Nonlinear Dyn (2015) 82:1831–1837
DOI 10.1007/s11071-015-2280-1

ORIGINAL PAPER

Deciphering an image cipher based on 3-cell chaotic map and biological operations

Yushu Zhang · Yantao Li · Wenying Wen · Yongfei Wu · Jun-xin Chen

Received: 21 March 2015 / Accepted: 14 July 2015 / Published online: 30 July 2015

Abstract In recent years, it is popular that the combination of chaos and DNA is employed for image ciphers. There have been a great number of image ciphers which are designed based on chaos and DNA, but the corresponding cryptanalytic works are insufficient and in-depth study should be made. In this paper, we decipher an image cipher combining a 3-cell chaotic map with DNA. It was claimed that this cipher has high security and can resist different well-known attacks. However, we demonstrate that the claim is not reasonable, since the cipher can be broken by chosen plaintext attack with the complexity $O(\alpha\beta)$, where α and β represent the number of the image rows and columns, respectively.

Y. Zhang
School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China

Y. Li (✉)
College of Computer and Information Sciences, Southwest University, Chongqing 400715, China
e-mail: yantaoli@foxmail.com; yantaoli@swu.edu.cn

W. Wen
School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330013, China

Y. Wu
College of Mathematics and Statistics, Chongqing University, Chongqing 401331, China

J. Chen
School of Information Science and Engineering, Northeastern University, Shenyang 110004, China

Keywords Image cipher · DNA · Chaos · Chosen plaintext attack

1 Introduction

Nowadays the usages of image data have become more and more widespread over various networks, thus the corresponding security has been receiving increasing attention. Chaos is one of the most common tools to protect image data since it has the sensitivity to initial condition and control parameter, which is similar to the basic properties of cryptography, confusion and diffusion. Meanwhile, the cryptanalysis of chaos-based image cipher is a vital work for its development. Alvarez and Li presented a general framework of basic guidelines involved with three main issues including implementation, key management and security analysis that a cryptosystem should follow [1]. In [2], chosen plaintext attack and chosen ciphertext attack were separately employed to break an image encryption algorithm based on hyper-chaos without any knowledge of the key value and with only three couples of plaintext/ciphertext. Rhouma and Belghith cryptanalyzed a chaos-based cipher for images and videos with two different attacks due to the weakness in the generation of the keystream [3]. The knowledge and significance of the cryptanalysis of chaotic ciphers have been discussed in [4,5] in detail. Çokal and Solak applied chosen plaintext and known plaintext attacks to reveal the secret parameters of a chaos-based image encryption

algorithm [6]. Two image encryption schemes consisting of a permutation operation and an XOR-like transformation of the shuffled pixels were cracked in [7] by use of a chosen plaintext attack. A differential cryptanalysis was leveraged by Li et al. [8] to aim at the Yen–Chen–Wu multimedia cryptography system with only seven chosen plaintexts. The image encryption cryptosystems based on multi-chaotic systems and improved hyper-chaotic sequences were also analyzed in terms of security in [9,10], respectively. In addition, Bigdeli algorithm was broken by using Çokal and Solak attack in [11]. In recent years, it is very interesting to combine the biological characteristics like DNA with chaos system for image ciphers. So far, a large number of image ciphers based on DNA and chaos have been designed [12–25]. Their basic idea is to encode the original image into DNA sequence according to some mapping rule. The obtained DNA sequence is then processed in the some way with the help of the secret DNA keystream which is typically controlled by chaos. The processed DNA sequence is finally decoded into the cipher image. In addition, some chaos-based cryptographic features can also be embedded to enhance the security. On the other hand, a small number of cryptanalytic works for a few of these image ciphers have been done [26–32], which stimulates the further development of the image ciphers based on DNA and chaos. In spite of this, such cryptanalytic works are insufficient and in-depth study should be made.

In [33], the combination of a 3-cell chaotic map and DNA is employed for designing image cipher. Specifically, the original image is firstly converted to a DNA sequence. Then, the obtained DNA sequence is scrambled under the control of cycling chaos. After that, a secret DNA sequence is generated by using cycling chaos to mask the scrambled DNA sequence. The results are decoded to form the final cipher image. It was claimed that this cipher has high security and can resist different well-known attacks. In this paper, we demonstrate that the claim is not reasonable, since the cipher can be broken by known attacks. The rest of the paper is organized as follows. The next section overviews the original image cipher based on 3-cell chaotic map and biological operations. Section 3 gives the corresponding cryptanalysis for the original image cipher followed by some discussions in Sect. 4. The last section concludes this paper.

2 Overview of the image cipher based on 3-cell chaotic map and biological operations

This section firstly re-introduces the preparatory work for the cipher design and then re-describes the original image cipher.

2.1 The preparatory work

The 3-cell cyclic chaos map used in the image cipher is defined as

$$\begin{cases} x_{n+1} = \delta_1 x_n - x_n^3 - \chi\,|y_n|^p\, x_n \\ y_{n+1} = \delta_2 y_n - y_n^3 - \chi\,|z_n|^p\, y_n \\ z_{n+1} = \delta_3 z_n - z_n^3 - \chi\,|x_n|^p\, z_n \end{cases}. \tag{1}$$

A 120-bit external key $k = k_{120}, k_{119}, k_{118}, \ldots, k_1$ is applied for providing the three initial values x_1, y_1, z_1 and the parameter p by the following formulas:

$$\begin{cases} x_1 = \left(\frac{\text{sum of } K_1 \text{ bits}}{35} \times 4\right) - 2, -2 < x_1 < 2, \\ \quad K_1 = k_{120}, k_{119}, k_{118}, \ldots, k_{86} \\ y_1 = \left(\frac{\text{Decimal value of } K_2}{2^{35}} \times 4\right) - 2, -2 < y_1 < 2, \\ \quad K_2 = k_{85}, k_{84}, k_{83}, \ldots, k_{51} \\ z_1 = \left(\frac{\text{sum of } K_3 \text{ bits}}{35} \times 4\right) - 2, -2 < z_1 < 2, \\ \quad K_3 = k_{50}, k_{49}, k_{48}, \ldots, k_{16} \\ p = \left(\frac{\text{Decimal value of } K_4}{2^{15}} \Big/ 5\right) - 0.1, 0.1 < p < 0.3, \\ \quad K_4 = k_{15}, k_{14}, k_{13}, \ldots, k_1 \end{cases}. \tag{2}$$

Each 8-bit pixel can be comprised of four 2-bits, i.e., 00, 01, 10 and 11, which can correspond to four nucleic acid bases T (thymine), A (adenine), C (cytosine), G (guanine), where A and T are complementary, while G and C are complementary, according to Watson–Crick complement rule, as shown in Table 1. The DNA algebraic operations including addition and subtraction are shown in Tables 2 and 3, respectively.

2.2 The encryption algorithm

The original image is firstly converted to a DNA sequence. Then, the obtained DNA sequence is scrambled under the control of cycling chaos. After that, a secret DNA sequence is generated by using cycling chaos to mask the scrambled DNA sequence. The

Table 1 Watson–Crick complement rule

Rules	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

Table 2 DNA addition operation

+	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	C	C
T	T	A	A	G

Table 3 DNA subtraction operation

−	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

results are decoded to form the final cipher image. The specific procedures are as follows:

Step 1: The DNA encoding phase
Encode each pixel of the original image into a DNA image according to the rule: "00"-A, "01"-C, "10"-G, and "11"-T.

Step 2: The scrambling phase

a. Let the number of the image rows and columns be α and β, respectively, and divide the DNA image into N equal blocks.
b. Generate the chaotic sequences $X = x_0, x_1, x_2, \ldots, x_\alpha$, $Y = y_0, y_1, y_2, \ldots, y_{4\beta}$, and $Z = z_0, z_1, z_2, \ldots, z_N$ with the initial values x_1, y_1, z_1 and the parameter p;
c. Normalize the values in the sequence Z to the integers between 1 to N;
d. Rearrange these integers into a new matrix Z';
e. Scramble the blocks using Z';
f. Normalize the values in X and Y to the integers between 1 to α and between 1 to β, respectively, rearrange these integers into row matrix and column matrix X' and Y';
g: Scramble the nucleic acid base values using the ordered pair $(x', y') \in (X', Y')$.

Step 3: The mask phase

a. Generate the chaotic sequence $X = x_0, x_1, x_2, \ldots, x_{4\alpha\beta}$ with the initial values x_1, y_1, z_1 and the parameter p;
b. Construct the mask image M in which each pixel value can be generated using the following formula:

$$\begin{cases} A, -2 < X \le 1.1 \\ C, -1.1 < X \le -0.2 \\ G, 0.2 \le X < 1.1 \\ T, 1.1 \le X < 2 \end{cases} \tag{3}$$

c. Perform the DNA addition of the scrambled DNA image and the mask image.

Step 4: The decoding phase

Decode the result into the final cipher image according to the same encoding rule: "00"-A, "01"-C, "10"-G, and "11"-T.

3 The deciphering process

After carefully observing the encryption algorithm, it seems that the security of the algorithm depends mainly on the 120-bit external key, which manipulates the generation of the three initial values x_1, y_1, z_1 and the parameter p for 3-cell cycling chaos map. However, with respect to different images, the same external key is utilized, thus keeping the same x_1, y_1, z_1 and p. Furthermore, the chaotic sequences remain unchanged, therefore X', Y', Z' and M are fixed. The encryption algorithm possesses the architecture of scrambling mask. The encoding and decoding phases do not involve cryptographic behaviors. The scrambling phase contains two operations. One is to scramble the blocks using Z' and the other is to process the whole bases using X' and Y'. The mask phase only leverages the mask image M. The goal of deciphering the image encryption algorithm is to reveal X', Y', Z' and M. In order to be understood for the proposed cryptanalysis, the encryption algorithm was simplified as:

Step 1: The DNA encoding phase

$$P\,(00, 01, 10, 11) \xrightarrow[\text{00-A,01-C,10-G,11-T}]{\text{Encode}} \times P'\,(A, C, G, T) \tag{4}$$

Step 2: The scrambling phase

$$P'\,(A, C, G, T) \xrightarrow[Z']{\text{1st Scramble}} P'_{S^1}\,(A, C, G, T) \tag{5}$$

$$P'_{S^1}\,(A, C, G, T) \xrightarrow[X', Y']{\text{2st Scramble}} \times P'_{S^2}\,(A, C, G, T) \tag{6}$$

Step 3: The mask phase

$$P'_{S^2}\,(A, C, G, T) \xrightarrow[M]{\text{Mask}} P'_{M,S^2}\,(A, C, G, T) \tag{7}$$

Step 4: The decoding phase

$$P'_{M,S^2}\,(A, C, G, T) \xrightarrow[\text{A-00,C-01,G-10,}T\text{-11}]{\text{Decode}} \times C\,(A, C, G, T) \tag{8}$$

Our attack adopts chosen plaintext attack. The basic idea is to select one or more special images, which are not or regularly affected by the scrambling phase. So the attacker can infer the mask image M at first with the knowledge of one or more pairs of plain/cipher images. The specific procedures are the followings:

(1) Select a special plain image, where each 8-bit pixel consists of the same four 2-bits, i.e.,

$$P\,(00, 00, 00, 00)\,, \quad P\,(01, 01, 01, 01)\,,$$
$$P\,(10, 10, 10, 10) \quad \text{and} \quad P\,(11, 11, 11, 11)\,,$$

corresponding to $P'\,(A, A, A, A)$, $P'\,(C, C, C, C)$, $P'\,(G, G, G, G)$ and $P'\,(T, T, T, T)$. Without loss of generality, $P\,(00, 00, 00, 00)$ is selected.

(2) The two scrambling operations do not work for $P'\,(A, A, A, A)$, thus

$$\begin{aligned} P'\,(A, A, A, A) &= P'_{S^1}\,(A, A, A, A) \\ &= P'_{S^2}\,(A, A, A, A) \end{aligned} \tag{9}$$

(3) The mask phase is changed as

$$P'\,(A, A, A, A) \xrightarrow[M]{\text{Mask}} P'_M\,(A, C, G, T) \tag{10}$$

The decoding phase is

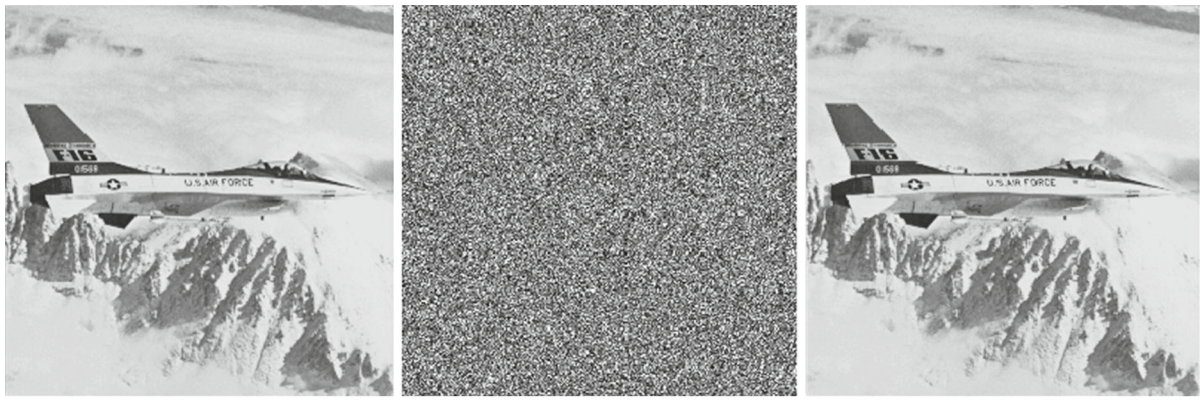
$$P'_M\,(A, C, G, T) \xrightarrow[\text{A-00,C-01,G-10,}T\text{-11}]{\text{Decode}} C^1\,(A, C, G, T) \tag{11}$$

(4) $P\,(00, 00, 00, 00)$ and $C^1\,(A, C, G, T)$ are known, so $P'\,(A, A, A, A)$ $P'_M\,(A, C, G, T)$ are also known. With the addition and subtraction operation rules in Tables 2 and 3 together with Eq. (10), the mask image M can be immediately calculated.

(5) After revealing M, the resultant encryption algorithm turns into a scrambling-only framework. The effect of the second scrambling is obviously stronger than that of the first one. The first scrambling can be integrated into the second one. The two scrambling operations can be equivalent to only once nucleic acid base value scrambling. The equivalent matrices for $\left(X', Y'\right)$ and Z' which need to be revealed are marked as $\left(X'', Y''\right)$.

(6) Alter three 2-bits of four 2-bits as 01, 10, and 11 for the first pixel in $P\,(00, 00, 00, 00)$. After the scrambling, the positions of these three altered values can be found such that three ordered pairs in (X'', Y'') are obtained. Next, the same processing way for the following pixels is repeatedly performed till the whole ordered pairs in (X'', Y'') are revealed.

The above steps demonstrate that the encryption algorithm can be broken by using chosen plaintext attack. The mask phase requires an image, while the scrambling phase requires about $4\alpha\beta/3$ images. Thus, the complexities in the mask and scrambling phases are $O(1)$ and $O(4\alpha\beta/3)$, respectively. The whole complexity is confined to $O(\alpha\beta)$, which is low. If there needs to be a blurry or rough image through the cryptanalysis, the number of the images when deciphering the scrambling phase can be further optimized by the methods [34,35], in which the scrambling-only image ciphers have been thoroughly and systematically cryptanalyzed. Figure 1 shows a validation example, in which a–c represents the original test image, the corresponding encrypted image and the cryptanalyzed image, respectively. It is worth mentioning in the end that the algebraic attack against the image encryption algorithm consisting of chaos and DNA is an efficient tool of the cryptanalysis. For example, in [27], Belazi et al. came up with an algebraic analysis against a RGB image encryption algorithm based on DNA encoding and chaotic map by constructing some systems of linear equations. However, in [33], the introduction of permu-



(a) (b) (c)

Fig. 1 Test of the attack. **a** The original test image; **b** the corresponding encrypted image; **c** the cryptanalyzed image

Table 4 One possible DNA XOR operation

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

tation which has the linearity impedes the construction of linear equations. Thus, the algebraic attack does not take effect on the cipher in [33].

4 Discussion

In the following, some improvements and suggestions with respect to the encryption algorithm are given:

1. There are eight kinds of coding schemes in total that satisfy the Watson–Crick complement rule. In the encryption algorithm, the coding rule is fixed and no cryptographic features are embedded in the encoding phase. Therefore, a new key can be added to control the encoding and decoding rules.
2. For the DNA algebraic operations, another DNA XOR operation can also be introduced to change the base values in the mask phase. For example, one possible definite for DNA operation is shown in Table 4. The DNA XOR operation corresponds to the binary XOR operation, which has been widely used in the field of cryptography.
3. The leading reason why the encryption algorithm is vulnerable to chosen plaintext attack is not related to plaintext information. The algorithm should depend on the plain image information during the encoding, scrambling and mask phases. As a result, different plain images can generate inconsistent keystreams.
4. In the scrambling and mask phases, the same initial values and parameter should not be utilized. Once one part of keystream is revealed by the attacker, the other part may also be known at once. The keystream used in mask phase can be perturbed by the encryption result in the scrambling phase to avoid the same keys and enhance the security
5. The A, C, G and T in the mask image are not uniform in terms of the distribution situation due to the fact that in general, the track of chaos system is not uniform. Thus, the encryption algorithm easily suffers from statistical attack. Some excellent DNA cipher techniques like [15] are worth referencing for better image cipher based on DNA and chaos.

5 Conclusion

An encryption algorithm based on a 3-cell chaotic map and DNA, including the encoding, scrambling, mask and decoding phases, has been analyzed in terms of security in this paper. The algorithm can be broken by chosen plaintext attack with a low complexity $O(\alpha\beta)$. At the same time, some improvements and suggestions have also been proposed for the purpose of designing better image ciphers based on DNA and chaos and stimulating the further development.

Acknowledgments The work was supported by the Fundamental Research Funds for the Central Universities (Grant Nos. SWU115016, XDJK2015C077, XDJK2015B030), the National Natural Science Foundation of China (Grant Nos. 61462032, 61402380, 61403313, 61374078), the Natural Science Foundation of Jiangxi Province (Grant No. 20142BAB217012), and the Natural Science Foundation Project of Chongqing CSTC (Grant No. cstc2014jcyjA40014).

References

1. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos **16**(8), 2129–2153 (2006)
2. Rhouma, R., Belghith, S.: Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Phys. Lett. A **372**, 5973–5978 (2008)
3. Rhouma, R., Belghith, S.: Cryptanalysis of a spatio-temporal chaotic image/video cryptosystem. Phys. Lett. A **372**, 5790–5794 (2008)
4. Arroyo, D., Li, S.: Lessons learnt from the cryptanalysis of chaos-based ciphers. In: Kocarev, L., Lian, S. (eds.) Chaos Based Cryptography Theory Algorithms and Applications, pp. 257–295. Springer, Berlin (2011)
5. Solak, E.: Cryptanalysis of chaotic ciphers. In: Kocarev, L., Lian, S. (eds.) Chaos Based Cryptography Theory Algorithms and Applications, pp. 227–256. Springer, Berlin (2011)
6. Çokal, C., Solak, E.: Cryptanalysis of a chaos-based image encryption algorithm. Phys. Lett. A **373**, 1357–1360 (2009)
7. Arroyo, D., Li, C., Li, S., Alvarez, G., Halang, W.: Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos Solitons Fract. **41**, 2613–2616 (2009)
8. Li, C., Li, S., Lo, K.-T., Kyamakya, K.: A differential cryptanalysis of Yen–Chen–Wu multimedia cryptography system. J. Syst. Softw. **83**(8), 1443–1452 (2010)
9. Solak, E., Rhouma, R., Belghith, S.: Cryptanalysis of a multi-chaotic systems based image cryptosystem. Opt. Commun. **283**, 232–236 (2010)
10. Özkaynak, F., Özer, A.B., Yavuz, S.: Cryptanalysis of a novel image encryption scheme based on improved hyper chaotic sequences. Opt. Commun. **285**, 4946–4948 (2012)
11. Özkaynak, F., Özer, A.B., Yavuz, S.: Cryptanalysis of Bigdeli algorithm using Çokal and Solak attack. Int. J. Inf. Secur. Sci. **1**(3), 79–81 (2012)
12. Babaei, M.: A novel text and image encryption method based on chaos theory and DNA computing. Nat. Comput. **12**(1), 101–107 (2013)
13. Huang, X.L., Ye, G.D.: An image encryption algorithm based on hyper-chaos and DNA sequence. Multimed. Tools Appl. **72**(1), 57–70 (2014)
14. Liu, L.L., Zhang, Q., Wei, X.P.: A RGB image encryption algorithm based on DNA encoding and chaotic map. Comput. Electr. Eng. **38**(5), 1240–1248 (2012)
15. Liu, H.J., Wang, X.Y., Kadir, A.: Image encryption using DNA complementary rule and chaotic maps. Appl. Soft Comput. **12**(5), 1457–1466 (2012)
16. Wei, X.P., Guo, L., Zhang, Q., Zhang, J.X., Lian, S.G.: A novel color image encryption based on DNA sequence operation and hyper-chaotic system. J. Syst. Softw. **85**(2), 290–299 (2012)
17. Zhang, Q., Guo, L., Wei, X.P.: Image encryption using DNA addition combining with chaotic maps. Math. Comput. Model. **52**(11–12), 2028–2035 (2010)
18. Zhang, Q., Guo, L., Wei, X.P.: A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik **124**(18), 3596–3600 (2013)
19. Zhang, Q., Liu, L.L., Wei, X.P.: Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU-Int. J. Electron. Commun. **68**(3), 186–192 (2014)
20. Zhang, Q., Wei, X.P.: A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik **124**(23), 6276–6281 (2013)
21. Jain, A., Rajpal, N.: A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimed. Tools Appl. doi:10.1007/s11042-015-2515-7
22. Liu, Y., Wang, J., Fan, J., Gong, L.: Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. Multimed. Tools Appl. doi:10.1007/s11042-015-2479-7
23. Enayatifar, R., Abdullah, A.H., Isnin, I.F.: Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Lasers Eng. **56**, 83–93 (2014)
24. Kulsoom, A., Xiao, D., Rehman, A., Abbas, S.: An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules, Multimed. Tools Appl. doi:10.1007/s11042-014-2221-x
25. Hermassi, H., Belazi, A., Rhouma, R., Belghith, S.: Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimed. Tools Appl. **72**(3), 2211–2224 (2014)
26. Özkaynak, F., Yavuz, S.: Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Nonlinear Dyn. **78**(2), 1311–1320 (2014)
27. Belazi, A., Hermassi, H., Rhouma, R., Belghith, S.: Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. Nonlinear Dyn. **76**(4), 1989–2004 (2014)
28. Zhang, Y.: Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik **126**(2), 223–229 (2015)
29. Xie, T., Liu, Y., Tang, J.: Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik **125**(24), 7166–7169 (2014)
30. Liu, Y., Tang, J., Xie, T.: Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Opt. Laser Tech. **60**, 111–115 (2014)
31. Zhang, Y.S., Wen, W., Su, M., Li, M.: Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik **125**(4), 1562–1564 (2014)
32. Zhang, Y.S., Xiao, D., Wen, W., Wong, K.-W.: On the security of symmetric ciphers based on DNA coding. Inf. Sci. **289**, 254–261 (2014)
33. SaberiKamarposhti, M., Mohammad, D., Rahim, M., Yaghobi, M.: Using 3-cell chaotic map for image encryp-

tion based on biological operations. Nonlinear Dyn. **75**(3), 407–416 (2014)
34. Li, S.J., Li, C.Q., Chen, G.R., Bourbakis, N.G., Lo, K.T.: A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. Image **23**(3), 212–223 (2008)
35. Li, C.Q., Lo, K.T.: Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. **91**(4), 949–954 (2011)