Sensors **2012**, *12*, 13441-13457; doi:10.3390/s121013441

OPEN ACCESS

sensors

ISSN 1424-8220

www.mdpi.com/journal/sensors

Article

Efficient Text Encryption and Hiding with Double-Random Phase-Encoding

Jun Sang [1,*], Shenggui Ling [1] and Mohammad S. Alam [2]

[1] School of Software Engineering, Chongqing University, Chongqing 401331, China; E-Mail: 20092402023@cqu.edu.cn

[2] Department of Electrical and Computer Engineering, University of South Alabama, Mobile, AL 36688, USA; E-Mail: malam@southalabama.edu

* Author to whom correspondence should be addressed; E-Mail: jsang@cqu.edu.cn; Tel.: +86-139-8369-7592.

Received: 28 August 2012; in revised form: 19 September 2012 / Accepted: 26 September 2012 / Published: 1 October 2012

Abstract: In this paper, a double-random phase-encoding technique-based text encryption and hiding method is proposed. First, the secret text is transformed into a 2-dimensional array and the higher bits of the elements in the transformed array are used to store the bit stream of the secret text, while the lower bits are filled with specific values. Then, the transformed array is encoded with double-random phase-encoding technique. Finally, the encoded array is superimposed on an expanded host image to obtain the image embedded with hidden data. The performance of the proposed technique, including the hiding capacity, the recovery accuracy of the secret text, and the quality of the image embedded with hidden data, is tested via analytical modeling and test data stream. Experimental results show that the secret text can be recovered either accurately or almost accurately, while maintaining the quality of the host image embedded with hidden data by properly selecting the method of transforming the secret text into an array and the superimposition coefficient. By using optical information processing techniques, the proposed method has been found to significantly improve the security of text information transmission, while ensuring hiding capacity at a prescribed level.

Keywords: double-random phase-encoding; text encryption; information hiding; hiding capacity; recovery accuracy

1. Introduction

In information security, cryptography, which encrypts the secret message before transmission to avoid information disclosure, is commonly used [1]. Usually, the encryption methods are based on digital methods [1]. By utilizing the high processing speed, high parallelism, and high-dimensional encryption characteristics of the optical information processing system, optical encryption methods outperform digital encryption methods for image encryption. A typical optical image encryption method is the double-random phase-encoding (DRPE) technique, which encodes the original secret image to a complex-valued encoded image by applying independent random phase encoding on the input plane and the Fourier plane, respectively [2]. Thereafter, the DRPE-based optical image encryption method has been improved [3–7] and applied to other transformation domains, including optical encryption in the fractional Fourier domain [8–12], optical encryption in the Fresnel domain [13,14] and encrypting information with digital holography [15,16].

For cryptography, the encrypted secret message, *i.e.*, the cyphertext, is usually unreadable. Therefore, an encrypted message may be easily detected during transmission on the public channel, which will disclose the existence of the secret transmission. On the other hand, information hiding techniques hide the secret message in public information to conceal the existence of the secret message and to achieve secure message storage and transmission [17]. Information hiding includes two main types [17]: (1) watermarking, which is usually used to protect the copyright of digital products or used to ensure the authenticity and integrity of the digital content; (2) steganorgraphy, which is usually used for secure transmissions.

The traditional information hiding methods usually use digital methods to hide the secret message in the spatial domain [18,19] or in the frequency domain [20–25]. Recently, optical information processing techniques were used for information hiding, including hiding images in halftone pictures [26], double-random phase-encoding [27,28], digital holography [29–33], Fresnel domain [34,35] and hybrid methods [36–38]. To enhance security, an information hiding technique is usually combined with encryption to encrypt the secret message before hiding it in the public information [39]. As a typical optical image encryption technique, the DRPE technique has been widely used to hide the secret image [27,28,40,41].

The existing DRPE-based information hiding methods are usually used for image hiding [28,40,41]. They are also employed to encrypt and hide the secret text in this paper. First, the secret text is transformed into a 2-dimensional array in the form of an image. The bit stream of the secret text is stored in the higher bits of the elements of the transformed array, while the lower bits of the elements are filled with specific values. Then, the transformed array is encoded with the DRPE technique and is hidden into an expanded host image. To recover the secret text, the encoded array is extracted from the image embedded with hidden data and decrypted with the DRPE technique. Thereafter, the bit stream of the secret text is obtained from the higher bits of the elements in the decrypted array. Thus, by using this bit stream, the secret text can be recovered. In the proposed method, the DRPE-based image encryption and decryption may be realized with optical method and the other steps may be realized with digital methods. The proposed method applies the optical information encryption and hiding method to text encryption and hiding, which increases the security of the secret text while utilizing the advantages of optical information processing techniques.

The rest of this paper is organized as follows: in Section 2, the proposed method is introduced. Section 3 incorporates the theoretical performance analysis of the proposed method, including the hiding capacity, the recovery accuracy of the secret text, and the quality of the image embedded with hidden data. Section 4 includes the results and discussions obtained from the numerical simulation experiments. Section 5 presents the concluding remarks.

2. The Proposed Scheme

In this Section, the proposed text encryption and hiding method based on DRPE technique is introduced. The main symbols used in this paper are listed in Table 1.

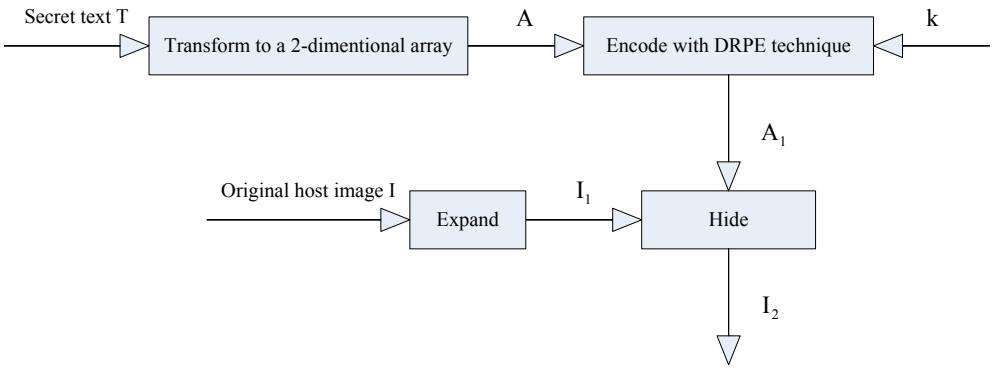
Table 1. Symbols used in the paper.

T	**Secret text**
A	2-dimentional array transformed from T
k	Secret key for DRPE encoding
A_1	Array obtained by encoding A with the DRPE technique
I	Original host image
I_1	Expanded host image
I_2	Image embedded with hidden data by embedding A_1 into I_1
α	Superimposition coefficient
A_1'	Array extracted from I_2
A'	Array decrypted from A_1 with the DRPE technique
T'	Recovered secret text

2.1. Encoding and Hiding Procedure

The encoding and hiding procedure used in this paper is shown in the block diagram of Figure 1.

Figure 1. Encoding and hiding procedure.



In the encoding and hiding procedure, at first, the secret text is transformed into a 2-dimensional array. Then, the transformed array is encoded with the DRPE technique and the encoded array is used to construct the hidden data array. Finally, the hidden data array is hidden into the expanded host image with superimposition. The detailed steps involved in this process are described as follows:

Step 1: Transform the secret text into a 2-dimensional array.

In this step, the secret text is transformed into a 2-dimentional array in the form of an image to encode with the DRPE technique. To transform the secret text T into a 2-dimentional array A, T is denoted as a bit stream. The bit stream is stored in the higher bits of the elements in A, while the lower bits of the elements in A are filled with 0 s or 1 s. Each element in A is an integer with a value ranging from 0 and 255 corresponding to 8 bits, which is the same as the pixel value in an 8-bit grayscale image. Thus, the transformed array A can be viewed as a grayscale image. The main reason for using the higher bits instead of the entire set of available bits to store the bit stream of the secret text T is to ensure the recovery accuracy of the secret text, since the DRPE-based information hiding method inherently generates computational errors [28,41]. Assume the secret text T with L ASCII codes is transformed into a 2-dimensional array A with a size of $M \times N$ pixels and the number of the higher bits used to store the bit stream of T is m. Therefore, at least $\frac{8 \times L}{m}$ elements in A will be needed to store the bit stream of T, *i.e.*, $(M \times N) \geq \frac{8 \times L}{m}$.

Step 2: Encode the transformed array with the DRPE technique.

In this step, the transformed array is encoded by using the DRPE technique [2]. The transformed array A with a size of $M \times N$ pixels can be encoded with the DRPE technique to obtain a 2-dimensional complex array A_1 with a size of $M \times N$ pixels as:

$$A_1(x,y) = FT^{-1}\{FT\{A(x,y)\exp[j2\pi n(x,y)]\}\exp[j2\pi b(\xi,\eta)]\} \quad (1)$$

where $n(x,y)$ and $b(\xi,\eta)$ denote two independent random functions, which are uniformly distributed with a range of 0 to 1 and can be taken as the secret key k for encoding. They can be created with the existing random sequence generation methods [1] by using a software, such as MATLAB, with different parameters. FT and FT^{-1} represent the Fourier transform and inverse Fourier transform, respectively. Assume that the encoded complex-valued array A_1 is defined as:

$$A_1 = A_{1R} + jA_{1I} \quad (2)$$

where A_{1R} and A_{1I} are the real part and the imaginary part of A_1, respectively. Both of these arrays are with size of $M \times N$ pixels.

Step 3: Construct the hidden data array.

To hide the encoded complex-valued array into the host image, in this step, the hidden data array is constructed from A_1. There are various ways to construct the hidden data array, which may result in different hiding capacities [28,41]. In reference [28], one element in the real part of A_1, *i.e.*, A_{1R}, and the corresponding element in the imaginary part of A_1, *i.e.*, A_{1I}, were used to construct a 2 × 2 subarray, expressed as:

$$\begin{bmatrix} a1 & -a2 \\ a2 & -a1 \end{bmatrix} \quad (3)$$

where $a1$ is the element in A_{1R}, while $a2$ is the corresponding element in A_{1I}. The hidden data array is composed of these 2 × 2 subarrays. In reference [41], two elements in A_{1R} and one element in A_{1I} are

used sequentially, or one element in A_{1R} and two elements in A_{1I} are used sequentially, to construct the 2 × 2 subarrays, expressed as:

$$\begin{bmatrix} a1 & a2 \\ a3 & 0 \end{bmatrix} \tag{4}$$

where $a1$, $a2$ and $a3$ are the elements taken from A_{1R} or A_{1I}. The hidden data array is composed of these 2 × 2 arrays.

Step 4: Expand the host image.

In this step, the original host image is expanded to hide the hidden data array, which is constructed using the above mentioned procedure. The original host image I with a size of $M_I \times N_I$ pixels is expanded to form another image I_1 with a size of $2M_I \times 2N_I$ pixels by expanding each pixel into a 2 × 2 subarray, such that:

$$\begin{cases} I_1(2x,2y) = I(x,y) \\ I_1(2x,2y+1) = I(x,y) \\ I_1(2x+1,2y) = I(x,y) \\ I_1(2x+1,2y+1) = I(x,y) \end{cases} \tag{5}$$

where x = 0,1,2,…, M_1–1, and y = 0,1,2,…, N_1–1, respectively. According to the procedure of reference [28], to hide the encoded complex-valued $M \times N$ array A_1, a total of MN pixels are needed (*i.e.*, $M_1 = M$ and $N_1 = N$). However, according to the procedure of reference [41], since three values can be hidden in a 2 × 2 subarray, when $M_1 = \left\lceil \sqrt{\frac{2}{3}} \cdot M \right\rceil$ and $N_1 = \left\lceil \sqrt{\frac{2}{3}} \cdot N \right\rceil$, a total of M_1 N_1 pixels are enough to hide A_1, where $\lceil \bullet \rceil$ denotes the ceiling operation.

Step 5: Hide the constructed hidden data array into the expanded host image.

In this step, the constructed hidden data array is hidden into the expanded host image I_1 by superimposing each 2 × 2 subarray in the hidden data array into the corresponding 2 × 2 subarray in I_1 by processing one pixel at a time as shown below:

$$\begin{bmatrix} c1 + \alpha \cdot a1 & c2 - \alpha \cdot a2 \\ c3 + \alpha \cdot a2 & c4 - \alpha \cdot a1 \end{bmatrix} \tag{6}$$

or:

$$\begin{bmatrix} c1 + \alpha \cdot a1 & c2 + \alpha \cdot a2 \\ c3 + \alpha \cdot a3 & c4 \end{bmatrix} \tag{7}$$

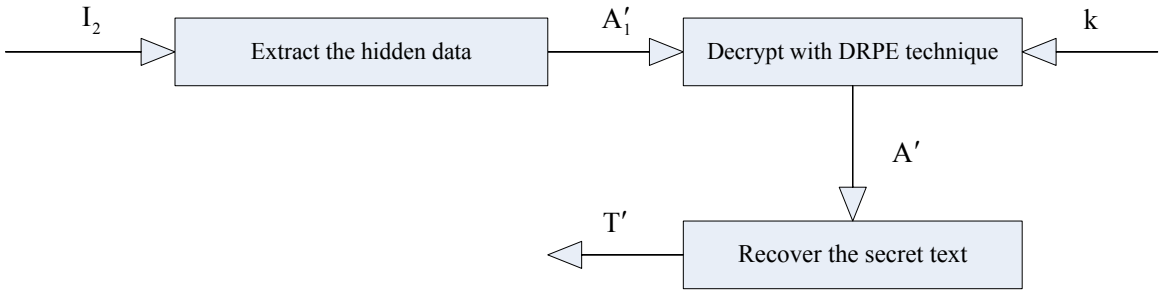
where α is the superimposition coefficient, which corresponds to the embedding strength. Equations (6) and (7) are used in conjunction with Equations (3) and (4), respectively, depending on the method used to construct the hidden data array in Step 3.

As mentioned in Step 4, $c1$, $c2$, $c3$ and $c4$ are obtained by expanding each pixel of the original host image I into a 2 × 2 subarray, *i.e.*, they are identical. By hiding the constructed hidden data array into the expanded host image I_1, the image embedded with hidden data I_2 is obtained.

2.2. Extraction and Recovery Procedure

The extraction and recovery procedure for the proposed technique is shown in Figure 2.

Figure 2. Extraction and recovery procedure.



To recover the secret text from image I_2, which is embedded with the hidden data, first, the hidden data array is extracted from I_2 to reconstruct the encoded array A_1'. Then, A_1' is decrypted by using the DRPE technique to obtain the decrypted array A'. Finally, the secret text T' is recovered from A'. This procedure involves the following steps:

Step 1: Extract the hidden data array from the image embedded with the hidden data.

Depending on whether the hidden data array is constructed with the procedure of reference [28] or that of reference [41], it is easy to extract $a1$ and $a2$ from I_2 using Equations (3) and (6) or extract $a1$, $a2$ and $a3$ from I_2 using Equations (4) and (7), respectively. Due to the inherent computational error, the extracted data may vary slightly from the hidden data.

Step 2: Reconstruct the encoded array.

The data extracted in Step 1 corresponds to the real part or the imaginary part of the complex array encoded with the DRPE technique. With the extracted data, a 2-dimensional complex array A_1' with a size of $M \times N$ pixels can be reconstructed, which corresponds to the encoded array A_1. Due to computational errors, A_1' and A_1 may have slight variations.

Step 3: Decrypt the reconstructed array A_1'.

By decrypting the reconstructed 2-dimensional complex array A_1' with the DRPE technique, an array A' can be obtained, which corresponds to the transformed array A, expressed as:

$$A'(x,y) = FT^{-1}\{FT[A_1'(x,y)]\exp[-j2\pi b(\xi,\eta)]\}\exp[-j2\pi n(x,y)] \tag{8}$$

Due to computational errors, A' and A may have slight variations.

Step 4: Recover the secret text.

In this step, the secret text T' is recovered from the transformed array A' obtained in Step 3 by applying the inverse operation of Step 1 in Section 2.1. Due to computational errors, the recovered secret text T' may have slight variation from the original secret text T. To recover the secret text accurately, the value of m, the method used to fill the lower bits and the value of the superimposition coefficient α should be selected carefully, which are discussed in detail in the following sections.

3. Performance Analysis

In this Section, the performance of the proposed method is investigated by using three criteria, *i.e.*, hiding capacity, recovery accuracy of the secret text, and the quality of the image embedded with hidden data.

3.1. Hiding Capacity

The hiding capacity is defined as the number of the bytes of the secret text T being hidden in a pixel of the image embedded with the hidden data I_2. The hiding capacity is directly related to the number of the higher bits of the elements in the transformed array A to be used for storing the bit stream of the secret text T, and the method of constructing the hidden data array. In a 2-dimensiontal transformed array A with a size of $M \times N$, assuming that m higher bits of the elements are used to store the bit stream of the secret text T, $\left\lfloor \frac{M \times N \times m}{8} \right\rfloor$ bytes of secret text can be stored in A, where $\lfloor \bullet \rfloor$ represents the floor operation. If the hidden data array is constructed according to Equation (3), an array A with a size of $M \times N$ pixels can be hidden into an expanded host image with a size of $2M \times 2N$ pixels. Then, the hiding capacity will be equal to $\frac{\left\lfloor \frac{M \times N \times m}{8} \right\rfloor}{2M \times 2N}$. On the other hand, if the hidden data array is constructed according to Equation (4), an array A with a size of $M \times N$ can be hidden into an expanded host image with a size of $2 \times \left\lceil \sqrt{\frac{2}{3}} \cdot M \right\rceil \times 2 \times \left\lceil \sqrt{\frac{2}{3}} \cdot N \right\rceil$ pixels. Then, the hiding capacity becomes equal to $\frac{\left\lfloor \frac{M \times N \times m}{8} \right\rfloor}{2 \times \left\lceil \sqrt{\frac{2}{3}} \cdot M \right\rceil \times 2 \times \left\lceil \sqrt{\frac{2}{3}} \cdot N \right\rceil}$, where the numerator $\left\lfloor \frac{M \times N \times m}{8} \right\rfloor$ represents the total bytes of the secret text being hidden and the denominator $2 \times \left\lceil \sqrt{\frac{2}{3}} \cdot M \right\rceil \times 2 \times \left\lceil \sqrt{\frac{2}{3}} \cdot N \right\rceil$ represents the total pixels being needed to hide the secret text.

3.2. Recovery Accuracy of the Secret Text

In this paper, the DRPE technique is used to encrypt and hide the desired secret text. The main objective is to accurately recover the hidden secret text. Assume that each character in the secret text is represented by one byte. To assess the secret text recovery result, the recovered secret text T' is compared with the original secret text T via byte-by-byte comparison instead of bit-by-bit comparison. Assume that the length of the secret text T is L bytes, and the number of the accurately recovered bytes is L'. The recovery accuracy (γ) of the secret text is defined as:

$$\gamma = \frac{L'}{L} \tag{9}$$

The recovery accuracy of the secret text is related to the following parameters:

- The number of higher bits of the elements in the transformed array A to be used for storing the bit stream of the secret text T. Due to the computational error inherent in the DRPE-based encoding and hiding technique, the recovered secret text may be slightly different from the original text. The greater the number (m) of higher bits of the elements in the transformed array A used to store the secret text T, the lower the recovery accuracy. To trade off the hiding capacity and the recovery accuracy of the secret text, the value of m must be considered carefully.
- The method used to fill the lower bits of the elements in the transformed array A. Note that the bit stream of the secret text T is stored in the higher bits of the elements in A. To recover the hidden secret text accurately, we may only consider how to accurately recover the higher bits of the elements in A instead of the lower bits. On the other hand, according to the characteristics of the DRPE-based information hiding method [28,41], the values of the elements in the decrypted array A' are usually not very different from those of the original transformed array A. By properly selecting the method used to fill the lower bits of the elements in A, *i.e.*, setting the values of the lower bits properly, the difference between A' and A will only influence the lower bits of the elements, while keeping the higher bits of the elements invariant. Therefore, to ensure the recovery accuracy of the secret text, the method used to fill the lower bits of the elements in A also needs to be considered carefully. It will be discussed with simulation experiments in the next Section.
- The value of the superimposition coefficient α. As discussed in references [28] and [41], the value of the superimposition coefficient α also influences the decrypted array A', which will influence the recovery accuracy of the secret text. The greater the value of α is, the higher the recovery accuracy.

3.3. Quality of the Image Embedded with Hidden Data

The quality of the image embedded with hidden data I_2 is directly related to the value of the superimposition coefficient α. The less the value of α is, the higher the quality of I_2. To trade off the recovery accuracy of the secret text and the quality of I_2, the value of α must be considered carefully.

4. Experimental Results and Discussion

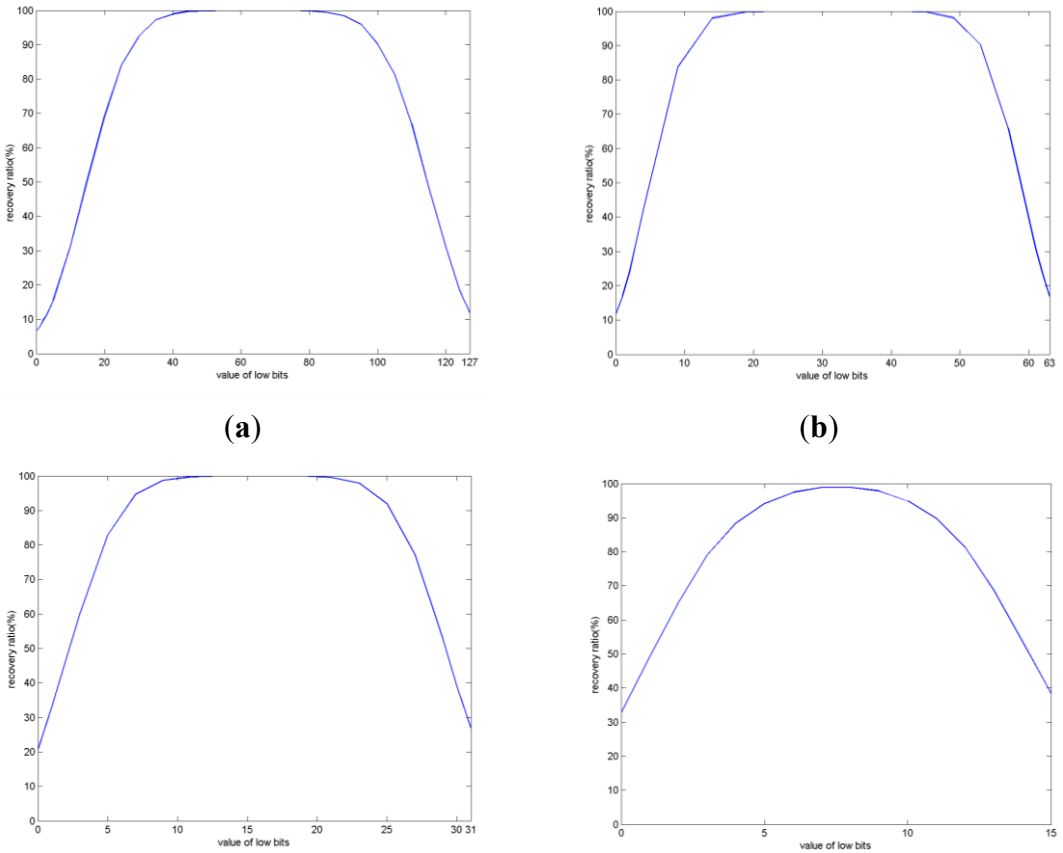
To evaluate the performance of the proposed method, a simulation software was developed for experimentation with real life data. In the experiments, five images each with a size of 256 × 256 pixels were used as the host images as shown in Figure 3 [42]. A passage in English was chosen as the secret text T. Since the recovery accuracy is defined as the ratio of the correctly recovered bytes, any text can be used as the secret text, while not influencing the experimental results significantly. The secret text T was transformed into a 2-dimensional array A by storing the bit stream of T in the higher bits of the elements in the transformed array A. Based on the number of higher bits of the elements in the transformed array A used for storing the bit stream of the secret text T, *i.e.*, the value of m, the hiding capacities of the secret text will be different. The transformed array A was encoded with the DRPE technique to hide into the expanded host images with a size of 512 × 512 pixels.

For simplicity, we only performed the simulation experiments following the hiding method in reference [28].

Figure 3. Images used for simulation experiments (**a**) Baboon. (**b**) Lena. (**c**) Boat. (**d**) Plane. (**e**) Peppers.

(**a**) (**b**) (**c**) (**d**) (**e**)

Figure 4. Recovery accuracies of the secret text with different methods being used to fill the lower bits of the elements in the transformed array *A*. The host image is Lena (**a**) m = 1, α = 0.02. (**b**) m = 2, α = 0.05. (**c**) m = 3, α = 0.08. (**d**) m = 4, α = 0.10.



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

(**c**) (**d**)

If *m* higher bits of the elements in the transformed array *A* are used to store the bit stream of the secret text *T*, while the remaining 8 – m lower bits are filled with 0 s or 1 s, the value of the 8 – m lower bits may range from 0 to $2^{8-m} - 1$. Figure 4 shows the experimental results corresponding to the recovery accuracies of the secret text when different methods are used to fill the lower bits of the elements in the transformed array *A*. The Lena image shown in Figure 3(b) is used as the host image.

From the experimental results shown in Figure 4, it is evident that the recovery accuracy is higher when the value of the lower bits is closer to 2^{7-m}. Our experimentation with other host images generated similar results. The reason for such results may be explained as follows: (1) Due to computational errors existing during the procedure of encoding, embedding, extraction and decryption of DRPE based information hiding, slight difference may exist between the decrypted array A' and the original transformed array A; (2) Since the bit stream of the secret text T is stored in the higher bits of the elements in the transformed array A, to increase the recovery accuracy, the influence of the computational errors to the higher bits of the elements in the transformed array should be decreased mostly; (3) If the value of the lower bits of the elements in the transformed array A is around 2^{7-m}, the higher bits of decrypted value will be invariant compared to those of the original value with the maximum possible, either the decrypted value is greater than or less than the original one. For example, when $m = 2$, the value of the lower bits of an element may range from 0 to 63. If we set the value of the lower bits to 32, then when the difference of the decrypted value and the original one is between –32 and 31, the 2 highest bits will be invariant. Therefore, if m higher bits of the elements in the transformed array A are used to store the bit stream of the secret text T. To obtain higher recovery accuracy of the secret text, it is better to set the values of the lower bits of the elements in A to around 2^{7-m}.

From Figure 4, it is evident that the number of higher bits (m) of the elements in the transformed array A being used to store the bit stream of the secret text T significantly influences the recovery accuracy of the secret text T. The less the value of m, the higher the recovery accuracy. The corresponding experimental results are shown in Table 2, where the values of m are set to 1, 2, 3, and 4, respectively. The values of the lower bits in the transformed array A are set to 2^{7-m} to maximize the recovery accuracies of the secret text T. The results in Table 2 include the recovery accuracies of the secret text T obtained by using Lena as the host image and the average recovery accuracies obtained by using the five images shown in Figure 3 as the host images.

With greater value of m, the recovery accuracy of the secret text is less, especially when the values of α are identical. For a fair comparison, the values of α should be identical, since they are also related to the recovery accuracy. For example, when $m = 1$, the value of the lower bits is 64, and $\alpha = 0.02$, the recovery accuracy approaches 100% by using Lena as the host image. For $m = 2$, the value of the lower bits is 32, and $\alpha = 0.02$, the recovery accuracy is 91.6687% by using Lena as the host image. However, for $m = 2$, the value of the lower bits is 32, and $\alpha = 0.05$, the recovery accuracy becomes 100% by using Lena as the host image. Finally, when $m = 3$, the value of the lower bits is 16, and $\alpha = 0.05$, the recovery accuracy is 98.697917% by using Lena as the host image. Our experimentation with other host images yielded similar results. Therefore, when transforming the secret text T into the 2-dimentional array A, the bit stream of T should be stored into the higher bits of elements in A as much as possible.

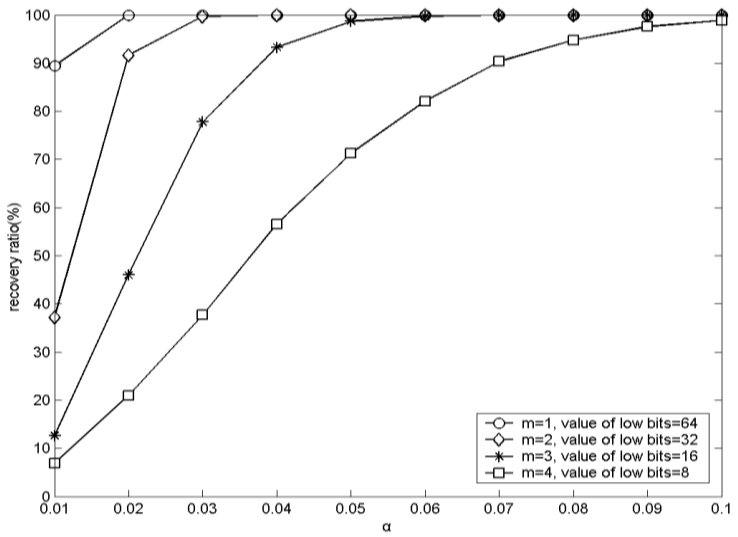
The experimental results corresponding to the recovery accuracies with different values of α by using Lena as the host image are shown in Figure 5. From Figure 5, it is evident that the greater the value of α, the higher the recovery accuracy. The experiments with other host images generated similar results. Due to the inherent characteristics of the DRPE based information hiding, with larger value of α, the decrypted array A' will be closer to the original transformed array A. Thus, the higher bits of the

elements in A' will be closer to those of the elements in A. Therefore, to obtain higher recovery accuracy, the value of α should be as high as possible.

Table 2. Recovery accuracies of the secret text T with different values of m. The values of the lower bits are set to 2^{7-m}.

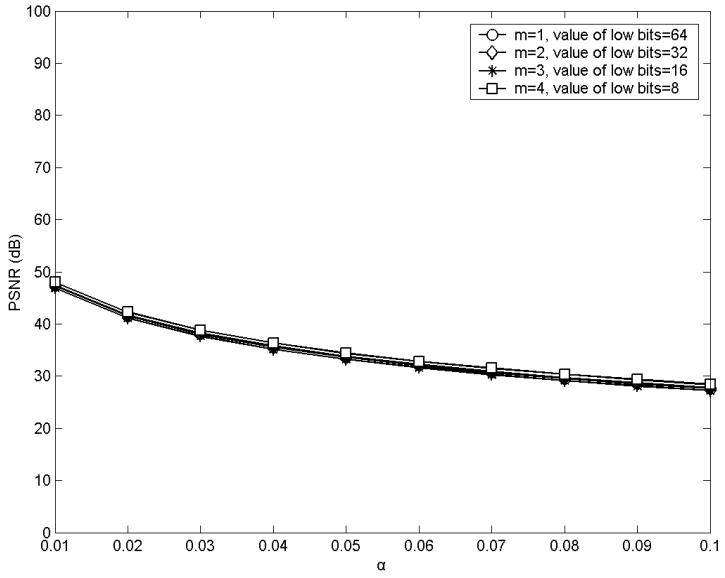
Value of m	m = 1			
Value of lower bits	64			
Value of α	α = 0.02		α = 0.05	
Host image	Lena	average	Lena	average
Recovery accuracy (%)	100	100	100	100
Value of m	m = 2			
Value of lower bits	32			
Value of α	α = 0.02		α = 0.05	
Host image	Lena	average	Lena	Average
Recovery accuracy (%)	91.6687	91.5759	100	100
Value of m	m = 3			
Value of lower bits	16			
Value of α	α = 0.05		α = 0.08	
Host image	Lena	average	Lena	Average
Recovery accuracy (%)	98.697917	98.2568	100	99.6997
Value of m	m = 4			
Value of lower bits	8			
Value of α	α = 0.08		α = 0.10	
Host image	Lena	average	Lena	Average
Recovery accuracy (%)	94.8029	91.7242	98.8617	94.6265

Figure 5. Recovery accuracies of the secret text T with different values of α by using Lena as the host image.



The experimental results corresponding to the qualities of the images embedded with hidden data may be determined by using the peak-signal-noise-ratio (PSNR) as a performance parameter. Figure 6 depicts these results for different values of α by using Lena as the host image.

Figure 6. The qualities of the images embedded with hidden data with different values of α by using Lena as the host image.



From Figure 6, it is obvious that the greater the value of α, the lower the quality of the image embedded with hidden data. Therefore, to obtain higher quality of the image embedded with hidden data, the value of α should be lower.

Based on the above mentioned results, we can infer the following:

(1) To increase the hiding capacity, the value of *m* should be higher;
(2) To increase the recovery accuracy, the value of *m* should be lower, while the value of α should be higher;
(3) Whatever the value of *m* is, the value of the lower bits of the elements in the transformed array should be set at around 2^{7-m} to obtain higher recovery accuracy;
(4) To increase the quality of the image embedded with hidden data, the value of α should be lower.

Thus, to increase the hiding capacity, the value of *m* should be higher, which may decrease the recovery accuracy. To increase the recovery accuracy, the value of α should be higher, which may decrease the quality of the image embedded with hidden data. Therefore, based on the secret text to be hidden, one may adjust the values of *m* and α to tradeoff the hiding capacity, the recovery accuracy and the quality of the image embedded with hidden data. After ensuring the hiding capacity, the value of *m* may be set as low as possible to increase the recovery accuracy. For example, when the value of *m* is set to 1, if it is enough to store all of the secret text information bits, then it is not necessary to set $m = 2$ to store some secret text information bits into the second highest bits of the elements in the transformed array. After ensuring the recovery accuracy, the value of α may be set as low as possible to increase the quality of the image embedded with hidden data. For example, for $m = 1$ and $\alpha = 0.02$, or $m = 2$ and $\alpha = 0.05$, and the value of the lower bits is set to 2^{7-m}, the recovery accuracy will be 100%. Therefore, to increase the quality of the image embedded with hidden data, for $m = 1$, the value of α should not be greater than 0.02; while for $m = 2$, the value of α should not be greater than 0.05.

To demonstrate the above analysis and conclusions more clearly, some images obtained in the simulation experiments are shown below. Here, we show the arrays transformed from the secret text

with, the images embedded with hidden data and the recovered transformed arrays. The arrays encoded with the DRPE technique are random resulting from the characteristics of the DRPE technique [2]. So, we did not show the arrays encoded with the DRPE technique. In addition, there are some parameters being used in the proposed method, such as the number (m) of the higher bits used to store the bit stream of the secret text, the method used to fill the lower bits in the transformed array and the value of the superimposition coefficient α. They may combine with different values, resulting in many combinations. Using image Lena as the host image, the representative results of m = 1, 2, 3, 4 corresponding to α = 0.02, 0.05, 0.08, 0.10, while setting the value of the lower bits of the elements in the transformed array to 2^{7-m} are shown from Figure 7 to Figure 10. Since it is hard to recognize the recovery accuracy of the secret text from the image of the recovered transformed array, we also give the values of the recovery accuracies.

Figure 7. (**a**) The array transformed from the secret text with m = 1. (**b**) The image embedded with hidden data with α = 0.02. (**c**) The recovered transformed array. The recovery accuracy is 100%.

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

Figure 8. (**a**) The array transformed from the secret text with m = 2. (**b**) The image embedded with hidden data with α = 0.05. (**c**) The recovered transformed array. The recovery accuracy is 100%.

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

Figure 9. (**a**) The array transformed from the secret text with m = 3. (**b**) The image embedded with hidden data with α = 0.08. (**c**) The recovered transformed array. The recovery accuracy is 100%.

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

Figure 10. (**a**) The array transformed from the secret text with m = 4. (**b**) The image embedded with hidden data with α = 0.10. (**c**) The recovered transformed array. The recovery accuracy is 98.86%.

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

5. Conclusions

The main purpose of this paper is to apply the DRPE-based image hiding method to text encryption and hiding. In this technique, the secret text is transformed to a 2-dimensional array by storing the text bit stream in the higher bits of the transformed array. The transformed array can be viewed as an image. The DRPE-based image hiding technique is used to encode and hide the transformed array to an expanded host image.

Detailed analytical and experimental results show that: (1) the greater number (m) of the higher bits of the elements in the transformed array to be used for storing the bit stream of the secret text results in higher hiding capacity and lower recovery accuracy; (2) the greater value of the superimposition coefficient α results in higher recovery accuracy and lower quality of the image embedded with hidden data; (3) setting the value of the lower bits of the elements in the transformed array to approximately 2^{7-m} results in the best recovery accuracy. By adjusting the values of m and α properly, one may achieve the optimal hiding capacity, recovery accuracy and quality of the image embedded with hidden data.

The proposed method combines the optical information processing technique by applying optical information hiding method to text encryption and hiding, which increases the security of the secret text and takes use of the advantages of optical information processing technique. In addition, it ensures acceptable hiding capacity and recovery accuracy of the secret text.

Acknowledgments

This work was supported by National Natural Science Foundation of China (No. 60972105), Natural Science Foundation Project of CQ CSTC (No. 2009BB2210)

References

1. Schneier, B. *Applied Cryptography*, 2nd ed.; John Wiley & Sons: New York, NY, USA, 1996.
2. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769.
3. Lu, P.; Xu, Z.; Lu, X.; Liu, X. Digital image information encryption based on compressive sensing and double random-phase encoding technique. *Optik* **2012**, doi:10.1016/j.ijleo.2012.08.017.
4. Abuturab, M.R. Color image security system using double random-structured phase encoding in gyrator transform domain. *Appl. Opt.* **2012**, *51*, 3006–3016.
5. Zhong, Z.; Chang, J.; Shan, M.; Hao, B. Double image encryption using double pixel scrambling and random phase encoding. *Opt. Commun.* **2012**, *285*, 584–588.
6. He, Y.; Cao, Y.; Lu, X. Color image encryption based on orthogonal composite grating and double random phase encoding technique. *Optik* **2012**, *123*, 1592–1596.
7. Mosso, F.; Tebaldi, M.; Torroba, R.; Bolognini, N. Double random phase encoding method using a key code generated by affine transformation. *Optik* **2011**, *122*, 529–534.
8. Unnikrishnan, G.; Joseph, J.; Singh, K. Optical encryption by double random phase encoding in the fractional Fourier domain. *Opt. Lett.* **2000**, *25*, 887–889.
9. Jin, W.; Yan, C. Optical image encryption based on multichannel fractional Fourier transform and double random phase encoding technique. *Optik* **2007**, *118*, 38–41.
10. Wang, Q.; Guo, Q.; Zhou, J. Double image encryption based on linear blend operation and random phase encoding in fractional Fourier domain. *Optics Commun.* **2012**, *285*, 4317–4323.
11. Liu, Z.; Li, S.; Liu, W.; Wang, Y.; Liu, S. Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. *Opt. Laser Eng.* **2012**, doi:10.1016/j.optlaseng.2012.08.004.
12. Liu, Z.; Xu, L.; Dai, J.; Liu, S. Image encryption by using local random phase encoding in fractional Fourier transform domains. *Optik* **2012**, *123*, 428–432.
13. Situ, G.; Zhang, J. Double random phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586.
14. Yuan, S.; Xin, Y.; Liu, M.; Yao, S.; Sun, X. An improved method to enhance the security of double random-phase encoding in the Fresnel domain. *Opt. Laser Eng.* **2012**, *44*, 51–56.
15. Javidi, B.; Nomura, T. Securing information by use of digital holography. *Opt. Lett.* **2000**, *25*, 28–30.
16. Das, B.; Yelleswarapu, C.S.; Rao, D.V.G.L.N. Dual-channel in-line digital holographic double random phase encryption. *Opt. Commun.* **2012**, *285*, 4262–4267.

17. Katzenbeisser, S.; Petitcolas, F. *Information Hiding Techniques for Steganography and Digital Watermarking*; Artech House: Norwood, MA, USA, 1999.
18. Bender, W.; Gruhl, D.; Morimoto, N. Techniques for data hiding. *Proc. SPIE* **1995**, *2420*, 164–173.
19. Wu, D.C.; Tsai, W.H. Spatial-domain image hiding using image differencing. *IEE Proc. Vis. Image Signal Process.* **2000**, *147*, 29–37.
20. Cox, I.J.; Kilian, J.; Leighton, F.T.; Shamoon, T. Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process.* **1997**, *6*, 1673–1687.
21. Ruanaidh, J.J.K.O.; Dowling, W.J.; Boland, F.M. Phase watermarking of digital images. In *Proceedings of IEEE International Conference on Image Processing*, Lausanne, Switzerland, 16–19 September 1996; pp. 239–242.
22. Piva, A.; Barni, M.; Bartolini, F.; Cappellini, V. DCT-based watermark recovering without resorting to the uncorrupted original images. In *Proceedings of IEEE International Conference on Image Processing*, Santa Barbara, CA, USA, 26–29 October 1997; pp. 520–523.
23. Barni, M.; Bartolini, F.; Cappellini, V.; Piva, A. DCT-domain system for robust image watermarking. *Signal Process.* **1998**, *66*, 357–372.
24. Xia, X.; Boncelet, C.G.; Arce, G.R. Wavelet transform based watermark for digital images. *Opt. Express* **1998**, *3*, 497–511.
25. Barni, M.; Bartolini, F.; Piva, A. Improved wavelet-based watermarking through pixel-wise masking. *IEEE Trans. Image Process*. **2001**, *10*, 783–791.
26. Rosen, J.; Javidi, B. Hidden Images in Halftone Pictures. *Appl. Opt.* **2001**, *40*, 3346–3353.
27. Kishk, S.; Javidi, B. Information hiding technique with double phase encoding. *Appl. Opt.* **2002**, *41*, 5462–5470.
28. Zhou, X.; Lai, D.; Yuan, S.; Li, D.; Hu, J. A method for hiding information utilizing double-random phase encoding technique. *Opt. Laser Tech.* **2007**, *39*, 1360–1363.
29. Takai, N.; Mifune, Y. Digital watermarking by a holographic technique. *Appl. Opt.* **2002**, *41*, 865–873.
30. Cai, L.; He, M.; Liu, Q.; Yang, X. Digital Image Encryption and Watermarking by Phase-Shifting Interferometry. *Appl. Opt.* **2004**, *43*, 3078–3084.
31. He, M.; Cai, L.; Liu, Q.; Yang, X. Phase-only encryption and watermarking based on phase-shifting interferometry. *Appl. Opt.* **2005**, *44*, 2600–2606.
32. Chang, H.T.; Tsan, C.L. Image watermarking by use of digital holography embedded in the discrete-cosine-transform domain. *Appl. Opt.* **2005**, *44*, 6211–6219.
33. Zhou, X.; Chen, L.; Shao, J. Investigation of digital hologram watermarking with double binary phase encoding. *Opt. Eng*. **2005**, *44*, doi:10.1117/1.1935268.
34. Shi, Y.; Situ, G.; Zhang, J. Optical image hiding in the Fresnel domain. *J. Opt. Pure Appl. Opt*. **2006**, *8*, 569–577.
35. Shi, Y.; Situ, G.; Zhang, J. Multiple-image hiding in the Fresnel domain. *Opt. Lett.* **2007**, *32*, 1914–1916.
36. Kim, K.T.; Kim, J.H.; Kim, E.S. Multiple information hiding technique using random sequence and Hadamard matrix. *Opt. Eng.* **2001**, *40*, 2489–2494.

37. Kim, J.J.; Choi, J.H.; Kim, E.S. Optodigital implementation of multiple information hiding and extraction system. *Opt. Eng*. **2004**, *43*, 113–125.
38. He, M.; Cai, L.; Liu, Q.; Wang, X.; Meng, X. Multiple image encryption and watermarking by random phase matching. *Opt. Commun.* **2005**, *247*, 29–37.
39. Salomon, D. *Data Privacy and Security: Encryption and Information Hiding*; Springer: New York, NY, USA, 2003.
40. Lin, K.T. Hybrid encoding method for hiding information by assembling double-random phase-encoding technique and binary encoding method. *Appl. Opt.* **2010**, *49*, 3814–3820.
41. Sang, J.; Xiang, H.; Sang, N.; Fu, L. Increasing the data hiding capacity and improving the security of a double-random phase-encoding technique based information hiding scheme. *Opt. Commun.* **2009**, *282*, 2713–2721.
42. USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 28 September 2012).