Optimization of encrypted holograms in optical security systems

Mitsuhiro Yamazaki
Junji Ohtsubo, MEMBER SPIE
Shizuoka University
Faculty of Engineering
3-5-1 Johoku
Hamamatsu, 432-8561
Japan
E-mail: ohtsubo@eng.shizuoka.ac.jp

Abstract. The method of the optimization for a binary phase hologram used in a security system is proposed. The hologram is made by a joint Fourier transform method and a simulated annealing technique is used for the optimization. A hologram of a fingerprint image with a random key reference is successfully optimized and almost the same image quality as the original one is obtained as a decoded image by the proposed method. The usefulness of the method in an optical security system is also discussed. © 2001 Society of Photo-Optical Instrumentation Engineers. [DOI: 10.1117/1.1334947]

Subject terms: optical encryption; optical decryption; optimization of binary hologram; optical security system; fingerprint identification; joint Fourier transform.

Paper 200002 received Jan. 3, 2000; revised manuscript received May 1, 2000; manuscript accepted for publication July 28, 2000.

1 Introduction

A hologram with a reference of a random pattern has been used for security encoding of biometric patterns.1–3 In these methods, a primary image is encoded with two random phase masks, one in the input plane and the other in the spatial frequency plane. The encoded pattern is like a white noise and the decryption of it is very difficult without knowing the random key for the encoding. For the decoding process, the encoded pattern is Fourier transformed and multiplied by the complex conjugate of the key random phase mask. The light that passes through this random phase filter is again Fourier transformed and the image is reconstructed in the output plane. In a security system such as a credit card system, the encoded pattern is printed on a card and the pattern is decoded where necessary. But it may not be easy to print the hologram data faithfully on a card, since the encoded hologram is complex. To avoid the complexity, the method of a joint transform power spectrum is introduced to make an encrypted hologram.4–6 In this method, an original image to be encrypted and a random key reference are put into the same input plane and they are jointly Fourier transformed. Then the encoded hologram is formed in the Fourier plane. The encoded hologram is reconstructed by using the key random pattern and the decoded image is reproduced in the image plane of a 4-f imaging system.

To obtain a good reconstruction of a hologram, a large dynamic range of its gray scale is usually required. It may not be practical to use a hologram with a large dynamic range on a card in security systems. Therefore, the binarization of holograms is considered. The method is very convenient for the fabrication of an encoded pattern in a security system and very robust in practical uses. Since optical security systems to verify the authenticity such as in credit card and passport identifications are usually used with electronic imaging systems, the binarization of the hologram is very suited for the preprocessing for the reconstruction and identification. However, the problem of the binarization is the deterioration of the reconstructed image quality. In this paper, we propose the method for the optimization of a binary phase hologram in a security system. The optical system employed is the joint Fourier transform system previously discussed.4–6 A hologram obtained in the system is binarized and converted to a binary phase hologram. A fingerprint image is used as an original image for the practical application and it is encrypted by a random phase pattern. Starting from the binarized hologram, it is optimized by a simulated annealing method7–10 to reproduce a good image almost equal to the original one. By the proposed method, the binary hologram that results in a low correlation with the original image at first is optimized and almost the same image as the original one is reconstructed by the optimization. The advantage of the optical method in a security system is the fast processing for decoding an encrypted image and identifying it. In the meantime, the time required to make an encryption pattern is not essential and the encryption of the image and printing the hologram on a card may be done offline. So the proposed method is useful for the practical application for verifying the authenticity such as in a credit card system.

2 Image Encryption and Decryption System

The optical security system we consider is fundamentally the same as that already proposed by Yang and Kim.4 The method is briefly summarized here. In the image encryption process, an image with a random phase mask is jointly Fourier transformed with another random pattern as shown in Eq. (1) and a hologram is formed at the Fourier plane. 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, re-
spectively, 2\(d\) is the separation between the centers of two functions, * denotes the complex conjugate, and \(H(u,v)\) is the resultant hologram. The image with a random phase is written by
\[
f(x, y) = f_0(x, y)\exp\{ib(x, y)\},
\]
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 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. 2. For the decryption corresponding to Eq. (1), we have
\[
p(x, y) = f(x, y - d) \otimes g(-x, -y) \otimes g(x, y) + f(-x, -y) \\
\otimes g(x, y) \otimes g(x, y) \otimes \delta(x, y + 3d),
\]
where \(\otimes\) 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.

In actual applications, such as in credit card identification, a binary hologram is suited for the digital-electronic preprocessing procedure of the pattern. The use of the binarization is one of the excellent methods to make a robust security system, so we employed a binary hologram as an encrypted pattern in the following. Figure 3 is an example of sets of patterns used in the simulations. Figure 3(a) shows a fingerprint image with 64×64 pixels and Fig. 3(b) is a random pattern used for the encryption key. Here we assume an 8-bit gray scale for the fingerprint image and \(\{0, 1\}\) binary random pattern (i.e., equivalently \((0, \pi)\) phase) as the encryption key. A random phase mask multiplied to the image in the input plane is assumed to be \((0, \pi)\) random phase different from the random key pattern. Figure 4 is the result of the encrypted binary hologram. The hologram that has a \((0, 1)\) binary distribution is printed on a card as a black and white pattern in the security system. However, for the reconstruction of the binary hologram, the value of each pixel is assigned to \(+1[\exp(i0)]\) when the pixel of the hologram has a positive value, while it is \(-1[\exp(-i\pi)]\) for a negative value. A hologram that has \((0, \pi)\) 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 \( \pi \) phase distribution has the advantage in the reconstruction, since the zeroth order diffraction is eliminated in the reconstruction pattern. Figure 4(a) shows an example of the calculated binary hologram corresponding to the original image with the random key pattern in Fig. 3. Figure 4(b) is the reconstructed or decrypted pattern. The hologram and the reconstructed image have the size of 256 \( \times \) 256 pixels. The lower noisy part in the figure is the second term in Eq. (3). The binarization of the 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 a result, the ability for 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.

### 3 Optimization of Encrypted Hologram

In optical security systems, fast processing is only required for the image reconstruction and the pattern matching between the reconstructed and reference images. For the optical security system considered here such as in a credit card identification system, the image encryption may be performed offline. 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 a digital computer. Here we 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 technique. In the simulated annealing, the \( (0, \pi) \) phase of each pixel in the hologram is flipped 0 to \( \pi \) 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

\[
E = \int \int [(f(x,y))^2 - \alpha I(x,y)]^2 dx dy,
\]

where \( f(x,y) \) is the amplitude of the original image to be reconstructed [defined by Eq. (2)], \( I(x,y) \) is the intensity of the estimate, and the scaling factor \( \alpha \) is defined by

\[
\alpha = \frac{\int \int |f(x,y)|^2 dx dy}{\int \int I(x,y) dx dy}.
\]

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. 5. 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 \( E(E_{\text{old}}) \) 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 \( \pi \) or \( \pi \) to 0. Then, the estimated hologram is reconstructed and the new cost function \( E_{\text{new}} \) is calculated.

- **Step 3:** the difference between the cost functions before and after the perturbation \( \Delta E = E_{\text{new}} - E_{\text{old}} \) 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

\[
P = \exp\left(\frac{-\Delta E}{T}\right).
\]
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: steps 2 and 3 are repeated for every pixel.
- Step 5: If the cost function of each iteration still has 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.

The process is almost the same as a usual simulated annealing method except for the random flipping of the $(0, \pi)$ phase pattern at the second step. When the cost function becomes small and the temperature is sufficiently cooled 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 Results and Discussion

In the simulations, the optimization of the binary phase hologram for the fingerprint image as shown in Fig. 4 (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). Figure 6 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 increases once with the increase of the iteration number and reaches its maximum point. Then it decreases for further increases of the iteration number. In usual simulated annealing, the cost function monotonically decreases with the increase of the iteration. However, in our case, it seems that the annealing process is trapped to a local minimum, since the perturbation to be added to the image is different from that of ordinary simulated annealing. In the ordinary method, an analog value is used as an original image intensity distribution. A small perturbation compared with the intensity value is added to each pixel of the image intensity and the perturbation is not a binary nature such as $1$ or $-1$ flipping for each pixel value. From the comparison between the two cooling schedules ($T = 1/\exp(n)$ and $T = 0.5(1 + n)$) in Fig. 6, it seems that a rapid cooling rate is rather effective for the optimization of the hologram. Surprisingly enough, the cost function monotonically and rapidly decreases without trapping any local minimum when $T = 0$, that is, there 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 our 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, but the reason is not clear at present. For either case, the optimized hologram well reproduces a fingerprint image very close to the original one.

The degree of the reconstruction for the optimized hologram is tested by a joint transform correlation method. Figure 7 shows the results. Figure 7(a) is the original fingerprint image (left) and the joint transform correlation between the same patterns (right). The result of the correlation is a 1-D 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 zeroth order correlation peak is normalized to 255 and the value of the correlation is only 39. Starting from the hologram corresponding to Fig. 7(b), the simulated annealing is performed along the procedure discussed in the previous section. Figure 7(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. 7(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 $n = 20$.

5 Conclusions

A practical image encryption method has been proposed for a security system such as for credit card and passport identifications. A binary phase hologram made by a joint Fourier transform system has been optimized based on a simulated annealing technique. In comparison with the binary hologram without optimization, the quality of the reconstructed image was much improved and the image was almost the same as the original one. The optimization of a binary hologram has already been reported, but, in our case, the reference to make a hologram and reconstruct it was a random pattern. The simulated annealing is usually a time consuming process, however, the time can be much saved by neglecting the stochastic process of the annealing (i.e., without the temperature cooling schedule) due to the random nature of the hologram as shown in the variations of the cost function in Fig. 6. As discussed in the introduction, the time required for the encryption is not essential in the system and the encryption of the image and printing the hologram on a card may be done offline. So the optimization of a hologram will be a powerful tool in the practical application for the verification of the authenticity in a card system. The advantages of the optical method in a security system are the fast decoding of an encrypted image and the identification of it. As mentioned, a $(0, \pi)$ binary hologram is easily made by using a liquid crystal spatial phase light modulator such as a PAL-SLM (Hamamatsu). We are now preparing such an experiment for optical decoding of encrypted fingerprint images and optical identification. When the decoded image is perfect, the following operations can be done very quickly based on the optical method. Due to high speed processing, it is easier to use multiple random keys for encoding images and to decode the image including the scan of the used key pattern.

References


Mitsuhiro Yamazaki received the BS degree in optoelectronics and mechanical engineering from Shizuoka University in 1998. He is now a master course student at the university. He is interested in optical information processing using spatial light modulators and optical security systems. He is a member of the Japanese Society of Applied Physics.

Junji Ohtsubo received the BS degree in electronics from the Kyushu Institute of Technology in 1973 and the MS and PhD degrees in electronics from Hokkaido University in 1975 and 1978, respec-
tively. In 1978, he joined the Mechanical Engineering Laboratory. From 1981 to 1982, he was a research associate at the Institute of Optics, University of Rochester. He joined Shizuoka University as an associate professor in 1985 and is presently a professor. His current research interests are statistical optics, optical information processing and computing, nonlinear dynamics in optics, and chaos in semiconductor lasers. Prof. Ohtsubo is a member of IEEE, the Optical Society of America, SPIE, the Japanese Society of Applied Physics, the Optical Society of Japan, and the Laser Society of Japan.