Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 603659, 8 pages
http://dx.doi.org/10.1155/2014/603659

Research Article

Hiding a Covert Digital Image by Assembling the RSA Encryption Method and the Binary Encoding Method

Kuang Tsan Lin[1] and Sheng Lih Yeh[2]

[1] *Department of Mechanical and Computer Aided Engineering, St. John's University, 499 Sec. 4, Tam King Road, Tamsui, New Taipei City 25135, Taiwan*
[2] *Department of Mechanical Engineering, Lunghwa University of Science and Technology, 300 Sec. 1, Wanshou Road, Kueishan, Taoyuan County 33306, Taiwan*

Correspondence should be addressed to Sheng Lih Yeh; slyeh@mail.lhu.edu.tw

Received 16 September 2013; Accepted 29 November 2013; Published 13 March 2014

Academic Editor: Chung-Hao Chen

Copyright © 2014 K. T. Lin and S. L. Yeh. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Rivest-Shamir-Adleman (RSA) encryption method and the binary encoding method are assembled to form a hybrid hiding method to hide a covert digital image into a dot-matrix holographic image. First, the RSA encryption method is used to transform the covert image to form a RSA encryption data string. Then, all the elements of the RSA encryption data string are transferred into binary data. Finally, the binary data are encoded into the dot-matrix holographic image. The pixels of the dot-matrix holographic image contain seven groups of codes used for reconstructing the covert image. The seven groups of codes are identification codes, covert-image dimension codes, covert-image graylevel codes, pre-RSA bit number codes, RSA key codes, post-RSA bit number codes, and information codes. The reconstructed covert image derived from the dot-matrix holographic image and the original covert image are exactly the same.

1. Introduction

Image hiding methods can encode covert images in the space domain or in the spatial frequency domain. For space-domain encoding cases, hidden covert images can be reconstructed without any distortion usually, but their hiding security is lower often. On the other hand, for spatial-frequency-domain encoding cases, their hiding security is higher often, but there is more or less distortion for reconstructed covert images usually. Because spatial-frequency-domain encoding cases cannot reconstruct exact covert images, this paper will focus on space-domain encoding cases only. Of course, both higher security and higher noise-attack resistance are discussed here.

Many methods for hiding covert images in the space domain have been proposed. Image-transform method [1–4], cellular automata method [5], chaotic sequence method [6], image-scrambling method [7, 8], light separation method [9, 10], histogram shifting method [11, 12], and communication channel method [13] are some examples. All the methods can work well, but most of them can be applied to printed or digital images only, whereas holographic images have become very popular and they appear on credit cards and bills. Therefore, other methods for hiding covert images on holographic holograms are needed. This paper will propose a hybrid hiding method to satisfy the requirement. The proposed method transforms a covert image with the Rivest-Shamir-Adleman (RSA) encryption method and encodes the transformed data into a dot-matrix holographic image with the binary encoding method.

The RSA encryption method is widely used in electronic document security. The RSA encryption method needs keys n, e, and d to encode and decode data [14–19]. The RSA encryption method usually uses very huge key n, which is, more than 100 bits, for assuring enough high security, so it is troublesome work to use the method. This paper will assemble the RSA encryption method and the binary encoding method [20] to allow keys with only tens of bits to be used and enough high security is still assured. The RSA encryption method includes three steps. Firstly, it

transforms a covert image to form a data string. Secondly, it transforms the data string to form a RSA encryption data string by using the standard RSA encryption method according to encryption keys. Finally, it transforms the RSA encryption data string to form an array. On the other hand, the binary encoding method uses binary data to denote all the element values of the RSA encryption string and encodes the binary data into a dot-matrix holographic image [21]. The pixels of the covert image contain seven groups of binary codes used for decoding the RSA encryption string. The seven groups of codes are identification codes, covert-image dimension codes, covert-image graylevel codes, pre-RSA bit number codes, RSA key codes, post-RSA bit number codes, and information codes. The RSA encryption string can be decoded directly from the dot-matrix holographic image.

Because the proposed hybrid hiding method possesses two layers of security (one layer is from the RSA encryption method and the other layer is from the binary encoding method), it can protect covert images very well. Unauthorized people can hardly reconstruct covert images correctly, but authorized people can easily reconstruct covert images correctly. Most of all, covert image reconstruction does not cause image distortion.

2. Theory

2.1. Reviewing the RSA Encryption Method. Assume that **C** is an $M \times N$ 2^g-graylevel covert image for encoding, and assume that **D** is an $M \times N$ matrix transformed by the RSA encryption method. For using the RSA encryption method, three keys (integers) are needed and the three keys are denoted by n, e, and d. The key n is an integer formed by the multiplication of two unequal prime numbers p and q; that is,

$$n = p \times q. \tag{1}$$

Let an integer r be formed by

$$r = (p-1) \times (q-1). \tag{2}$$

Then the key e should be an integer between 2 and r, that is, $2 < e < r$, and the highest common factor of e and r is 1. The key d is derived when the remainder for the division $(e \times d)/r$ equals 1; that is,

$$1 \equiv (e \times d) \bmod r, \tag{3}$$

where the symbol "mod" denotes the modulus-after-division operation.

The keys for the encoding and decoding are used as below.

(1) An integer s (before the RSA encoding) modulated by the RSA encryption must be smaller than n.

(2) Another integer t (after the RSA encoding) is derived from the RSA encryption modulation of the integer s according to

$$t \equiv s^e \bmod n. \tag{4}$$

(3) The integer s can be derived from the RSA encryption modulation of the integer t according to

$$s \equiv t^d \bmod n. \tag{5}$$

Equations (6a) and (6b) are an illustration to explain the RSA encryption processes for a 3×4 matrix. Equation (6a) is a matrix **C** before the RSA encoding and (6b) is a matrix **D** after the RSA encoding, where the keys n, e, and $d =$ 55, 13, and 37). Every element s in **C** and its corresponding element t in **D** have the relationships as described by (4) and (5):

$$\mathbf{C} = \begin{bmatrix} 9 & 2 & 22 & 27 \\ 28 & 33 & 17 & 10 \\ 5 & 34 & 12 & 14 \end{bmatrix}, \tag{6a}$$

$$\mathbf{D} = \begin{bmatrix} 14 & 52 & 22 & 37 \\ 18 & 33 & 7 & 10 \\ 15 & 34 & 12 & 49 \end{bmatrix}. \tag{6b}$$

2.2. The Hybrid Hiding Method. Let **T** be a $P \times Q$ matrix to encode an $M \times N$ covert image **C**, and let **H** be a $P \times Q$ holographic image for hiding the matrix **T**. All the binary data encoded in the matrix **T** are binary codes and they are categorized into seven groups of codes, identification codes, covert-image dimension codes, covert-image graylevel codes, pre-RSA bit number codes, RSA key codes, post-RSA bit codes, and information codes. Identification codes are used to judge if the codes encoded in the matrix **T** belong to the binary encoding method or not; covert-image dimension codes M and N are used to denote the size of the covert image; covert-image graylevel codes 2^g are used to denote the graylevels of the covert image; pre-RSA bit number codes are used to denote the number of bits corresponding to every element of a data string before the RSA encryption; RSA key codes are used for the RSA encoding and decoding; and post-RSA bit number codes are used to denote the number of bits corresponding to every element of a data string after the RSA encryption. All the above six groups of codes are located at the first row of the matrix **T**. Information codes are used to denote the binary data encoded from the data string after the RSA encryption and they are located at the second to final rows of the matrix **T**.

To avoid using too many similar equations in this paper, an equation for plural uses is defined as

$$k = \sum_{i=1}^{T} k_i \cdot 2^{i-1} + k_0, \tag{7}$$

where k is an integer; all $k_1, k_2, \ldots$, and k_T are 0 or 1; and k_0 is another integer.

Identification codes are a set of private binary codes used to judge if the data hidden in the covert image is encoded with the binary encoding method or not. The bit amount of the codes has to be big enough, for example, 1111001111001010110000110000 with 28 bits. The codes locate at bits 1~28 in the first row of the matrix **T**.

Covert-image dimension codes M and N are used to derive the size $M \times N$ of the covert image, and they include

two sets of ten binary codes. The parameter M is indicated by the first set of ten binary codes $M_1, M_2, \ldots, M_9$, and M_{10}. The relationship of M and $M_1 \sim M_{10}$ is similar to (7), but every k has to be replaced by M, and $M_0 = 3$ and $T = 10$. The parameter N is indicated by the second set of ten binary codes $N_1, N_2, \ldots, N_9$, and N_{10}. The relationship of N and $N_1 \sim N_{10}$ is similar to (7), but every k has to be replaced by N, and $N_0 = 3$ and $T = 10$. The codes locate at bits 29~48 in the first row of the matrix **T**.

Covert-image graylevel codes are used to derive the parameter g corresponding to the 2^g graylevels of the covert image. The parameter g is indicated by six binary codes g_1, g_2, g_3, g_4, g_5, and g_6. The relationship of g and $g_1 \sim g_6$ is similar to (7), but every k has to be replaced by g, and $g_0 = 1$ and $T = 6$. The codes locate at bits 49~54 in the first row of the matrix **T**.

Pre-RSA bit number codes are used to denote the number of bits b corresponding to every element of a data string for the RSA encryption process. The parameter b is indicated by six binary codes b_1, b_2, b_3, b_4, b_5, and b_6. The relationship of b and $b_1 \sim b_6$ is similar to (7), but every k has to be replaced by b, and $b_0 = 1$ and $T = 6$. The codes locate at bits 55~60 in the first row of the matrix **T**.

RSA key codes are used to denote the keys n and d. Although three keys n, e, and d are needed for encoding and decoding data strings, e is needed for the encoding only. The key n is indicated by thirty-five binary codes $n_1, n_2, \ldots, n_{34}$, and n_{35}. The relationship of n and $n_1 \sim n_{35}$ is similar to (7), but every k has to be replaced by n, and $n_0 = 100$ and $T = 35$. The codes locate at bits 61~95 in the first row of the matrix **T**. The key d is indicated by thirty-five binary codes $d_1, d_2, \ldots, d_{34}$, and d_{35}. The relationship of d and $d_1 \sim d_{35}$ is similar to (7), but every k has to be replaced by d, and $d_0 = 2$ and $T = 35$. The codes locate at bits 96~130 in the first row of the matrix **T**.

Post-RSA bit number codes are used to specify the number of bits a corresponding to every element of the RSA encryption data string. The parameter a is indicated by six binary codes a_1, a_2, a_3, a_4, a_5, and a_6. The relationship of a and $a_1 \sim a_6$ is similar to (7), but every k has to be replaced by a, and $a_0 = 2$ and $T = 6$. The codes locate at bits 131~136 in the first row of the matrix **T**.

Information codes are used to reconstruct the RSA encryption data string for decoding the covert image **C**.

2.3. Encoding Processes. The processes to encode the $M \times N$ covert image **C** into the $P \times Q$ holographic image **H** are explained below.

(1) Set a binary-data array **R** with $1 \times Q$ elements. The elements of **R** are copied from identification codes (for the first range), covert-image dimension codes (for the second range), covert-image graylevel codes (for the third range), pre-RSA bit number codes (for the fourth range), RSA key codes (for the fifth range), and post-RSA bit number codes (for the sixth range), whereas the other elements of **R** not copied from the six groups of codes are all set as 0.

(2) The elements of the $M \times N$ covert image **C** are copied to form the elements (from the left side to the right side) of a string **A** with $M \times N$ elements from the first row to the last row (the first priority) and from the left side to the right side (the second priority).

(3) Decompose every element $\mathbf{A}(k)$ of **A** into g (because the covert image possesses 2^g graylevels) binary codes $c_i(k)$ $(i = 0, 1, \ldots, g-1)$ according to

$$\mathbf{A}(k) = \sum_{i=0}^{g-1} c_i(k) \times 2^i. \tag{8}$$

(4) Create a binary-data string **B** with $M \times N \times g$ elements according to

$$\mathbf{B}\left(i + g \times (k-1)\right) = c_i(k), \tag{9}$$

where $1 \le k \le M \times N$ and $0 \le i \le g-1$.

(5) Create a data string **E** with $M \times N \times g/b$ elements from the $M \times N \times g$ elements of the binary-data string **B** (all b bits of binary data are used to form an element of the data string for the RSA encryption) according to

$$\mathbf{E}(k) = \sum_{m'=1}^{b} \mathbf{B}\left(b \times (k-1) + m'\right) \times 2^{b-m'}, \tag{10}$$

where $1 \le k \le M \times N \times g/b$.

(6) Transform the data string **E** with $M \times N \times g/b$ elements to a data string **F** with $M \times N \times g/b$ elements by using (4) with the keys n and e.

(7) Decompose every element $\mathbf{F}(k)$ of **F** into a binary codes $f_i(k)$ $(i = 0, 1, \ldots, a-1)$ (all a bits of binary data are used to denote every element of the RSA encryption data string) according to

$$\mathbf{F}(k) = \sum_{i=0}^{a-1} f_i(k) \times 2^i, \tag{11}$$

where $1 \le k \le M \times N \times g \times a/b$.

(8) Create a binary-data string **G** with $M \times N \times g \times a/b$ elements according to

$$\mathbf{G}\left(i + g \times (k-1)\right) = f_i(k), \tag{12}$$

where $1 \le k \le M \times N \times g/b$ and $0 \le i \le a-1$.

(9) Copy all of the $M \times N \times g \times a/b$ binary elements of **G** (from the left side to the right side) to form a $(P-1) \times Q$ binary-data matrix **S** (from the first row to the last row and from the left side to the right side). Since the amount $M \times N \times g \times a/b$ of the elements of **G** is smaller than $(P-1) \times Q$, there are $(P-1) \times Q - M \times N \times g \times a/b$ elements in **S** not copied from the elements of **G**. The values of these extra elements are all set as 0.

(10) Combine the $1 \times Q$ binary-data array **R** and the $(P-1) \times Q$ binary-data matrix **S** to form a $P \times Q$ binary-data matrix **T**. The first row of **T** comes from **R**, and the other rows of **T** come from **S**.

(11) Hide the $P \times Q$ binary-data matrix **T** into the $P \times Q$ dot-matrix holographic image **H** with the specified grating dot feature [21].

Equations (13a)–(13i) illustrate an example of the encoding processes. The binary-data array **R** with 1×6 elements is

shown in (13a), the covert matrix **C** is shown in (13b), the data string **A** is shown in (13c), the binary-data string **B** is shown in (13d), the data string **E** is shown in (13e), the RSA encryption data string **F** with the keys $(n, e) = (55, 13)$ is shown in (13f), the binary-data string **G** is shown in (13g), the binary-data matrix **S** is shown in (13h), and the binary-data matrix **T** is shown in (13i):

$$\mathbf{R} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \tag{13a}$$

$$\mathbf{C} = \begin{bmatrix} 2 & 7 \\ 3 & 6 \end{bmatrix}, \tag{13b}$$

$$\mathbf{A} = \begin{bmatrix} 2 & 7 & 3 & 6 \end{bmatrix}, \tag{13c}$$

$$\mathbf{B} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}, \tag{13d}$$

$$\mathbf{E} = \begin{bmatrix} 5 & 13 & 14 \end{bmatrix}, \tag{13e}$$

$$\mathbf{F} = \begin{bmatrix} 15 & 8 & 49 \end{bmatrix}, \tag{13f}$$

$$\mathbf{G} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \tag{13g}$$

$$\mathbf{S} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{13h}$$

$$\mathbf{T} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{13i}$$

2.4. Decoding Processes. The processes for reconstructing the covert image $\mathbf{C}^*$ from the dot-matrix holographic image **H** are explained below.

(1) Determine every element $\mathbf{T}(i, j)$ of the $P \times Q$ binary-data matrix **T** from every grating dot feature of the $P \times Q$ dot-matrix holographic image **H** according to the specified grating dot feature.

(2) Check the identification codes located at bits 1~28 in the first row of **T** to judge whether the covert image $\mathbf{H}^*$ contains codes encoded by the binary encoding method or not.

(3) According to the codes located at bits 29–136 in the first row of **T** decode the parameters M, N, g, n, d, b, and a.

(4) Copy the first $M \times N \times g \times a/b$ elements in the second to final rows (from the top to the bottom and from the left side to the right side) of **T** to form the $M \times N \times g \times a/b$ elements (from the left side to the right side) of the binary-data string **G**.

(5) Create the data string **F** with $M \times N \times g/b$ elements from the elements of the $M \times N \times g \times a/b$ binary-data matrix **G** according to

$$\mathbf{F}(k) = \sum_{m'=1}^{a} \mathbf{G}\left(a \times (k-1) + m'\right) \times 2^{a-m'}, \tag{14}$$

where $1 \le k \le M \times N \times g/b$.

(6) Transform the data string **F** with $M \times N \times g/b$ elements to a data string **E** with $M \times N \times g/b$ by using (5) with the keys n and d.

(7) Decompose every element $\mathbf{E}(k)$ of **E** into b binary codes $h_i(k)$ $(i = 0, 1, \ldots, a-1)$ according to

$$\mathbf{E}(k) = \sum_{i=0}^{b-1} h_i(k) \times 2^i \tag{15}$$

and form a binary-data matrix **B** with $M \times N \times g$ elements according to

$$\mathbf{B}(i(b-1) + k) = h_i(k), \tag{16}$$

where $0 \le k \le a-1$.

(8) Create a data string **A** with $M \times N$ elements from the elements of the $M \times N \times g$ binary-data matrix **B** according to

$$\mathbf{A}(k) = \sum_{m'=1}^{g} \mathbf{B}\left(g \times (k-1) + m'\right) \times 2^{g-m'}, \tag{17}$$

where $1 \le k \le M \times N$.

(9) Create the $M \times N$ matrix **C** from the data string **A** with $M \times N$ elements according to

$$\mathbf{C}(i, j) = \mathbf{A}\left((i-1) \times N + j\right), \tag{18}$$

where $1 \le i \le M$ and $1 \le j \le N$.

(a) (b)

Figure 1: Covert images for simulations. (a) A 64 × 64 128-graylevel image; (b) a 128 × 128 binary image.

Figure 2: 256 × 256 256-graylevel image used for the covert image.

3. Experiments

Figure 1 is used as the covert images, where Figure 1(a) is a 64 × 64 128-graylevel image and Figure 1(b) is a 128 × 128 binary image. Figure 2 shows a 256×256 256-graylevel image used as the host image for two simulations.

The first experiment for encoding the covert image in Figure 1(a) by assembling the modified RSA encryption method and the binary encoding method to form a holographic image **H** is shown below. The elements in the 1 × 256 binary-data string **R** are firstly determined, where **R** is used to encode identification codes, covert-image dimension codes, covert-image graylevel codes, pre-RSA bit number codes, RSA key codes, and post-RSA bit number codes. The first to 28th elements (the first range) in **R** are specified as the identification codes, and they are set as 1111001111001010110000110000. The 29th to 48th elements (the second range) in **R** are specified as the covert-image dimension codes. Since the size of the covert image in Figure 1(a) is 64 × 64, the dimension codes for M are 0000111101 (i.e., $64 = \sum_{i=1}^{10} M_i \cdot 2^{i-1} + 3$) and they are encoded at the 29th to 38th elements in **R**. The dimension codes for N are also 0000111101 and they are encoded at the 39th to 48th elements in **R**. The 49th to 54th elements (the third range) in **R** are specified as the covert-image graylevel codes. Since the parameter g of the covert image used in this case is seven (i.e., $128 = 2^7$), the codes are 000110 (i.e., $7 = \sum_{i=1}^{6} g_i \cdot 2^{i-1} + 1$). The 55th to 60th elements (the fourth range) in **R** are specified as the pre-RSA bit number codes. Because the selected pre-RSA bit number b in this case is four, the codes are 000011 (i.e., $4 = \sum_{i=1}^{6} b_i \cdot 2^{i-1} + 1$). The 61st to 130th elements (the fifth range) in **R** are specified as the RSA key codes for the keys n and d. Because the key n both for the encoding and decoding is set as 247, the 61st to 130th elements in **R** are 0000000000000000000000000010010011 (i.e., $247 = \sum_{i=1}^{35} n_i \cdot 2^{i-1} + 100$). Because the key e for the encoding is set as 11, the key d for the decoding must equal 59. Therefore, the 96th to 130th elements in **R** are 0000000000000000000000000000111001 (i.e., $59 = \sum_{i=1}^{35} d_i \cdot 2^{i-1} + 2$). The 131st to 136th elements (the sixth range) in the first row of **R** are the post-RSA bit number codes. Because the selected post-RSA bit number a used in this case is eight, the 131st to 136th elements in the first row of **R** are 000110 (i.e., $8 = \sum_{i=1}^{6} a_i \cdot 2^{i-1} + 2$). The 137th to 256th elements in the first row of **R** are all set as 0.

After that, create the 57344 (= 64×64×7/4×8) binary-data string **G** by encoding the 1 × 7168 modified RSA encryption data string **F**. Then copy the binary-data elements of **G** to form the 255 × 256 binary-data matrix **S**. Because the matrix **S** contains 65280 (= 255 × 256) elements and the binary-data string **G** only contains 57344 elements, the values of the extra 7936 elements of **S** are all set as 0. The 256 × 256 binary-data matrix **T** combined from the 1 × 256 binary-data string **R** and the 255 × 256 binary-data matrix **S** is shown in Figure 3. Figure 4 shows a dot-matrix holographic image (composed of many grating dots) created by a two-beam writer (Sparkle) [22]. The holographic image is used to hide the binary-data

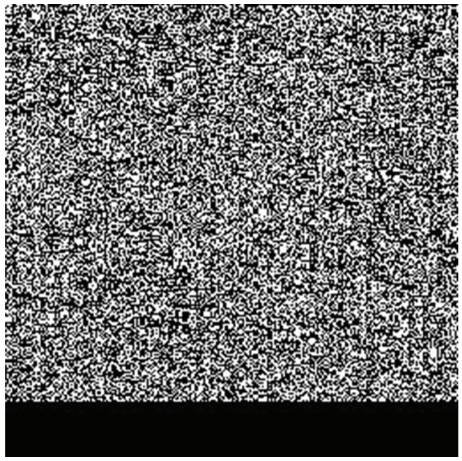


Figure 3: Binary-data matrix **T** for Figure 1(a).

Figure 4: Dot-matrix holographic image **H** for hiding the binary-data matrix **T** for Figure 1(a).

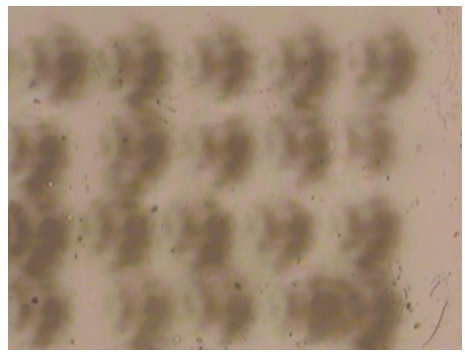


Figure 5: Some grating dots at the upper-right corner of the dot-matrix holographic image **H** for Figure 1(a).

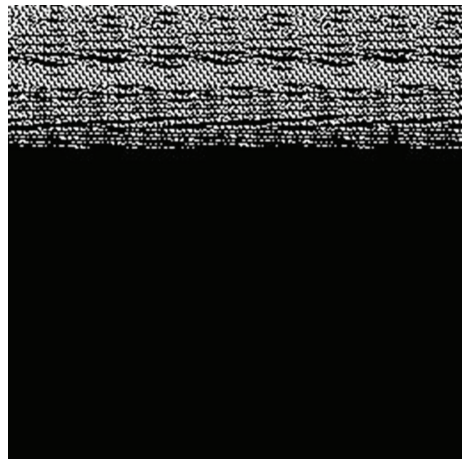


Figure 6: Binary-data matrix **T** for Figure 1(b).

T for the covert image in Figure 1(a). The holographic image is on a Shipley 1813 photoresist plate and it contains 256 × 256 grating dots. All the grating dots have the same grating pitch of 1 μm, but they have different grating orientations. The relation between the orientation $\theta(i, j)$ (measured from the x-axis) of a grating dot and the gray value $H(i, j)$ of a corresponding image pixel in Figure 2 is

$$\theta(i, j) = \frac{H(i, j) - 128}{1000} \times 180^{\circ}. \tag{19}$$

The grating dot pitch is about 63.5 μm. The size of the holographic image is about 16.2 mm × 16.2 mm. The grating dots in the same column or row should be in a line for a dot-matrix hologram without hiding binary data, whereas the grating dots in the same column are in two separated lines for the dot-matrix hologram in Figure 4. The grating dots in the right line are used to denote the datum "1" and the grating dots in the left line are used to denote the datum "0". The distance between the two lines is about 15 μm. All the grating dots on the hologram in Figure 4 correctly hide the data in the binary-data matrix **T** for Figure 3. Figure 5 shows some of the grating dots at the upper-right corner of the dot-matrix holographic image. The original covert image **C** and the reconstructed covert image $\mathbf{C}^*$ derived from the holographic image **H** are exactly the same.

The second experiment for encoding Figure 1(b) is shown below. The first to 28th elements in **R** are also specified as the identification codes, and they are set as 1111001111001010110000110000. The 29th to 48th elements in **R** are specified as the covert-image dimension codes. Since the size of the covert image in Figure 1(b) is 128 × 128, the dimension codes for M are 0001111101 (i.e., $128 = \sum_{i=1}^{10} M_i \cdot 2^{i-1} + 3$) and they are encoded at the 29th to 38th elements in **R**; the dimension codes for N are also 0001111101 and they are encoded at the 39th to 48th elements in **R**. The 49th to 54th elements in **R** are specified as the covert-image graylevel codes. Since the parameter g of the covert image used in this case is one (i.e., $2 = 2^1$), the codes are 000000 (i.e., $1 = \sum_{i=1}^{6} g_i \cdot 2^{i-1} + 1$). The 55th to 60th elements (the fourth range) in **R** are specified as the pre-RSA bit number codes. Because the selected pre-RSA bit number b in this case is eight, the 55th to 60th elements in **R** are 000111 (i.e., $8 = \sum_{i=1}^{6} b_i \cdot 2^{i-1} + 1$). The 61st to 130th elements in **R**

are specified as the RSA key codes for the keys n and d. Because the key n is set as 323, the 61st to 130th elements in **R** are 00000000000000000000000000011011111 (i.e., $323 = \sum_{i=1}^{35} n_i \cdot 2^{i-1} + 100$). Because the key e is set as 23, the key d must equal 263. Therefore, the 96th to 130th elements in **R** are 00000000000000000000000000100000101 (i.e., $263 = \sum_{i=1}^{35} d_i \cdot 2^{i-1} + 2$). The 131st to 136th elements in the first row of **R** are the post-RSA bit number codes. Because the selected post-RSA bit number a used in this case is ten, the 131st to 136th elements in the first row of **R** are 001000 (i.e., $10 = \sum_{i=1}^{6} a_i \cdot 2^{i-1} + 2$). The 137th to 256th elements in the first row of **R** are all set as 0.

After that, create the 20480 (= 128×128×1/8×10) binary-data string **G** by encoding the 1×4096 RSA encryption data string **F**. Then copy the binary-data elements of **G** to form the 255×256 binary-data matrix **S**. Because the matrix **S** contains 65280 (= 255 × 256) elements and the binary-data string **G** only contains 20480 elements, the values of the extra 44800 elements of **S** are all set as 0. The 256×256 binary-data matrix **T** combined from the 1 × 256 binary-data string **R** and the 255 × 256 binary-data matrix **S** is shown in Figure 6. The dot-matrix holographic image **H** for this case is shown in Figure 7, almost the same as that in Figure 4. Some of the grating dots at the left-upper corner of the dot-matrix holographic image **H** are shown in Figure 8. All the grating dots on the holographic image correctly hide the data in the binary-data matrix **T** for Figure 6. The original covert image **C** and the reconstructed covert image $\mathbf{C}^*$ derived from the holographic image **H** are exactly the same.

The above-mentioned processes for encoding the covert image **C** can be concluded as follows: (1) use **C**, n, and e to form **G** and **R**; (2) use **G** and **R** to form **T**; and (3) hide **T** to form **H**. On the other hand, the processes for reconstructing $\mathbf{C}^*$ can be concluded as follows: (1) derive **T** from **H**; (2) use **T** to form **G** and **R**; and (3) use n, d, **G**, and **R** to form $\mathbf{C}^*$. Since the reconstruction possesses are the reversed version of the encoding processes, the former are not demonstrated here.

Figure 7: Dot-matrix holographic image **H** for hiding the binary-data matrix **T** for Figure 1(b).

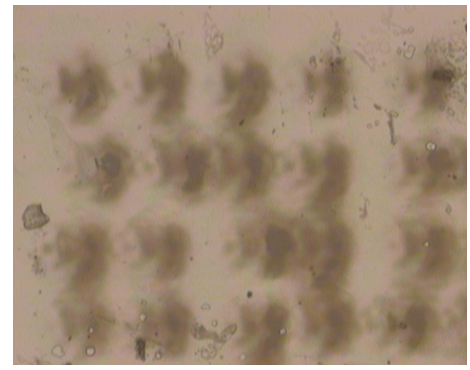


Figure 8: Some grating dots at the upper-left corner of the dot-matrix holographic image **H** for Figure 1(b).

4. Discussions

The values of M_0, N_0, g_0, n_0, d_0, and a_0 are determined according to the idea of a designer and no reasons are needed. Because these values are uncertain for unauthorized people, the binary encoding method has high security.

The proposed hiding method is only demonstrated for clearness and simplification in this paper. If higher security is needed for the hiding method, more complex processes can be used, for example, changing the specified code positions in **R**, changing the length of selected bit number codes, or changing the values of M_0, N_0, g_0, n_0, d_0, and a_0.

The security of the proposed method depends on both the RSA encryption and the binary encoding method. For the RSA encryption, a very big n is not necessary for the proposed method because private RSA keys unknown for unauthorized people are used (normal RSA encryption methods use public keys known by everyone). For the binary encoding method, it is difficult to decode codes because many uncertain parameters (for unauthorized people) are used. Both the RSA encryption and the binary encoding method have high security, so the security of the proposed method is high.

The direct calculation for $s \equiv t^d \bmod n$ is not accepted by a computer usually because the number t^d is too huge. Therefore, a calculation accepted by a computer is needed. A simple method is to multiply t^2 with t and do the modulus-after-division operation with n for d-1 times; that is,

$$s \equiv \Big(\Big(\Big(\big(t^2 \bmod n\big) \times t\Big) \times (\bmod n) \times t\Big) \bmod n, \ldots,\Big) \bmod n. \tag{20}$$

5. Conclusions

The proposed hiding method combines the RSA encryption method and the binary encoding method to encrypt a covert image **C** into a dot-matrix holographic image **H**. The RSA encryption method uses the covert image **C** to form a RSA

encryption data string. The binary encoding method encodes the RSA encryption data string into binary codes and encodes the binary codes into the dot-matrix holographic image **H**. The reconstructed covert image $\mathbf{C}^*$ can be decoded directly from the dot-matrix holographic image **H**. Furthermore, there is no distortion for the decoding work of the covert image.

Conflict of Interests

The authors declare no conflict of interests regarding all the aspects related to this paper.

Acknowledgment

This paper was partially supported by the National Science Council of the Republic of China (Grant no. NSC 102-2221-E-129-004 and Grant no. NSC 101-2221-E-262-008).

References

[1] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding: Techniques for Steganography and Digital Watermarking*, Artech House, Norwood, UK, 2000.

[2] Y.-L. Yang, N. Cai, and G.-Q. Ni, "Digital image scrambling technology based on the symmetry of Arnold transform," *Journal of Beijing Institute of Technology*, vol. 15, no. 2, pp. 216–220, 2006.

[3] Y. Zhou, S. Agaian, V. M. Joyner, and K. Panetta, "Two Fibonacci P-code based image scrambling algorithms," in *Image Processing: Algorithms and Systems VI*, vol. 6812 of *Proceedings of SPIE*, San Jose, Calif, USA, January 2008.

[4] W. Chen and X. Chen, "Optical image encryption using multilevel Arnold transform and noninterferometric imaging," *Optical Engineering*, vol. 50, no. 11, Article ID 117001, 2011.

[5] O. Lafe, "Data compression and encryption using cellular automata transforms," *Engineering Applications of Artificial Intelligence*, vol. 10, no. 6, pp. 581–591, 1997.

[6] H. Zhang, J. Huang, and Z. Li, "New method of digital image scrambling based on binary tree generated by chaotic sequences," in *Remote Sensing and GIS Data Processing and Applications; and Innovative Multispectral Technology and Applications (MIPPR '07)*, vol. 6790 of *Proceedings of SPIE*, Wuhan, China, November 2007.

[7] D. M. Wang, "The quasi-period of odd order magic square transformation on digital image," *Journal of Zhejiang University of Technology*, vol. 33, pp. 292–296, 2005.

[8] K. T. Lin, "Information hiding based on binary encoding methods and pixel scrambling techniques," *Applied Optics*, vol. 49, no. 2, pp. 220–228, 2010.

[9] S. K. Rajput and N. K. Nishchal, "Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask," *Applied Optics*, vol. 51, pp. 5377–5386, 2012.

[10] W. Chen, X. Chen, A. Anand, and B. Javidi, "Optical encryption using multiple intensity samplings in the axial domain," *Journal of Optics Society of America A*, vol. 30, pp. 806–812, 2013.

[11] L. C. Huang, L. Y. Tseng, and M. S. Hwang, "The study of data hiding in medical images," *International Journal of Network Security*, vol. 14, pp. 301–309, 2012.

[12] L. C. Huang, L. Y. Tseng, and M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, 2013.

[13] Z. Liao, Y. Huang, and C. Li, "Research on data hiding capacity," *International Journal of Network Security*, vol. 5, pp. 140–144, 2007.

[14] H. C. Williams, "A modification of the RSA public-key encryption procedure," *IEEE Transactions on Information Theory*, vol. 26, no. 6, pp. 726–729, 1980.

[15] L. Kocarev, M. Sterjev, and P. Amato, "RSA encryption algorithm based on torus automorphisms," in *Proceedings of the IEEE International Symposium on Cirquits and Systems*, pp. V-577–V-580, May 2004.

[16] S. J. Aboud, M. A. Al-Fayoumi, M. Al-Fayoumi, and H. S. Jabbar, "An efficient RSA public key encryption scheme," in *Proceedings of the International Conference on Information Technology: New Generations (ITNG '08)*, pp. 127–130, April 2008.

[17] R. S. Dhakar, A. K. Gupta, and P. Sharma, "Modified RSA Encryption Algorithm (MREA)," in *Proceedings of the 2nd International Conference on Advanced Computing and Communication Technologies (ACCT '12)*, pp. 426–429, January 2012.

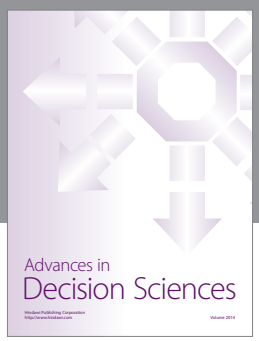
[18] N. Anane, M. Anane, H. Bessalah, M. Issad, and K. Messaoudi, "RSA based encryption decryption of medical images," in *Proceedings of the 7th International Multi-Conference on Systems, Signals and Devices (SSD '10)*, pp. 1–4, June 2010.

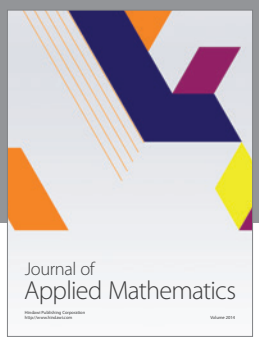
[19] N. Saini and A. Sinha, "Key management of the double random-phase-encoding method using public-key encryption," *Optics and Lasers in Engineering*, vol. 48, no. 3, pp. 329–334, 2010.

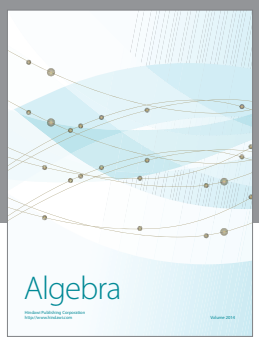
[20] K. T. Lin, "Digital information encrypted in an image using binary encoding," *Optics Communications*, vol. 281, no. 13, pp. 3447–3453, 2008.

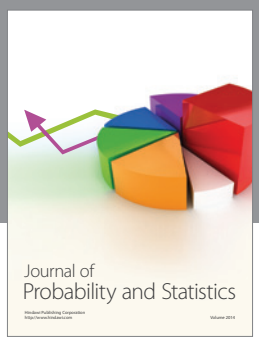
[21] S. L. Yeh, "Dot-matrix hologram with and encrypted figure," *Optical Engineering*, vol. 45, no. 9, Article ID 095801, 2006.

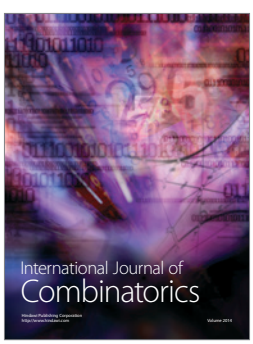
[22] http://www.ahead.com.tw.

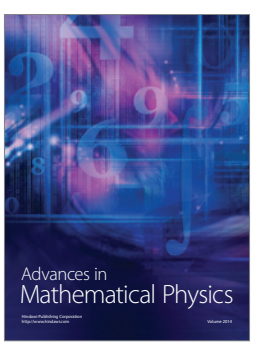


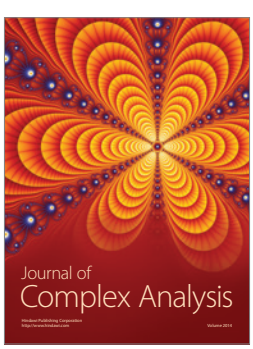


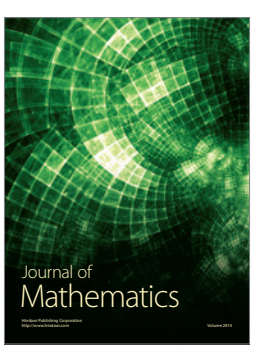


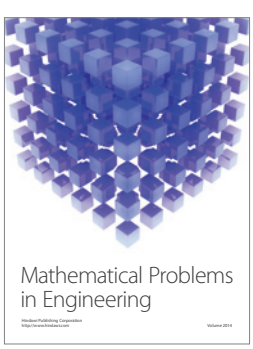


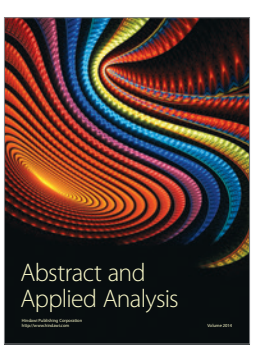


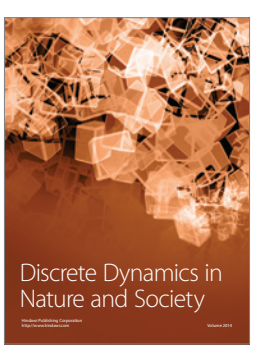


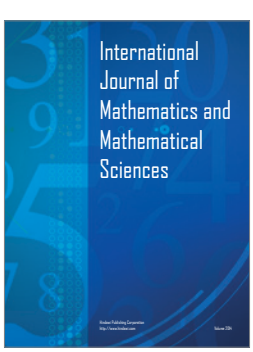












Hindawi

Submit your manuscripts at
http://www.hindawi.com