14

Optimization of Hologram for Security Applications

Junji Ohtsubo
Shizuoka University
Japan

1. Introduction

Optical pattern recognition for validation and security verifications has been one of the important issues of optical image processing for the past decade. As one technique, a method of joint transform correlation (JTC) has frequently been used for optical security systems for identification of biometric images. In that method, an image such as a fingerprint pattern is encrypted by a random key mask, and the joint Fourier transform of the image to be encrypted and the key pattern conforms an encrypted hologram. The hologram is printed on a card or a document for authenticity, such as a credit card or a passport. The hologram is read when and where necessary and decoded by using the same key that is used for the encryption. In practical optical security systems, a digital technique is used for the image encryption, since the time required to calculate an encryption pattern is not a critical factor and the encryption of an image and printing of the encrypted hologram on a card may be done offline. On the other hand, fast processing is required to decode an encrypted image and verify it. Accordingly, the optical technique is very suitable for such processing.

In this chapter, we discuss optical security systems suitable for the use of holograms. For the congeniality of the method with real optical systems, binary holograms are frequently used in those systems. By the binarization of hologram, the reconstructed hologram is greatly degraded and, therefore, the optimization of hologram is required for the identification of a reference image. We study the method of the optimization of binary holograms based on a simulated annealing technique. The method of the simulated annealing usually takes a long time to reach a correct estimate, so that the fast optimization for binary hologram is applied. We also demonstrate an image decryption by the optimization of a binary hologram when both the hologram and the key for decryption are embedded in real electronic displays with periodic lattice structures. Finally, we discuss a technique to obtain an exact decryption image based on a phase-encoding technique, which enables easier realization for the practical applications in optical security systems. Even in this technique, the optimization of phase-encoded hologram plays an important role to obtain a good image-reconstruction.

2. Optical security systems

In this section, we discuss a fundamental optical security system treated throughout this chapter. The optical security system under consideration is shown in Fig. 1 (Yamazaki &

Ohtsubo, 2001). The system consists of three parts. Fig. 1(a) is an encryption system of a target image. An image, for example a finger print image, is encrypted with an encoding key with holographic technique and the encoded image is binarized according to a certain rule to make it easier for reading the image and to match the post processing system. The encrypted binary image printed on a security card is optically decrypted with the decoding key in Fig. 1(b). The decoded image is compared with a test image for identification with optical joint transform correlation as shown in Fig. 1(c). The advantage of the optical method in a security system is the fast processing for decoding an encrypted image and identifying it. In practical optical security systems, a digital technique may be used for the image encryption, since the time required to calculate an encryption pattern is not essential and the encryption of an image and printing the encrypted hologram on a card may be done by offline. On the other hand, the fast processing is required for decoding an encrypted image and verifying it. Accordingly, optical technique is very suited for such processing.

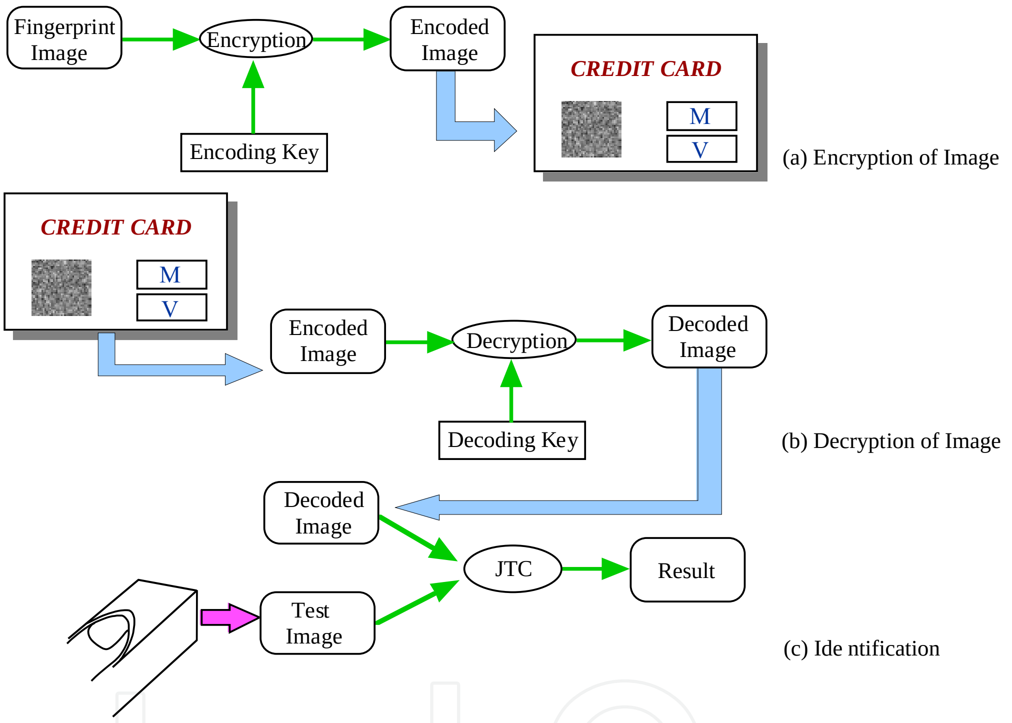

Fig. 1. Schematic example of optical security system. (a) Image encryption, (b) Image decryption, and (c) identification systems.

The encrypted image is binarized to print it, for example on a credit card, and it is read when and where necessary. Binarization of hologram may be performed according to the sign of each pixel value of the encrypted hologram. By the binarization of hologram, we can avoid the load for pre-processing of an encrypted hologram for the decryption and to make a robust optical security system. Due to the binarization of hologram, the encrypted image may be degraded, so that the optimization of the encrypted binary hologram is essential. In the decryption process, the reconstruction of the encrypted image should be quickly processed. Therefore, we assume an optical image processing in the decryption system. Also, the image identification with a test image should be quickly done. We also assume an optical system for image identification. Image identification based on optical methods is an attractive issue, however the methods, especially the methods of optical correlation, are well established (Kobayashi & Toyoda,1999). So we do not treat them in detail in this chapter. Therefore, in the following, we will discuss how to make an encryption hologram suitable for optical decryption and how to optimize it.

3. Encryption and decryption of hologram

3.1 Theory of image encryption and decryption of hologram

The method of image encryption for optical security system, which is considered here, is a common one already proposed (Javidi & Horner, 1994, Refregier & Javidi, 1995, and Javidi, 1997). In the image encryption process, an image with a random phase mask is jointly Fourier transformed with another random pattern, which is a key for encryption and decryption, as shown in Fig. 2 and a hologram is formed at the Fourier plane (Yang & Kim, 1996, Javidi et al., 1996, and Unnikrishnan et al., 1998). The phase random mask put in front of the image to be embedded plays a role for scrambling the image, however it little affects the reconstruction of hologram, since the reconstruction is only the intensity of them. The holographic fringe terms are given by

$$H(u,v) = F(u,v)G^{*}(u,v)\exp(-i4\pi dv) + F^{*}(u,v)G(u,v)\exp(i4\pi dv) \tag{1}$$

where $F(u,v)$ and $G(u,v)$ are the Fourier transformed functions of the image with a random phase, $f(x,y)$, and the random pattern $g(x,y)$ used as an encryption key, respectively, $2d$ is the separation between the centers of two functions, * denotes the complex conjugate, and $H(u,v)$ is the resultant hologram. We, here, only consider the AC components of the hologram. The image with a random phase is written by

$$f(x,y) = f_{0}(x,y)\exp\{ib(x,y)\} \tag{2}$$

where $f_0(x,y)$ is the original image function and $b(x,y)$ is also a random function but different from $g(x,y)$. To make an encrypted image, we assume a digital synthesis of the hologram. Fig. 3 is an example of sets of patterns used in the numerical simulations. Fig. 3(a) shows a fingerprint image with 64×64 pixels and Fig. 3(b) is a random pattern used for the encryption key. We here assume 8-bit gray scale for the fingerprint image and (1,-1) binary random pattern (i.e., equivalently $(0,\pi)$ phase) as the encryption key. As a random phase mask multiplied to the image in the input plane is also assumed to be $(0,\pi)$ random phase different from the random key pattern.

To reconstruct the image from the encrypted pattern, the hologram is illuminated by the same random phase pattern used for the encryption as shown in Fig. 4. For the decryption corresponding to Eq.(1), we obtain

$$\begin{aligned} p(x,y) &= f(x,y-d)\otimes g(-x,-y)\otimes g(x,y) \\ &\quad + f(-x,-y)\otimes g(x,y)\otimes g(x,y)\otimes \delta(x,y+3d) \end{aligned} \tag{3}$$

where ⊗ denotes the convolution operation. The first term in Eq.(3) is the reconstructed image since the convolution between $g(-x,-y)$ and $g(x,y)$ reduces to a delta function due to the random nature of the function. On the other hand, the second term is the convolution between the image and the random function and it is a noise term in the reconstruction. Two terms can be spatially separated with each other. Thus, the encrypted image is successfully decrypted in the image plane without noise terms.

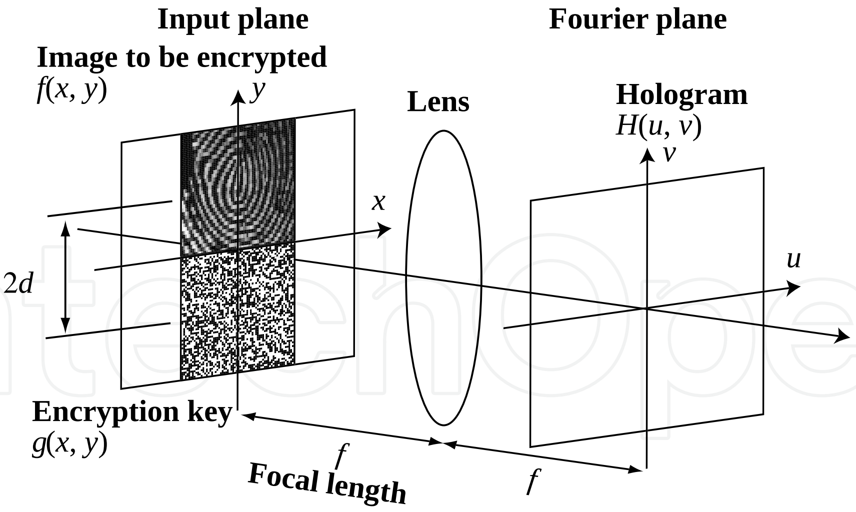

Fig. 2. Optical encryption system using joint Fourier transform

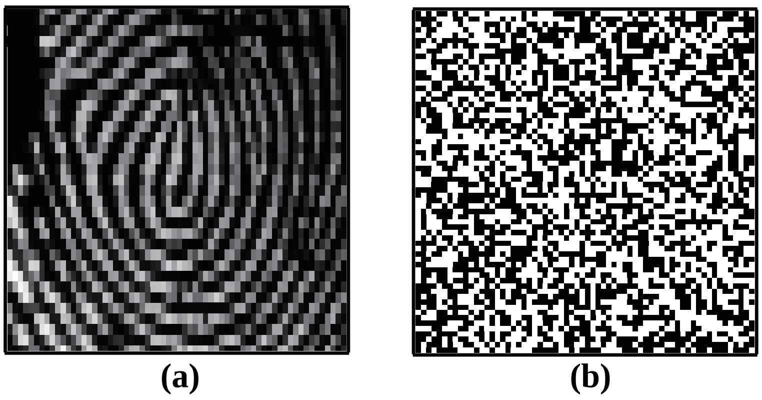

Fig. 3. (a) Original input image and (b) random key pattern for encryption.

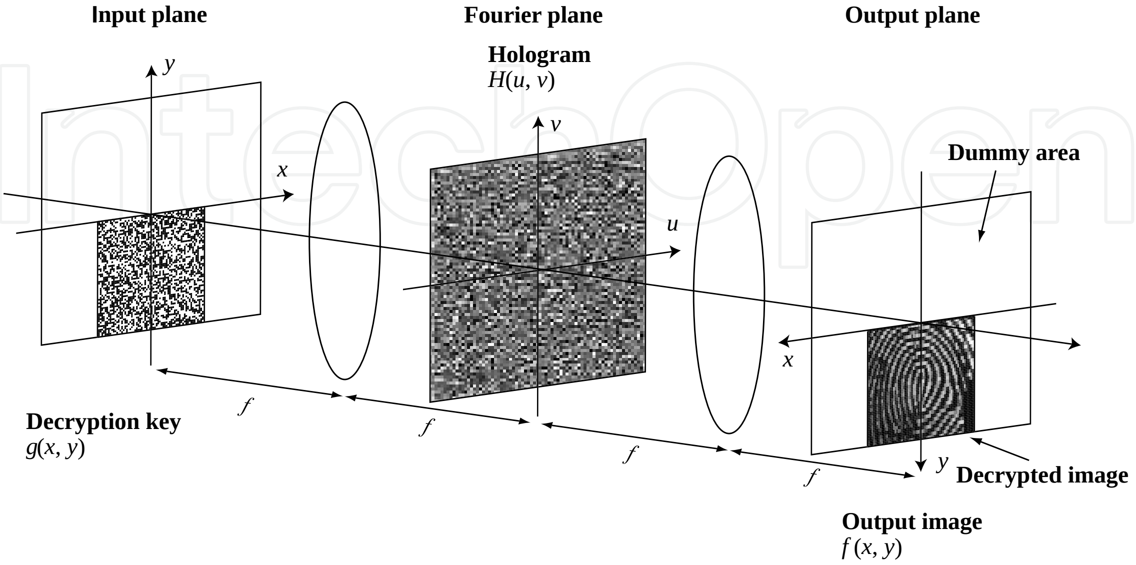

Fig. 4. Optical decryption system

3.2 Reconstruction of binary hologram

In actual applications, such as in credit card identification, a binary hologram is suited for acquiring electronic image and digital-electronic pre-processing. Thus, the use of the binarization of hologram is one of excellent methods to make a robust security system, so that we employed a binary hologram as an encrypted pattern in the following. The calculated hologram is binarized according to the sign of each element of the composite pattern. Fig. 5 is the result of the encrypted binary hologram. In the figure, the hologram that has a (0,1) binary distribution is printed on a card as a black and white pattern. However, for the reconstruction of the binary hologram, the value of each pixel is assigned to +1 ($\exp(i0)$) when the pixel hologram has a value of 1, while it is -1 ($\exp(i\pi)$) for 0. A hologram that has (0,π) phase distribution can be easily realized by using a phase modulation spatial light modulator such as a parallel aligned liquid crystal display. The hologram that has 0 and π phase distribution has the advantage in the reconstruction, since the zero-th order diffraction is eliminated in the reconstruction pattern. Fig. 5(a) shows the calculated binary hologram corresponding to the original image with the random key pattern in Fig. 3. Fig. 5(b) is the decrypted pattern. The hologram and the reconstructed image have the size of 256×256 pixels. The lower noisy part in the figure is the second term in Eq.(3). The binarization of hologram is suited for printing it on a credit card in practical use. However the image is not completely reconstructed because of the binarization for the original hologram as shown in Fig. 5(b). As a result, the ability for the identification between the reconstructed and reference images is deteriorated. Therefore, the optimization of the binary hologram is expected to obtain a good reconstructed image. The method is discussed in the following section.

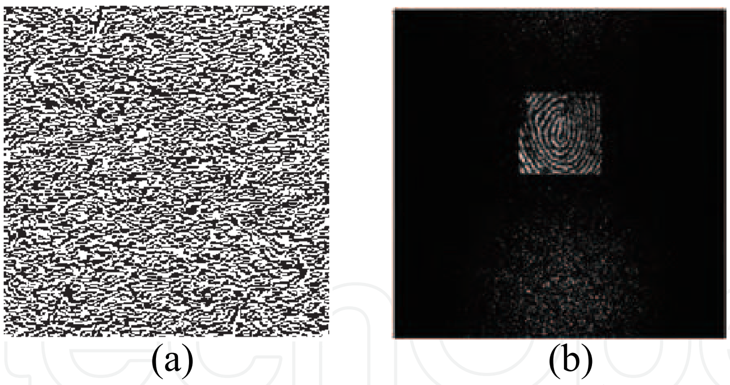

Fig. 5. (a) Binary phase hologram and (b) reconstruction of hologram with random key pattern.

4. Optimization of binary hologram

4.1 Procedure for optimization of binary hologram

For an optical security system considered here such as in a credit card identification system, the image encryption may be performed in off-line. In that case, the hologram to be printed such as on a credit card may not necessarily be made by the optical method. The encryption of an image and the optimization of the hologram to reconstruct a good image can be performed on digital computer. We here discuss the optimization of the encrypted hologram to obtain a good reconstruction of it based on the numerical method. The method employed for the optimization is a simulated annealing like technique (Kirkpatrick et al., 1983, Ohtsubo & Nakajima, 1991, and Bättig et al., 1992). In ordinary sense, a small perturbation is applied to each pixel of a analogue-valued hologram in a simulated annealing method and the reconstructed image is gradually improved through the iterations (Metropolis et al., 1953, and Aarts and Korst, 1990). However, the method proposed here is somewhat different from the strict simulated annealing technique, since a large perturbation for each pixel value of 1 (zero-phase) or -1 (pi-phase) flipping is applied to each pixel.

In the simulated annealing in the present method, (0,π) phase of each pixel in the hologram elements is flipped 0 to π or vice versa as a perturbation. Then the cost function is calculated and the perturbation is accepted or not according to the simulated annealing. The cost function defined here is the mean-square error between the original image intensity to be reconstructed and the estimated one and is given by

$$E = \iint \left| |f_0(x,y)|^2 - \alpha |f_n(x,y)|^2 \right|^2 dxdy \tag{4}$$

where $f(x,y)$ is the amplitude of the original image to be reconstructed (defined by Eq.(2)), $f_n(x,y)$ is the n-th estimate, and the scaling factor α is defined by

$$\alpha = \frac{\iint |f_0(x,y)|^2 \, dxdy}{\iint |f_n(x,y)|^2 \, dxdy} \tag{5}$$

The cost function is evidently zero when the estimate converges to the original image.

The basic flow of the simulated annealing employed here is shown in Fig. 6. According to the diagram, each step in the simulated annealing is described as follows;

Step 1. As an initial input for the iteration, a binary phase hologram calculated from Eq.(1) is used. The hologram is reconstructed and the initial cost function E (E_{old}) is calculated. The reference for the reconstruction is the random key pattern used for the encryption. The temperature for the annealing is set with a relatively high value.

Step 2. The perturbation is applied to one of the pixels of the hologram and the other pixels are remained unchanged. The phase is flipped 0 to π or π to 0. Then the estimated hologram is reconstructed and the new cost function E_{new} is calculated.

Step 3. The difference between the cost functions before and after the perturbation $\Delta E = E_{new} - E_{old}$ is calculated. If $\Delta E < 0$, the new phase is accepted and the cost function is retained as an old cost function for the next perturbation. Otherwise ($\Delta E \geq 0$), the acceptance or rejection is stochastically determined according to the Boltzmann distribution

$$P = \exp(-\frac{\Delta E}{T}) \tag{6}$$

where T is the temperature of the annealing. If $P < r$ (r is a random number between 0 and 1), the perturbation is accepted. On the other hand, it is rejected when $P \geq r$

Step 4. Step 4: Steps 2 and 3 are repeated for every pixel.

Step 5. If the cost function of each iteration has still a large value, the temperature for the annealing is lowered and the next iteration is performed again. If the cost function is lowered enough, the iteration is stopped.

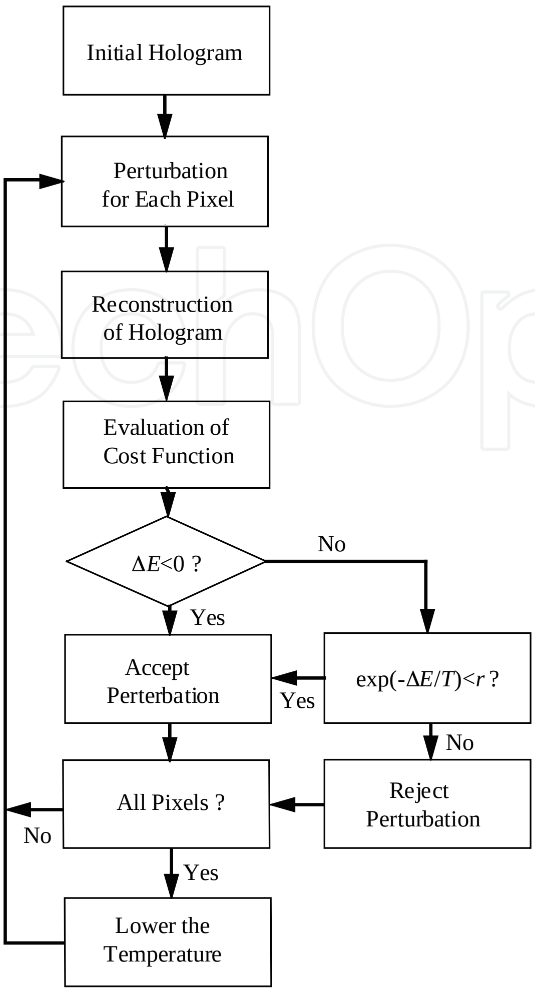

Fig. 6. Algorithm for optimizing hologram by simulated annealing method.

he process is almost the same as a usual simulated annealing method except for the random flipping of the (0,π) phase pattern at the second step. When the cost function becomes small and temperature is sufficiently cool down, the obtained pattern should be a good estimate for the hologram that well reproduces the original image to be reconstructed and thus the optimization of the hologram is realized.

4.2 Results of optimization

In the simulations, the optimization of the binary phase hologram for the fingerprint image as shown in Fig. 3(a) is performed. The reference for the reconstruction of the hologram is the random (1,-1) pattern in Fig. 3(b). Three cooling schedules of the temperature are used in the simulations, i.e., T=0 (this corresponds to no annealing), T=1/exp(n), and T=0.5/(1+n) (n being the iteration number). Fig. 7(a) shows the variations of the cost functions for the iteration number during the simulated annealing. When the annealing process exists ($T \neq 0$), the value of the cost function once increases with increase of the iteration number and reaches its maximum point. Then it decreases for further increase of the iteration number. In usual simulated annealing, the cost function monotonically decreases with increase of the iteration. However, in our case, the annealing process once trapped to a local minimum, since the perturbation to be added to the image is different from that of ordinary simulated annealing. From the comparison between the two cooling schedules (*T*=1/exp(*n*) and *T*=0.5/(1+*n*)), a rapid cooling rate is rather effective for the optimization of the hologram. The cost function monotonically and rapidly decreases without trapping any local minimum when *T*=0, that is, no annealing process. The point of the simulated annealing method is the moderate perturbation with random fluctuations to escape local minima in the energy function. The reference to construct the hologram in the method is a binary random pattern and the hologram itself is also a random like pattern, so that random fluctuations are automatically given without introducing the stochastic process (Step 3) in the iteration. This may come from a random nature of the reconstruction process in the present method. For either case, the optimized hologram well reproduces a fingerprint image very close to the original one. Fig. 7(b) is the result of the optimized hologram at *T*=0.

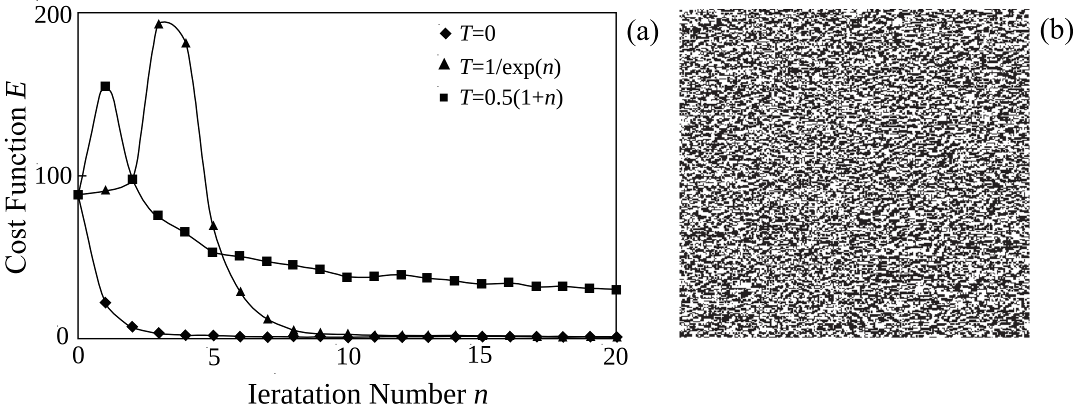

Fig. 7. (a) Variations of cost functions for each cooling schedule and (b) optimized binary hologram at *T*=0.

The degree of the reconstruction for the optimized hologram is tested by a joint transform correlation method. Fig. 8 shows the results. Fig. 8(a) is the original fingerprint image (left) and the joint transform correlation between the same patterns (right). The result of the correlation is a one-dimensional scan along the correlation peaks. For the calculation of the correlation function, the power spectrum is filtered by a band-pass filter in the Fourier plane to eliminate the unwanted noise floor. The zero-th order correlation peak is normalized to 255 level and the value of the correlation peak is 63. Fig. 8(b) is the decrypted image from the original binary hologram (not optimized one) and its correlation with the original fingerprint image. The fingerprint image is vague compared with the original one due to the binarization of the hologram and its correlation peak value is only 39. Starting from the hologram corresponding to Fig. 8(b), the simulated annealing is performed along the procedure discussed in the previous section. Fig. 8(c) shows the reconstructed fingerprint image by the optimized hologram for *T*=0 and its correlation with the original image. The image is perfectly recovered (compare the pattern in Fig. 8(a)) and its correlation peak is 63, which is completely the same value with the correlation between the original images. For the iteration cycle of $n \geq 5$ the hologram is almost optimized. The optimization is also successful for the cooling schedule of *T*=1/exp(*n*) and the fingerprint image having the correlation value of 63 is obtained for $n \geq 10$. The reconstructed image is much improved for the cooling schedule of *T*=0.5/(1+*n*), however, the optimization speed is slower and the value of the correlation is 58 at *n*=20.

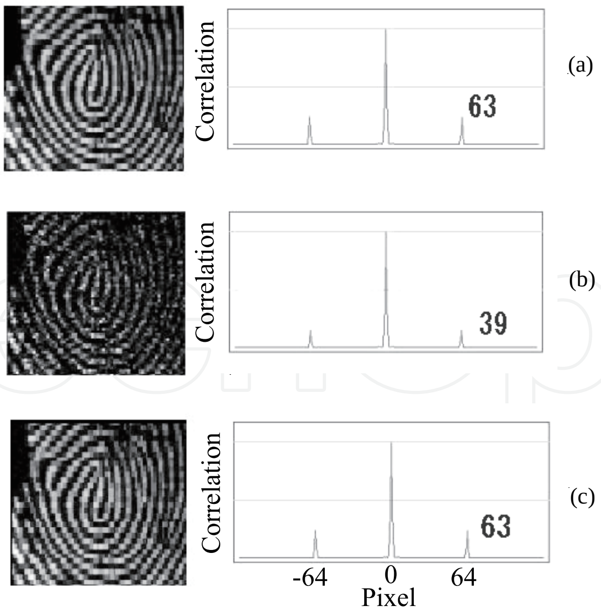

Fig. 8. Reconstructed images (left) and correlations with original image (right). (a) Original fingerprint image, (b) reconstructed image without optimization, and (c) reconstructed image with optimization.

5. Fast optimization method

5.1 Algorithm of fast optimization

Though the method based on the simulated annealing algorithm discussed in the previous section is very effective for the optimization of encrypted holograms, it is time consuming. Here, we propose an error correction method by which we can perform very fast optimization of encrypted binary holograms (Nakayama & Ohtsubo, 2007). The simulated annealing technique introduced in the previous section is a like Boltzmann machine system, while the proposed error correction method here is similar to a back propagation technique in neural net works. Before discussing the method, we first define two terms; 'decrypted image' is the part of the decrypted area where the pattern corresponding to the encrypted image is reconstructed as shown in Fig. 4. The 'dummy area' is the rest of the pattern in the output plane. The complex amplitude of the output image reconstructed from the binary encrypted hologram after n iterations is given by $f_n(x,y) = f_{0n}(x,y)\exp\{ib_n(x,y)\}$. Then, we introduce the error function $e(x,y)$ for the decrypted image;

$$|\beta f_n(x,y) + e(x,y)|^2 = |f_0(x,y)|^2 \tag{7}$$

where the coefficient β is defined by

$$\beta = \sqrt{\frac{\iint |f_0(x,y)|^2 \,\mathrm{d}x\mathrm{d}y}{\iint_{\text{decrypted area}} |f_n(x,y)|^2 \,\mathrm{d}x\mathrm{d}y}} \tag{8}$$

The function $e(x,y)$ defines the difference between the decrypted and original images and can be given by

$$\begin{array}{ll} e(x,y) = (|f_0(x,y)| - \beta|f_n(x,y)|)\exp\{ib_n(x,y)\} & \text{within decrypted image} \\ e(x,y) = 0 & \text{in dummy area} \end{array} \tag{9}$$

In this method, the error information is used not only for evaluating the intensity of the decrypted image but also for selecting the flipping pixels in the hologram plane. For the concern of intensity, the phase of the decrypted image may be ignored as far as the optimization is performed only in the decryption plane. However, the phase $b_n(x,y)$ is included in the error function. The error projected back into the hologram plane, namely generated from $e(x,y)$ by the inverse Fourier transform operation, is affected by the phase as shown in the following and it plays a crucial role in this algorithm.

Also, the error function is accounted in the hologram plane. The expression of the error function $\Delta H(u,v)$ in the hologram plane is deduced from the following relation;

$$\begin{aligned} \beta f_n(x,y) + e(x,y) &= \beta\mathrm{IFT}[H_n(u,v)G(u,v)] + \mathrm{IFT}[\mathrm{FT}[e(x,y)]] \\ &= \mathrm{IFT}[\beta H_n(u,v)G(u,v) + \mathrm{FT}[e(x,y)]] \\ &= \beta\mathrm{IFT}\left[\left\{H_n(u,v) + \frac{\mathrm{FT}[e(x,y)]}{\beta G(u,v)}\right\}G(u,v)\right] \\ &= \beta\mathrm{IFT}[\{H_n(u,v) + \Delta H(u,v)\}G(u,v)] \end{aligned} \tag{10}$$

where $H_n(u,v)$ is the hologram after n-th iterations and FT and IFT are the forward and inverse Fourier transform operations. Then, the error function in the hologram plane reads

$$\Delta H(u,v) = \frac{\mathrm{FT}[e(x,y)]}{\beta G(u,v)} \tag{11}$$

Equation (11) indicates that $\Delta H(u,v)$ is like as a gradient vector to the locally or globally optimal solution with respect to $H_n(u,v)$. However, we cannot directly use the error information ΔH for the correction for $H_n(u,v)$, since the hologram is a binary nature and $\Delta H(u,v)$ is a continuous complex valued function. Therefore, we require some modifications for the application of the error correction method for the binary encrypted hologram.

In accordance with the above discussion, we adopt the following processes for the optimization of a binary hologram;

Step 1. At first, $\Delta H(u,v)$ is calculated by Eq. (11). Then, each pixel of the hologram is ranked by the magnitude of the value $|\mathrm{Re}[\Delta H(u,v)]|$ for the optimization, namely, the pixel with the largest value of $|\mathrm{Re}[\Delta H(u,v)]|$ has the highest priority for the flip.

Step 2. On the descending order of the priority for the error correction, each pixel value is flipped according to the following rules;

$$\begin{array}{l} \text{if } H_n(u,v)\text{=-1 and } \mathrm{Re}[\Delta H(u,v)] > 0, \text{ then } H_{n,new}(u,v) = 1 \\ \text{if } H_n(u,v)\text{= 1 and } \mathrm{Re}[\Delta H(u,v)] < 0, \text{ then } H_{n,new}(u,v) = -1 \\ \text{else } n\text{o flip} \end{array} \tag{12}$$

where $H_{n,new}(u,v)$ is a temporal hologram to be tested for the new reconstruction, which is generally called *neighborhood* in the field of the combinatorial optimization theory. This flipping trial is continued until it reaches a certain number.

Step 3. When the image decrypted from $H_{n,new}(u,v)$ is closer to the original image than that from $H_n(u,v)$, $H_{n,new}(u,v)$ is adopted as a new $H_n(u,v)$. Then, the above process is repeated. In this stage, we introduce the measure for the optimization of binary hologram and define the cost function in the decryption plane as

$$E = \iint |e(x,y)|^2 \mathrm{d}x\mathrm{d}y \ . \tag{13}$$

The optimization is performed so as to lower the above cost function.

The steps 1~3 are the essentials of the proposed algorithm. The method has many advantages over the existing optimization methods. Firstly, the most effective pixel to be corrected is selected for the optimization. Secondly, not only one pixel but also multiple pixels can be flipped at the same time on the basis of the priority order for the error correction. Therefore, we can expect faster calculation for the optimization of encrypted holograms.

5.2 Multiple-flip algorithm

In ordinary single flipping for pixel elements in the simulated annealing like method, it usually takes a long time to obtain a good reconstruction. On the other hand, the error correction method has a merit of simultaneous flipping of multi-pixels for the correction of the binary hologram. We could perform a faster optimization for encrypted hologram by the method of the error correction. In the multiple-flip algorithm, many pixels of the encrypted hologram are selected according to the priority order calculated from the error function and the respective pixels are simultaneously flipped. Then, the hologram is reconstructed and the iteration is either accepted or rejected for the evaluation of the cost function. The iteration is stopped either when the cost function is sufficiently lowered or when the process is trapped to a local minimum.

Fig. 9 shows the results of the cost function for a fixed multiple-flip algorithm. Two multiple-flip schemes are plotted; one is a 7-flip and the other is a 655-flip. The optimization stopped at 1818 iterations for the 7-flip, while it stopped only at 19 iterations for the 655-flip. The number of iterations to reach an optimized hologram is drastically reduced for a large number of simultaneous flipping, however the iteration stopped at a higher value of the cost function and the quality of image is rather poor compared with that for a lower number of the multiple-flip algorithm. The final iteration number for the 655-flip algorithm is 1/96 of that for the 7-flip algorithm. The actual calculation time on the computer is 1/86. Therefore, as a rough estimate, the calculation time is inversely proportional to the number of pixels to be flipped at the same time. The final costs for the 655-flip and the 7-flip are 117.67 and 67.78, respectively, while it is only 9.47 for the single-flip algorithm. Accordingly, the quality of the decrypted image for a higher number of the multiple-flip is worse than that of the lower case. There exists a trade-off between the final quality of the decrypted image and the calculation speed for the optimization. To show the trade-off, the dependence of the final iteration number and the cost function were investigated for various numbers of the multiple-flip algorithm. Fig. 10 is the results for two different fingerprint images. Similar trends have been observed for respective fingerprint images.

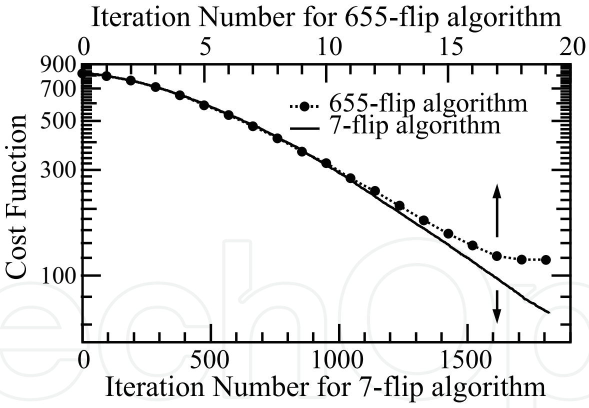

Fig. 9. Cost function for flip number in a fixed multiple-flip algorithm

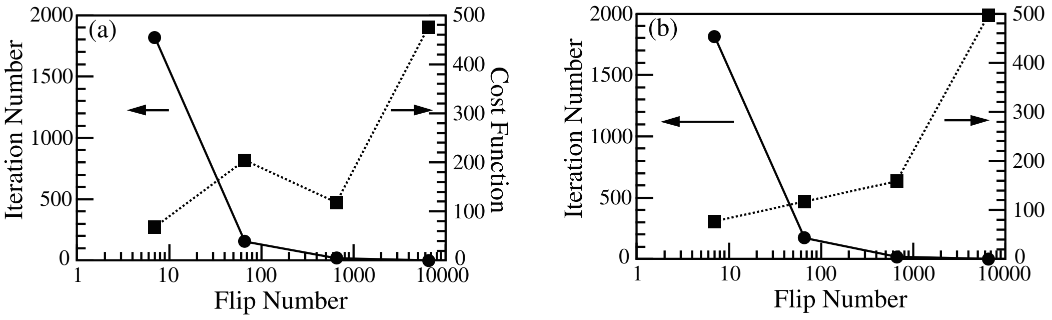

Fig. 10. Dependence of final iteration number and its cost on the number of simultaneous multiple flipping pixels. (a) corresponds to the fingerprint image in Fig. 3(a), and (b) is also for the fingerprint image in Fig. 12(a).

5.3 Variable multiple-flip algorithm

To avoid the trap of a local minimum and obtain a good decryption, we employ a scheme of a variable multiple-flip algorithm. In this algorithm, the flip number is dynamically changed. We first set the flip number at a certain value and started the iteration. When the iteration stops due to the trapping of a local minimum, the flip number is lowered and the next iteration is repeated. This process is repeated until the cost function is much lowered.

Fig. 11 is the results of the algorithm for the variable multiple-flip number. Fig. 11(a) is the decrypted image for the final optimized hologram with the encryption key and Fig. 11(b) is that with a wrong key. Fig. 11(c) is the change of the cost function for the iteration number. The flip number was at first chosen to be 655 and it was lowered as 66 after the trapping a local minimum. Then, the iteration was continued as lowering the flip number as 7, 4, and finally 2. The boundaries of the changing points are indicated as broken lines. We calculated the joint transform correlation between the obtained pattern and the original fingerprint image. The value of the correlation peaks calculated in Fig. 11(a) is 0.243 (normalized by the initial cost to unity), while that of the simulated annealing method of single flipping is 0.247. Almost the same quality of the reconstruction as the simulated annealing method is achieved by the current technique. We also compared the calculation time both for the proposed and the previous methods. For the optimization of the simulated annealing method, the calculation time at which the value of cost function became 0.243 was evaluated. The calculation times for the proposed and previous methods are 1149 and 39364 s, respectively, i.e., the calculation time of the proposed method is only 2.9 % of that of the simulated annealing method. Thus, we can attain a very fast optimization of encrypted holograms by using the error correction method with the variable multiple-flip algorithm without loosing the quality of the reconstruction. Finally, the variable multi-flip algorithm was applied to other types of images. Fig. 12 shows the results. It is clear that the proposed algorithm is applicable not only to fingerprint image but also to other images (binary logo of Shizuoka University and stamp of Chinese characters).

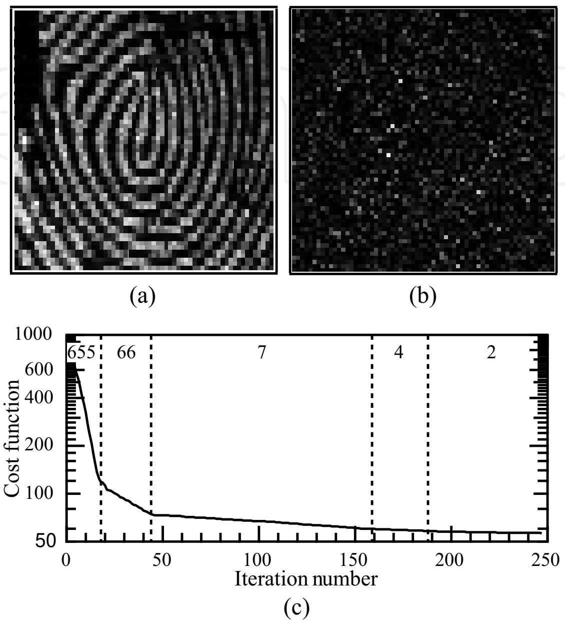

Fig. 11. Results for variable multiple-flip algorithm. Decrypted images from optimized hologram (a) with the encryption key and (b) with a wrong key. (c) Cost function for the iteration number.

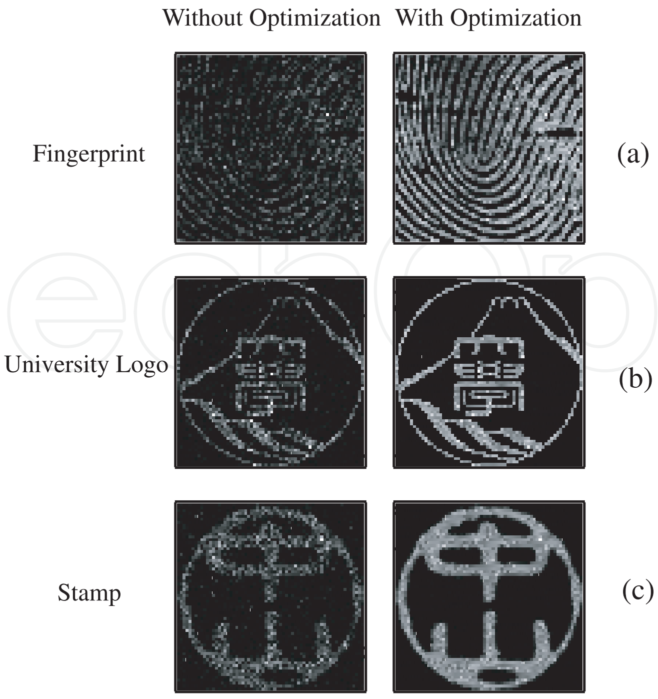

Fig. 12. Decrypted images from optimized holograms for various image structures in variable multiple-flip algorithm.

6. Optimization of hologram in real systems

6.1 Optical devices in real optical security systems

In the previous section, a binary encrypted hologram is used for easiness of optical reading and the degraded decryption image due to the binarization is successfully recovered by the optimization of hologram. In that system, we assume that not only a hologram but also a decryption key are displayed through electronic imaging devices. Even when we use optically addressed spatial light modulators (SLMs) with smart-pixel in optical security systems, we must inevitably use some electronic devices for the projection of images onto the SLMs. For example, a liquid crystal television display panel is frequently used for such purpose either of amplitude or phase modulation device. Such an imaging device has a lattice structure, in which the clear aperture is less than 100 % and only a limited light by the lattice structure passes through each pixel. Fig. 13 shows an example of a microscopic image of a liquid crystal display used as an electronically addressed SLM. The aperture ratio is about 0.55 in this case. In the joint transform system using real electronic devices, the decrypted image is greatly degraded due to the presence of the lattice structure, if we use an encrypted hologram generated from pure numerical calculation without considering the lattice structure. Or at worst case, we could not reconstruct any original image due to the degradation (Ohtsubo & Fujimoto, 2002). In this section, we apply the method of the simulated-annealing like optimization for binary hologram in real optical security systems and demonstrate successful decryptions of original images in the presence of lattice structures. The optical security system we treat here is the joint Fourier transform system. Both for the displays or projections of the hologram and the decryption key, we consider the use of electronically addressed SLMs such as liquid crystal television panels.

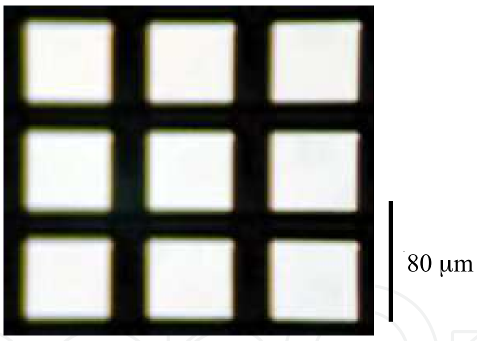

Fig. 13. Example of lattice structure of a liquid crystal television display used for electronically addressed spatial light modulator.

6.2 Holographic reconstruction in the presence of lattice structure

Here, we suppose the use of electronic display devices for the decryption of the encrypted hologram in a real optical security system. We assume that each pixel of an image in the input plane has a clear aperture ratio of 25 %. Actual display devices, for example LCTV panel, may have a rather larger value of the clear aperture, however, we take the value for the easiness of the numerical simulations. Fig. 14 shows the result of the numerical simulation for such a case. Fig. 14(a) is the same hologram as in Fig. 7(b), but it is embedded into the periodic lattice structure. The total size of the pattern in the input plane is expanded to 256x256 due to the presence of the periodic lattice structure. Fig. 14(b) is the same random key pattern as that in Fig. 3(b), but it is also embedded into the periodic lattice structure.

Using the hologram and the random key pattern in Figs. 14(a) and (b), the decryption was performed. The result is shown in Fig. 14(c). We cannot see any information of the original pattern of the fingerprint image. In the optical security system discussed here, the decryption is not a simple reconstruction of hologram, such as illumination by a plane wave. The hologram is illuminated by the Fourier transform of the random key pattern. Therefore the illumination of the Fourier transform of the periodic lattice structure greatly affects the performance of the reconstruction of hologram. It has less redundancy compared with a simple holographic reconstruction done by a plain wave illumination. Without considering the lattice structure, at worst case, we cannot extract any information from the reconstructed pattern as shown in Fig. 14(c).

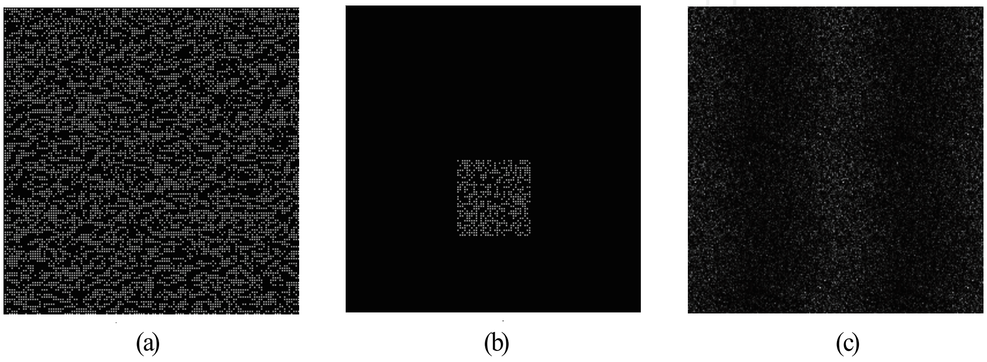

Fig. 14. Image decryption in the presence of opaque lattice structures on the hologram and the decryption key pattern. (a) Hologram, (b) decryption key pattern, and (c) decryption of image.

6.3 Optimization of hologram in the presence of lattice structure

The procedure for optimization of hologram in the presence of a lattice structure is almost the same as discussed in section 3. Starting from a hologram as shown in Fig. 14(a) together with a decryption key in Fig. 14(b) all including the lattice structures, the optimization of hologram to obtain good reconstruction is performed following the step 1~5 as discussed in section 3. Throughout the following optimization, the decryption key pattern, which also has a periodic lattice structure, is not changed and is assumed to be the same pattern as shown in Fig. 14(b). On the other hand, starting from the encryption hologram shown in Fig. 14(a), the value of each pixel of the hologram is modified by flipping from +1 to –1 or vice versa. In each flipping, we test the newly decrypted image as to whether it gives rise to a good reconstruction or not. The flipping is successively repeated for every pixel. If the cost function for the optimization still has a large value, the next iteration is performed. When the value of the cost function is sufficiently lowered, the iteration stops. Then, the image is optimized to reach a good estimation.

In the numerical simulation for the optimization, the area of the image to be compared with the decrypted pattern is expanded to 64x64 pixels due to the presence of the periodic opaque lattice structure. Therefore, we used the fingerprint image with 64x64 pixels as the ideal target image as shown in Fig. 15(a). Fig. 15(b) is the optimized hologram calculated by the proposed method when it contains the lattice structure. Using the optimized hologram together with the random key pattern in Fig. 14(b), we obtain the decrypted pattern as shown in Fig. 15(c). We can successfully decrypt an image close to the original one, though the periodic multiple images are reconstructed. The multiple images are originated due to the presence of the periodicity of the lattice structure in the display panels. The value of the cost function rapidly decreases in a few iterations and it reaches almost less than 10 % of the initial cost. At the final iteration number, the cost function is less than 5 % of the initial cost. The cost function of 5 % is considered as an enough criterion for the reconstruction of the original images. Indeed, the correlation between the original and decrypted images over 95 % is obtained at this criterion and the reconstructed image can be used for the identification in the security system (Nakayama & Ohtsubo,2007).

Flipping each pixel value of the hologram on the SLM through a computer control, we can optically and electronically perform the same optimization as done by the numerical simulation discussed here. In actual situation, a lattice structure to display an image is not only the issue to be overcome. However, based on the same principle proposed here, structures of image acquisition devices, a misalignment between optical acquisition and display devices, and even aberrations though optical elements can be compensated by the optimization of binary hologram. Then we can obtain optically an optimized binary hologram for image decryption for a particular optical system.

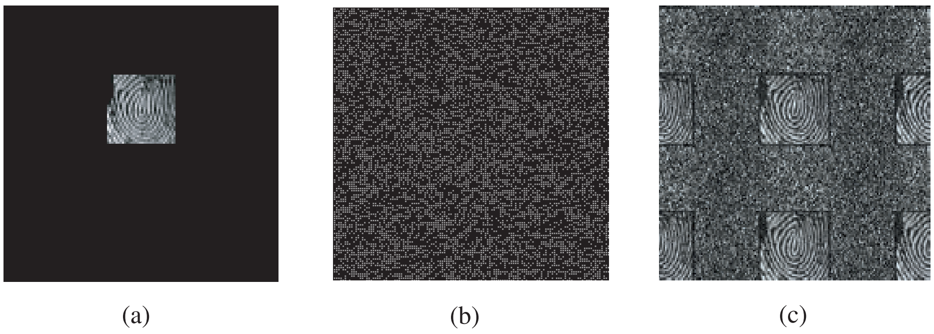

Fig. 15. Optimization of hologram to obtain the exact image. (a) Original image to compare the estimate of the decryption, (b) optimized hologram, and (c) result of the decryption from the optimized hologram.

7. Phase-coding method and optimization of hologram

7.1 Method of phase-coding

A hologram with a reference of a random pattern has been used for security encoding of biometric patterns. The methods have been proved to be useful by numerical simulations. Phase-coding techniques have widely been used due to the suitability for optical encoding and decoding with high degree of security (Neto & Sheng, 1996, Javidi & Ahouzi, 1998, Towghi et al., 1999, Tan et al., 2000, and Mogensen &Gluckstad, 2000 & 2001). However, they have some difficulties due to the lack of efficient optical devices used in the systems. In those methods, an image for authenticity is encrypted as a hologram and the hologram is illuminated and reconstructed by a random decode key that is the same as the encryption key and, thus, the methods have some difficulties for actual optical implementation (Yan & Kim, 1996). For example, the size of each pixel of a decryption key must be exactly matched to the corresponding area of a hologram in the Fourier space. To avoid the difficulty, Park *et al*. (2001) proposed a technique to obtain a decrypted image by a simple joint Fourier transform of an encrypted pattern and a decryption key. Another difficulty is the availability of optical devices with sufficient resolution having a large dynamic range to implement a compact optical security system. Optical security systems to verify the authenticity such as credit cards and passport identifications are usually used with electronic imaging systems. Therefore, diffraction effects induced by array structures of electronic addressed spatial light modulators as input optical devices may also degrade the image quality of the reconstruction of holograms.

We here discuss a simpler method of image encryption and decryption in this section, which is different from one in the previous sections. In this method, an encryption of an image for the identification is done by a digital technique, and the decryption and the identification are assumed to be performed by optical systems. We here focus on the method of encryption and decryption of images. The degree of security for an encryption may not be so high, since the information of an original image is partially obtained from the reconstructed phase from the complex encrypted pattern. Therefore, we further consider the use of real-valued encrypted pattern instead of complex-valued encrypted pattern to enhance the degree of the security. Binarization of a complex-valued encrypted pattern that is obtained from the real-valued data is an another common technique to match optical read-out of images in practical optical security systems. Then, we also perform a binarization of an encrypted pattern and propose the method of the optimization for it to obtain a good quality image of the decryption.

7.2 Phase-coding: Theory

We here discuss the theoretical background of the phase-coding method. At first we assume that an original image $f_0(x,y)$ to be encrypted has binary values. The image is transformed to a phase pattern and the phase-coded pattern is multiplied by a binary random phase mask. The distribution of the total coded image is written by

$$f(x,y) = \exp[i\pi f_0(x,y)] \cdot \exp[i\pi r_0(x,y)] \tag{14}$$

where $r_0(x,y)$ is a random function that plays a role for the encryption key and both the functions $f_0(x,y)$ and $r_0(x,y)$ take values of "0" or "1." The Fourier transform of the coded function $f(x,y)$ is an encrypted pattern. Since the original image is transformed to a phase pattern and it is also scrambled by a random phase, one cannot exactly extract the information of the original image from the encrypted pattern without knowing the random key. It is noted here that the encrypted pattern has a complex-valued function and we need a complex representation of the encrypted pattern for the implementation in optical security systems. However, as discussed later, one can extract the original image with good quality from the real-valued binarized data of the encrypted pattern.

In the Fourier space, the amplitudes of the encrypted pattern and the Fourier-transform of the random phase key are simply added together for the decryption. Writing the encrypted pattern defined by the Fourier transform of Eq. (14) as $F(u,v)$, the amplitude distribution of the addition is given by

$$H(u,v) = F(u,v) + R(u,v) \tag{15}$$

where $R(u,v)$ is the Fourier transform of the function $r(x,y)=\exp\{i\pi r_0(x,y)\}$. The function $R(u,v)$ plays the role for the decryption key. Also it is noted that the decryption key is a complex-valued function. Then, the decryption is simply performed by an inverse-Fourier transform for the added pattern. The intensity of the inverse-Fourier transform $h(x,y)$ of Eq. (15) is easily calculated and written by

$$\begin{aligned}|h(x,y)|^2 &= |f(x,y)|^2 + |r(x,y)|^2 + f(x,y)r^*(x,y) + f^*(x,y)r(x,y) \\ &= 2 + 2\cos[\pi f_0(x,y)]\end{aligned} \tag{16}$$

Since we assumed that the original image has a binary value either "0" or "1," we obtain a negative binary image as a decryption for the input that has a value "4" or "0." The merit of the method is that the inverse-Fourier transform of Eq. (15) is exactly equal to the original image itself and the decrypted image does not contain a zero-th order diffraction or other components.

The method is straightforwardly applicable to a gray scale image. For a gray scale image, we need no change of the procedure for encryption and decryption. If analogue values of the function $f_0(x,y)$ are normalized by its maximum value and they are distributed between 0 and 1, we can also obtain a negative image of the input as easily understand from Eq. (16), though the decrypted image is nonlinearly transformed with a cosine function. But the nonlinearlity can be easily compensated by a digital method due to one to one correspondence between the intensity distributions of the two images. Alternatively, the original image $f_0(x,y)$ may be nonlinearly transformed in advance by an arccosine function to give rise to the exact distribution of the image in the encryption process.

7.3 Decryption of image by phase-coding method

The method is applied to a gray scale image and the real and imaginary parts of the hologram (not a binary hologram) are used in this subsection. Fig. 16 shows the simulation result. A fingerprint image in Fig. 16(a) has a gray scale distribution between 0 and 1. The image is encrypted with a random phase pattern and, then, decrypted following the theory. Finally, we obtain a negative image of the original one as shown in Fig. 16(b). The nonlinearlity of the image distribution due to a cosine function is not compensated in the figure. The size of the original image is also 64x64 pixels and the original intensity level of 8-bit gray scale is normalized to be unity.

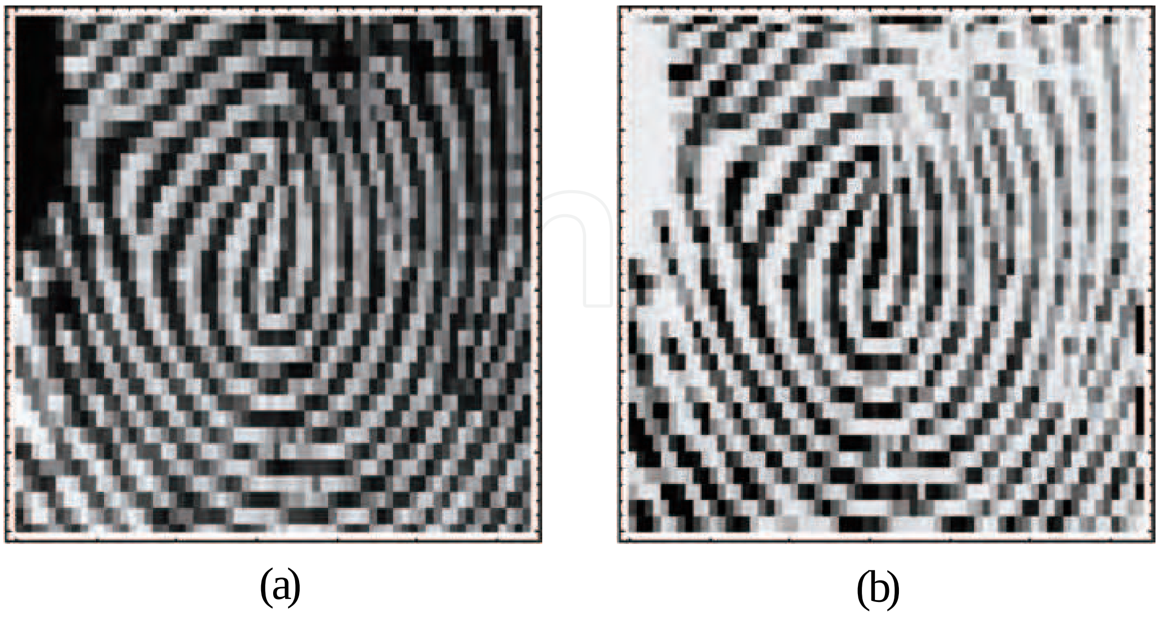

Fig. 16. Encryption (a) and decryption (b) for gray scale fingerprint image based on phase-coding method.

The degree of the security to hide an image behind a random mask is usually not so high when a phase function is reconstructed from an encrypted pattern. Furthermore, the representation of complex values of an encrypted pattern may not be suited for the implementation of practical optical security systems, since optical images are usually read out through an electronic interface. Therefore, we consider the use of a real-valued data from a complex encrypted pattern. For that purpose, we consider only real parts of an encrypted pattern and a decryption key. Using the real-valued data, the original image is exactly decrypted as shown in Fig. 17. Fig. 17(a) is an input fingerprint image to be decrypted. Here, we used an inverted gray scale and nonlinearly processed (arccosine transformed) fingerprint image to obtain the exactly expected image (compare it with Fig. 16(a)). The converted image is placed only in the area quarter of the input plane, since a mirror image is reconstructed due to the use of real-valued patterns in the following operation. Therefore, the total pixel size of the patterns used throughout the simulations is 128x128. Fig. 17(b) is a random key corresponding to the function $r_0(x,y)$. The encrypted pattern and the decryption key are calculated according to Eq. (14) and the Fourier transform of the random phase function, respectively. Next, we take the real parts of the Fourier transformed patterns. They are shown in Figs. 17(c) and (d). Then, the real-valued functions in Figs. 17(c) and (d) are added together and the result is inversely Fourier-transformed. The decrypted image is shown in Fig. 17(e). We obtain the exact image as a decryption, however a mirror image is also reconstructed due to the lack of the information of the imaginary parts of the encrypted image and the decryption key. From the standpoint of the degree of security, the use of a real-valued data from a complex encrypted image is not secure, since the imaginary part of the complex pattern can be easily reconstructed from its real part. Therefore, the binarization of encrypted image is essential for enhancing the degree of the security.

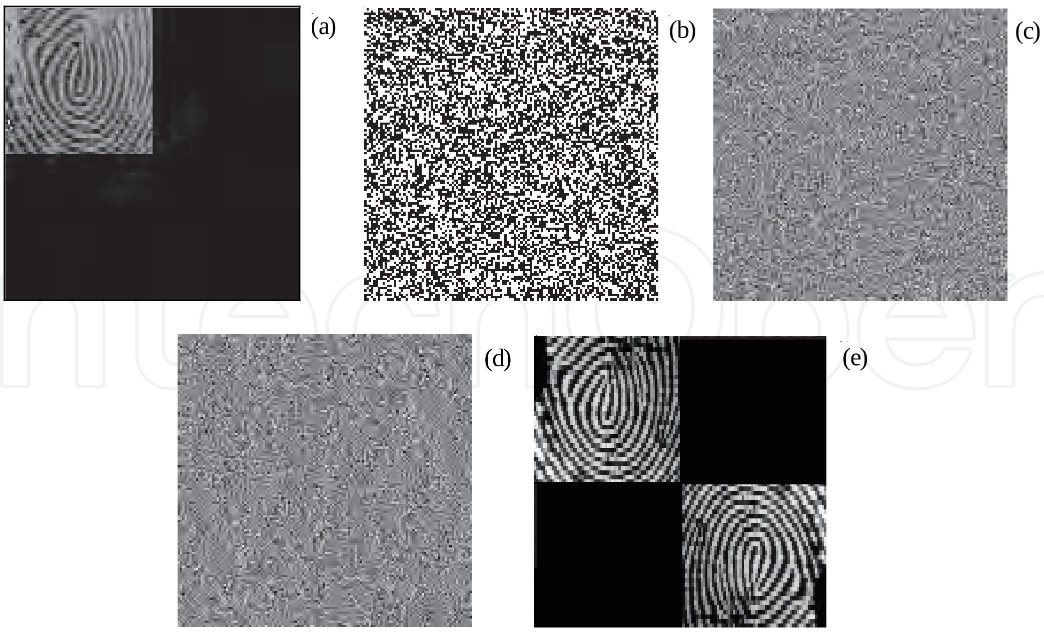

Fig. 17. Decryption using real-valued patterns. (a) Original image. The fingerprint image is inverted and the gray scale of each pixel is nonlinearly transformed by an arccosine function (compare it with Fig. 2(a)). (b) Encryption key, (c) real part of the encrypted pattern, (d) real part of the decryption key, and (e) decrypted image.

7.4 Binarization of encrypted image and its optimization

In actual applications, the format of an encrypted pattern must be congenial to an electronic interface in decryption process. Fast processing is only required for image decryption and identification. The binarization of a real-valued data also greatly enhances the degree of security for encryption and decryption in optical security systems as have already been discussed. We again employ the method of the binarization for an encrypted pattern. Fig. 18 shows the result of the binarizations both for the encrypted pattern and the decryption key. The binary encrypted pattern is obtained from the signs of the real part values of the original encryption pattern in Fig. 17(c). Namely, when a real part of each pixel of the encrypted pattern is positive, we set the pixel value to be +1 (optical phase is 0), while it is –1 (optical phase is π) for a negative value. The binary decryption key is made from the pattern in Fig. 17(d) as the same manner. Here we assume the use of optically addressed spatial light modulators (SLMs) with phase modulation in actual optical systems. The binarized patterns still have the original information. Then, adding the two binary patterns of the encrypted pattern and the decryption key shown in Figs. 18(a) and (b), the decryption of the image is performed. The result is shown in Fig. 18(c). Though we can recognize a dim structure of the fingerprint image, the decrypted image is greatly degraded due to the binarizations of the encrypted pattern and the decryption key.

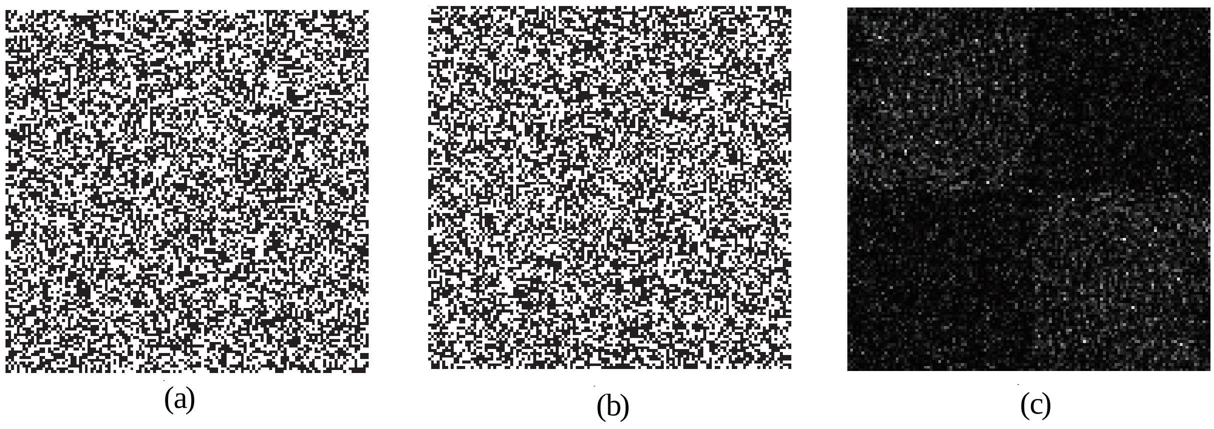

Fig. 18. Decryption using binarized patterns of encryption pattern and decryption key. (a) Binarized encryption pattern, (b) binarized decryption key, and (c) decrypted image. The patterns are binarized according to the signs of the real part values.

Therefore, we consider the optimization of the binary encrypted pattern. In the optimization, the decryption key is not changed and remains the same binary pattern as shown in Fig. 18(b) throughout the iterations. Starting from the binary encrypted pattern shown in Fig. 18(a), the value of each pixel of the pattern is flipped form +1 to –1 or vice versa. In each flipping, we test the newly decrypted image whether it gives rise to a good reconstruction or not. Then, the image is optimized to reach a good estimate. The method is one like a simulated annealing technique and the detail of the method is the same as that in the pervious section. The area to be compared for the optimization in the decryption image plane is only a quarter of the original pattern where the ideal fingerprint image is reconstructed. Figs. 19(a) and (b) show the optimized binary encrypted pattern and the result of the decrypted image, respectively. From the comparison between Figs. 19(b) and 18(c), the optimization goes well and almost the same image as the original fingerprint image is recovered as easily recognized from the comparison with the pattern in Fig. 17(e).

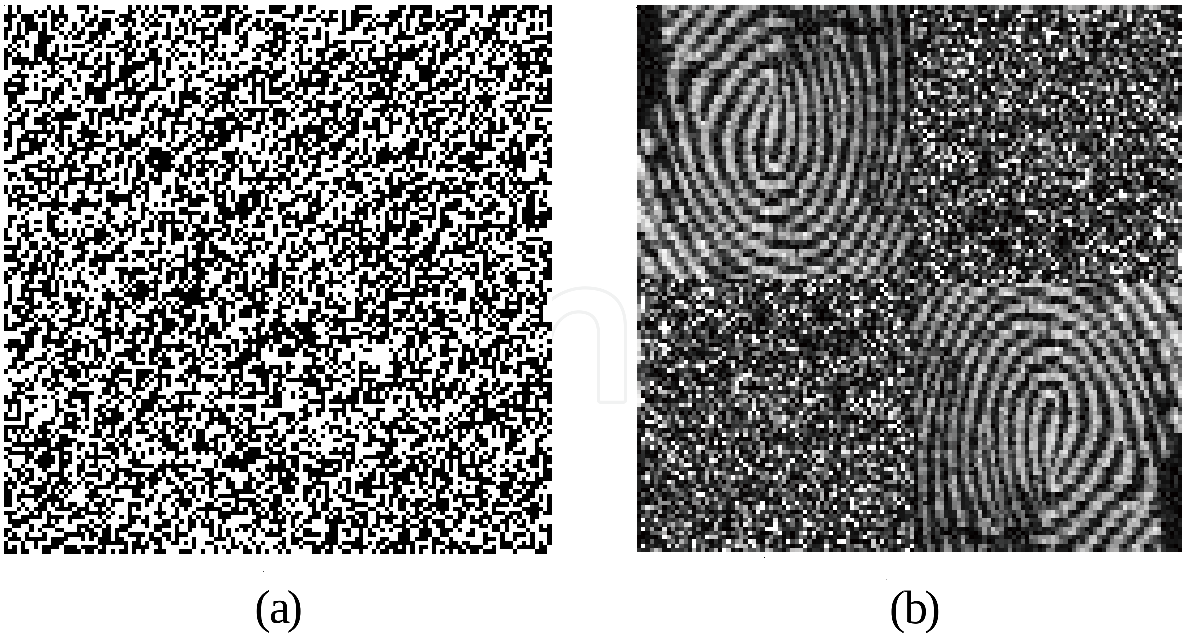

Fig. 19. Optimization of encrypted pattern. (a) Optimized binary hologram for Fig. 4(a) and (b) decryption of it.

Beside of the security problems in the proposed method, we must consider the congeniality of the method with optical systems. One of the merits of optics is a complex representation of information. Therefore, encryption and decryption of a complex image is easily performed and a high quality image of the decryption can be obtained in optical security systems. However, real systems include electronic interfaces and a complex image must be replaced by real-valued patterns. Furthermore, analogue write-in and read-out of optical data sometimes cause difficulties, for example a gray scale of a pattern must be faithfully recorded in the write-in process and the analogue gray level must be correctly scaled in read-out process. Reducing such problems, binarization of a complex-valued pattern is used as a common technique. However, the quality of a reconstructed pattern usually results in degraded one. Therefore, the optimization for a binary encrypted pattern is essential in optical security systems. As already discussed, we can obtain an excellent decrypted image based on a statistical optimization technique. In the system, we employed an optical phase encoding method, however we can alternatively consider an amplitude encoding technique. For example, instead of 0 (+1) or π (-1) phase encoding of the pattern, a binary amplitude, i.e. amplitude of 0 or 1, can be used. However, the amplitude encoding in the proposed method leads to the same result as that of the phase encoding except for a zero-th order diffraction spot in the reconstructed plane, since the addition of an encrypted pattern and a decryption key takes only three values, 0, 1, and 2. In the meantime, that for the phase coding has also three values of –2, 0, and 2 and the decrypted image reduces to the same pattern as that of the amplitude encoding. Therefore, we here employed the phase encoding technique. An optical phase modulation device is commercially available. The device can be used as a phase modulation spatial light modulator over 2π modulation depth. Generation and addition of phase images can be optically performed by using phase-controlled SLMs together with electronically addressed liquid crystal display panels as input imaging devices. Thus, optical decryption from encrypted pattern proposed here is easily implemented by using such devices. Fig. 20 is an example of the experimental results using

LCTV SLM. Fig. 20(a) is the experimentally reconstructed image and the nurerical reconstruction image is shown in Fig. 20(b) for comparison.

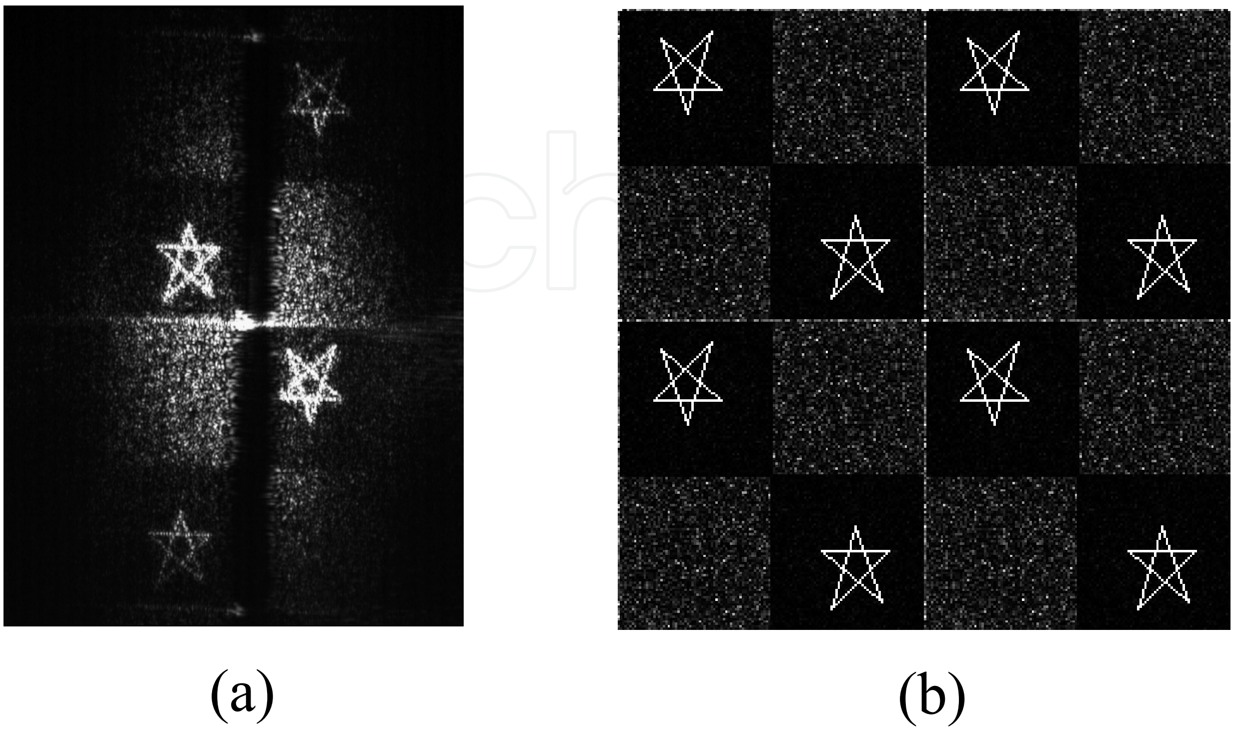

Fig. 20. Experimental result of optical phase-coding method. (a) Optical and (b) simulation results.

8. Conclusion

We have studied optical security systems for practical applications in verification of the authenticity, such as in a card system. The advantages of the optical method in a security are the fast decoding of an encrypted image and the identification of it. Firstly, we study a common method of joint transform correlation for optical security systems and the optimization of binary holograms and proved that the optimization of a hologram will be a powerful tool in the systems. As an alternative method, a phase-coding technique is introduced to congenital with the uses of real optical devices in optical security systems. Originally, the merit of optical systems is fast processing of decryption of hologram and identification of it. However, the methods discussed here, i.e., not only image encryption, but also decryption of hologram and identification of it, can be applicable in all-digital techniques using a recent fast computer.

9. References

Aarts E.; & Korst J. (1990). *Simulated Annealing and Boltzmann Machines*, John Wiley & Sons, Chichester

Bättig R. K.; Guest C. C.; Schaefer S. R.; & Toms D. J. (1992). Simulated Annealing of Binary Holograms for the Interconnection of Single-Mode Sstructures, *Appl. Opt.*, Vol.31, pp.1059-1066

Javidi B.; & Horner J. L. (1994). Optical Pattern Recognition for Validation and Security Verification, *Opt. Eng.*, Vol.33, pp.1752-1756

Javidi B.; Zhang G. S.; & Li J. (1996). Experimental Demonstration of the Random Phase Encoding Technique for Image Encryption and Security Verification, *Opt. Eng.*, Vol.35, pp.2506-2512

Javidi B. (1997). Securing Information with Optical Technologies, *Phys. Today,* Vol.50, pp.27-32

Javidi B.; & Ahouzi E. (1998). Optical Security System with Fourier Plane Encoding, *Appl. Opt.*, Vol.37, pp.6247-6255

Kipatrick S.; Gelatt Jr. C. D.; & Vecchi M. P. (1983). Optimization by Simulated Annealing, *Science,* Vol.220, pp.671-679

Kobayashi Y.; & Toyoda H. (1999). Development of an Optical Joint Transform Correlation System for Fingerprint Recognition, *Opt. Eng.*, Vol.38, pp.1250-1210

McCallum B. C. (1990). Blind Deconvolution by Simulated Annealing, *Opt. Commun.*, Vol.75, pp.101-105

Metropolis N.; Rosenbluth A.; Rosenbluth M.; Teller A.; & Teller E. (1953). Equation of State Calculations by Fast Computing Machines, *J. Chem. Phys.*, Vol.21, pp.1087-1092

Mogensen P. C.; & Gluckstad J. (2000). Phase-Only Optical Encryption, *Opt. Lett.*, Vol.25, pp.566-568

Mogensen P. C.; & Gluckstad J. (2001). Phase-Only Optical Encryption of a Fixed Mask, *Appl. Opt.* Vol.40, pp.1226-1235

Nakayama K.; & Ohtsubo J. (2007). Fast Optimization of Binary Encrypted Hologram Based on Error Correction Method in Optical Security Systems, *Opt. Rev.*, Vol.14, pp.290-296

Neto L. G.; & Sheng Y. (1996). Optical Implementation of Image Encryption using Random Phase Encoding, *Opt. Eng.*, Vol.35, pp.2459-2463

Ohtsubo J.; & Nakajima K. (1991). Image Recovery by Simulated Annealing with Known Fouier Modulus, *Opt. Commun.*, Vol.86, pp.265-270

Ohtsubo J.; & Fujimoto A. (2002). Practical Image Encryption and Decryption by Phase-Coding Technique for Ooptical Security Systems, *Appl. Opt.*, Vol.41, pp.4848-4855

Ohtsubo J.; & Fujimoto A. (2007). Optimization of Binary Hologram Degraded by Periodic Lattice Structure of LCTV Panel in Real Optical Security Systems, *Opt. Rev.*, Vol.14, pp.266-270

Park S. J.; Kim J. Y.; Bae J. K.; & Kim S. J. (2001). Fourier-Plane Encryption Technique Based on Removing the Effect of Phase Terms in a Joint Transform Correlator, *Opt. Rev.*, Vol.8, pp.413-415

Refregier P.; & Javidi B. (1995). Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding, *Opt. Lett.*, Vol.90, pp.767-769

Tan X.; Matoba O.; Shimura T.; Kuroda K.; & Javidi B. (2000). Secure Optical Storage that uses Fully Phase Encryption, *Appl. Opt.*, Vol.39, pp.6689-6694

Towghi N.; Javidi B.; & Luo Z. (1999). Fully Phase Encrypted Image Processor, *J. Opt. Soc. Am. A*, Vol.16, pp.1915-1927

Unnikrishnan G.; Joseph J.; & Singh K. (1998). Optical Encryption System that Uses Phase Conjugation in a Photorefractive Crystal, *App. Opt.*, Vol.37, pp.8181-8186

Yamazaki M.; & Ohtsubo J. (2001). Optimization of Encrypted Holograms in Optical Security Systems, *Opt. Eng.*, Vol.40, pp.132-137

Yang H-G.; & Kim E-S. (1996). Practical Image Encryption Sscheme by Real-Valued Data," *Opt. Eng.*, Vol.35, pp.2473-2478