Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **2**, March **2018**

A New Scheme for Image Steganography based on Hyperchaotic Map and DNA Sequence

Dejian Fang[1,2], Shuliang Sun[2]

[1] College of Computer Science, Chongqing University,
Chongqing, 400044, China

[2] School of Electronics and Information Engineering,
Fuqing Branch of Fujian Normal University, Fuqing, 350300, China
fffdj@sina.com

Received December, 2017; revised December, 2017

Abstract. *A novel image steganography method based on hyperchaotic map and DNA sequence is presented. Four chaotic sequences are generated with 4-D hyperchaotic system and initial keys. Secret image is encoded with one of complementary rules. The choice of complementary rules is to use the pseudo-random number which is produced with 4-D hyperchaotic map. DNA Ex-OR is also applied to generate DNA encoded matrix. The DNA encoded matrix is converted to 1-D bit streams. 2 secret bits are embedded in selected cover image pixels. The method of* 2^k *correction is applied to reduce the difference between the cover and stego images and to obtain better visual quality. The experiments prove that the proposed algorithm is superior to other schemes in PSNR and IF values.*

Keywords: Hyperchaotic map; DNA sequence; 2^k correction.

1. **Introduction.** Cryptography and steganography are two kinds of techniques which are used for data hiding in secret communication. Cryptography is a method in which the data is scrambled so that illegal users will not be able to extract the secret message without secret key [1]. Steganography is derived from the Greek for covered writing and essentially means to hide in plain sight [2].

Anybody could find that both parties are secret communicating in cryptography. However, in steganography, invalid recipients will not suspect the cover media containing secret data at all. In this paper, two kinds of skills are combined together to increase the security of the secret message. Payload, security (imperceptibility) and robustness are three important aspects in modern steganography system.

Chaos is known as remarkable properties that are sensitive to initial values and system parameters, unpredictable, pseudorandom and ergodic [3-4]. It is increasingly employed to information security. Ghebleh and Kanso [5] proposed a robust chaotic algorithm for steganography based on 3-D chaotic cat map and lifted discrete wavelet transforms. Secret image was embedded in the irregular outputs of the cat map and discrete wavelet transform was used to provide robustness. Cycling chaos-based steganography algorithm was put forward in [6]. Pseudorandom number was used to determine the channel and the pixel positions of the cover image. Omain [7] proposed a novel method for image steganography based on chaotic map. A 3-2-2 LSB insertion method was applied for secret communication.

DNA is famous for high parallelism, huge storage and ultra-low power consumption, and some DNA-based steganographic methods have been proposed nowadays [8-11]. Wang et

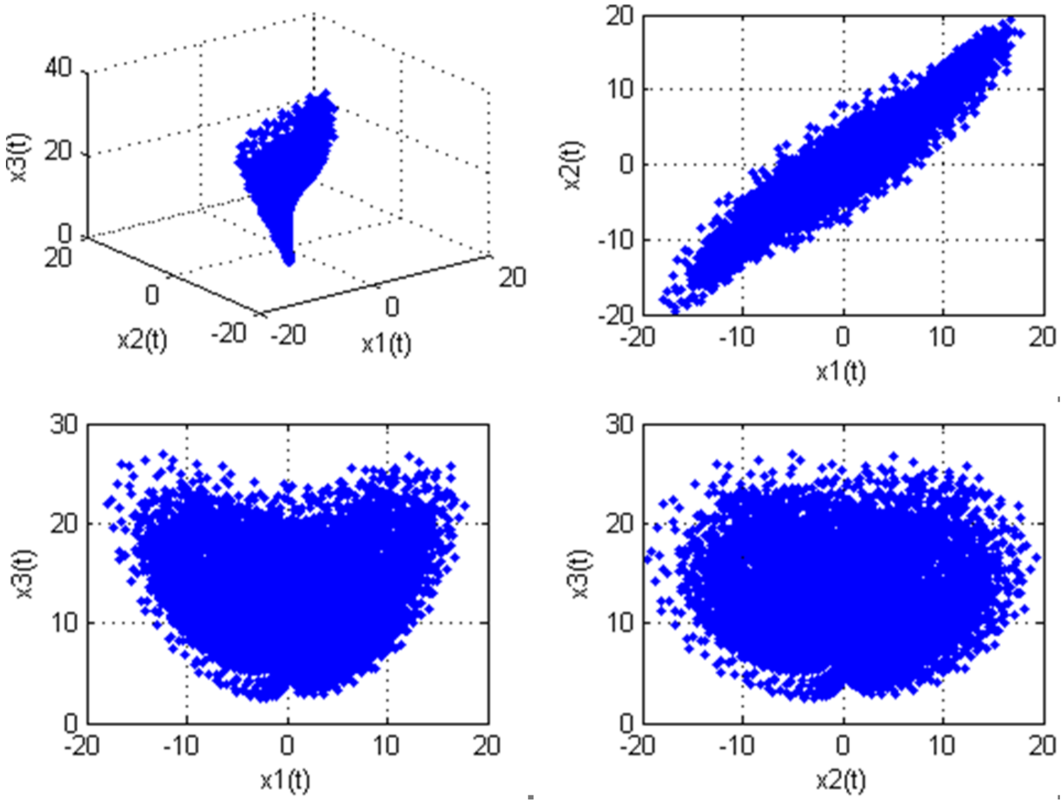

Figure 1. Sequence trajectories of system (1) with parameters $a = 36, b = -16, c = 28, d = 3$ and $e = 0.3$

al. [8] put forward a novel method based on DNA and CML system. Plain image was performed bitwise exclusive OR operation with pseudorandom sequence. DNA matrix was obtained by encoding confused matrix. A couple of 128 bit publicly DNA sequences were taken to form secret keys in [9]. Two rounds encryption were carried out among the cover image. A high capacity data hiding method with low distortion was proposed in [10]. Min-Max Normalization method was adopted to provide space to hide secret message into image pixels. The image pixels were normalized into short range and then denormalized. Sun [11] proposed a new method based on improved logistic map and DNA sequence. The two-by-two complementary rules were put forward and canny edge detector was applied.

2. **4-D Hyperchaotic Map.** 4-D hyperchaotic system [12] is shown as Eq. (1):

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) \\ \dot{x}_2 = -x_1x_3 + bx_1 + cx_2 \\ \dot{x}_3 = x_1x_2 - dx_3 \\ \dot{x}_4 = x_2x_3 + ex_4 \end{cases} \tag{1}$$

where a, b, c, d and e are system parameters. If $a = 36, b = -16, c = 28, d = 3$ and $e \in [-0.7, 0.7]$, the system is in a hyperchaotic state. Sequence trajectories of system (1) are depicted in Fig. 1 when $a = 36, b = -16, c = 28, d = 3$ and $e = 0.3$.

3. **DNA Techniques.** Deoxyribonucleic Acid (DNA) is composed of four nucleotides which are adenine (A), cytosine (C), thymine (T) and guanine (G). A and G are complements with T and C, which is famous for Watson-Crick base-pairing [13]. Six major

Table 1. Ex-OR operation of DNA sequence

⊕	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

complementary based pairing rules are often applied for DNA encoding [14]. For the letter $x, B(x), B(B(x))$, and $B(B(B(x)))$ are not equal, where$B(x)$ is the complement of x.

1. C→T , T→A , A→G , G→C
2. C→T , T→G , G→A , A→C
3. C→A , A→T , T→G , G→C
4. C→A , A→G , G→T , T→C
5. C→G , G→T , T→A , A→C
6. C→G , G→A , A→T , T→C

T, G, C and A are designated as two binary values 11, 10, 01 and 00. Table 1 shows the Ex-OR operation of DNA sequence [8].

4. **The Approach of 2^k Correction.** The approach of 2^k correction is adopted to obtain better visual effects of stego image. Often there are some differences between the cover and stego pixels. The method of 2^k correction is applied to reduce the differences [15, 16]. The steps of 2^k correction are depicted as follows:

```
If (SPV-APV>$2^{k-1}$) & (SPV-$2^k$>=0)
    NSPV = SPV -$2^k$
Else if (SPV- APV<-$2^{k-1}$) & (SPV+$2^k$<=255)
    NSPV = SPV +$2^k$
Else
    NSPV = SPV
End
```

where APV, SPV and NSPV respectively means actual pixel value, stego pixel value and new stego pixel value. The parameter k is the number of bits which are embedded in actual pixel value.

5. **Proposed Algorithm.** Steps of embedding process are shown as follows:
Step 1: Compute the initial values x'_1, x'_2, x'_3 and x'_4 of 4-D hyperchaotic system (1) as

follows:

$$s = \sum_{i=1}^{m} \sum_{j=1}^{n} P_{ij} \tag{2}$$

$$\begin{cases} x_1^{'}(1) = \text{mod}\left(s + x_1^0, 1\right) \\ x_i^{'}(1) = \text{mod}\left(x_{i-1}^{'}(1) + x_i^0, 1\right) \;\; i = 2, 3, 4 \end{cases} \tag{3}$$

Where $x_i^0$and s are the initial key,$i = 1, 2, 3, 4.M$ and n are the size of row and column of secret image P.

Step 2: Iterate 4-D hyperchaotic system 300 times to avoid the transient effect. Continue to iterate 4-D hyperchaotic system $4m \times n$ times and get 4 chaotic sequences a_1, a_2, a_3 and a_4. Especially $a_l = [a_l(1), a_l(2), .., a_l(4mn)], l = 1, 2, 3, 4$.

Step 3: The chaotic sequences a_1, a_2, a_3 and a_4 are performed as Eqs. (4) - (7).

$$a_1(i) = floor(\text{mod}(abs(a_1(i)) \times 10^{12}, 6)) + 1 \tag{4}$$

$$a_2(i) = floor(\text{mod}(abs(a_2(i)) \times 10^{12}, 4)) \tag{5}$$

$$a_3(i) = floor(\text{mod}(abs(a_3(i)) \times 10^{12}, 256)) \tag{6}$$

$$a_4(i) = \begin{cases} 0, \; if \; abs(a_4(i)) - abs(\lfloor a_4(i) \rfloor) < 0.5 \\ 1, \; else \end{cases} \tag{7}$$

where a_1, a_2, a_3 and a_4 are integers, and $a_1 \in [1, 6], a_2 \in [0, 3], a_3 \in [0, 255], a_4 \in [0, 1], i = 1, 2, .., 4mn$.

Step 4: Convert$\{P(i)\}_{i=1}^{mn}$ and$\{a_3(i)\}_{i=1}^{mn}$ into DNA sequences$\{c(i)\}_{i=1}^{4mn}$ and $\{d(i)\}_{i=1}^{4mn}$.

Step 5: Perform the DNA EX-OR to get the DNA sequence F.

$$F(i) = c(i) \oplus d(i) \tag{8}$$

where $i = 1, 2, .., 4mn$.

Step 6: Select a rule from six complementary rules according $a_1(i)$. Based on $a_2(i)$ and selected complementary rule, perform DNA replacement operation on DNA sequence $F(i)$ and obtain DNA complementary sequence $F'(i)$.

$$F^{'}(i) = B^{a_2(i)}(F(i)) = \begin{cases} F(i), \; if \; a_2(i) = 0 \\ B(F(i)), \; if \; a_2(i) = 1 \\ B(B(F(i))), \; if \; a_2(i) = 2 \\ B(B(B(F(i)))), \; if \; a_2(i) = 3 \end{cases} \tag{9}$$

where $B(x)$ is the base pair of $x, i = 1, 2, .., 4mn$.

Step 7: Decode F' to binary sequence G.

Step 8: 2 least significant bits (2-LSBs) of cover image pixel $I(a_4(i))$ are replaced by 2 secret bits if $a_4(i) = 1$. I is the cover image.

Step 9: The way of 2^k correction is executed to obtain better visual effects.

Step10: Stego image is achieved finally.

Steps of extracting process are the reverse the steps of the embedding process.

6. **Experiments and Analysis.** In this paper, the experiment is simulated using MATLAB 10 program on Windows 7. Lena, Cameraman, Man and Peppers with size of 512 × 512 are used as the cover images. The sizes of secret images are 32 × 32, 64 × 64, and 81×81. Peak signal-to-noise ratio (PSNR) and the image fidelity *(IF)* [17] are applied

Figure 2. Cover images and their stego images with different methods (a) cover image (b) the result of Battikh's [17] (c) the result of Singhs [18](d) the result of our method (size of secret image : 64×64)

Table 2. Three values versus of payload size

Cover	Payload 1. 32×32		Payload 1. 64×64		Payload 1. 128×128	
Image	PSNR	IF	PSNR	IF	PSNR	IF
Lena	63.3657	0.9999	57.5682	0.9997	52.3804	0.9985
Cameraman	63.1458	0.9999	57.3954	0.9996	52.1689	0.9984
Man	62.8599	0.9998	57.0792	0.9996	51.7543	0.9982
Peppers	63.8746	0.9999	57.8426	0.9997	52.5054	0.9987

to measure image quality of the proposed scheme. To calculate PSNR, first mean square error (MSE) is calculated using equation 10:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\|I(i,j) - S(i,j)\|^2 \tag{10}$$

I is cover image and S is stego image. M and N are the size of row and column of cover image. Thereafter PSNR value is calculated using equation 11 in decibels. A higher value of PSNR is better because of the superiority of the signal to that of the noise.

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{11}$$

IF is given in equation 12.

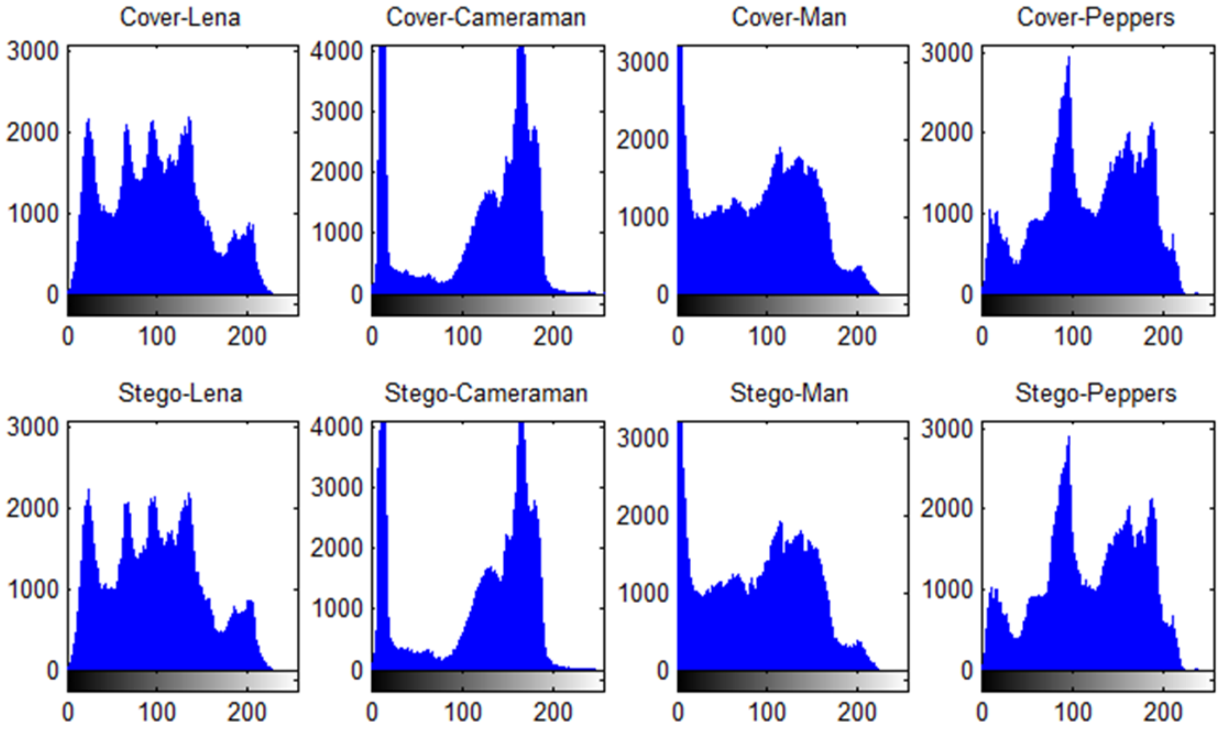

Figure 3. Histograms of original images and stego images (size of payload: 64 × 64)

Table 3. Values of PSNR and IF versus of different methods (payload size 64 × 64)

Cover	**Battikh's [17]**		**Singh's [18]**		**Proposed**	
Image	PSNR	IF	PSNR	IF	PSNR	IF
Lena	54.4685	0.9991	41.8367	0.9833	57.5682	0.9997
Cameraman	54.3426	0.9990	41.7652	0.9831	57.3954	0.9996
Man	54.1728	0.9988	41.7354	0.9827	57.0792	0.9996
Peppers	54.5761	0.9992	41.9613	0.9839	57.8426	0.9997

$$IF = 1 - \frac{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N}(P(i,j) - S(i,j))^2}{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N}P(i,j) * S(i,j)} \tag{12}$$

The higher value of IF is, the better is the quality of stego image. The different cover images and their stego images with different methods are shown in Fig. 2. The histograms of cover images and corresponding stego images are displayed in Fig. 3. The size of payload is 64 × 64.

From table 2, it can be found that the values of PSNR and IF decrease when the size of the secret payload increases. The proposed method is compared with the schemes of [17-18] in this paper.

From table 3, it can be concluded that proposed method is superior to other methods.

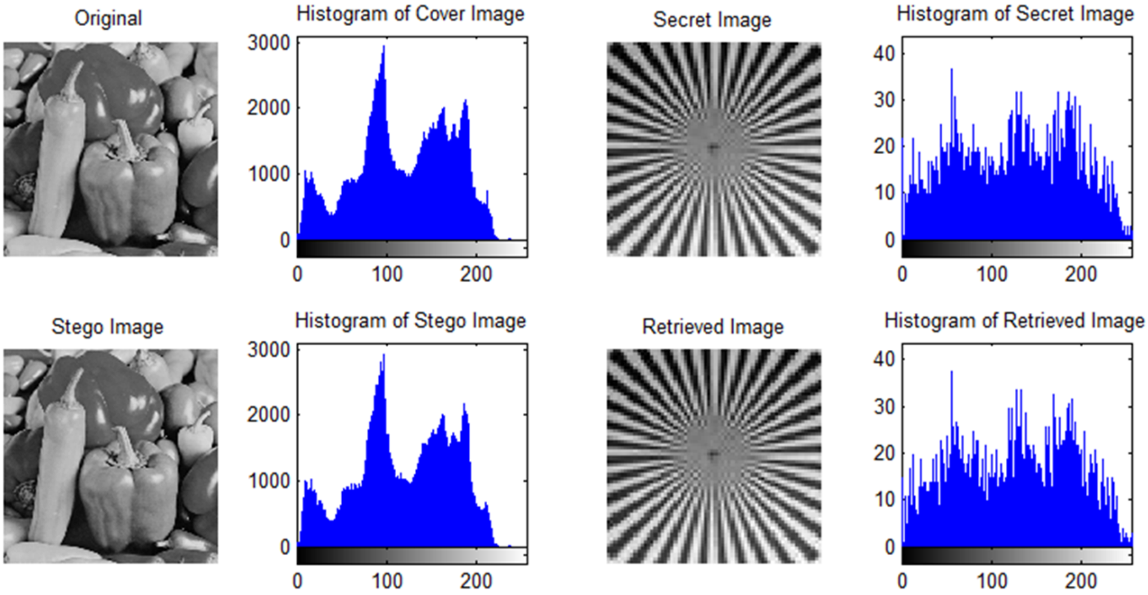

FIGURE 4. Cover image, secret image, stego image, retrieved image and their histograms

Secret image is embedded in cover image and stego image is achieved in Fig. 4. Retrieved image is obtained finally after extraction. The figure also displays that retrieved image is the same as original secret image. The conclusions also could be acquired from their histograms.

7. **Conclusions.** In this paper, a novel steganography method based on hyperchaotic map and DNA sequence is proposed. Secret image is encoded with one of complementary base pairing rules. The choice of mapping rules is used the pseudo-random number which is generated with 4-D hyperchaotic map. DNA Ex-OR is also applied. DNA encoded matrix is converted to 1-D bit streams. 2 secret bits are embedded in selected cover image pixels. The way of 2^k correction is adopted to release the difference between the cover and stego images and to get better image quality. The experiments show that the proposed scheme is superior to other schemes in PSNR and IF values

REFERENCES

[1] J. S. Pan, W. Li, C. Yang, et al. Image steganography based on subsampling and compressive sensing, *Multimedia Tools and Applications*, vol. 74 , no. 21, pp. 9191-9205, 2015.

[2] S. Channalli, A. Jadhav. Steganography. An art of hiding data, *International Journal on Computer Science and Engineering,* vol. 1, no. 3, pp. 137-141, 2009.

[3] C. Chen, L. Xu, T. Wu, et al. On the security of a chaotic maps-based three-party authenticated key agreement protocol, *Journal of Network Intelligence*, 1, no. 2, pp. 61-66, 2016.

[4] S. Sun. Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules, *Optical Engineering,* vol. 56, no. 11, pp. 116117, 2017.

[5] M. Ghebleh, A. Kanso. A robust chaotic algorithm for digital image steganography, *Communications in Nonlinear Science and Numerical Simulation*, vol. 19 , no. 6, pp. 1898-1907, 2014.

[6] M. Aziz, M. H. Tayarani-N, M. Afsar. A cycling chaos-based cryptic-free algorithm for image steganography, *Nonlinear Dynamics,* vol. 80 , no. 3, pp. :1271-1290, 2015.

[7] D Omain. A novel secure image steganography method based on chaos theory in spatial, *International Journal of Security, Privacy and Trust Management,* vol. 3, no. 1, pp. 11-22, 2014.

[8] X. Wang, Y. Zhang, X. Bao. A novel chaotic image encryption scheme using DNA sequence operations, *Optics and Lasers in Engineering,* vol. 73, pp. 53-61, 2015.

[9] A. Majumdar, M. Sharma. Enhanced information security using DNA cryptographic approach, *International Journal of Innovative Technology and Exploring Engineering,* vol. 4, no. 2, pp. 72-76, 2014.

[10] D. Brabin, J.R.P. Perinbam, D. Meganathan. A high capacity data hiding scheme for digital images using normalization, *International Journal of Applied Engineering Research*, vol. 10, no. 1, pp. 1341-1350, 2015.

[11] S. Sun. A novel secure image steganography using improved logistic map and DNA techniques, *Journal of Internet Technology*, vol. 18, no. 3, pp. 647-652, 2017.

[12] G. Ye, J. Zhou. A block chaotic image encryption scheme based on self-adaptive modeling, *Applied Soft Computing*, vol. 22 , no. 5, pp. 351-357, 2014.

[13] X. Chai, Y. Chen, L. Broyde. A novel chaos-based image encryption algorithm using DNA sequence operations, *Optics and Lasers in Engineering*, vol. 88, pp.197-213, 2017.

[14] A.U. Rehman, X. Liao, A. Kulsoom, et al. Selective encryption for gray images based on chaos and DNA complementary rules, *Multimedia Tools and Applications*, vol. 74, no. 13, pp. 4655-4677, 2014.

[15] S. Sun. A novel edge based image steganography with 2k correction and huffman encoding, *Information Processing Letters*, vol. 116, no. 2, pp. 93-99, 2016.

[16] A. Kaur, S. Kaur. Image steganography based on hybrid edge detection and 2^k correction method, *International Journal of Engineering and Innovative Technology,* 1, no. 2, pp. 167-170, 2012.

[17] D. Battikh, S.E. Assad, B Bakhache, et al. Chaos-based spatial steganography system for images, *International Journal of Chaotic Computing,* vol. 3, no. 1, pp. 36-44, 2014.

[18] S. Singh, A. Datar. Improved hash based approach for secure color image steganography using canny edge detection method, *International Journal of Computer Science and Network Security*, vol. 14, no. 7, pp. 82-89, 2014.