Signal Processing 142 (2018) 340–353

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption

Junxin Chen[a,*], Zhi-liang Zhu[b], Li-bo Zhang[c], Yushu Zhang[d], Ben-qiang Yang[c,*]

[a] Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China
[c] Department of radiology, The General Hospital of Shenyang Command PLA, Shenyang 110016, China
[d] School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China

ARTICLE INFO

Article history:
Received 8 January 2017
Revised 22 April 2017
Accepted 29 July 2017
Available online 31 July 2017

Keywords:
Chaos
Permutation and diffusion
Self-adaptive mechanism
DNA random encoding

ABSTRACT

This paper presents a solution for secure and efficient image encryption with the help of self-adaptive permutation–diffusion and DNA random encoding. The plain image is firstly converted to DNA sequence using random encoding rules, so as to disarrange the bit distribution of the plaintext. A self-adaptive permutation–diffusion procedure is subsequently introduced for further encryption. The quantization processes of the permutation and diffusion procedures are disturbed by the intrinsic features of the plaintext, with the introduced disturbances can be automatically retrieved in the decryption end. The security of the system originates from the plaintext-related quantization of the encryption process which makes the cryptosystem secure against plaintext attack. Besides, the reusability of the random variables can dramatically promote the efficiency of the cryptosystem, which renders great potential for real-time secure image applications.

1. Introduction

With the dramatic developments of computer and communication technologies, multimedia contents such as images, audios, videos have become the widest and most important information of networks, owing to their clarity, lifelikeness and vividness. As the images always involve commercial, military, medical and political sensitive affairs, how to secure their transmission and storage over public networks has drawn much more attention than ever before in cryptographic and information security fields. However, recent research achievements have revealed the fact that traditional block ciphers such as DES, AES are poorly suited for image encryption [1]. For ciphering images, one should pay attention to their intrinsic features such as large volume and high pixel correlation etc., which are much distinct from textual contents.

The achievements of chaos theory have paved an illuminating perspective for image encryption. Chaos is a deterministic non-linear system, from which the resultant sequences are pseudo-random, possess infinite period and behave like Gaussian white noise. Besides, as the chaotic system is high sensitive to the control parameter and initial condition, the produced sequence is un-predictable and can provide huge key space. In 1998, Fridrich proposed the groundbreaking substitution-diffusion architecture for image encryption [2], and then be developed to the classical permutation–diffusion architecture by Chen, Lian and Wong [3–5]. This structure subsequently draws world-wide concern and promotes the development of chaos-based encryption. The innovations lie in various aspects, such as novel permutation techniques [3–6,8–10], new diffusion approaches [7,11,12], high security key stream generators [13], simultaneous image encryption-compression scheme [14,15], as well as novel transform domains [16,17]. On the other hand, DNA coding based cryptosystems have emerged as revolutionary encryption techniques due to the excellent features of DNA computing, such as massive parallelism, huge storage and ultra-low power consumption [18,19]. It is natural that a number of cryptosystems combining chaos theory with DNA encoding have been investigated in the past several years [20–30]. In [20–24], logistic map and its variants are adopted as key stream generators, whereas coupled map lattice is employed in [23,25,26]. In order to promote the randomness of key stream and further enhance the security, hyper-chaotic systems have been introduced to cooperate with DNA coding in the very recent proposals [27–30]. For plaintext attack resistance, various plaintext-related key stream generation mechanisms have been investigated [22,24,26–28,30], with majority of them operating in one time pad (OTP) pattern essentially. Taking the scheme in [26] as an example, the plaintext is firstly confused (in pixel level) with the masks produced by the input secret key. Then the confused image is transformed into

* Corresponding authors.
E-mail addresses: chenjx@bmie.neu.edu.cn (J. Chen), benqiang.y@gmail.com (B.-q. Yang).

http://dx.doi.org/10.1016/j.sigpro.2017.07.034
0165-1684/

DNA sequences according to a certain encoding rule. The extended Hamming distances of the produced DNA sequences are subsequently computed as the alteration to disturb the initial secret key and therefore make the subsequent key stream related to the plaintext. With the plaintext-related key stream components, the DNA sequences are then permutated and masked to produce the ciphertext. With such plaintext-related key stream generation mechanism, cryptosystem in this type is of high sensitivity to the plaintext and hence possesses satisfactory resistance to plaintext attacks. Besides, the initial secret key which is independent of the plaintext, the plaintext-dependent alteration of the key (such as the extended Hamming distances in [26]) is also required in the decryption end. Therefore, one should transfer the distinct alteration for different images through a secret channel, which essentially makes the system working in OTP fashion and increases much implementation complexity for practical applications.

Regarding this, we propose to encrypt images using DNA random encoding and self-adaptive permutation–diffusion. Three innovations are contributed in this work. Firstly, DNA random coding is investigated and adopted in the proposed cryptosystem, rather than the widely used DNA coding with fixed rule. The prepositive DNA random encoding procedure can resist a widely launched chosen-plaintext attack, which is adopted to bypass the permutation performance using a deliberate image with identical pixel value. On the second, self-adaptive permutation and diffusion is investigated based on a novel plaintext-related quantization mechanism. To the best of our knowledge, it is the first time to report the security potential of quantization process for chaos-based image encryption. Specially speaking, a plaintext-related disturbance is embedded into the quantization process rather than the generation of chaotic variables, of the permutation and diffusion procedures. Such that, the chaotic variables can be multiply used for encrypting different images and further promote the encryption efficiency as different plaintexts lead to distinct key streams. The third is the self-synchronizing capability of this plaintext-related disturbance. As the name suggests, this alteration is drawn from the plaintext, whereas it can be automatically retrieved in the decryption process. Therefore, it is not part of the secret key and hence not required to be transferred to the decoder privately; the input initial conditions of the employed hyper-chaotic system completely serve as the secret key. A hyper-chaotic Lorenz system is introduced for key stream generation.

The remainder of this paper is organized as follows. The preliminaries including DNA encoding, employed chaos system and the permutation–diffusion architecture are given out in Section 2. The proposed cryptosystem is described in detail in Section 3, whereas security analyses and discussions are given in Section 4. Finally, Section 5 concludes the paper.

2. Preliminaries

2.1. DNA coding

A DNA sequence contains four nucleic acid bases i.e., A (Adenine), C (Cytosine), G (Guanine) and T (Thymine), where A pairs with T, C pairs with G, or in other words A and T are complementary, and C and G are complementary. Generally, the four DNA bases A, C, G, and T correspond to binary numbers with two bits, i.e., 00, 01, 10 and 11. In the binary encoding theory, 0 and 1 are complementary, the binary numbers 00 and 11 are complementary, 01 and 10 alike. If one uses the four bases A, C, G and T to denote the binary numbers 00, 01, 10 and 11, there are total $4! = 24$ kinds of DNA coding combinations. Whereas, taking the complementary requirement into consideration, there are only eight valid kinds of coding rules, as listed in Table 1 [31].

Table 1
Valid DNA coding rules.

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

Table 2
DNA XOR operations with rule 1.

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

In order to further promote the application of DNA computing in cryptography, some biological and algebraic computation disciplines are introduced for DNA sequences, such as exclusive and XOR. The XOR operations for DNA sequences are performed according to its traditional rule in binary formation, and there are 8 kinds of DNA XOR rules corresponding to 8 kinds of DNA encoding rules. In this paper, DNA XOR is performed according Rule 1, as shown in Table 2.

In the proposed cryptosystem, DNA sequences are employed to encrypt 256 gray-scale digital images, whose pixel (expressed as 8 bit binary number) can be encoded into a DNA sequence with length-4 using A, C, T and G to represent the binary arrays 00, 01, 10 and 11, respectively. For example, a pixel with value 216 is expressed as [11011000] in binary fashion, and it will be transformed to a DNA sequence [T G C A] according to the first coding rule. Conversely, the original binary sequence can be recovered by the same decoding rule, and consequently different DNA decoding rules will lead to distinct binary sequences. The DNA sequence [T G C A] is converted to binary series [11011000] with decimal sense 216 using Rule 1, whereas it will be translated as [10110001] to represent decimal number 177 through the fourth decoding rule. With this property, the plaintext can be encoded with Rule $K1$ and then decoded with Rule $K2$, so as to conceal the original information. The security of such encryption approach depends on $K1$ and $K2$, which can separately take eight different values, i.e., Rule 1–8. Outwardly, the key space is $8 \times 8 = 64$, whereas the total valid number of possible combinations of $K1$ and $K2$ is only 8, as pointed out in [31], which means majority of the ($K1$, $K2$) pairs are equivalent ones.

2.2. Hyper-chaotic Lorenz system

In the proposed scheme, a hyper-chaotic system that is obtained by adding an additional state and couple it to the second equation of Lorenz chaotic system [32], is employed for key stream generation. Other chaotic systems can also be adopted as alternatives for (pseudo) random variable generation to cooperate with the developed DNA random encoding and self-adaptive permutation–diffusion procedures. The employed fourth-order system is described by in Eq. (1).

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = bx - xz - cy + w. \\ \dot{z} = xy - dz \\ \dot{w} = -ky - rw \end{cases} \tag{1}$$