Current Optics and Photonics
Vol. 3, No. 6, December 2019, pp. 548-554

ISSN: 2508-7266(Print) / ISSN: 2508-7274(Online)
DOI: https://doi.org/10.3807/COPP.2019.3.6.548

A Joint Transform Correlator Encryption System Based on Binary Encoding for Grayscale Images

Kaifei Peng, Xueju Shen*, Fuyu Huang, and Xuan He

Department of Opto-electronics Engineering, Shijiazhuang Campus, Army Engineering University,
Shijiazhuang, Hebei 050003, China

(Received July 10, 2019 : revised August 14, 2019 : accepted September 10, 2019)

A binary encoding method for grayscale images is proposed to address their unsatisfactory decryption results from joint transform correlator (JTC) encryption systems. The method converts the encryption and decryption of grayscale images into that of binary images, and effectively improves decrypted-image quality. In the simulation, we replaced unencoded grayscale images with their binary encoded counterparts in the JTC encryption and decryption processes, then adopted a median filter to suppress saturation noise while keeping other settings unchanged. Accordingly, decrypted-image quality was clearly enhanced as the correlation coefficient (CC) between a decrypted image and its original rose from 0.8237 to 0.9473 initially, and then further to 0.9937, following the above two steps respectively. Finally, optical experimental results confirmed that the proposed encryption system works correctly.

Keywords : Optical communications, Optical image encryption, Joint transform correlator, Grayscale image, Binary encoding

OCIS codes : (060.4785) Optical security and encryption; (100.4998) Pattern recognition, optical security and encryption; (070.4550) Correlators

I. INTRODUCTION

In the field of optical information security, various techniques for optical image encryption have recently been proposed. Réfrégier and Javidi proposed an original double random phase optical encryption system [1], in which two independent random phase masks are located respectively in the input plane and the Fourier plane of the 4*f* system to encrypt the input image. Since the encryption system is structurally a 4*f* system, the two random phase masks must be precisely aligned in space, and a complex-conjugate key for decryption needs to be created. The encrypted image is a complex amplitude distribution, which is difficult to record and transmit. With the deepening of research, a variety of new encryption methods and improved techniques have been proposed. For example, Lang proposed an optical encryption method based on fractional Fourier transform [2]; Javidi and Nomura proposed an optical method based on digital holography [3]; and Nomura and Javidi proposed an optical encryption system using a JTC [4].

Among them, the JTC optical encryption system is a practical one that does not require a complex-conjugate key or precise alignment of the key mask, and whose encryption images are in grayscale, and easily recorded and transmitted [5-9]. Those advantages aside, one of the typical drawbacks here is poor decrypted-image quality, especially when the input is a grayscale image. Better decryption quality is attainable through a series of noise-control measures for binary-image inputs, because of their simple spectra [10-13]. On the contrary, when facing grayscale images, which intrinsically come with complicated spectra, decryption results are still not satisfying even after similar actions are taken. QR-based JTC encryption systems can only deal with images of very limited data content [14-17], even though they could recover images without any loss. Therefore, it is urgent and desirable to improve the decryption quality of

*Corresponding author: qgilxz@163.com, ORCID 0000-0002-4402-0682

Color versions of one or more of the figures in this paper are available online.

JTC optical encryption systems when faced with grayscale image inputs.

In response to that demand, this article offers a binary-encoding approach for grayscale images that actively restrains non-saturation noises for JTC systems during the encryption and decryption processes, and improves system output quality for grayscale-image inputs.

II. THE BINARY CODING APPROACH FOR GRAY SCALE IMAGES

If $g(i,j)$ denotes a 256 level grayscale image, then $0 \le g(i,j) \le 255$ and $g(i,j) \in N$, within which i and j are a pixel's horizontal and vertical coordinates respectively. Because a decimal number between 0 and 255 can be represented by an 8-digit binary number, any pixel of the grayscale image $g(i,j)$ could be encoded into a binary image of 8 pixels. Thus the grayscale image $g(i,j)$ can be enciphered into a binary image with 8 times as many pixels. To keep the same aspect ratio, we encrypted each grayscale-image pixel into a binary image of 3 × 3 pixels and tagged as $c(i',j')$, in which $i' \in \{3i-2, 3i-1, 3i\}$ while $j' \in \{3j\text{-}2,3j\text{-}1,3j\}$. Consequently, one pixel in the 3 × 3-pixel binary image is superfluous, and can function as a check code. Here are the steps to encode a grayscale image $g(i,j)$ into a binary image $c(i',j')$:

1. Convert the value of a pixel of $g(i,j)$ into an 8-digit binary number.
2. Put the 8 digits, in their original order, into slots $c(3i\text{-}2,3j\text{-}2)$, $c(3i\text{-}2,3j\text{-}1)$, $c(3i\text{-}2,3j)$, $c(3i\text{-}1,3j\text{-}2)$, $c(3i\text{-}1,3j)$, $c(3i,3j\text{-}2)$, $c(3i,3j\text{-}1)$ and $c(3i,3j)$.
3. Fill a parity check code into slot $c(3i\text{-}1,3j\text{-}1)$, to verify whether the encoding is correct.

By reversing the above steps, a binary-encoded image would be turned into its original grayscale image.

In the following example, Fig. 1 illustrates how a pixel in the original image of panel (a) is encoded into a 3 × 3-pixel binary image. Panel (b) presents a pixel's grayscale value from panel (a), 73, which equals the binary number 01001001, subsequently laid out in panel (c). Panel (d) is the binary-encoded image for that pixel, including a check code. The above steps change Fig. 1(a)'s original grayscale image into Fig. 1(e)'s binary image, with a size triple that of the original.

A 256-level grayscale image has 256 possible gray values, whereas a binary image only has 2 possible gray values, which are 0 and 255. For that reason, when an original grayscale image is subject to an optical system and produces a light field that is then recorded by a CCD, noise greater than 0.5 gray levels at a spot would increase the corresponding location's documented grayscale value by more than 1. In contrast, for the light field produced by a binary image after going through an identical system, if we implement binarization using a threshold gray level of 128, then an output pixel's grayscale value would flip from 0 to 255 only when afflicted by noise exceeding 128 gray levels. Accordingly, system noise affects binary images far less than grayscale images, when those images go through identical optical systems and generate pictures. That is, compared to grayscale images, binary images are much less sensitive to non-saturation noise.

III. OUTLINE AND PRINCIPLES OF A JTC ENCRYPTION AND DECRYPTION SYSTEM BASED ON A BINARY-ENCODED GRAY-SCALE IMAGE

In light of JTC systems' poor decryption quality for grayscale images, binary images are used to tackle the issue, since they are not sensitive to non-saturation noise.

Figure 2(a) illustrates a JTC encryption system, in which the focal length of the lens is *f*. The input plane's center is used as the origin to set up a rectangular coordinate system (x,y). An $n \times n$-pixel image is encoded into an $n' \times n'$-pixel binary image $c(x,y)$, in which $n' = 3n$. The binary image $c(x,y)$ attached to a random phase mask $r(x,y)$ of $n' \times n'$ pixels is placed at the object window, centered at the point $(\text{-}a,0)$ on the input plane. A random phase mask $k(x,y)$ is used as a key and placed at the key window, centered at point $(a,0)$ on the input plane. When illuminated by monochromatic plane waves of wavelength λ, items $c(x+a,y)r(x+a,y)+k(x+a,y)$ at the above two windows undergo optical Fourier transformation, and the joint power spectrum (namely the cryptograph) can be documented by a CCD at the spectrum plane [4]:

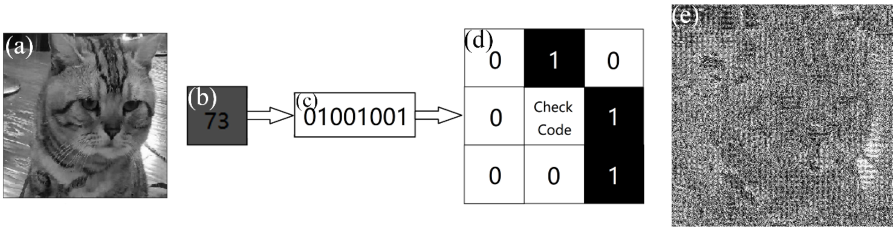


FIG. 1. Diagram of the binary-encoding approach: (a) Original grayscale image, (b) Sample pixel's grayscale value, (c) Binary grayscale value, (d) Binary-encoding image of the original pixel, (e) Complete binary-encoded image.

$$\begin{aligned}P(u,v) &= \left|\Im\{c(x+a,y)\cdot r(x+a,y)+k(x-a,y)\}\right|^2\\ &= \left|C(u,v)*R(u,v)\right|^2+\left|K(u,v)\right|^2\\ &+[C(u,v)*R(u,v)]^*K(u,v)\exp[\text{-}j2\pi(2a)u]\\ &+[C(u,v)*R(u,v)]K(u,v)^*\exp[\text{-}j2\pi(\text{-}2a)u]\end{aligned} \tag{1}$$

In the above formula, (u,v) and (x',y') are the spatial frequency coordinates on the spectrum plane respectively, and $u = x'/\lambda f, v = y'/\lambda f$. $C(u,v)$, $R(u,v)$ and $K(u,v)$ are individual Fourier-transform results for $c(x,y)$, $r(x,y)$ and $k(x,y)$. The $\Im\{\cdot\}$ stands for Fourier transformation, the symbol $*$ represents convolution, and the notation $[]^*$ denotes a complex conjugate.

Figure 2(b) sketches a JTC decryption system. A key, centered at point $(a,0)$, is put on the input plane. A cryptograph is laid over the spectrum plane, such that their centers coincide. When illuminated by monochromatic plane waves, the key experiences optical Fourier transformation and creates decrypting beams on the spectrum plane. Those beams pass through the cryptograph, undergo reverse optical Fourier transformation, and generate a light field on the output plane with a complex amplitude of [4]

$$\begin{aligned}g(x'',y'') &= \Im^{-1}\{\Im[k(x-a,y)]P(u,v)\}\\ &= k(x'',y'')*[r(x'',y'')c(x'',y'')]\otimes[r(x'',y'')c(x'',y'')]*\delta(x''-a,y'')\\ &+k(x'',y'')*\delta(x''-a,y'')\\ &+k(x'',y'')*k(x'',y'')\otimes[r(x'',y'')c(x'',y'')]*\delta(x''-3a,y'')\\ &+r(x'',y'')c(x'',y'')*\delta(x''+a,y'')\end{aligned} \tag{2}$$

In Eq. (2), $\otimes$ stands for the correlation operator, and (x'',y'') are the rectangular coordinates on the output plane.

The fourth formula component indicates the light field's power distribution, which is the plaintext. If the distances between the centers of the light fields denoted by those formula components on the output plane become large enough, those light fields remain separated in space, and a decrypted image can be retrieved from position $(\text{-}a,0)$.

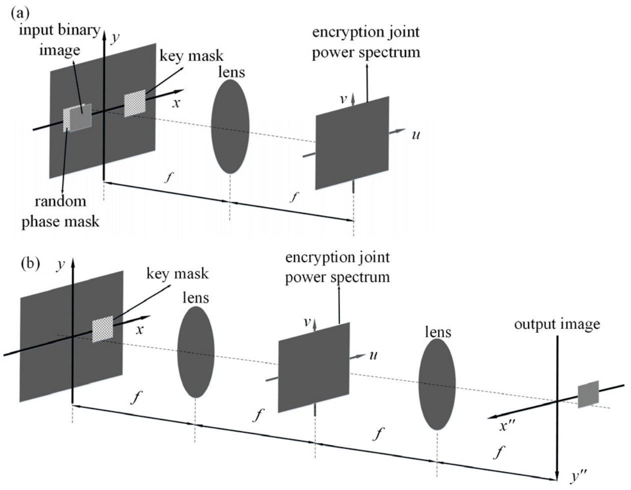


FIG. 2. Diagrams of JTC encryption and decryption: (a) JTC encryption system, (b) JTC decryption system.

During enciphering and deciphering, decrypted images are impaired by many factors: The illumination beams are collimated laser beams and not exactly monochromatic plane waves. The optical systems are actually low-pass filtering structures. The key windows and object windows are of limited area. Over the output plane of the decryption system, there are disturbances besides the deciphered image. The preceding examples are just some of the factors. Some actions targeted [11, 12] at those factors are taken, to remove noise and improve the deciphered image. In spite of that, the impact of those causes cannot be completely erased. Accordingly, binary images recovered through decryption are not perfect binary images, and so on, before they are converted to grayscale images, decrypted images need to go through binarization. The results are then transformed into grayscale images, which are used as the final, deciphered images.

IV. ENCRYPTION AND DECRYPTION SIMULATION AND ANALYSIS OF THE RESULTS

To prove that a binary-encoded picture of a grayscale image can improve decrypted image quality for a JTC cryptosystem, a grayscale image and its binary-encoded picture were used separately in simulations of a JTC cryptosystem's encryption and decryption processes. The original grayscale image used, shown in Fig. 1, is 160 × 160 pixels and has 256 gray levels. The laser beam has a wavelength of 632.8 nm, and the Fourier lens's focal distance is 400 mm.

4.1. Encrypting and Decrypting a Grayscale Image

When a grayscale image is encrypted, both windows on the input plane are 160×160 pixels. The object window's center is at $(\text{-}240,0)$, while the key window's center is at $(240,0)$. The random phase mask $r(x,y)$ and key $k(x,y)$ used here were presented in Figs. 3(a) and 3(b) respectively. The joint power spectrum is computed using Eq. (1), and then noise-erasing measures [11, 12] are applied to remove the noise term. The answer is then divided by the key's power spectrum to fabricate a new cryptograph, shown in Fig. 3(c). During the decryption process, the key $k(x,y)$, with center set at $(240,0)$, is put over the input plane. Next, the cryptograph is placed over the spectrum plane's center and the decrypted image, displayed in Fig. 3(d), is computed via Eq. (2) and retrieved over the output plane.

Correlation coefficient (CC) between the decrypted image and its original image is employed to evaluate decrypted image quality quantitatively. The CC is defined through this formula [10]

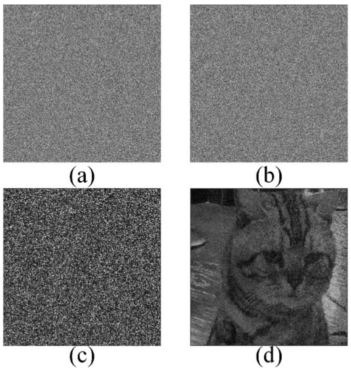


FIG. 3. Simulation results of encrypting and decrypting a grayscale image: (a) Random phase mask $r(x,y)$, (b) Key $k(x,y)$, (c) New cryptograph, (d) Decrypted image.

$$X_{cc}=\frac{\left|\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-\overline{f}][I(i,j)-\overline{I}]\right|}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-\overline{f}]^{2}}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-\overline{I}]^{2}}}\tag{3}$$

In this definition, i and j denote pixel coordinates, and the symbols f and $\overline{f}$ stand for the original image's gray level and the average gray level respectively. I represents gray level, while $\overline{I}$ symbolizes average gray level, of the deciphered image. The letters M and N signify the horizontal and vertical maximum coordinates of pixels individually.

Equation (3) yields a CC value of 0.8237 for Fig. 3(d). In the simulation, due to the diffraction caused by the limited area of the two windows on the input plane, the decrypted image contains a large amount of noise. In spite of the noise-reduction measures taken, such as eliminating noise terms and dividing the cryptograph by the key's power spectrum, the decrypted image presents some strong, obvious noise. Whereas its contours are moderately clear, it is still not quite satisfactory.

4.2. Encrypting and Decrypting a Grayscale Image through Its Binary-encoded Counterpart

When a grayscale image's binary-encoded counterpart is encrypted, both windows on the input plane are 480 × 480 pixels. The object window's center is at (-720,0), while the key window's center is at (720,0). The random phase mask $r'(x,y)$ and key $k'(x,y)$ used were presented in Figs. 4(a) and 4(b) respectively. The joint power spectrum is computed using Eq. (1), and then noise-erasing measures [11, 12] are applied to the cryptograph to remove the noise term. The answer is then divided by the key's power spectrum to fabricate a new cryptograph, shown in Fig. 4(c). During the decryption process, the key $k'(x,y)$, centered at (720,0), is put over the input plane. Next, the new cryptograph, after undergoing noise-reduction, is placed over the spectrum plane's center, and the decrypted image, displayed in Fig. 4(d), is computed via Eq. (2) and retrieved over the output plane. Binarization with a threshold set at 128 gray levels turns Fig. 4(d) into binary image 4(e). Thereafter, the processes in Section 1 are followed in reverse order to transform Fig. 4(e) into 4(f). This image shows that its noise basically is due to spots of saturation, since non-saturation noise is substantially muffled through using binary images in encryption and decryption operations. To further subdue saturation noise in the deciphered image, Fig. 4(f) was median filtered to arrive at the grayscale decrypted image in 4(g).

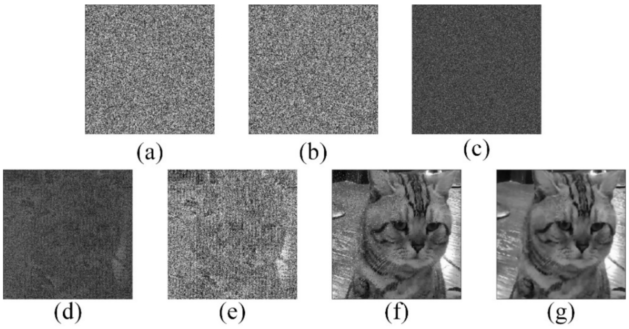


FIG. 4. Simulation results for encrypting and decrypting a grayscale image: (a) Random phase mask $r'(x,y)$, (b) Key $k'(x,y)$, (c) New cryptograph of the binary-encoded image, (d) Decrypted binary-encoded image, (e) Decrypted binary-encoded image after binarization, (f) Decrypted grayscale image converted with the decrypted binary-encoded image, (g) Decrypted grayscale image after median filtering.

The CC between the grayscale decrypted image in Fig. 4(f) and the original grayscale image reaches 0.9473. That value proves that the decryption outcome for a gray scale image has been remarkably improved through exercising the binary image's capability for suppressing non-saturation noise in enciphering and deciphering operations. There is only some saturation noise in certain areas of Fig. 4(f), which indicates that non-saturation noise created during decryption must have been substantially suppressed. This image demonstrates much higher quality than that of Fig. 3(d). Moreover, median filtering was effectively harnessed to further abate remaining saturation noise and produce Fig. 4(g). The CC between image 4(g) and the original was boosted to 0.9937, which suggests that the original picture has been reconstructed with almost no loss.

4.3. Effect of the Input-plane Window's Center Distance on Noise Strength in Decrypted Images

From Eq. (2) it can be inferred that the smaller the distances those light fields designated by the first three formula components have from a decrypted image's center, the greater the noises those light fields generate in the decrypted image, and vice versa. On those grounds, the magnitude of $2a$, the window distance over the input plane, directly affects noise strength in decrypted images [18].

Several $2a$ values are chosen, and the two encryption and decryption methods under comparison in this paper are applied separately to Fig. 1. Those deciphered images are illustrated in Fig. 5. Figures 5(a)~5(d) correspond respectively to $2a$ values of n, $2n$, $3n$, and $4n$ while a grayscale image is used directly in enciphering and deciphering. In Figs. 5(e)~5(h), the same $2a$ values are used, but a binary-encoded picture is used in encrypting and decrypting that same grayscale image.

The curve of CC values between the decrypted and original images, obtained by the two approaches above, is calculated according to Eq. (3) and shown in Fig. 6.

One can observe from Fig. 5 that if $2a$ remains unchanged, the approach that this article proposes consistently yields decrypted images with lower noise than the approach of directly encrypting and decrypting grayscale images. While $2a \le 2n$, noise within decrypted images attained through both methods diminishes as $2a$ rises. When $2a > 2n$, increasing $2a$ does not contribute much to subduing noise in decrypted images, for either technique.

From Fig. 6 it can be gathered that under the same $2a$ value, the CC values achieved using this paper's suggested method are invariably greater (by more than 0.1) than those obtained using the other approach. The CC values for both approaches rise as $2a$ builds up, as long as $2a \le 2n$. When $2a > 2n$, a change in $2a$ has little influence over CC values by either procedure. Under those conditions, the CC values are approximately 0.9 if grayscales images are enciphered and deciphered straightforwardly, but the CC values approach 1.0 if this article's suggested procedure is employed. A CC value close to 1.0 means a restoration with nearly zero loss.

Thus the method proposed in this paper has a capacity for greatly suppressing non-saturation noise (induced by the limited span between windows on the input plane) in decrypted images.

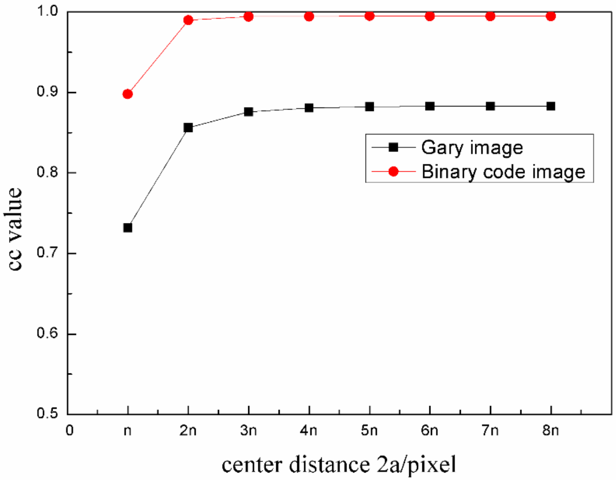


FIG. 6. Decrypted image's CC value versus center distance $2a$.

4.4. Influence of Image Encoding on Encryption and Decryption Speed

One of the most important advantages of optical encryption is its high processing speed. That considered, image pre-processing ought not to compromise a system's encryption and decryption speed too much. To evaluate the impact on a JTC encryption and decryption system's processing speed made by binary-encoding and QR-encoding techniques, their encoding speeds were contrasted.

It takes the QR-encoding method over five hours to encode 1,000,000 randomly created, 10 × 10-pixel, 256-level grayscale pictures. To complete the same job, binary encoding needs just 74 seconds. Hence binary encoding has a much smaller impact on a JTC encryption and decryption system's processing rate than QR-encoding does.

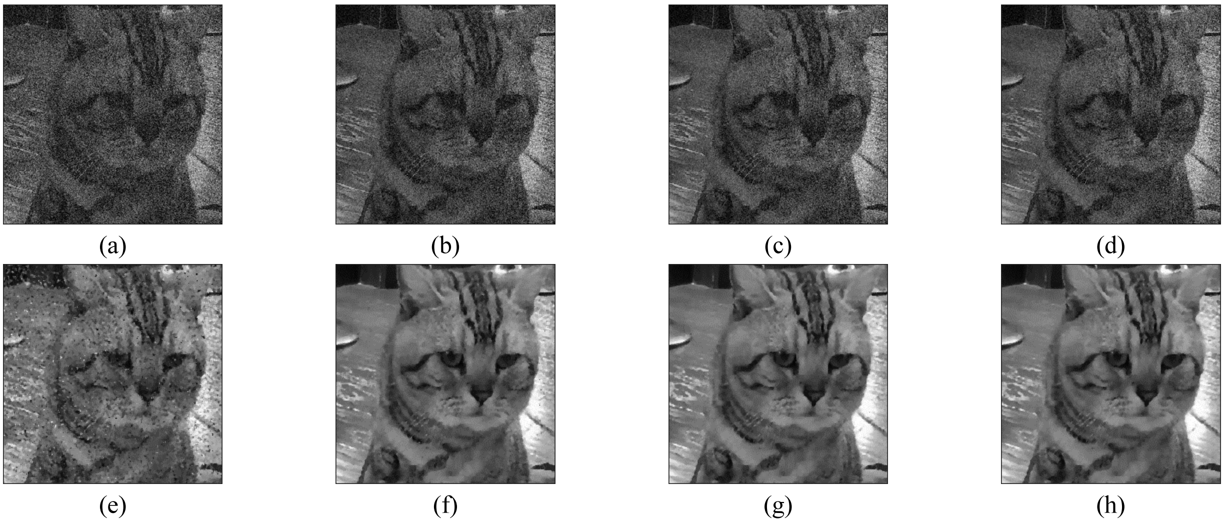
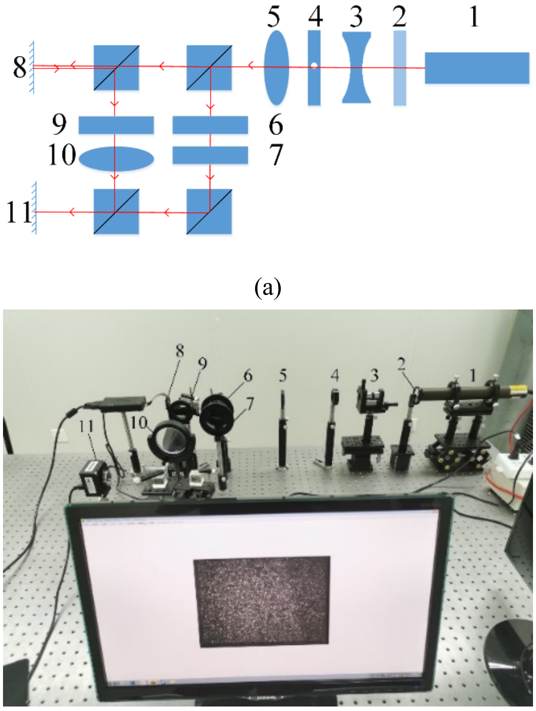


FIG. 5. Decrypted images using two methods under different center distances: (a),(e) $2a=n$, (b),(f) $2a=2n$, (c),(g) $2a=3n$, (d),(h) $2a=4n$, (a),(b),(c),(d) direct encryption and decryption, (e),(f),(g),(h) encryption and decryption using binary encoding.

V. AN OPTICAL EXPERIMENT TO VALIDATE THE SCHEME

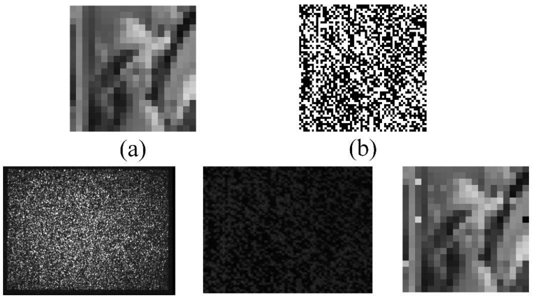
An optical experiment was set up to confirm that the proposed JTC encryption system based on binary-encoded grayscale images works properly. Figure 7 shows the experiment's arrangement. A He-Ne gas laser produces beams of wavelength 632.8 nm. The spatial light modulator (SLM) Holoeye PLUTO-VIS-014, has 1920 × 1080 pixels with spans of 8 μm. The CCD has 768 × 576 pixels with spans of 8.3 μm. The focal length of the Fourier lens is 400 mm.



(a)

(b)

FIG. 7. The experimental system: (a) Schematic diagram of the experimental system, (b) Photograph of the experimental system. (1) He-Ne gas laser, (2) Attenuator, (3) Spatial filter, (4) Aperture, (5) Lens, (6,7, and 9) polarizers, (8) SLM, (10) Fourier lens, (11) CCD.



(a) (b)

(c) (d) (e)

FIG. 8. Experimental results: (a) Original grayscale image, (b) Binary-encoding image, (c) Cryptograph, (d) Decrypted binary image, (e) Decrypted grayscale image converted from the decrypted binary image.

In the experiment, when the binary encoded image was loaded onto the SLM, the small area of each pixel incurred considerable diffraction. Due to its limited resolution the CCD lost some picture details which made the system unable to decipher appropriately. To address this issue, every pixel in the binary-encoded image was reconstructed with 10 × 10 pixels before the image was loaded.

Figure 8(a) shows the 20 × 20-pixel grayscale image waiting for encryption. After every one of its pixels was rebuilt with 10 × 10 pixels, the binary-encoded image of that picture (Fig. 8(b)) was fed to the SLM. Over the output plane the CCD registered the cryptograph, as shown in Fig. 8(c). Using the digital method [19], we retrieved the original decryption image Fig. 8(d), whereas when the approach in Section 4.2 was used, the grayscale decryption image of Fig. 8(e) was obtained. The latter has a CC value of 0.9363 regarding the source grayscale image, which indicates a decent deciphering result.

VI. CONCLUSION

This article proposes a binary-encoding method for grayscale images. This simple approach's encoding speed is much higher than that of QR encoding. Applying this binary-encoding method in JTC encryption systems is able to effectively constrain non-saturation noise generated during encryption and decryption, enhancing the quality of decrypted images. Simulation results showed that the CC between the deciphered and source images rose from 0.8237 to 0.9473 through employing that encoding methodology. In a lab test, the same CC reached 0.9363, which further substantiated that the scheme proposed works appropriately.

REFERENCES

1. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767-769 (1995).
2. J. Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation," Opt. Lasers Eng. **50**, 929-937 (2012).
3. B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. **25**, 28-30 (2000).
4. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**, 2031-2035 (2000).
5. E. Rueda, J. F. Barrera, R. Henao, and R. Torroba, "Optical encryption with a reference wave in a joint transform correlator architecture," Opt. Commun. **282**, 3243-3249 (2009).
6. D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Wavelength multiplexing encryption using joint transform correlator architecture," Appl. Opt. **48**, 2099-2104 (2009).

7. J. Liu, T. Bai, X. Shen, S. Dou, C. Lin, and J. Cai, "Parallel encryption for multi-channel images based on an optical joint transform correlator," Opt. Commun. **396**, 174-184 (2017).
8. J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, "Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain," Opt. Lasers Eng. **89**, 88-94 (2017).
9. J. F. Barrera, M. Tebaldi, E. Rueda, N. Bolognini, and R. Torroba, "Experimental multiplexing of encrypted movies using a JTC architecture," Opt. Express **20**, 3388-3393 (2012).
10. L. C. Lin and C. J. Cheng, "Optimal key mask design for optical encryption based on joint transform correlator architecture," Opt. Commun. **258**, 144-154 (2006).
11. S. Xueju, L. Xumin, C. Ning, and C. Jianjun, "Nonlinear image encryption system based on JTC and its removing noise and resisting attack properties research," Chin. J. Lasers **42**, 0709003 (2015).
12. S. Dou, X. Shen, B. Zhou, L. Wang, and C. Lin, "Experimental research on optical image encryption system based on joint Fresnel transform correlator," Opt. Laser Technol. **112**, 56-64 (2019).
13. A. J. Osorio, J. F. B. Ramírez, S. Montoya, A. Mira-Agudelo, A. V. Zea, and R. Torrobab, "Improved decryption quality with a random reference beam cryptosystem," Opt. Lasers Eng. **112**, 119-127 (2019).
14. J. F. Barrera, A. Mira, and R. Torroba, "Optical encryption and QR codes: Secure and noise-free information retrieval," Opt. Express **21**, 5373-5378 (2013).
15. S. Jiao, W. Zou, and X. Lia, "QR code based noise-free optical encryption and decryption of a gray scale image," Opt. Commun. **387**, 235-240 (2017).
16. J. Shuming, J. Zhi, and Z. Changyuan, "Is QR code an optimal data container in optical encryption systems from an error-correction coding perspective?," J. Opt. Soc. Am. A **35**, A23-A29 (2018).
17. Y. Oin, Z. Wang, H. Wang, and Q. Gong, "Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code," Opt. Laser Technol. **103**, 93-98 (2018).
18. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photonics **1**, 589-636 (2009).
19. L. Jie, B. Tingzhu, S. Xueju, D. Shuaifeng, L. Chao, and C. Qi, "Robustness analysis and optimization of parallel encryption system for multi-channel images in an optical joint transform correlator architecture," Acta Opt. Sin. **37**, 120001 (2017).