Image Encryption Based on Phase Decomposition Technique

KATSUHIRO UNO*† Member,  HOANG HOA TIEN DUNG† Non-member

(Received April 6, 2016, revised September 20, 2016)

Abstract: Novel technique for image encryption, which is based on a phase decomposition of the optical wave, and for decryption with an interferometric technique, was proposed. The phase decomposition was successfully performed by splitting pixel brightness into two vectors with random phases. The two encrypted images have constant amplitude and purely random phase, so that no one could see existence of the image. The hidden image was recovered by superposing and interfering with the two encrypted images. The decrypted image was exactly the same as the original with no noise. Our technique was applicable not only to binary images but also to grayscale images. We confirmed our technique by the computer simulation.

Keywords: visual cryptography, visual secret sharing, phase decomposition, interferometry, encryption, decryption.

1. Introduction

Visual cryptography (VC) was invented by Naor and Shamir [1] in 1995. They decomposed an image into n-transparencies with randomly assigned black and white blocks. Each transparency is called as “shar”. Therefore, the technique is also called as “visual secret sharing”. The image is recognizable only if k’s out of n shares are stacked together. The share consists of coded blocks with several black and white pixels, which are assigned to appearing as black/white color according to image brightness when all shares are stacked together. However, when we see stacking shares from far away, the white area of the image results in gray color because black pixels in one of the share cannot recover white color. Since the block size is inevitably bigger than one pixel, the share size is also bigger than the original image size.

The random-grid (RG) cryptography invented by O. Kafri and E. Keren [2] is one of the encryption methods without such pixel expansion. The RG uses the random grid that consists of randomly distributed black and white pixels as one of the share. The other share is constructed by assigning the pixel brightness same as the random grid provided that the image has a white pixel, and setting the complementary brightness provided that the image pixel is black. After stacking two shares together, pixels representing black brightness become always black and pixels representing white brightness become either white or black, which is dependent on brightness of the random grid. The black pixels that are supposed to be the white pixels become a noise and decrease the contrast of decrypted image.

Many researchers have tackled the problems about the VC, such as the contrast enhancement of the decrypted image, and avoidance of the pixel expansion problem [3]-[9]. However, quality of decrypted image has not improved enough for practical use. Moreover, the image type applicable to the ordinary VC has been limited to binary type.

We propose a novel technique for VC where the pixel brightness is broadened to the complex value with random phase. The complex value is decomposed to two vectors. Either vector becomes a component of one of the shares. Shares made by our proposed method have uniform amplitude with random phase angle, so that no one can find any image in those shares. The encrypted image can be decoded by the vectorial superposition between the two shares. As far as we know, S-S. Lee et al. [10] were first ones that used the interferometric technique to VC. They still used binary images and binary phase coding. Our technique uses continuous phase coding and is applicable to every type of images, such as grayscale and color images. Apart from some diffraction effects, the encrypted image by our technique will have no noise and be exactly the same as the original image.

Theory for proposed cryptography is described following section. Numerical results are presented in section 3. Finally, some concluding remarks are stated in section 4.

2. Theory

2.1 Image encryption method

All images that are displayed on the TV monitor or the projector are represented by some pixel brightness whether monochromatic images or not. Even though color images, pixel brightness values are assigned for each primary color component, i.e. red, green, and blue. The pixel brightness is converted to the light intensity when viewing the images on the monitor or projector.

Let us consider that the light intensity transmitted through or reflected from the display device is represented by $I(i, j)$. Here, indices $i$ and $j$ indicate the $i$-th row and
the $j$-th column of the image pixel. The light intensity represents a light energy impinging on unit area per second and is proportional to the square modulus of the electric or magnetic vector. In the isotropic media, we allow to deal with only either electric or magnetic vector as a scalar wavefield, without loss of generality. We denote the scalar wavefield as $U(x, y)$. The wavefield has two variables, i.e. the amplitude $A$ and the phase $\phi$, and can be expressed as $U = A \exp(j\phi)$. Then, the intensity is related to the amplitude as $I = |U|^2 = A^2$ and not related to its phase. Therefore, one degree of freedom can be added to express the light intensity, when expressing it as the wavefield.

We consider the phase $\phi$ to be a random variable of which value uniformly ranges from $-\pi$ to $\pi$. The amplitude $A$ is equal to the square root of the light intensity of the image, i.e. $A = \sqrt{I}$. When the wave field transmitted or reflected from the display device has the same profile as $U$, the light intensity received by human eyes or projection screen will depict the original image regardless of the feature of the phase distribution because of $|U|^2 = |A \exp(j\phi)|^2 = A^2 = I$.

It is known that the liquid crystal display device can alter the phase of the wavefield in proportion to the pixel brightness of the image. If the amplitude transmittance or reflectance of the device is $r$ ($0 \leq r \leq 1$), and the maximum light intensity of the incident wave is $I_{\text{max}}$, then the transmitted or reflected wave amplitude becomes $A_r = r \sqrt{I_{\text{max}}}$.

Now we denote the wavefield $U$ as a vector having length $A$ and phase angle $\phi$ as shown in Fig. 1. Let us consider how to compose the field $U$ with two vectors having the same length as $A_r$. This can be easily implemented as shown in Fig. 2. Both of two vectors have the same rotational angle $\theta$ from the field vector $U$. As shown in the geometry of Fig. 2, the angle $\phi_1$ and $\phi_2$ are related to the random phase $\phi$ and $\theta$ as

$$\phi_1 = \phi - \theta, \quad \phi_2 = \phi - \theta.$$  

The following cosine theorem is applicable between the field vector $U$ and one of the two vectors.

$$A^2 + A_r^2 - 2AA_r \cos \theta = A_r^2.$$  

Then, we obtain

$$\theta = \cos^{-1}\left(\frac{A}{2A_r}\right).$$  

It should be noted that the phase angles $\phi_1$ and $\phi_2$ are also random variables since $\phi$ is random. Therefore, two wavefields, $U_1 = A_t \exp(j\phi_1)$ and $U_2 = A_t \exp(j\phi_2)$, have random phase profiles. However, their amplitudes are constant value of $|U_1| = |U_2| = A_t$, so that no one is able to see what the device displays since we can only see constant intensity of $|U_1|^2 = |U_2|^2 = A_t^2 = r^2I_{\text{max}}$.

### 2.2 Image decryption

Image decryption can be performed by the interferometric technique. This means that two wavefields are superposed at the observation plane. When the wave field $U_1$ is added to $U_2$ coaxially, the total wave field $V$ is written as

$$V = U_1 + U_2 = A_t[\exp(j\phi_1) + \exp(j\phi_2)].$$  

Since only the light intensity is detectable for all existing detectors or human eyes, we will only receive the signal that is a square modulus of the wave field, i.e. $|V|^2$. Substituting eqs. (1), (2), and (4) into eq. (5) and performing the square modulus of it, we can finally obtain the original image intensity profile as

$$|V|^2 = A_t^2[\exp(j\phi_1) + \exp(j\phi_2)]^2 = 2A_t^2[1 + \cos(2\theta)] = 4A_t^2 \cos^2(\theta) = 4A_t^2 \frac{A}{2A_t} = A^2 = I.$$  

It should be noted that we do not set any premise about the intensity profile $I(x, y)$, so that all kind of images not only binary images can be encryptable.

### 3. Simulation Results

Based on the theory of previous section, we demonstrated the image encryption and decryption. Two kinds of images were used for encryption. One is a binary image as shown in Fig. 3 and the other is a gray scale image as shown in Fig. 4.

Procedures for encryption and decryption are shown as flow charts in Fig. 5. For comparison, the encryption and decryption process of the random grid method are also shown in Fig. 6. In the encryption, we set parameters,
I_{\text{max}} = 1$ and $r = 1$, so that $A_t = 1$. As shown in Fig. 5 and Fig. 6, the number of calculation steps of the proposed method is larger than that of the random grid method. However, the bitwise exclusive OR operation in the random grid method is heavier than other operation. When we used Scilab program for calculation, computation time of the random grid method was about 10 times larger than the proposed method.

According to the encrypted method shown in Fig. 5(a), we decomposed images in Fig. 3 and Fig. 4 into two randomly distributed phase profiles, respectively. The phase profiles made from the binary image in Fig. 3 are shown in Fig. 7. Phase components of the wave fields were randomized completely. Needless to say, the amplitude components of the wave fields are constant value of $A_t = 1$ (not shown in the figure). Therefore, no one can figure out the image contents.

We calculated histograms of the original image and one of two phase profiles, $\phi_1$, as shown in Fig. 8. The histogram of phase profile is completely uniform and is significantly different from that of the original image.

When the two wave fields, $U_1$ and $U_2$, were interferometrically superposed to pixel by pixel according to eq. (5), i.e.

$$V(i, j) = U_1(i, j) + U_2(i, j)$$

the intensity profile $I = |V|^2$ became completely the same as original image. The optical decryption can be performed by the interferometric apparatus as shown in Fig. 9. A laser source is divided into two beams impinging on a LCD panel. LCD depicts two phase profiles, share 1 and share 2, as shown in Fig. 7, where two arms of the laser beams go through. Two beams are coherently superposed on the mirror 3 and finally create the decrypted image at the screen. Unfortunately, owing to the current resource limitation in our laboratory, we just made some numerical simulations to verify the feasibility and effectiveness of the proposed method.

The decrypted image calculated by eq. (7) is shown in Fig. 10. By the interferometric superposition, the decoding error, which is inherent in the conventional visual secret sharing, was completely eliminated from the decrypted image.
Another result of phase profiles of two wave fields encrypted from the grayscale image of Fig. 4 is shown in Fig. 11. The decrypted image from those two shares is shown in Fig. 12. The decrypted image was completely the same as the original. The histograms of encrypted phase profile $\phi_1$ and the original image are shown in Fig. 13. The histogram of the phase profile is again uniform and is greatly different from that of the original.

We also estimated sensitivity against a noise. We added the Gaussian noise with zero mean and 0.1 standard deviation to one of the share. Conventional random grid method was used for comparison. Decoded images from two shares with noise are shown in Fig. 14. As shown in those figures, the decrypted image by the proposed method is clearer than that of the random grid method. The mean square error (MSE) of two images is measured for estimating noise sensitivity, which is defined as

$$MSE(I_1, I_2) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I_2(i, j) - I_1(i, j))^2$$  (8)

The MSE between the original image and decrypted image is tabulated in Table 1. The error of proposed method is significantly low, when the standard deviation $\sigma$ of Gaussian noise is 0, i.e. no noise. However, the proposed method is
Figure 13: The histogram of (a) original grayscale image and (b) decomposed phase profile.

more sensitive to the noise, since the MSE at $\sigma = 0.1$ is $10^{28}$ times larger than that of no noise while MSEs of the random grid are almost unchanged.

Table 1: The mean square error between the original image and the decrypted image. Encrypted image was Fig. 3. $\sigma$ is a standard deviation of Gaussian noise.

<table>
<thead>
<tr>
<th>$\sigma$</th>
<th>Proposed method</th>
<th>Random grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$4.66\times10^{-30}$</td>
<td>0.392</td>
</tr>
<tr>
<td>0.1</td>
<td>0.136</td>
<td>0.396</td>
</tr>
</tbody>
</table>

4. Conclusions

We proposed new encryption technique that utilized wave nature of light for VC. For encryption, the pixel brightness was decomposed to two vectors with constant amplitudes and random phases. Two shares made from that vectors had random phase distributions and constant amplitudes. This means that no one can see what the share itself display.

We also confirmed by the simulation that the interferometric technique was available for decryption. The encrypted image was successfully decrypted by superposing wavefields from two shares. It is noteworthy that the decrypted images were almost the same as the originals. This means that the proposed technique is able to recover the image without noise.

We estimated noise sensitivity of proposed method. If the shares contain some noise, they may bring significantly deteriorated result.

We have succeeded in performing the image encryption and decryption against not only binary images but also grayscale images. This means that the proposed technique is applicable to all types of images. Our method may advance VC to the practical level. Experimental result will be presented in the near future.

References

Katsuhiro Uno (Member) was born in Hokkaido, Japan, on August 19, 1967. He received a Ph.D. degree in engineers from Hokkaido University in 1995, and is presently an assistant professor at Ibaraki University. He has worked on image processing. He is a member of IIAE.

Hoang Hoa Tien Dung (Non-member) was born in Hanoi, Vietnam, on February 11, 1991. She is a student of graduate school of Science and Engineering of Ibaraki University. She is now studying the visual secret sharing and holography. She is a member of IIAE.