Displays 41 (2016) 1–8

Contents lists available at ScienceDirect

Displays

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

A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images

Türker Tuncer [a,*], Engin Avci [b]

[a] Department of Digital Forensic Engineering, Technology Faculty, Firat University, Elazig, Turkey
[b] Department of Software Engineering, Technology Faculty, Firat University, Elazig, Turkey

ARTICLE INFO

Article history:
Received 19 March 2015
Received in revised form 7 October 2015
Accepted 13 October 2015
Available online 22 October 2015

Keywords:
Data hiding
Probabilistic DNA-XOR secret sharing
Image steganography
Watermarking
Information security

ABSTRACT

In this paper, a new data hiding method is proposed based on secret sharing scheme with the DNA exclusive or (DNA-XOR) operator for color images. The DNA-XOR secret sharing scheme uses a DNA-XOR truth table. Each input value of truth table is evaluated and according to that evaluation, highest PSNR (Peak Signal-to-Noise Ratio) value is selected for secret sharing. These selected values are embedded into cover image. Cover image is used as an encryption key in the proposed secret sharing process. In this study, the hidden data are divided into three secret shares and embedded into the red, green and blue channels of a cover image respectively. In here, the DNA-XOR operator has been firstly used as secret sharing operator in data hiding literature. Our proposed data hiding method was compared with previous methods. The comparison of these methods shows that our proposed method gives the most successful result.

1. Introduction

Nowadays, in parallel to improvements in technology, information security techniques have been developed. Data hiding is one of these techniques [1]. Data hiding is a technique, which involves hidden data that is known only by the sender and the receiver. In this technique, hidden data is obtained only by a person who has stego key. Data can be hidden in seemingly innocent multimedia files (image, audio signal, video, etc.) with the condition not to exceed size of the cover data during transmission. If the receiver side knows the stego key, he/she can obtain the hidden data by operating embedding function in reverse [2,3].

Multimedia data (image, audio, video) has more size than plain text in computer environment. Therefore, images, audios, videos are very convenient to use as cover objects [4]. In order to prevent hidden data in cover object from third parties, embedding algorithm must satisfy some certain criteria. Not to be perceived by the human visual system is one of these criteria. At the same time to hide the data with embedding algorithm, data must be able to embed with appropriate capacity into cover data. In order to evaluate the success of data hiding algorithms the following points should be considered [5].

- The optimum way of embedding mechanism.
- The optimum way of extraction of embedded data.
- The optimum amount of data: Capacity.
- Robustness to attacks.
- Transparency.
- Reliability.

To ensure these criteria, various data hiding algorithms have been developed [6–9]. The data hiding algorithms usually examined in 3 groups, according to the domain of data hiding algorithm.

Spatial Domain: In this domain, Least Significant Bit (LSB) [10,11] method is widely used. The pixel values of the cover object are used for data hiding process.
Frequency Domain: Data hiding process is used by obtaining coefficients from conversions of Discrete Cosine Transform (DCT) [12,13], Discrete Wavelet Transform (DWT) [14] and Discrete Fourier Transform (DFT) [15].
Compression Domain: In this domain, Vector Quantization (VQ) method is used for data hiding [16].

Also, histogram shifting mechanism is used for data hiding and steganographic schemes [17].

Frequency domain is used for increasing durability [18,19]. Many studies are available for improving the data hiding algorithm by obtaining the coefficients of cover data in Frequency domain.

Recently, some researchers started to use the complementary rule of the DNA to ensure information security and data hiding.

* Corresponding author.
E-mail addresses: turkertuncer@firat.edu.tr (T. Tuncer), enginavci@firat.edu.tr (E. Avci).

http://dx.doi.org/10.1016/j.displa.2015.10.005
0141-9382/© 2015 Elsevier B.V. All rights reserved.

Huang et al. [20] suggested a DNA-based data hiding technique with low modification. This method solved many problems of previous DNA based data hiding algorithms. Liu et al. [21] proposed a new data hiding method based on deoxyribonucleic acid (DNA) coding, which used a word document as a cover object. In their method, the plain message became a cipher sequence after being encoded to a DNA sequence and being encrypted by the addition operation. The cipher sequence was attached to a random DNA primer sequence and circularly shifted for finite times, then the whole sequence was embedded into a Word document through substituting each character's color. The plaintext was extracted according to the keys, and the key space was large enough to resist brute force attacks. Zhang et al. [22] presented a new image fusion encryption algorithm based on image fusion and DNA sequence operation and hyper-chaotic system. Two DNA sequence matrices were obtained by encoding the original image and the key image. Secondly, the chaotic sequences generated by Chen's hyper-chaotic maps were used to scramble the locations of elements in the DNA sequence matrices which were generated from the original images. Finally using a XOR operator matrix was embedded. Lee [18] addressed issues regarding watermarking DNA coding sequences in the frequency domain. Chang et al. [23] proposed two data hiding schemes. In their schemes, secret messages were hidden in a DNA sequence. The host DNA sequence could be reconstructed after the reverse operation. This property ensured the security of the secret data and preserved the functionality of the original DNA. Risca [24] presented an implementation of steganography using DNA molecules. This study showed that the steganographically hidden message was retrieved only by using the two secret primers, meaning that the only applicable cryptanalytic approach was a brute-force search for the two primer sequences. At the same time in the literature, there are many studies supported by the secret sharing method to improve the success of data hiding application. Liu et al. [25] presented a robust readable H.264/AVC data hiding algorithm without intra-frame distortion drift. They first divided the original embedded data into several groups by using the secret sharing technique. Then they used the BCH syndrome code (BCH code) technique to encode each grouping of data. Finally, they embed the encoded data into the paired-coefficients of the 4 × 4 Discrete Cosine Transform (DCT) block of the selected frames which meet our conditions to avert the distortion drift. Lee and Tsai [26] presented a new data hiding method via PNG images based on Shamir's (k,n)-threshold secret sharing scheme. Wei et al. [27] proposed new information hiding scheme for color images based on the concept of visual cryptography and the XOR operation. Three different schemes with noise-like, meaningful and binary shares were presented. Their proposed model could be extended from 256 colors to 65,536 or true color images by expanding the block size from 3 × 3 to 4 × 4 or 5 × 5. In this paper, for improving the success rate of data hiding techniques an efficient method is proposed based on DNA-XOR secret sharing. In Section 2, we briefly describe the basic concept of DNA encoding and decoding for color image. Section 3 contains a detailed explanation of the proposed algorithm. In Section 4, we describe the results of proposed method in the context of PSNR, bit error rate (BER), pixel distortion (PD) and structural similarity (SSIM). Finally, we present our conclusion in Section 5.

2. DNA sequence

A DNA sequence consists of DNA molecules. DNA sequence is essential information for living, surviving and reproducing [28]. A DNA sequence is formed by four nucleic acids which are A (adenine), C (cytosine), G (guanine), T (thymine). A, T and G, C are complementary like 0 and 1 in binary. DNA sequencing is important for biological research [29].

Table 1
Eight kinds of schemes encoding map rule of DNA sequence.

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

Table 2
XOR operator for DNA sequences.

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

2.1. DNA encoding and decoding for color image

In a DNA sequence, there are four different nucleic acids which are, A (adenine), T (thymine), C (cytosine), and G (guanine). Therefore, Watson–Crick complement rule is valid in here [30]. Table 1 shows encoding and decoding map by using DNA sequence in this paper.

The Watson–Crick complementarity rule gives fundamental information which can be transferred to daily life. Firstly, a color image is separated to RGB channels. Secondly, these RGB channels are converted to binary coding. Then, each pixel of RGB channels can be expressed as a DNA sequence. For example, the binary code of the pixel value of blue channel image is [11001001]. DNA sequence of this binary code is [TACG] according to definition of first column in Table 1 [31].

A x-bit color image, which has $m \times n$ size and can be defined as a three-dimensional (Red, Green and Blue) binary matrix, which is denoted as $A = [s_{i,j,k}]_{m\times n\times k}$. Where $s_{i,j,k} \in \{0,1\}$, and $(i,j,k) \in \{0,1,\ldots,m-1\} \times \{0,1,\ldots,n-1\} \times \{0,1,\ldots,k-1\}$.

The XOR operation for R, G, B channels of the image are defined in Eq. (1):

$$\mathrm{R} \oplus \mathrm{G} \oplus \mathrm{B} = \left[s_{i,j,1} \oplus s_{i,j,2} \oplus s_{i,j,3}\right]_{m\times n\times k} \quad (1)$$

Binary code of the represented value of pixel $A_{i,j}$ at point (i,j) can be converted to a decimal number by using Eq. (2) [32].

$$A_{i,j} = a_{i,j,k-1}2^{k-1} + a_{i,j,k-2}2^{k-2} + \ldots + a_{i,j,1}2^{1} + a_{i,j,0}2^{0} \quad (2)$$

In DNA computing, biological and mathematical operators based on DNA sequences are used. XOR operator has been widely utilized in DNA computing. Table 2 shows the DNA-XOR rules [30].

Fig. 1 illustrates the deterministic finite automata of XOR operator for DNA sequences using a state diagram [33].

3. The proposed method

In this study, the secret data is divided into three secret shares with using DNA-XOR operator. Each part of hidden data is embedded into each channel of color image. Cover images size is 512 × 512 × 3. Size of each secret share is 512 × 1024 (524,288) bits which is embedded into the cover image.

3.1. Probabilistic DNA-XOR secret sharing scheme

Secret sharing based methods have been introduced to protect the reliability of the encryption key or data. Shamir's (k,n) threshold method is the best known of these methods. Purpose of secret sharing is to provide the key reliability. In the literature, many