Visual Cryptography Based on an Interferometric Encryption Technique

Sang-Su Lee, Jung-Chan Na, Sung-Won Sohn, Cheehang Park,
Dong-Hoan Seo, and Soo-Joong Kim

This paper presents a new method for a visual cryptography scheme that uses phase masks and an interferometer. To encrypt a binary image, we divided it into an arbitrary number of slides and encrypted them using an XOR process with a random key or keys. The phase mask for each encrypted image was fabricated under the proposed phase-assignment rule. For decryption, phase masks were placed on any path of the Mach-Zehnder interferometer. Through optical experiments, we confirmed that a secret binary image that was sliced could be recovered by the proposed method.

Manuscript received Aug. 20, 2001; revised July 4, 2002.

Sang-Su Lee (phone: +82 42 860 1613, email: sangsu@etri.re.kr), JungChan Na (e-mail: njc@etri.re.kr), SungWon Sohn (e-mail: swsohn@etri.re.kr), and Cheehang Park (e-mail: chpark@etri.re.kr) are with Network Security Department, ETRI, Daejeon, Korea.

Dong-Hoan Seo (e-mail: dhseo@palgong.knu.ac.kr) and Soo-Joong Kim (e-mail: sjkim@palgong.knu.ac.kr) are with the Department of Electronic Engineering, Kyungpook National University, Daegu, Korea.

I. INTRODUCTION

The ability to share all kinds of information and resources is fundamental in today's global environment. However, at the same time a whole variety of security systems using encryption methods have also been developed to prevent information from being accessed or used by unauthorized people [1]-[5]. Visual cryptography is a very powerful method for sharing and encrypting information, especially an image [6]-[8]. The simplest version of the visual secret sharing method assumes that the image to be encrypted consists of a collection of black and white pixels and each pixel is handled separately. It divides an image into several encrypted slides under its encryption rule. Each original pixel appears in n modified versions (called shares), one for each transparency. Each share is a collection of m black and white subpixels, that is, one pixel in a secret image is magnified m times and shared among n slides. For decryption, the divided and encrypted slides must be stacked without any decryption algorithm. However, the resulting encrypted image has low contrast and signal-to-noise ratio (SNR) because of the subpixels generated during the encryption process.

This paper proposes a new visual cryptography scheme that uses an optical method with phase masks and a Mach-Zehnder interferometer [9], [10]. To encrypt a binary image, it is divided into an arbitrary-n of slides and the slides are encrypted using an XOR process with a binary random key or keys. The phase mask for each encrypted image is then fabricated using the proposed phase-assignment rule. For decryption, the phase masks are placed on any path of a Mach-Zehnder interferometer. Optical results confirm the efficiency of the proposed method.

II. VISUAL CRYTOGRAPHY METHOD AND OPTICAL INTERFERENCE

1. Visual Cryptography

Naor and Shamir [7] defined a model describing the visual cryptography as follows.

The visual cryptography scheme can be described by an $n \times m$ Boolean matrix $S=[s_{ij}]$, where $s_{ij} = 1$ iff the j-th subpixel in the i-th transparency is black. When the transparencies are stacked together in a way that properly aligns the subpixels, a combined share can be seen where the black subpixels are represented by a Boolean "OR" of rows in S. The gray level of this combined share is proportional to the Hamming weight $H(V)$ of the "OR"ed m-vector V. This gray level will be interpreted by the visual system of the user as black if $H(V) \geq d$ and as white if $H(V) < d - am$ for a certain fixed threshold $1 \leq d \leq m$ and relative difference $a > 0$.

Definition. A solution to the k out of the n visual secret sharing scheme consists of two collections of $n \times m$ Boolean matrices, C_0 and C_1. To share a white pixel, the dealer randomly chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the gray level of m subpixels in each of n transparencies. The solution is considered valid if the following three conditions are met:

① For any S in C_0, the "OR" V of any k of n rows satisfies $H(V) \leq d - am$.

② For any S in C_1, the "OR" V of any k of n rows satisfies $H(V) \geq d$.

③ For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t (where $t = 0, 1$) to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Conditions ① and ② represent the contrast, whereas condition ③ implies the security stacking fewer than k shares does not offer any advantage when deciding whether a shared pixel is white or black. S ($=S_0$) of C_0 satisfying condition ① and S ($=S_1$) of C_1 satisfying condition ② are

$$S_0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Each column of S_i represents visual subpixels.

The generating process of subpixels for (0110), the first row of S_0, is shown in Fig. 1(a) and an example of the (3,3) visual secret method is shown in Fig. 1(b), where the threshold ($=d$) and relative difference ($=a$) are 4 and 1/4, respectively. In this

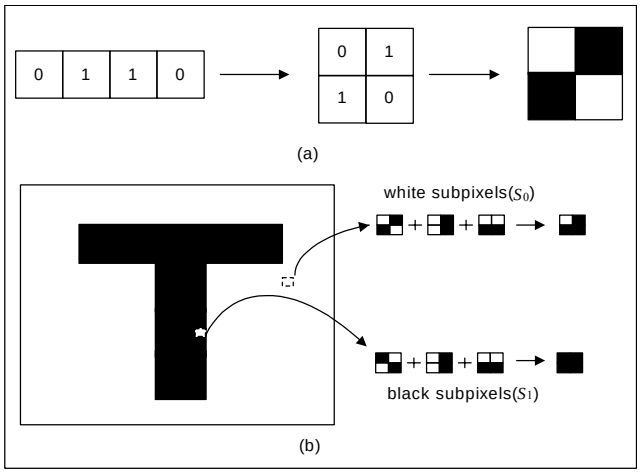

Fig. 1. (a) Generating process of subpixels and (b) visual (3, 3) secret sharing scheme.

conventional visual cryptography, the original image cannot be obtained from each slide, but rather by superposing all or several slides. Therefore, the original image cannot be obtained without assembling the whole group. Due to its simplicity, this system can be used without any knowledge of cryptography and without performing any cryptographic computations. Yet to make subpixels, each slide requires more resolution than the original image. Figure 2 shows (a) a secret image and (b) the decrypted image by conventional visual cryptography. The decrypted image has many noises around the reconstructed secret image but these noises are inevitable. Consequently, as mentioned in previous reports [6]-[8], conventional visual cryptography has low contrast and a worse SNR in the reconstructed image because of the subpixels.

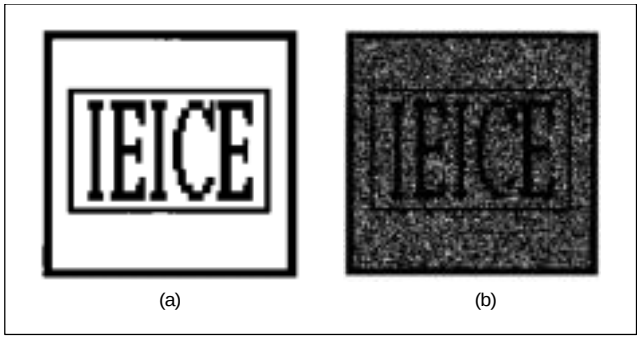

Fig. 2. (a) An original secret image and (b) decrypted image by conventional visual cryptography.

2. Interference between Two Waves

Let the two plane waves propagating in the z-direction with the same frequency ω, wavelength λ, amplitude E_0, and polarization be

$$E\ (z,t) = E_0 \cos(kz - \omega t + \phi), \tag{1}$$

where ϕ is the initial phase, t is the time, and k is the propagation constant.

Suppose that there are two waves, E_1 and E_2, with the same frequency and speed. The superposition wave between the two waves at a given instant can be written as

$$\begin{aligned} E_3 &= E_1 + E_2 \\ &= E_{01}\cos(kz - \omega t + \phi_1) + E_{02}\cos(kz - \omega t + \phi_2), \end{aligned} \tag{2}$$

where E_{01} and E_{02} respond to the amplitudes of E_1 and E_2, while ϕ_1 and ϕ_2 respond to the initial phases of E_1 and E_2, respectively. Within a linear, homogeneous, and isotropic dielectric, its intensity, I, becomes

$$I = \varepsilon \upsilon < E^2 >, \tag{3}$$

where the constant ε is the electric permittivity of the medium, υ is propagation velocity of a wave, and $< >$ denotes the time average of the function. Inasmuch as we are only concerned with relative irradiances with the same medium, the constants are simply neglected, thereby producing:

$$\begin{aligned} I &= < E_3^2 > \\ &= < (E_1 + E_2)\overline{(E_1 + E_2)} > \\ &= < E_1^2 > + < E_2^2 > + 2 < E_1 E_2 > \\ &= I_1 + I_2 + I_{12}, \end{aligned} \tag{4}$$

where $\overline{(E_1 + E_2)}$ means the exact conjugate of $(E_1 + E_2)$.

Recall that the time average of some function f(t), taken over an interval T, is

$$< f(t) > = \frac{1}{T}\int_{\tau}^{\tau+T} f(\tau)\, d\tau. \tag{5}$$

The interference term is then

$$I_{12} = E_{01}E_{02}\cos[k(z_1 - z_2) - (\phi_1 - \phi_2)], \tag{6}$$

where upon the total irradiance is

$$\begin{aligned} I &= I_1 + I_2 + 2\sqrt{I_1 I_2}\cos[k(z_1 - z_2) - (\phi_1 - \phi_2)] \\ &= I_1 + I_2 + 2\sqrt{I_1 I_2}\cos\Delta, \end{aligned} \tag{7}$$

where the phase difference(Δ) is the difference in the path length transversed by the two waves, as well as the difference in the initial phase angle, that is

$$\Delta = k(z_1 - z_2) - (\phi_1 - \phi_2). \tag{8}$$

At various points in space, the resultant irradiance depends on Δ. The maximum irradiance is obtained when $\cos\Delta = 1$. When the phase difference between the two waves is an even multiple of π, the disturbances are said to be in phase. This is referred to as a total constructive interference. In contrast, the minimum irradiance results when $\cos\Delta = -1$. This occurs when the phase difference is an odd multiple of π, and the waves are 180° out of phase. This is referred to as a total destructive interference, as shown in Fig. 3.

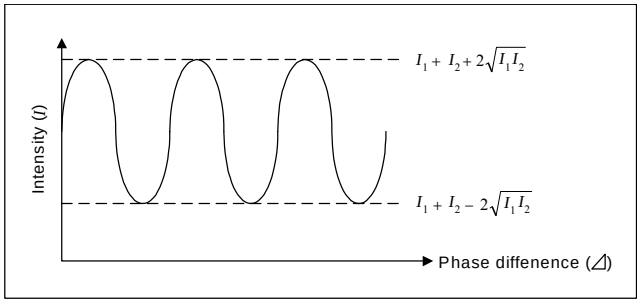

Fig. 3. Interference between waves due to phase difference.

If phase difference between E_1 and E_2 is an even multiple of π, the intensity of the interference pattern becomes the maximum value, and if the phase difference is an odd multiple of π, the intensity becomes the minimum value. As such, the interference pattern has two-level intensity values and can be changed to a binary image pattern after thresholding with a proper value. Accordingly, one intensity distribution is considered as a combination of a pair of phase distributions. If one phase distribution out of the pair is known, the other one can be easily determined from the interference intensity distribution. Finally, the binary intensity image can be represented by interfering with the two phase images. This idea is applied as a new method to generate phase masks for a binary image. The interference intensity in the interference plane can be controlled by the phase difference of the two beams in an interferometer, such as a Mach-Zehnder interferometer (Fig. 4). The phase difference between two beams can be generated by placing two phase masks on each arm of the interferometer. If the phase difference between the two waves split by the beam splitter BS1 is an even multiple of π, the intensity is maximized, whereas, if the phase difference between the two waves is an odd multiple of π, the intensity is minimized. The resulting interference pattern forms an intensity image.

Let's consider the case in which two phase-only images are placed on each arm of the interferometer, and every pixel of the two images has a phase value of 0 or π. If two pixels with the same phase value interfere with each other, the corresponding intensity value will be the maximum. On the other hand, interference between pixels with a different phase value will

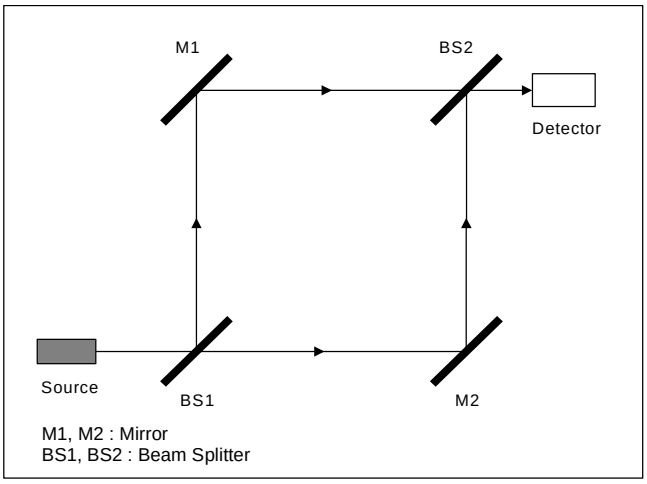

Fig. 4. Mach-Zehnder interferometer.

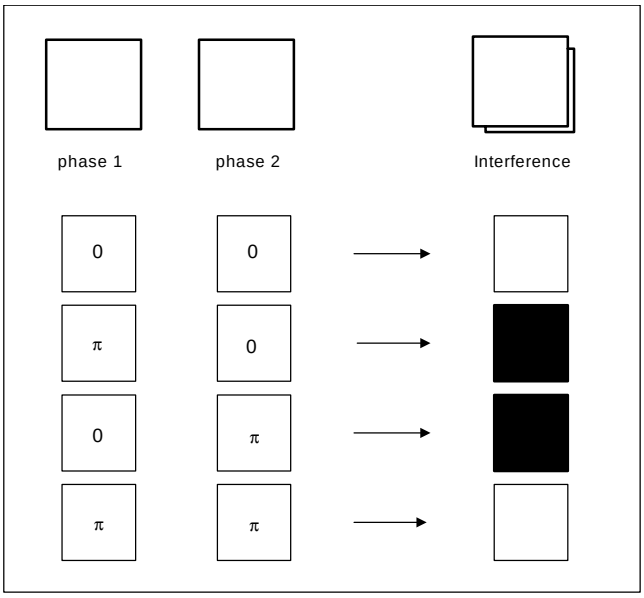

Fig. 5. Interference between two beams.

result in the minimum intensity (Fig. 5). This is very similar to the digital XOR logic operation.

III. PROPOSED ENCRYPTION METHODS: IMAGE ENCRYPTION USING VISUAL CRYPTOGRAPHY AND INTERFERENCE

We propose a new encryption technique using the visual cryptographic concept and a simple image decryption system using an optical interferometer. The technique includes two approaches according to the phase-assignment rule; however, they have the same encryption steps as those shown in Fig. 5. Each method divides an image to be encrypted into an arbitrary number of *n* slides and encrypts these slides through an XOR process with a random key or keys. Under phase-assignment rules, encrypted images can be transformed into encrypted phase masks. The proposed phase-assignment rules are followed.

It is true that in the proposed method slide images must be multiplied *n* times by different random keys, but these processes can be easily done using computers. Finally, fabricated phase masks cannot be copied using general intensity detectors, such as CCDs or human eyes. Additionally, this technique does not have to generate subpixels for encryption, whereas conventional visual cryptography has to. As we mentioned, subpixels are the main problem causing decrypted images to have low contrast and SNR. Ideally, if there are no environmental effects, such as vibration of air, setup errors in the interferometer, or incorrectly fabricated phase masks, the reconstructed binary image will have exactly the same image as the original binary image.

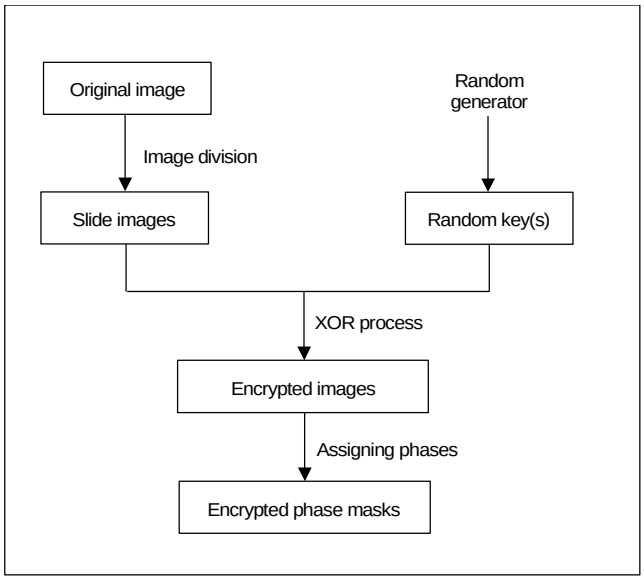

Fig. 6. Block diagram for the proposed encryption technique.

1. The 1-Key 4-Phase Method

The 1-key 4-phase method uses only one random key in the XOR process and four phase values in the phase-assignment process. Assume that we want to encrypt the image shown in Fig. 7(a). It consists respectively of binary values of zero and one according to black and white. First we divide the image into three slides (Figs. 7(b), (c), and (d)). Each slide has some portion of the original image. They can be obtained randomly or in a specified way. Figure 8(a) shows the XOR process for one random key, and Figs. 8(b), (c), and (d) show the XOR process for the encrypted slides for each of the three slide images. The next step is to fabricate phase masks from the encrypted slides under our proposed phase-assignment rule.

One can see that each divided slide has some regions in which the values of the pixels are the same as those of the original image and other regions in which those values are zeros as shown in Figs. 7(b), (c), and (d). We assigned 0 to white pixels and π to black pixels where the pixels corresponded to the encrypted pixels of the former regions (Figs. 8(b) and (c)). In the latter regions (Figs. 8(b) and (c)), we assigned 0 to the black pixels and π/2 to the white pixels. For the rest of the slides [4], a similar rule was applied except that π/2 was replaced with 3π/2. All phase masks under the described phase-assignment rule are shown in Figs. 9(a), (b), and (c). For decryption, we placed the phase mask having the values 0, π, or 3π/2 on one path of the Mach-Zehnder interferometer and the phase masks with π/2 together on the other path so that the total phase delay by the two masks could be added [5]-[8]. In the output plane of the interferometer we could obtain the original image because of the interference between the phase delayed lights that passed through each phase mask. For example, the phase delay due to the light passing through the pixels of the two phase masks in Figs. 9(a) and (b), which are placed on the same path of the interferometer, is 0 + π/2 = π/2, but the phase delay due to the light passing through the pixels of the phase mask in Fig. 9(c) is 3π/2. Consequently, the interference between the two lights generates the minimum intensity, that is, a totally dark pattern. In this way, the original image can be reconstructed. In general, when the number of slides is any number of *n*, one encrypted slide can have the phase values of 0, π, and *n**π/(*n*-1), and the others the phase values of 0, π, and π/(*n*-1). Each phase mask can be fabricated by the chemical etching of glass, such as lithography.

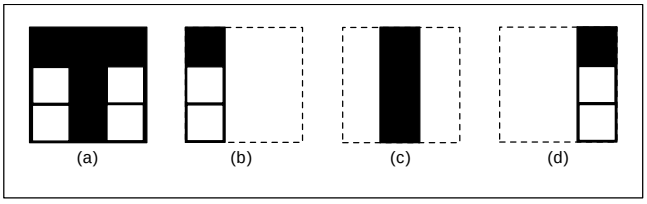

Fig. 7. (a) An original image, (b), (c), and (d) its divided images.

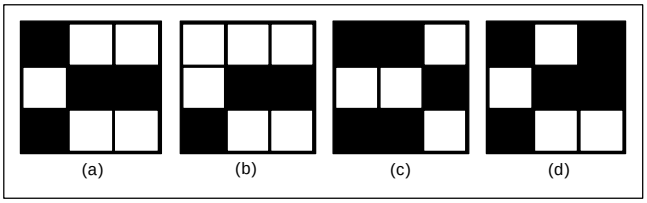

Fig. 8. (a) A random key, (b), (c), and (d) encrypted slides by XOR processing Fig. 6(b)-(d) with (a).

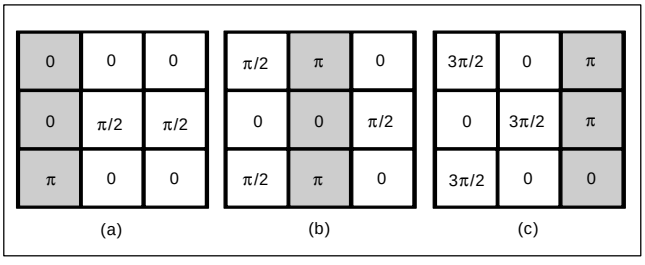

Fig. 9. (a), (b), and (c) Phase mask patterns.

2. The Multi-Key 2-Phase Method

The multi-key 2-phase method uses two phase values, 0 and π, for all the pixels in the phase-assignment process. If a secret image is divided into any number of *n* slide images, (*n*-1) random keys are prepared. The *n*-th random key can be obtained by the XOR process from among all the (*n*-1) random keys. The XOR of all the random keys gives just white images and this property plays the key role in encryption and decryption. Each slide is encrypted by an XOR operation with each key.

The following figures show an example of the two-phase method when *n* equals 5. An original image is divided into five other different slide images (Fig. 10). To encrypt the slide images, four random keys are generated and another random key is obtained by XOR processing. Figure 11 shows the generation of the five random keys. Through XOR processing between each slide and the random key, we obtained five encrypted slides (Fig. 12). The phase mask corresponding to each encrypted image can be made using the procedure of assigning 0 to white pixels and π to black pixels of the encrypted image [9]. For decryption we put each phase mask on any arm of the Mach-Zehnder interferometer. Thus, the

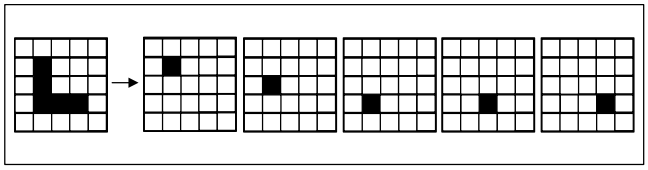

Fig. 10. Original binary image and its divided images.

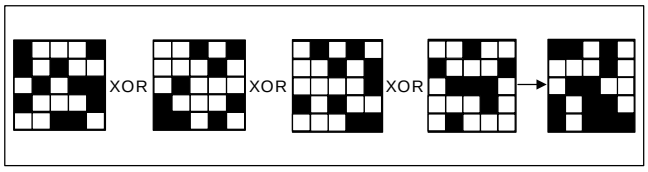

Fig. 11. Four random keys and another random key generation.

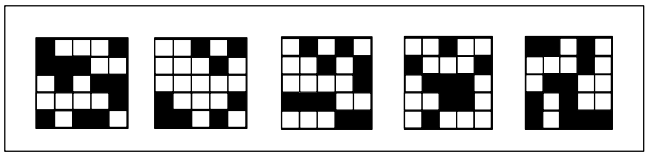

Fig. 12. Encrypted five images.

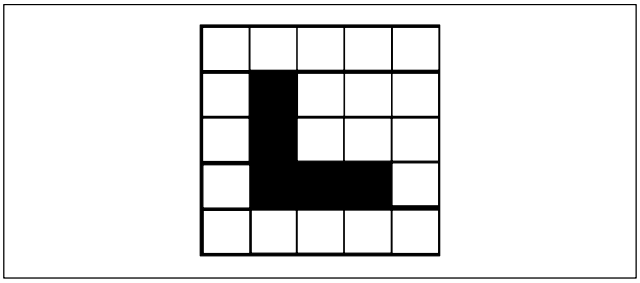

Fig. 13. Decrypted image.

phase delayed lights passing through the phase masks created an interfering intensity pattern as shown in Fig. 13, and it is the same as the original image in Fig. 10.

IV. OPTICAL EXPERIMENTS

Figure 14 depicts the decryption system for our simple optical experiment using the 2-phase method. We divided the original image (Fig. 15(a)) into two slide images (Figs. 15(b) and (c)) and encrypted them with the XOR process using the randomly generated key [10] (Fig. 15(d)). Two encrypted images are shown in Figs. 15(e) and (f) and their corresponding phase masks in Figs. 16(a) and (b). To fabricate the phase masks we used the phase-assignment rule as well as optical lithography. In optical lithography processing, a transparent glass plate is etched by a chemical solution, such as buffered hydrofluoric acid, in order to get the proper thickness pattern which represents the phase pattern. We controlled the etched thickness of the transparent glass under following formula,

$$D = \frac{\lambda \phi}{2\pi (n-1)},$$

where D is the thickness of the each pixel, λ is the wavelength of the light used in the decryption system shown in Fig. 11, ϕ is the phase value to be obtained, and n means the refractive index of the glass. The values of all parameters we used for our experiment are in Table 1. Finally, the value of D obtained from the values in Table 1 was 3.0423 μm and the size of each pixel was (2 mm×2 mm).

For decryption, the phase masks were placed on either of the two optical paths of a Mach-Zehnder interferometer. The path length difference between the two paths in the Mach-Zehnder interferometer should be zero or an integer multiple of 2π for an exact interference result. Finally, we obtained the experimental result shown in Fig. 16(c).

It is clear that the recovered image has fewer noises than the recovered image shown in Fig. 2(b). It is true that the decoded

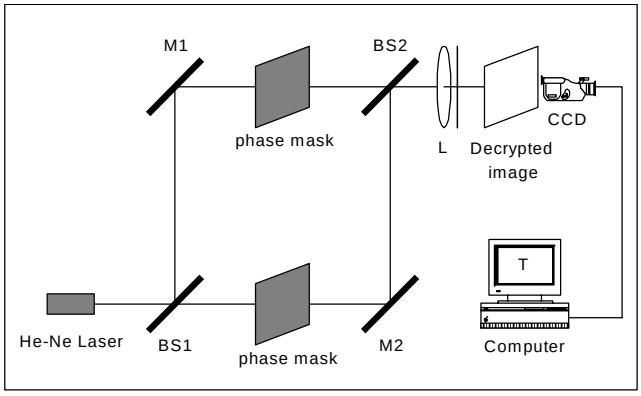

Fig. 14. Mach-Zehnder interferometer for image decryption system.

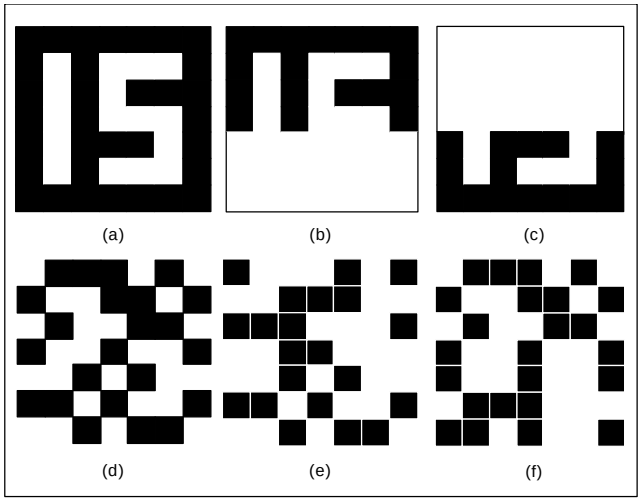

Fig. 15. Images and phase patterns for experiment: (a) original image; (b) and (c) divided images; (d) random key; (e) (b) XOR (d); (f) (c) XOR (d).

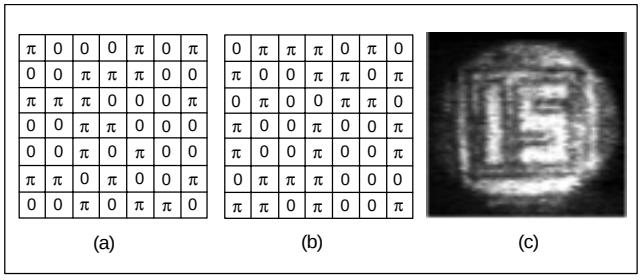

Fig. 16. (a) and (b) each phase pattern of Figs. 15(e) and (f); (c) interference result.

image shown in Fig. 16(c) has some noises around the image; this is likely due to errors in constituting the Mach-Zehnder interferometer and in fabricating the phase masks using the etching process. These errors may cause quality degradation, including noises, of the reconstructed image. Vibration of air or dust particles in the air may be another reason for the degradation. If the etching facilities were precise and the setup

of the interferometer accurate, the recovered image would have fewer noises than the image which was obtained from our experimental environment.

Table 1. The value of each parameter.

Parameter	Value
λ	632.8 nm
ϕ	5π
n	1.52

V. CONCLUSION

Although visual cryptography, which divides an image into several encrypted slides, is a very powerful method for sharing and encrypting information, its decrypted image has low resolution and SNR because of subpixels. To overcome this limitation, we proposed a new visual cryptography method that applies a phase-assignment rule to every encrypted image. The binary image to be encrypted was divided into any number of n slides. Only one random key or (n–1) randomly generated keys and the n-th random key from an XOR process between (n–1) random keys were prepared to encrypt these slides. The XOR operation between each divided image and each random key made the encrypted images. Each phase mask was obtained by assigning four phase values or binary phase values [11] to each encrypted image according to a new phase-assignment rule. For decryption, the phase masks were placed on interferometer paths and their interference pattern produced the same image as the original one. In the proposed system, the original image and decrypted image have the same resolution. Computer simulation and optical experiments demonstrated that the proposed method is feasible for optical security systems. However, though it is true that the proposed method has achieved a high level of security, it has done so at the price of a high redundancy, such as several times of multiplication between the sliced images and random keys. In addition, an exact alignment of phase masks, an exact setup of the interferometer, and accuracy of the phase masks are very important to get a clear decrypted image.

Encryption using an XOR operation is less robust than double random phase encryption [11]. To overcome this limitation, we are researching various methods to increase the robustness of the proposed encryption system against spatial noises. The results from this research will be addressed in the near future.

REFERENCES

[1] B. Javidi and J.L. Honer, "Optical Pattern Recognition for Validation and Security Verification," *Optical Engineering*, vol. 33, no. 6, 1994, pp. 1752-1756.

[2] P. Refregier and B. Javidi, "Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding," *Optics Lett.*, vol. 20, no. 7, 1995, pp. 767-769.

[3] B. Javidi, G. Zhang, and Jian Li, "Experimental Demonstration of the Random Phase Encoding Technique for Image Encryption and Security Verification," *Optical Engineering*, vol. 35, no. 9, 1996, pp. 2506-2512.

[4] R.K. Wang, "Random Phase Encoding for Optical Security," *Optical Engineering*, vol. 35, no. 9, 1996, pp. 2464-2469.

[5] L.G. Neto, "Implementation of Image Encryption Using the Phase-Contrast Technique," *Proc. of SPIE*, vol. 3386, 1998, pp. 284-290.

[6] A. Shamir, "How to Share a Secret," *Communications of ACM*, vol. 22, 1979, pp. 612-613.

[7] M. Naor and A. Shamir, "Visual Cryptography," *Advanced in Cryptography–Eurocrypt* 94, vol. 950, no. 7, 1995, pp. 1-12.

[8] C. Blundo, A. De Santis, and D.R. Stinson, "On the Contrast in Visual Cryptography Schemes," ftp:/theory.lcs.mit.edu/pub/ tcrypol/96-13.ps, 1996.

[9] Hecht, *Optics*, 2nd Ed, Addison-Wesley, Ch. 9, 1987.

[10] J.-Y. Kim, S.-J. Park, C.-S. Kim, J.-G. Bae, and S.-J. Kim, "Optical Image Encryption Using Interferometry-Based Phase Masks," *Electronics Lett.*, vol. 36, no, 10, 2000, pp. 874-875.

[11] B. Javidi, L. Bernard, and N. Towghi, "Noise Performance of Double-Phase Encryption Compared with XOR Encryption," *Optical Engineering*, vol. 38, Jan. 1999, pp. 9-19.

Sang-Su Lee received his BS and MS degrees in electronic engineering in 1999 and 2001, respectively, from Kyungpook National University, Korea. He has been a Research Staff Member of the Network Security Department in ETRI, Korea since 2001. His research interests include optical information processing, optical security, and active network.

Jung-Chan Na received his MS degree in computer science in 1989 from Soongsil University, Korea. He has been a Senior Member of Technical Staff in ETRI since 1989. His research interests include network security, active networks, and real time system.

Sung-Won Sohn is currently a Director of Network Security Department at Electronics and Telecommunications Research Institute (ETRI), Korea. He received his PhD degree in computer engineering from Choongpook University, Korea, in 1999. Since joining ETRI in 1991, his work has focused on the network technology and information security network security, optical security, active network, and biometry.

Cheehang Park received the BS degree in applied physics from Seoul National University, Korea, in 1974, the MS degree in computer science from Korea Advanced Institute of Science and Technology, Korea, in 1980, and the PhD degree in computer science from University of Paris 6, France, in 1987. During last 10 years he has been involved as Project Leader with several large projects such as multi-media computer system development and high speed parallel computer system development. His research interests include multi-midea systems, distributed systems, middleware, groupware, network virtual computing, and mobile agent architecture. He is currently the Vice President of Computer Technology Division of Electronics and Telecommunications Research Institute.

Dong-Hoan Seo received his BS and MS degrees in electronic engineering in 1996 and 1999, respectively, from Kyungpook National University, Korea, where he is currently pursuing his PhD degree in the Department of Electronics Engineering. His research interests include optical information processing, optical computing and optical security.

Soo-Joong Kim received his BS, MS, and PhD degrees in electronic engineering from Inha University, Korea, in 1962, 1966, and 1979, respectively. Since 1971, he has been with Kyungpook National University, Korea, where he is currently a Professor in the School of Electronic and Electrical Engineers. In 1976 and 1980 he was a Visiting Assistant and Associate Professor at the State University of New York at Buffalo and the University of Texas at Austin. He was the President of the Institute of Electronic Engineers of Korea in 1998. His research interests include optical information processing, optical security, optical computing, holography, and optical pattern recognition. Dr. Kim is a member of IEEE, SPIE, and OSA.