacks. In this paper, the satellite image cryptosystem described in [16] is successfully cryptanalyzed. It is shown that we can recover the original plain-image from given cipher-image using three types of attacks (chosen-plaintext, chosen-ciphertext and known-plaintext attacks) without knowing the secret key. Moreover, it is also shown that the cryptosystem is not at all sensitive to a small change in the plain-image, which is a very desirable feature of a good cryptosystem. The outline of the rest of paper is as follows: Section 2 briefly describes the satellite image cryptosystem under study. The cryptanalysis results with simulations are illustrated in Section 3 and finally the conclusions are drawn in the Section 4.

2 Brief Description of Cryptosystem under Study

This section concerns with the review and description of the cryptosystem recently proposed in [16]. The cryptosystem is a block cipher in which the efficiencies of six one-dimensional chaotic maps are exploited to improve the security of the cryptosystem by enhancing its confusion and diffusion properties. The 1D chaotic maps namely Chebyshev Map, Logistic Map, Cubic Map, Sine Map, Henon Map and Tent Map are employed in the system, the governing equations of chaotic maps are:

Chebyshev Map	:	$x_{n+1} = cos(\lambda cos^{-1}(x_n))$
Logistic Map	:	$x_{n+1} = \lambda x_n(1-x_n)$
Cubic Map	:	$x_{n+1} = \lambda x_n(1-x_{n*}x_n)$
Sine Map	:	$x_{n+1} = \lambda sin(\pi x_n)$
Henon Map	:	$x_n = 1+ \lambda(x_{n-2} - x_{n-3})+a x_{n-2*} x_{n-2}$
Tent Map	:	$x_{n+1} = x_n/\mu$ if $x_n \leq \mu$ else $(1-x_n)/(1-\mu)$

The Usama *et al*. cryptosystem takes an integer value n and a variable length secret key S of ρ (=128/256/512) bits as input. It evaluates the initial conditions of all the 1D chaotic maps using the secret key S. Reader may consult the Table 2 in [16] for the

initial values of system parameters taken. The chaotic maps generate conjointly n number of encryption keys $\boldsymbol{K_i}$ each of ρ bits. The plain-image P is broken into m number of blocks of size ρ. The blocks of satellite plain-image are encrypted sequentially using generated encryption keys K_i to produce blocks of cipher-image C.

Secret key : $S = S_1S_2S_3.....S_\rho$
Plain-image : $P = P_1P_2P_3.....P_m$
Cipher-image : $C = C_1C_2C_3.....C_m$

The size of block P_j/C_j (j = 1 to m) is equal to size of secret key S. The secret key S is converted into byte format as: $S = B_1B_2B_3.....B_\sigma$ (where $\sigma=\rho/8$) and the same initial condition IC of all one-dimensional chaotic maps is calculated from the secret key S through following equations:

$$N = \sum_{i=1}^{\sigma} (decimal(B_i)/256)$$

$$IC = N - floor(N)$$

Using the initial condition IC, the chaotic maps are iterated to produce n keys, each of ρ bits, the keys generated from each map can be expressed as.

Chebyshev map keys $\boldsymbol{BK}: BK_1, BK_2, BK_3, ...BK_n$
Logistic map keys $\boldsymbol{LK}: LK_1, LK_2, LK_3, ...L\,K_n$
Cubic map keys $\boldsymbol{CK}: CK_1, CK_2, CK_3, ...CK_n$
Sine map keys $\boldsymbol{SK}: VK_1, SK_2, SK_3, ...SK_n$
Henon map keys $\boldsymbol{HK}: HK_1, HK_2, HK_3, ...HK_n$
Tent map keys $\boldsymbol{TK}: TK_1, TK_2, TK_3, ...TK_n$

The cryptosystem creates n keys from each chaotic map using single secret key S. The above set of keys are then combined through XOR operation to generate the n distinct encryption keys $\boldsymbol{K_i}$, where i = 1, 2, 3, …. n.

$$\boldsymbol{K_i} = BK_i \oplus LK_i \oplus CK_i \oplus SK_i \oplus HK_i \oplus TK_i \qquad \text{where } i = 1 \text{ to } n$$

The block diagram of key generation procedure is shown in Figure 1. These keys are actually used to encrypt the blocks of plain-image using the XOR operation to get the blocks of cipher-image. The block diagram of encryption mechanism involved in the cryptosystem is shown in Figure 2. The decryption process is similar to the encryption process i.e. the encrypted image is decoded by simply XORing the blocks of cipher-image with keys generated through key generation process depicted in Figure 1 to obtained the whole decrypted image.

In Usama *et al.* cryptosystem, the way in which the features of multiple 1D chaotic maps are utilized for the sake of improved security of the cryptosystem is appreciable. Accordingly, the results of statistical analyses such as maximum deviation, information entropy, key space analysis, key sensitivity analysis and encryption time

analysis given in section 4 of [16] reveal the virtuous and excellent performance of the cryptosystem. However, there still exist some weaknesses that may be exploited by the attacker to break the system.

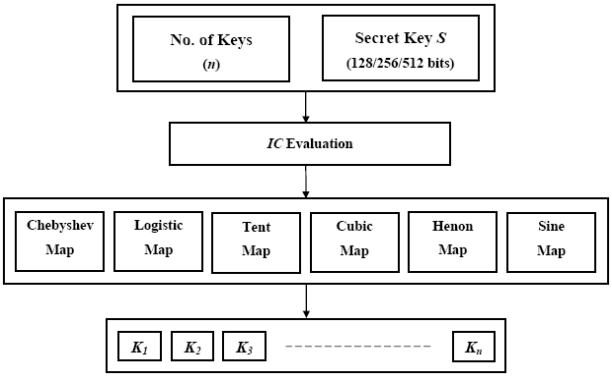


Fig. 1. Key generation process in encryption/decryption

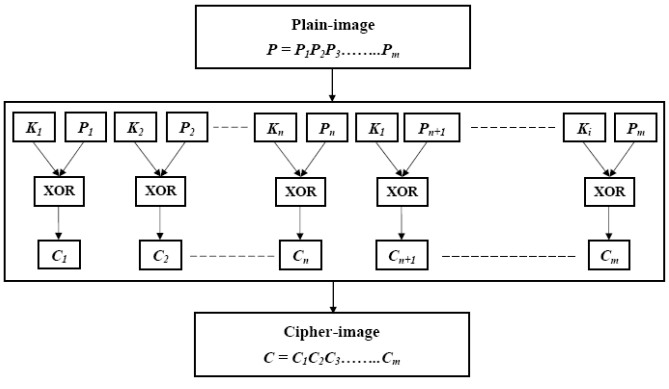


Fig. 2. Block diagram of Encryption mechanism

3 Cryptanalysis of Usama *et al.* Cryptosystem

In this section, the method of breaking the cryptosystem under study is reported. A cryptosystem is supposed to be secure if it resists all known types of cryptographic attacks. An attempted cryptanalysis is called an attack. In cryptanalysis, the fundamental assumption enunciated by Kerchoff is that the attacker knows the complete details of cryptographic algorithm and its implementation. This is known as Kerchoff's principle [1]. In other words, the attacker has the temporary access to the encryption and decryption machine. The goal of the attacker is to recover the plaintext without having any knowledge of secret key used. This is because recovering the

plaintext is as good as deducing the secret key. Now, there are four types of classical cryptographic attacks. A brief description of each attack is given below:

1. ***Chosen-Plaintext attack***: In this case, the attacker has the temporary access to encryption machine; he cleverly selects one or more plaintext(s) and gets the corresponding ciphertext(s), which in turn allows the attacker to decode the received encrypted plaintext. This attack is one of the potential classical attacks.

2. ***Chosen-Ciphertext attack***: In this case, the attacker has the temporary access to decryption machine; he selects special ciphertext(s) and gets the associated plaintext(s), which helps in decoding the received encrypted plaintext.

3. ***Known-Plaintext attack***: In this case the attacker has the access not only to ciphertext(s) but also to the plaintext(s) of those ciphertext(s). This facilitates the attacker to deduce the key using these pair(s).

4. ***Ciphertext-only attack***: This is hardest type of attack, as the attacker posses only the ciphertexts of several plaintexts, all of which are encrypted using same encryption algorithm. The attacker tries to analyze them in order to deduce the key.

Any cryptographic algorithm which cannot resist any of the attack is said to be insecure. Therefore, the best cryptographic algorithms are the ones that have been made public, have been attacked by the world's best cryptanalysts for years, and are still unbreakable [1]. The serious weakness of the cryptosystem under study lies in the key generation process, which is same for every plain-image/cipher-image i.e. it is neither depend on the plain-image nor does it depend on the cipher-image, hence it remain unchangeable in every encryption/decryption process. This makes the classical attacks applicable to the cryptosystem. The details of cryptanalysis along with simulation under three different attacks are described in the following subsections.

3.1 Chosen-Plaintext Attack

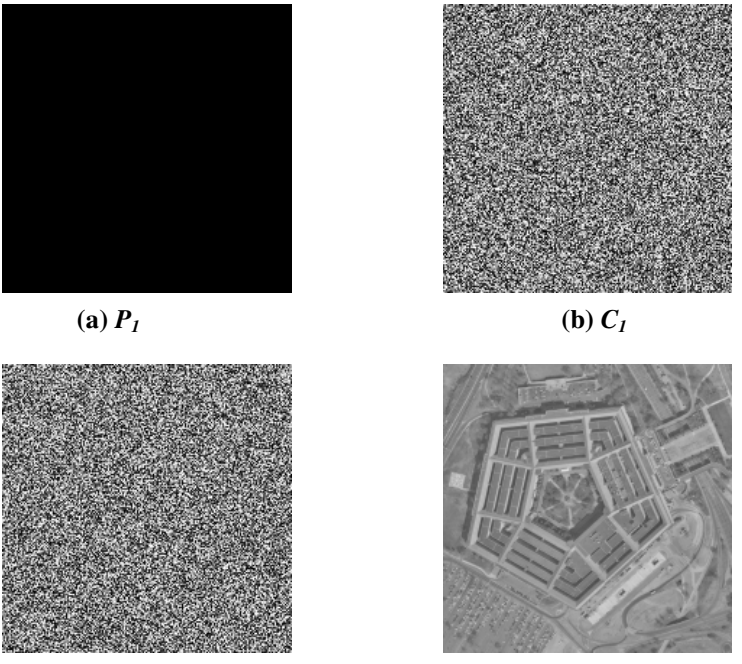
Assume that we have temporary access to the encryption machine and ciphertext C_2 which is to be decoded. Let us select a plain-image that consists of all zero-valued pixels i.e. P_1=*000……0*. The cipher-image C_1 corresponding to the plain-image P_1 is obtained using the encryption machine.

$$C_1 = P_1 \oplus K = (000\ldots\ldots0) \oplus K = K$$

It can be easily understood that the cipher-image C_1 is nothing but the key K which was generated to encrypt the plain-image P_1 during the encryption process. As the key generation process is independent to the plain-image to be encrypted. This means that the same key K is used every time to encrypt any plain-image. Thus, the plain-image P_2 can be recovered from the received cipher-image C_2 as:

$$C_2 \oplus C_1 = C_2 \oplus K = P_2$$

The simulation of the chosen-plaintext attack is shown in Figure 3.



(a) P_1 **(b)** C_1

(c) C_2 **(d)** P_2

Fig. 3. Simulation of chosen-plaintext attack: (a) Selected plain-image P_1=*00.....0*, (b) Cipher-image C_1 of P_1 which is equal to the key (c) Received cipher-image C_2 to be decoded and (d) Recovered image $P_2 = C_2 \oplus C_1$

3.2 Chosen-Ciphertext Attack

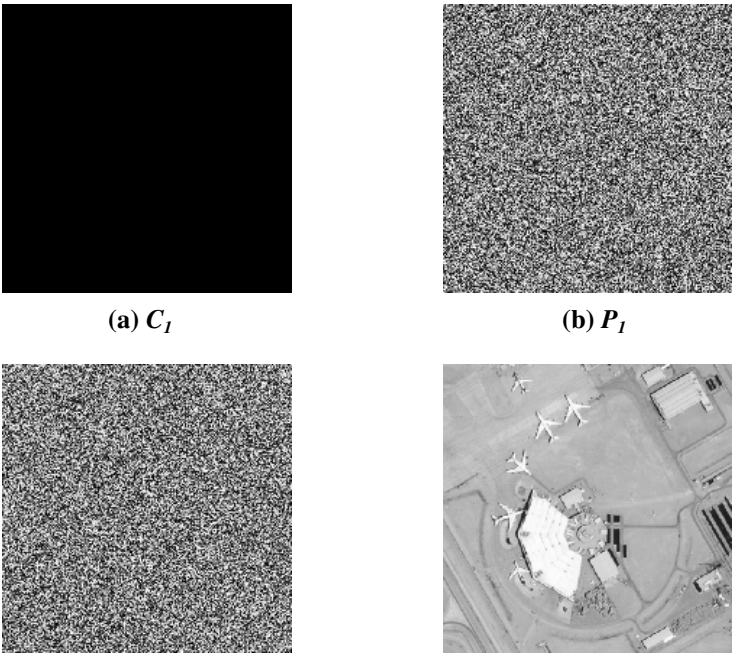
The approach of this attack is somewhat similar to the previous one. Assume that we have temporary access to the decryption machine and ciphertext C_2 which is to be decoded. We select a special cipher-image that consists of all zero-valued pixels i.e. C_1 = *000.....0*. The plain-image P_1 associated to the cipher-image C_1 is obtained using the decryption machine.

$$P_1 = C_1 \oplus K = (000.....0) \oplus K = K$$

We get the secret key K as the plain-image P_1 for the chosen cipher-image. Thus, the plain-image P_2 can be recovered from the received cipher-image C_2 as:

$$C_2 \oplus P_1 = C_2 \oplus K = P_2$$

The simulation of the chosen-ciphertext attack is shown in Figure 4.



(a) C_1 **(b)** P_1

(c) C_2 **(d)** P_2

Fig. 4. Simulation of chosen-ciphertext attack: (a) Selected cipher-image C_1=*00.....0*, (b) Plain-image P_1 of C_1 which is equal to the key (c) Received cipher-image C_2 to be decoded and (d) Recovered image $P_2 = C_2 \oplus P_1$

3.3 Known-Plaintext Attack

In this attack, we do not choose any special plain-image or cipher-image. Instead, we have access to a pair consists of plain-image P_1 and its associated cipher-image C_1, where

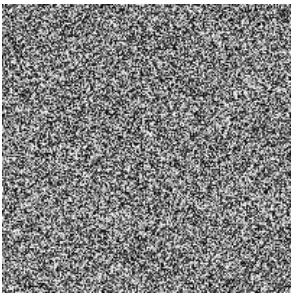
$$C_1 = P_1 \oplus K$$

Let we have to decode the received cipher-image C_2. Consider an intermediate image D which is XOR of images P_1 and C_1 i.e. $D = C_1 \oplus P_1$, the plain-image P_2 can be recovered from the received cipher-image C_2 under *KPA* attack as:

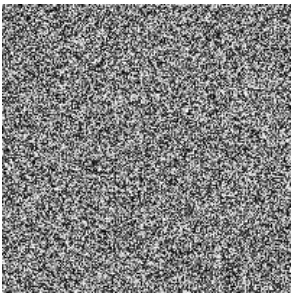
$$\begin{aligned} C_2 \oplus D &= C_2 \oplus \{C_1 \oplus P_1\} \\ &= C_2 \oplus \{(P_1 \oplus K) \oplus P_1\} \\ &= C_2 \oplus K \oplus \{P_1 \oplus P_1\} \\ &= C_2 \oplus K = P_2 \end{aligned}$$

The simulation of the chosen-ciphertext attack is shown in Figure 5.

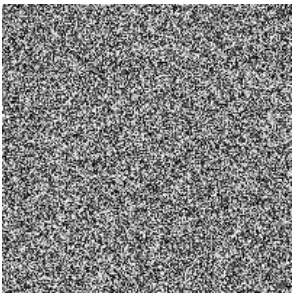
(a) P_1



(b) C_1



(c) D



(d) C_2

(e) P_2

Fig. 5. Simulation of known-plaintext attack: (a) Plain-image P_1 (b) Cipher-image C_1 of P_1 (c) Intermediate-image $D=C_1 \oplus P_1$ (d) Received cipher-image C_2 and (e) Recovered image $P_2=C_2 \oplus D$

3.4 Sensitivity to Plain-Image

To fulfill the Shannon's requirements of confusion and diffusion properties in a cryptographic system for secure encryption, the cryptosystem should be very sensitive to a tiny change in the plain-image. Unfortunately, the cryptosystem under study is not at all sensitive to a small change in the plain-image. To understand the severity of the problem clearly, let us consider two plain-images I_1 and I_2 with only one pixel value difference at central position i.e. the pixel-values of image I_1 are identical to the

pixels-values of image I_2 except the pixel-value positioned at centre. Since, the pixels of the two images are identical except the central one, the cipher-images J_1 and J_2 obtained after encrypting them using the cryptosystem under study will also be identical to each other. This is because the cryptosystem is not made sensitive to a change in plain-images. This weakness of poor sensitivity to plain-image is illustrated through a simulation example shown in Figure 6. It can be easily seen in the Figure 6 that the differential cipher-image is zero for all pixels except the central one.

(a) **(b)** **(c)**

Fig. 6. Sensitivity to Plain-image: (a) Plain-image I_1 (b) Plain-image I_2 and (c) Differential cipher-image $J_1 \oplus J_2$

4 Conclusion

In this paper, the security of chaos-based satellite imagery cryptosystem recently proposed by Usama *et al.* has been thoroughly analyzed. The cryptosystem has some good cryptographic properties. However, it has been found that the cryptosystem is susceptible to classical attacks like chosen-plaintext attack, chosen-ciphertext attack and known-plaintext attack. It has been shown that the plain-image can be recovered without knowing the secret key under the above attacks and only a pair of plain-image/cipher-image is needed to completely break the cryptosystem. Moreover, the cryptosystem has poor sensitivity to small change in the plain-image. The serious weakness of the cryptosystem lies in the key generation process, which is independent to the plain-image/cipher-image. One of the solutions to make the above attacks impractical is that design such cryptosystem in Cipher Block Chaining (CBC) mode of block encryption. Hence, the complete cryptanalysis of the cryptosystem is presented along with simulation. The work demonstrates that the Usama *et al.* cryptosystem highly lacks security and cannot be utilized for the protection of sensitive multimedia images such as satellite imagery.

References

1. Schneier, B.: Applied Cryptography: Protocols Algorithms and Source Code in C. Wiley, New York (1996)
2. Matthews, R.: On the Derivation of a Chaotic Encryption Algorithm. Cryptologia 13(1), 29–42 (1989)

3. Fridrich, J.: Symmetric Ciphers based on two-dimensional Chaotic Maps. International Journal of Bifurcation and Chaos 8(6), 1259–1284 (1998)
4. Chen, G.Y., Mao, Y.B., Chui, C.K.: A Symmetric Image Encryption Scheme based on 3D Chaotic Cat maps. Chaos, Solitons & Fractals 21(3), 749–761 (2004)
5. Mao, Y., Lian, S., Chen, G.: A Novel Fast Image Encryption Scheme based on 3D Chaotic Baker maps. International Journal of Bifurcation and Chaos 14(10), 3616–3624 (2004)
6. Lian, S., Sun, J., Wang, Z.: A Block Cipher based on a Suitable use of Chaotic Standard map. Chaos, Solitons and Fractals 26(1), 117–129 (2005)
7. Lian, S., Sun, J., Wang, J., Wang, Z.: A Chaotic Stream Cipher and the Usage in Video Protection. Chaos, Solitons & Fractals 34(3), 851–859 (2007)
8. Tong, X., Cui, M.: Image Encryption Scheme based on 3D Baker with Dynamical Compound Chaotic Sequence Cipher Generator. Signal Processing 89(4), 480–491 (2008)
9. Patidar, V., Pareek, N.K., Sud, K.K.: A New Substitution-Diffusion based Image Cipher using Chaotic Standard and Logistic Maps. Communication in Nonlinear Science and Numerical Simulation 14(7), 3056–3075 (2009)
10. Tang, Y., Wang, Z., Fang, J.: Image Encryption using Chaotic Coupled Map Lattices with Time Varying Delays. Communication in Nonlinear Science and Numerical Simulation 15(9), 2456–2468 (2009)
11. Lian, S.: Efficient Image or Video Encryption based on Spatiotemporal Chaos System. Chaos, Solitons & Fractals 40(5), 2509–2519 (2009)
12. Wang, Y., Wong, K., Liao, X., Xiang, T., Chen, G.: A Chaos-based Image Encryption Algorithm with Variable Control Parameters. Chaos, Solitons & Fractals 41(4), 1773–1783 (2009)
13. Wang, Y., Wong, K., Liao, X.: A Block Cipher with Dynamic S-boxes based on Tent Map. Communication in Nonlinear Science and Numerical Simulation 14(7), 3089–3099 (2009)
14. Lian, S.: A Block Cipher based on Chaotic Neural Networks. Neurocomputing 72(4-6), 1296–1301 (2009)
15. Corron, N.J., Reed, B.R., Blakely, J.N., Myneni, K., Pethel, S.D.: Chaotic Scrambling for Wireless Analog Video. Communication in Nonlinear Science and Numerical Simulation 15(9), 2504–2513 (2010)
16. Usama, M., Khan, M.K., Alghathbar, K., Lee, C.: Chaos-based Secure Satellite Imagery Cryptosystem. Computers and Mathematics with Applications 60(2), 326–337 (2010)
17. Amin, M., Faragallah, O.S., Abd El-Latif, A.A.: A Chaotic Block Cipher Algorithm for Image Cryptosystem. Communication in Nonlinear Science and Numerical Simulation 15(11), 3484–3497 (2010)
18. Ahmad, M., Farooq, O.: A multi-level blocks scrambling based chaotic image cipher. In: Ranka, S., Banerjee, A., Biswas, K.K., Dua, S., Mishra, P., Moona, R., Poon, S.-H., Wang, C.-L. (eds.) IC3 2010. Communications in Computer and Information Science, vol. 94, pp. 171–182. Springer, Heidelberg (2010)
19. Chen, Z., Ip, W.H., Cha, C.Y., Yung, K.: Two-level Chaos based Video Cryptosystem on H.263 Codec. Nonlinear Dynamics 62(3), 647–664 (2010)
20. Furht, B., Kirovski, D.: Multimedia Security Handbook. CRC Press, Boca Raton (2005)
21. Lian, S.: Multimedia Content Encryption: Techniques and Applications. CRC Press, Boca Raton (2008)
22. Wang, K., Pei, W., Zou, L.: On the Security of 3D Cat Map based Symmetric Image Encryption Scheme. Physics Letters A 343(6), 432–439 (2005)
23. Alvarez, G., Li, S.: Breaking an Encryption Scheme based on Chaotic Baker Map. Physics Letters A 352(1-2), 78–82 (2005)

24. 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)
25. Rhouma, R., Belghith, S.: Cryptanalysis of a Spatiotemporal Chaotic Image/Video Cryptosystem. Physics Letters A 372(36), 5790–5794 (2008)
26. Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G.: On the Security Defects of an Image Encryption Scheme. Image and Vision Computing 27, 1371–1381 (2009)
27. Rhouma, R., Belghith, S.: Cryptanalysis of a Chaos-based Cryptosystem on DSP. Communication in Nonlinear Science and Numerical Simulation 16(2), 876–884 (2011)