entropy

MDPI

Article

A Multi-User Encryption and Authentication System Based on Joint Transform Correlation

Tieyu Zhao * and Yingying Chi

Information Science Teaching and Research Section, Northeastern University at Qinhuangdao, Qinhuangdao 064000, China; cyyzhenbang@163.com

* Correspondence: zty03y3213@163.com

Received: 5 August 2019; Accepted: 29 August 2019; Published: 31 August 2019



Abstract: Optical image encryption technology based on joint transform correlation (JTC) has attracted increasing attention from researchers. We propose a multi-user secure communication system based on the special properties of JTC. Multiple users utilize their own fingerprints to encrypt the plain-text in the encryption process, and each user must be first authenticated at the beginning of the decryption process. Only users with legitimate identities can perform the decryption process, whereas unauthorized users with false identities cannot, so the security of the system is greatly improved. Furthermore, we propose a multi-user double-image encryption method, which can better meet the needs of different security environments. Considering the possibility of overlapping images at the output end, we prove that a JTC-based image encryption system can avoid overlapping images at the output when the distance between the input images is 3W (W is the side length of a square image), which provides a theoretical foundation for further research. Finally, a numerical simulation demonstrates the effectiveness and feasibility of the proposed idea.

Keywords: image encryption; joint transform correlation; optical signal processing

1. Introduction

An optical image encryption method based on joint transform correlation (JTC) is simple and easy to implement and combine with other encryption methods. It has thus become an important branch of optical information security. In 2000, Nomura and Javidi proposed an image encryption system based on JTC [1]. The advantage of its nonlinearity greatly improved the security and reliability of the system. Subsequently, JTC systems have been thoroughly studied and elaborate structures have been proposed [2,3]. Further, Mela and Lemmi introduced an optical encryption technique using three-step phase-shifting interferometry based on JTC in the Fresnel domain [4]. The technique allows a high-speed encryption–decryption process for binary data and is able to operate in a robust and extremely simple optoelectronic system. Soon after, Amaya et al. proposed a multi-channeling encryption method using multiple random-phase mask apertures based on JTC [5,6]. The multiplexing system was immune to known attack procedures because of the existence of an input encryption image pair. Therefore, in order to improve the security of the JTC system, various encryption schemes have been proposed. A multiple phase-shifted encryption method with four parallel channels was proposed by Islam [7]. Alsamman et al. proposed a novel JTC system in which the stored reference image is phase-encrypted prior to applying JTC [8]. The encryption disperses all of the trivial correlation peaks in the correlator output, and the reference image is encrypted electronically, which simplifies the need for a complex optical setup. Meanwhile, the digital holographic configuration was introduced to JTC and the encryption methods were presented with three-dimensional keys [9,10] and a hidden information-encoding architecture [11], and a double-image encryption method using two-step-only quadrature phase-shifting digital holography based on JTC was proposed [12]. Recently,

Vilardy et al. analyzed JTC encryption methods and found that it is possible to significantly improve the quality of the decrypted image by introducing a simple nonlinear operation in the encrypted function that contains the joint power spectrum [13–15]. Moreover, the JTC system has been applied to different transformation domains, such as the fractional Fourier transform domain [16], Fresnel transform domain [17], and chaotic maps [18,19], which greatly expanded the application of JTC. As is known, cryptography and cryptanalysis are complementary to each other. Therefore, attack schemes against JTC encryption system are proposed [20–26]. At the same time, the researchers introduced authentication to improve the security of the system [27–30].

In the JTC encryption system, the common feature is that the classified information is controlled by one user. However, in some cases, this information cannot be owned by one user alone. The classified information can be obtained only if two or more users are present simultaneously. In the current study, a multi-user encryption system is proposed based on JTC. The proposed cryptosystem is uniquely useful in practical applications such as co-signing important documents, the control of nuclear buttons, access to certain crucial information, and so on.

The remainder of this paper is organized as follows. Section 2 proves the feasibility of the proposed scheme through mathematical theory and the analysis of potential risks. Multi-user double image encryption is proposed, and the position distribution of the output image is analyzed in Section 3. Simulation results are shown in Section 4. Finally, the conclusions are presented in Section 5.

2. The Proposed Cryptosystem

On he basis of JTC, the current report proposes a multi-user encryption system with fingerprint keys. Different system users utilize their own fingerprints to encrypt the same plaintext. The decryption process is flexible because different authorized users can accomplish decryption through varying decryption procedures. The optical setup of the proposed system is shown in Figure 1.

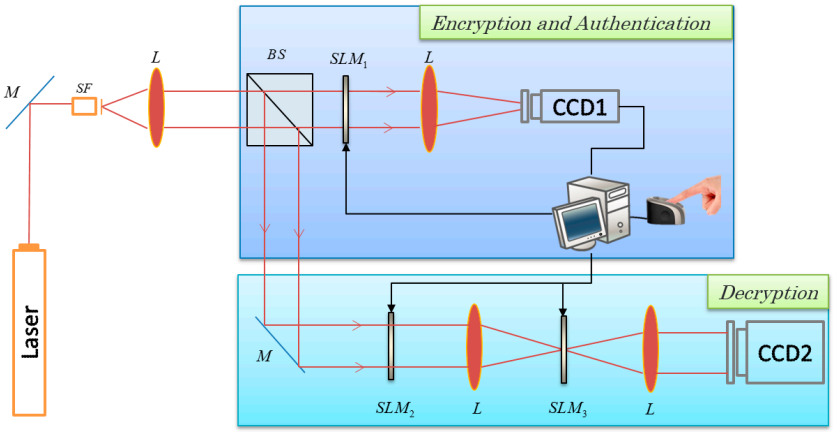


Figure 1. Optical setup. SLM, spatial light modulator. CCD, charge coupled device.

A two-user encryption system was recently proposed based on JTC [31], which is the special case presented in this paper. An encryption design for three users, as shown in Figure 2, is used as an example to illustrate how the system works.

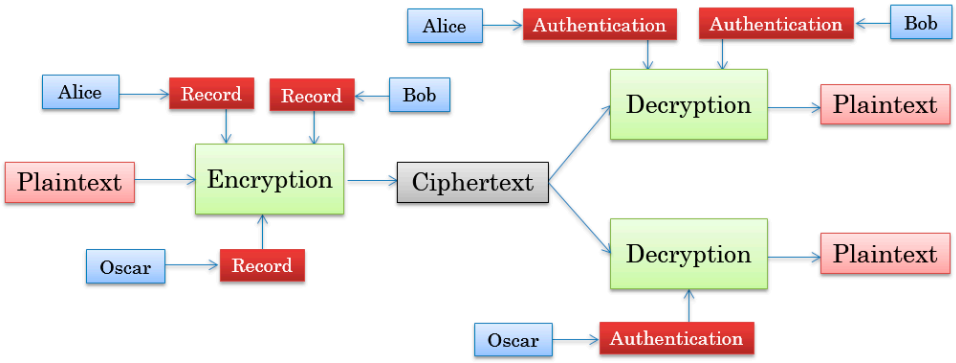


Figure 2. Schematic diagrams.

The detailed process is as follows:

(1) The fingerprints of Alice, Bob, and Oscar are recorded and processed by the computer, respectively, and the encryption keys are obtained.

(2) The plain-text and keys are placed at different locations in the spatial light modulator (SLM) so that the combined transformation power spectrum is obtained as cipher-text.

(3) The users must be authenticated before the decryption. Only authorized users with verified identities can participate in decryption, whereas unauthorized users with uncertified identities cannot conduct the decryption.

(4) The decryption process is flexible. Any authorized user (such as Oscar) can accomplish the decryption themselves. Alternatively, the other two users (Alice and Bob) together can conduct the decryption (each alone cannot complete the decryption).

Assuming that the system has P users, considering the need for decryption, users should be grouped before encryption. For example, the first group has m users; the second group has n users. Here, $P = m + n$. The requirement for obtaining plain-text is that users not only pass authentication, but also satisfy the specified number of users. For example, the first group must have m users appearing at the same time to perform decryption, while the second group must have n users appearing at the same time to perform decryption.

The proposed scheme has a wide range of application scenarios in real life, such as in business or the military; some secrets will require the presence of multiple participants in order to obtain them. Another advantage of the scheme is that there are alternatives, and once a group of users has an accident, another group can be enabled. The flexibility of the scheme is that the number of users in each group can be set according to the decryption requirements.

2.1. Fingerprint Recording and Encryption Process

With the rapid development of information technology, the use of human biological features as passwords has been integrated into our lives, such as fingerprint unlocking for mobile phones, face unlocking for computers, and so on. These biological codes are inherent biological characteristics of the human body. Once they are leaked, they will cause immeasurable losses for users [32–34].

In order to protect user privacy, fingerprints are pre-processed and phase extracted as encryption/decryption keys stored in the computer. The recorded fingerprints (f_a is Alice, f_b is Bob, and f_s is Oscar) are processed by the computer, yielding the keys k_a, k_b, and k_s, respectively.

$$k_a = FT[f_a] / \left| FT[f_a] \right|, \tag{1}$$

$$k_b = FT[f_b] / \left| FT[f_b] \right|, \text{ and} \tag{2}$$

$$k_s = FT[f_s] / \left| FT[f_s] \right|, \tag{3}$$

where FT denotes the Fourier transform.

In Figure 3, the product of the plaintext $f(x, y)$ and the random-phase mask $n(x, y)$ is placed at the coordinate $(x = a, y = 0)$. The key $k_a \cdot k_b$ and the key k_s are placed at the coordinates $(x = -a, y = -b)$ and $(x = -a, y = b)$, respectively.

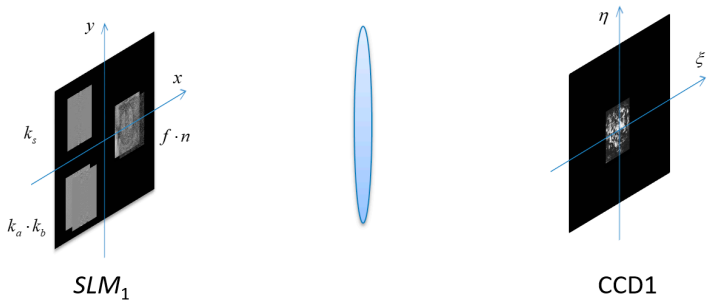


Figure 3. Schematic diagrams of the encryption process.

Let

$$g(x-a, y) = f(x-a, y) \cdot n(x-a, y), \text{ and} \tag{4}$$

$$k_\phi(x+a, y+b) = k_a(x+a, y+b) \cdot k_b(x+a, y+b). \tag{5}$$

Thus, the joint transform power spectrum is obtained:

$$E(\xi, \eta) = \left| FT\Big[g(x-a, y) + k_s(x+a, y-b) + k_\phi(x+a, y+b) \Big] \right|^2, \tag{6}$$

let

$$G(\xi, \eta) = FT[g(x, y)], \tag{7}$$

$$K_s(\xi, \eta) = FT[k_s(x, y)], \text{ and} \tag{8}$$

$$K_\phi(\xi, \eta) = FT\Big[k_\phi(x, y)\Big], \tag{9}$$

so

$$FT[g(x-a, y)] = G(\xi, \eta) \cdot \exp(-j2\pi a\xi), \tag{10}$$

$$FT[k_s(x+a, y-b)] = K_s(\xi, \eta) \cdot \exp(j2\pi a\xi) \cdot \exp(-j2\pi b\eta), \text{ and} \tag{11}$$

$$FT\Big[k_\phi(x+a, y+b)\Big] = K_\phi(\xi, \eta) \cdot \exp(j2\pi a\xi) \cdot \exp(j2\pi b\eta). \tag{12}$$

Thus, Equation (6) can be written as

$$\begin{aligned} E(\xi, \eta) \quad &= |G|^2 + G \cdot K_s^* \cdot \exp(-j4\pi a\xi) \exp(j2\pi b\eta) + G \cdot K_\phi^* \cdot \exp(-j4\pi a\xi) \exp(-j2\pi b\eta) \\ &+ K_s \cdot G^* \cdot \exp(j4\pi a\xi) \exp(-j2\pi b\eta) + 1 + K_s \cdot K_\phi^* \cdot \exp(-j4\pi b\eta) \\ &+ K_\phi \cdot G^* \cdot \exp(j4\pi a\xi) \exp(j2\pi b\eta) + K_\phi \cdot K_s^* \cdot \exp(j4\pi b\eta) + 1. \end{aligned} \tag{13}$$

From this, we can obtain the cipher-text $E(\xi, \eta)$.

2.2. Authentication

As previously mentioned, the user must first be authenticated before decrypting the cipher-text; that is, the cipher-text can only be decrypted by a user with an authorized identity. After Alice presses her original registered finger on the scanner again, a new fingerprint f_N is obtained similar to the original fingerprint f_a, as shown in Figure 4.

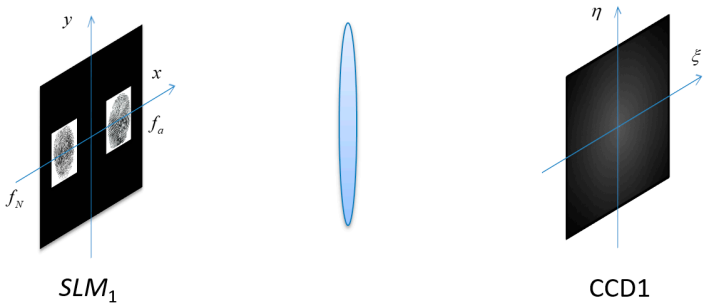


Figure 4. Schematic diagrams of the authentication.

The light intensity distribution is obtained:

$$\begin{aligned} O(\xi,\eta) &= \left|FT[f_a(x-a,y)+f_N(x+a,y)]\right|^2 \\ &= |F_a|^2+|F_N|^2+F_a{}^*\cdot F_N\exp(-j4\pi a\xi)+F_a\cdot F_N^*\exp(j4\pi a\xi). \end{aligned} \tag{14}$$

The intensity spectrum $O(\xi,\eta)$ is again put into the input plane and then Fourier transformed:

$$\begin{aligned} I(x,y) &= f_a(x,y)\bigstar f_a(x,y)+f_N(x,y)\bigstar f_N(x,y) \\ &+f_a(x,y)\bigstar f_N(x,y)*\delta(x+2a,y)+f_a(x,y)\bigstar f_N(x,y)*\delta(x-2a,y). \end{aligned} \tag{15}$$

where ★ denotes the correlation operation and $*$ denotes the convolution operation.

Inspired by the works of [35,36], we find that the peak value of cross-correlation affects the results of authentication. The test results are shown in Figures 5 and 6, respectively.

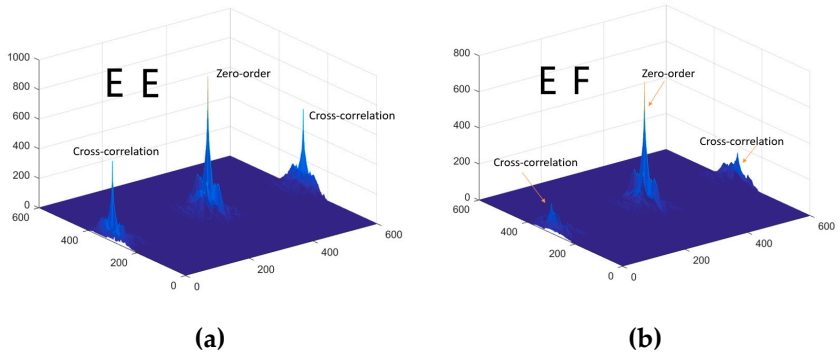


Figure 5. The matching process of letters. (**a**) The same letter, E; (**b**) different letters, E and F.

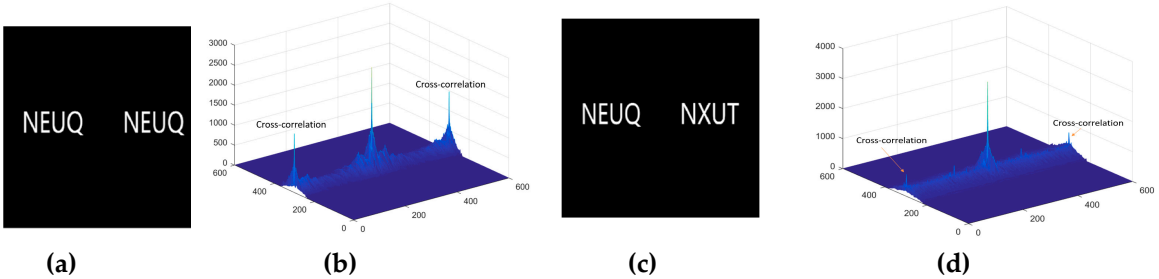


Figure 6. Sensitivity analysis. (**a**) The same letters; (**b**) the peak value of correlation for (**a**); (**c**) different letters; (**d**) the peak value of correlation for (**c**).

The test result shows that the matching system based on JTC is very effective. Only an exact match can achieve the maximum peak. The third and fourth terms in Equation (15). show the similarity

between the two fingerprints—the left two fingerprints, as shown in Figure 7—while an unauthorized user with an unregistered fingerprint, such as the right image in Figure 7, fails the authentication.

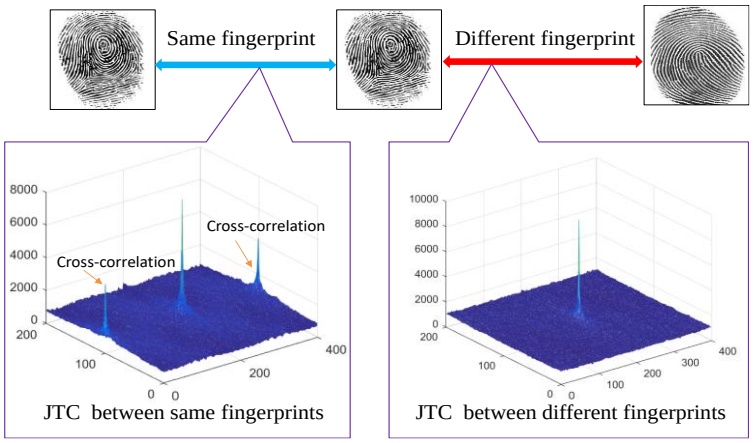


Figure 7. Fingerprint matching. JTC, joint transform correlation.

However, we find that the rotation of the fingerprint seriously affects the matching results (as in our recent research work, presented in the work of [31]). When fingerprints are corrupted by noise, it will affect the authentication process. Here, the fingerprint is partially damaged, and the verification results obtained are shown in Figure 8. From the comparison results, we can see that the fingerprint recognition system based on JTC has good robustness against noise attacks.

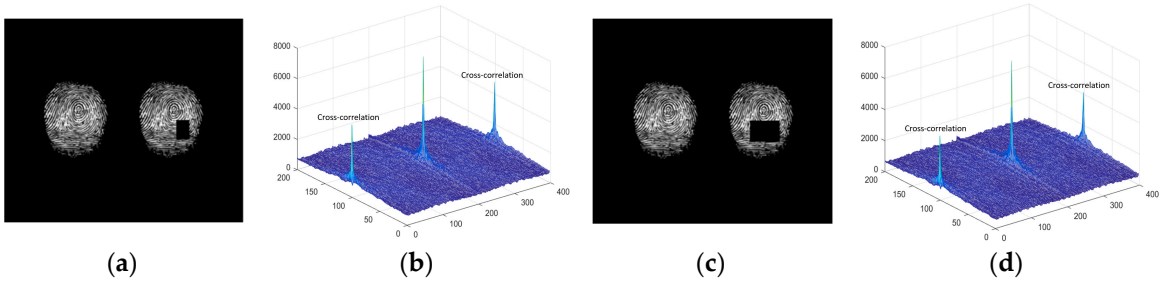


Figure 8. Verification results for locally damaged fingerprints (**a**) The damaged fingerprint; (**b**) the peak value of correlation for (**a**); (**c**) the damaged fingerprint; (**d**) the peak value of correlation for (**c**).

2.3. Decryption Process

The decryption process is flexible, and two alternative solutions are presented: (1) Oscar conducts the decryption process alone, and (2) Alice and Bob perform the decryption operation together.

2.3.1. Oscar's Decryption

When Oscar passes the authentication, the recorded fingerprint key k_s and the cipher-text $E(\xi, \eta)$ are input into the input plane (SLM2) and the spectrum plane (SLM3), respectively, as shown in Figure 9.

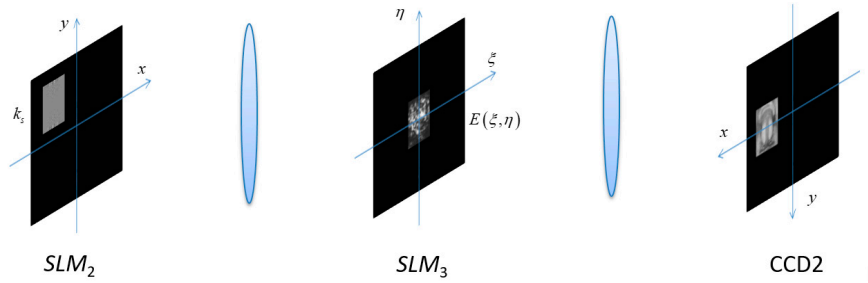


Figure 9. Oscar's decryption process.

The detailed process is as follows:
Because

$$FT[k_s(x+a, y-b)] = K_s \cdot \exp(j2\pi a\xi) \cdot \exp(-j2\pi b\eta), \tag{16}$$

according to Equation (13), the Fourier spectrum on the front focal plane is

$$\begin{aligned} P(\xi,\eta) &= E(\xi,\eta) \cdot FT[k_s(x+a, y-b)] \\ &= E(\xi,\eta) \cdot K_s \cdot \exp(j2\pi a\xi) \cdot \exp(-j2\pi b\eta) \\ &= |G|^2 \cdot K_s \cdot \exp(j2\pi a\xi) \cdot \exp(-j2\pi b\eta) + G \cdot \exp(-j2\pi a\xi) \\ &+\left(G \cdot K_\phi^*\right) \cdot K_s \cdot \exp(-j2\pi a\xi) \cdot \exp(-j4\pi b\eta) \\ &+(K_s \cdot G^*) \cdot K_s \cdot \exp(j6\pi a\xi) \cdot \exp(-j4\pi b\eta) \\ &+K_s \cdot \exp(j2\pi a\xi) \cdot \exp(-j2\pi b\eta) \\ &+\left(K_s \cdot K_\phi^*\right) \cdot K_s \cdot \exp(j2\pi a\xi) \cdot \exp(-j6\pi b\eta) \\ &+\left(K_\phi \cdot G^*\right) \cdot K_s \cdot \exp(j6\pi a\xi) \\ &+K_\phi \cdot \exp(j2\pi a\xi) \cdot \exp(j2\pi b\eta) \\ &+K_s \cdot \exp(j2\pi a\xi) \cdot \exp(-j2\pi b\eta) \end{aligned} \tag{17}$$

Then, using the inverse Fourier transform,

$$\begin{aligned} p(x,y) &= FT^{-1}[P(\xi,\eta)] \\ &= (g \bigstar g) * k_s * \delta(x+a, y-b) \\ &+g * \delta(x-a, y) + \left(g \bigstar k_\phi\right) * k_s * \delta(x-a, y-2b) \\ &+(k_s \bigstar g) * k_s * \delta(x+3a, y-2b) + k_s * \delta(x+a, y-b) \\ &+\left(k_s \bigstar k_\phi\right) * k_s * \delta(x+a, y-3b) + \left(k_\phi \bigstar g\right) * k_s * \delta(x+3a, y) \\ &+k_\phi * \delta(x+a, y+b) + k_s * \delta(x+a, y-b). \end{aligned} \tag{18}$$

In Equation (18), the plain-text $g(x,y) = f(x,y) \cdot n(x,y)$ is obtained using the second term of the sum on the right-hand side of the equation; that is, the plain-text $\left|g(x,y)\right| = f(x,y)$ is obtained at coordinates $x = a$.

2.3.2. Alice and Bob's Decryption

Both Alice and Bob must provide their fingerprints together for the decryption, as each alone cannot accomplish the decryption. The decryption process is shown in Figure 10.

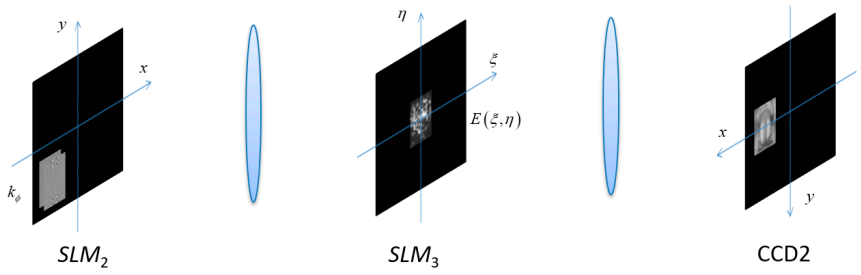


Figure 10. Alice and Bob's decryption.

According to Equation (13), the Fourier spectrum on the front focal plane is

$$\begin{aligned} Q(\xi,\eta) &= E(\xi,\eta)\cdot FT\left[k_\phi(x+a,y+b)\right] \\ &= E(\xi,\eta)\cdot K_\phi\cdot\exp(j2\pi a\xi)\cdot\exp(j2\pi b\eta) \\ &= |G|^2\cdot K_\phi\cdot\exp(j2\pi a\xi)\cdot\exp(j2\pi b\eta) \\ &+(G\cdot K_s^*)\cdot K_\phi\cdot\exp(-j2\pi a\xi)\cdot\exp(j4\pi b\eta) \\ &+G\cdot\exp(-j2\pi a\xi)+(K_s\cdot G^*)\cdot K_\phi\cdot\exp(j6\pi a\xi) \\ &+K_\phi\cdot\exp(j2\pi a\xi)\cdot\exp(j2\pi b\eta) \\ &+K_s\cdot\exp(j2\pi a\xi)\cdot\exp(-j2\pi b\eta) \\ &+\left(K_\phi\cdot G^*\right)\cdot K_\phi\cdot\exp(j6\pi a\xi)\cdot\exp(j4\pi b\eta) \\ &+\left(K_\phi\cdot K_s^*\cdot\right)K_\phi\cdot\exp(j2\pi a\xi)\cdot\exp(j6\pi b\eta) \\ &+K_\phi\cdot\exp(j2\pi a\xi)\cdot\exp(j2\pi b\eta). \end{aligned} \tag{19}$$

Using the inverse Fourier transform, we obtain

$$\begin{aligned} q(x,y) &= FT^{-1}[Q(\xi,\eta)] \\ &= (g\bigstar g)*k_\phi*\delta(x+a,y+b)+(g\bigstar k_s)*k_\phi*\delta(x-a,y+2b) \\ &+g*\delta(x-a,y)+(k_s\bigstar g)*k_\phi*\delta(x+3a,y)+k_\phi*\delta(x+a,y+b) \\ &+k_s*\delta(x+a,y-b)+\left(k_\phi\bigstar g\right)*k_\phi*\delta(x+3a,y+2b) \\ &+\left(k_\phi\bigstar k_s\right)*k_\phi*\delta(x+a,y+3b)+k_\phi*\delta(x+a,y+b). \end{aligned} \tag{20}$$

The plain-text $g(x,y)=f(x,y)\cdot n(x,y)$ is obtained using the third term in the sum of Equation (20). Thus, the plain-text $\left|g(x,y)\right|=f(x,y)$ is obtained at coordinates $x=a$.

From Equations (18) and (20), we can determine that the position of the recovered plain-text has not changed. However, at the same time, a security risk was found. In Equation (18), the key k_ϕ is restored, while in Equation (20), the key k_s is restored. Obviously, such a situation is not advisable in information security. Thus, we perform the following further analysis.

3. Further Analysis

3.1. Double-Image Encryption

The image encryption system based on JTC can achieve multi-image encryption. It does not require the special treatment of plain-text, so it is more convenient than the previously proposed encryption methods [37–39].

Here, we use two keys to encrypt two plain-text messages, as shown in Figure 11. Next, we analyze its basic principle. Here, $f(x,y)$ and $g(x,y)$ denote the plain-text, and $k_1(x,y)$ and $k_2(x,y)$ denote the keys. To simplify the proving process, the coordinate position is ignored.

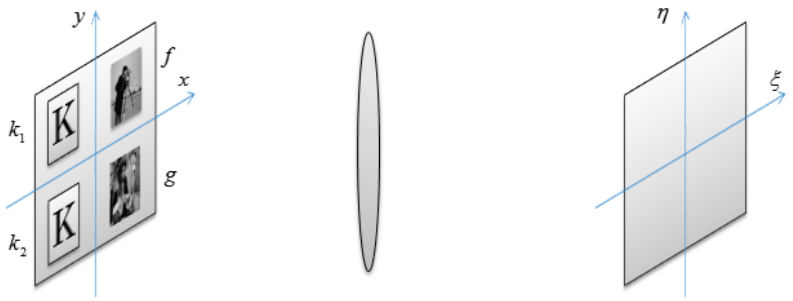


Figure 11. The encryption process diagram.

Then, in Figure 11, the cipher-text can be written as

$$\begin{aligned} E(\xi,\eta) &= \left|FT[f(x,y)+g(x,y)+k_1(x,y)+k_2(x,y)]\right|^2 \\ &= \left|F(\xi,\eta)+G(\xi,\eta)+K_1(\xi,\eta)+K_2(\xi,\eta)\right|^2 \\ &= (F+G+K_1+K_2)(F^*+G^*+{K_1}^*+{K_2}^*). \end{aligned} \tag{21}$$

When using the key $k_1(x,y)$ for decryption, its expression can be written as

$$\begin{aligned} D(\xi,\eta) &= E(\xi,\eta)\cdot FT[k_1(x,y)] \\ &= E(\xi,\eta)\cdot K_1(\xi,\eta) \\ &= (F+G+K_1+K_2)(F^*+G^*+{K_1}^*+{K_2}^*)\cdot K_1 \\ &= (F+G+K_1+K_2)\left(F^*\cdot K_1+G^*\cdot K_1+K_1^*\cdot K_1+{K_2}^*\cdot K_1\right) \\ &= (F+G+K_1+K_2)(F^*\cdot K_1+G^*\cdot K_1+1+{K_2}^*\cdot K_1) \\ &= (F+G+K_1+K_2)(F^*\cdot K_1+G^*\cdot K_1+{K_2}^*\cdot K_1)+(F+G+K_1+K_2). \end{aligned} \tag{22}$$

Using the inverse Fourier transform, we obtain

$$\begin{aligned} d(x,y) &= FT^{-1}[D(\xi,\eta)] \\ &= FT^{-1}[(F+G+K_1+K_2)(F^*\cdot K_1+G^*\cdot K_1+{K_2}^*\cdot K_1)]+ \\ &f(x,y)+g(x,y)+k_1(x,y)+k_2(x,y). \end{aligned} \tag{23}$$

Equation (23) is solved, and its complete decryption result is obtained as Equation (24).

$$\begin{aligned} d(x,y) &= FT^{-1}[D(\xi,\eta)] \\ &= FT^{-1}[(F+G+K_1+K_2)(F^*\cdot K_1+G^*\cdot K_1+{K_2}^*\cdot K_1)]+f(x,y)+g(x,y)+k_1(x,y)+k_2(x,y). \\ &= (f\bigstar f)*k_1*\delta(x+a,y-b)+(f\bigstar g)*k_1*\delta(x+a,y-3b)+(f\bigstar k_2)*k_1*\delta(x-a,y-3b) \\ &+(g\bigstar f)*k_1*\delta(x+a,y+b)+(g\bigstar g)*k_1*\delta(x+a,y-b)+(g\bigstar k_2)*k_1*\delta(x-a,y-b) \\ &+(k_1\bigstar f)*k_1*\delta(x+3a,y-b)+(k_1\bigstar g)*k_1*\delta(x+3a,y-3b)+(k_1\bigstar k_2)*k_1*\delta(x+a,y-3b) \\ &+(k_2\bigstar f)*k_1*\delta(x+3a,y+b)+(k_2\bigstar g)*k_1*\delta(x+3a,y+b)+k_1*\delta(x+a,y-b) \\ &+f*\delta(x-a,y-b)+g*\delta(x-a,y+b)+k_1*\delta(x+a,y-b)+k_2*\delta(x+a,y+b). \end{aligned} \tag{24}$$

When the key k_2 is used for decryption, the result of the decryption is as in Equation (25).

$$\begin{aligned} d(x,y) &= FT^{-1}[D(\xi,\eta)] \\ &= FT^{-1}[(F+G+K_1+K_2)(F^*\cdot K_2+G^*\cdot K_2+{K_1}^*\cdot K_2)]+f(x,y)+g(x,y)+k_1(x,y)+k_2(x,y). \\ &= (f\bigstar f)*k_2*\delta(x+a,y+b)+(f\bigstar g)*k_2*\delta(x+a,y-b)+(f\bigstar k_1)*k_2*\delta(x-a,y+b) \\ &+(g\bigstar f)*k_2*\delta(x+a,y+3b)+(g\bigstar g)*k_2*\delta(x+a,y+b)+(g\bigstar k_1)*k_2*\delta(x-a,y+3b) \\ &+(k_1\bigstar f)*k_2*\delta(x+3a,y+b)+(k_1\bigstar g)*k_2*\delta(x+3a,y-b)+k_2*\delta(x+a,y+b) \\ &+(k_2\bigstar f)*k_2*\delta(x+3a,y+3b)+(k_2\bigstar g)*k_2*\delta(x+3a,y+b)+(k_2\bigstar k_1)*k_2*\delta(x+a,y+3b) \\ &+f*\delta(x-a,y-b)+g*\delta(x-a,y+b)+k_1*\delta(x+a,y-b)+k_2*\delta(x+a,y+b). \end{aligned} \tag{25}$$

In Equation (24), we notice that when the key k_1 is used for decryption, only the plain-text $g(x,y)$ is obtained. We are unable to obtain other information because it is overlapped. Some attack schemes

want to extract information from cipher-text, which will be very difficult in reality [22]. Similarly, when decrypting with the key k_2, we can only obtain the plain-text $f(x, y)$, as shown in Equation (25).

Further, the keys k_1 and k_2 can be combined, such as $k_1 = \phi_1 \cdot \phi_2 \cdots \phi_m$ and $k_2 = \varphi_1 \cdot \varphi_2 \cdots \varphi_n$. Thus, k_1 means that there are m users (Alice, Tom, ... , Emma), and k_2 means n users (Olivia, Hannah, ... , John). Thus, it can be decrypted only when m users appear simultaneously or n users appear simultaneously. Of course, in the keys k_1 and k_2, there can be the same key (user); in other words, the user can obtain both the plain-text g and plain-text f.

Furthermore, the proposed scheme does not need to pre-process the plain-text and realizes double image encryption in a real sense compared with other research methods [37–39]. In the process of decryption, each group of users can only obtain one plain-text. For example, the first group of users (Alice, Tom, ... , Emma) can only obtain plain-text g, and the second group of users (Olivia, Hannah, ... , John) can only obtain plain-text f. If a user is in both groups, he/she has the right to access two plain-texts.

In some scenarios, secrets not only need to be shared by multiple users, but also have hierarchical relationships among users [40]. For example, in a company, managers usually have more resources than employees; in the army, officers usually have more information than soldiers. At this time, the traditional cryptosystem we know is insufficient for this, and the scheme proposed in this section has significant advantages.

In Equations (24) and (25), the plain-text messages are restored during decryption; at this time, the position of the restored image is particularly important. Here, we analyze and discuss the circumstances that can ensure that the output images are separated from each other.

3.2. Image Position Distribution on Output

Researchers have previously discovered that the positional distribution of the input image affects the distance between the output spots based on JTC's identification system [41–43]. Assuming that the edge length of the given input object image and reference image are both W, when the distance between the two images is greater than $2W$, the output images are separated from each other.

Here, $g(x - a_1, y)$ and $r(x - a_2, y)$ denote the object image and the reference image, respectively. The light intensity of the output can be expressed as

$$\begin{aligned} E(\xi, \eta) &= \left| FT[g(x - a_1, y) + r(x - a_2, y)] \right|^2 \\ &= [G(\xi, \eta) \exp(-j2\pi a_1 \xi) + R(\xi, \eta) \exp(-j2\pi a_2 \xi)] \cdot \\ &\quad [G^*(\xi, \eta) \exp(j2\pi a_1 \xi) + R^*(\xi, \eta) \exp(j2\pi a_2 \xi)] \\ &= |G|^2 + |R|^2 + G \cdot R^* \exp(j2\pi(a_2 - a_1)\xi) + R \cdot G^* \cdot \exp(j2\pi(a_1 - a_2)\xi). \end{aligned} \tag{26}$$

Using the inverse Fourier transform, we obtain

$$\begin{aligned} I(x, y) &= IFT[E(\xi, \eta)] \\ &= g \bigstar g * \delta(x, y) + r \bigstar r * \delta(x, y) \\ &\quad + g \bigstar r * \delta(x + (a_2 - a_1), y) + g \bigstar r * \delta(x + (a_1 - a_2), y). \end{aligned} \tag{27}$$

In Equation (27), four items are obtained. Two items are at the coordinate origin, and the other two are at the two sides of the coordinate origin, as shown in Figure 12. When the distance between the input images is 2W, the output images are guaranteed to be separated from each other; thus, $|a_1 - a_2| \geq 2W$ (note that the input images' size is 200 × 200 pixels, so W = 200).



(**a**) (**b**) (**c**)

Figure 12. (**a**) The input image, (**b**) the light intensity distribution at the output end, and (**c**) the energy distribution of (**b**).

An analysis of the image encryption system based on JTC indicates that the distance between the plain-text and the key is 3W at the input, which can ensure that the output images are separated from each other. The detailed proof is as follows.

Here, $f(x-a_1,y)$ and $k(x-a_2,y)$ denote the plain-text and the key, respectively, so the cipher-text is obtained in the encryption system and its expression can be written as

$$\begin{aligned} E(\xi,\eta) &= \left|FT[f(x-a_1,y)+k(x-a_2,y)]\right|^2 \\ &= |F|^2+|K|^2+F\cdot K^*\exp(j2\pi(a_2-a_1)\xi)+K\cdot F^*\cdot\exp(j2\pi(a_1-a_2)\xi). \end{aligned} \tag{28}$$

When using the key $k(x-a_2,y)$ for decryption, the decryption process can be expressed as

$$\begin{aligned} D(\xi,\eta) &= E(\xi,\eta)\cdot FT[k(x-a_2,y)] \\ &= E(\xi,\eta)\cdot K(\xi,\eta)\exp(-j2\pi a_1\xi) \\ &= \Big[|F|^2+|K|^2+F\cdot K^*\exp(j2\pi(a_2-a_1)\xi) \\ &\quad +K\cdot F^*\cdot\exp(j2\pi(a_1-a_2)\xi)\Big]\cdot K(\xi,\eta)\exp(-j2\pi a_2\xi). \end{aligned} \tag{29}$$

Using the inverse Fourier transform, we obtain

$$\begin{aligned} d(x,y) &= FT^{-1}[D(\xi,\eta)] \\ &= f\bigstar f*k*\delta(x-a_2,y)+k\bigstar k*k*\delta(x-a_2,y) \\ &\quad +f*\delta(x-a_1,y)+k\bigstar f*k*\delta(x+a_1-2a_2,y). \end{aligned} \tag{30}$$

As demonstrated by Equation (30), each form is unified as $z_1(x)\bigstar z_2(x)*z_3(x)$.

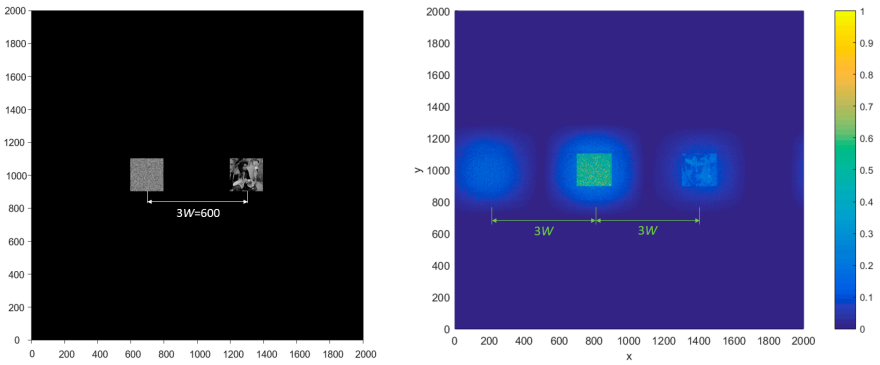
Because

$$z_1(x)*z_2(x)*z_3(x)=\int_{-\infty}^{\infty}\left[\int_{-\infty}^{\infty}z_1(\lambda)z_2(\tau-\lambda)d\lambda\right]z_3(x-\tau)d\tau, \tag{31}$$

$$z_1(x)\bigstar z_2(x)*z_3(x)=z_1(x)*z_2(-x)*z_3(x). \tag{32}$$

When the distance between the images is greater than 3W at the input end, the images are mutually separated at the output end.

In Equation (30), the coordinate position is $(a_1,0)$, $(a_2,0)$, and $(2a_2-a_1,0)$, respectively. When $|a_1-a_2|\geq 3W$, we obtain $\left|(2a_2-a_1)-a_2\right|=|a_2-a_1|\geq 3W$ and $\left|(2a_2-a_1)-a_1\right|=2\left|(a_2-a_1)\right|\geq 6W$, so that the output images are separated from each other, as shown in Figure 13. Here, the input images' size is 200×200 pixels, so $W=200$.



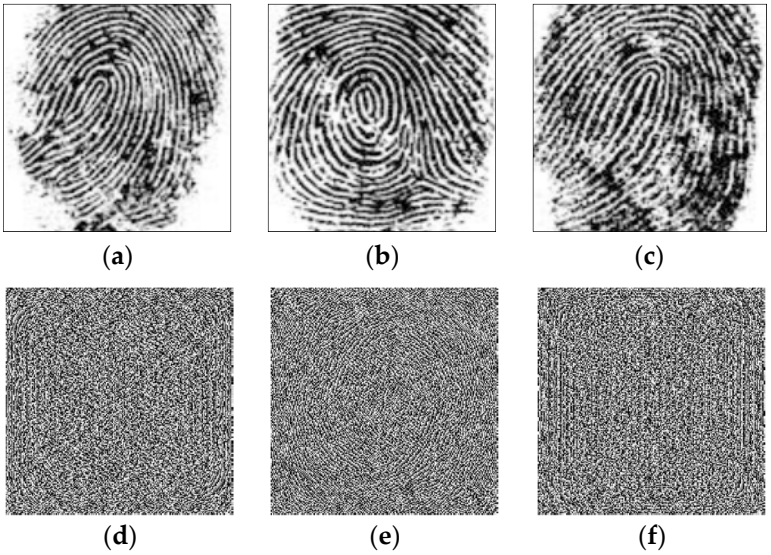
(**a**) (**b**)

Figure 13. (**a**) The plain-text and key and (**b**) the intensity distribution after decryption.

For JTC's image encryption system, the output image is $z_1\left(x_{i_1}, y_{j_1}\right) \bigstar z_2\left(x_{i_2}, y_{j_2}\right) * z_3\left(x_{i_3}, y_{j_3}\right)$ and does not depend on the number of input images. Therefore, the distance between the input images is either $\left|x_i - x_j\right| \geq 3W$ or $\left|y_i - y_j\right| \geq 3W$, which ensures that the output images are separated.

4. Numerical Simulation

The fingerprints (Alice, Bob, and Oscar) are shown in Figure 14a–c, respectively, and the phase of each fingerprint is used as a key, as demonstrated in Figure 14d–f.



(**a**) (**b**) (**c**)

(**d**) (**e**) (**f**)

Figure 14. (**a**) Alice's fingerprint, (**b**) Bob's fingerprint, (**c**) Oscar's fingerprint, (**d**) the phase of Alice's fingerprint, (**e**) the phase of Bob's fingerprint, and (**f**) the phase of Oscar's fingerprint.

We perform experimental simulations for the proposed cryptosystem, as shown in Figure 15. In Figure 15a, the images' size is 200 × 200 pixels ($W = 200$). The vertical distance between the two keys at the input is 600, and the horizontal distance between the two keys and the plain-text is also 600. This ensures that the images at the output are independent of each other.

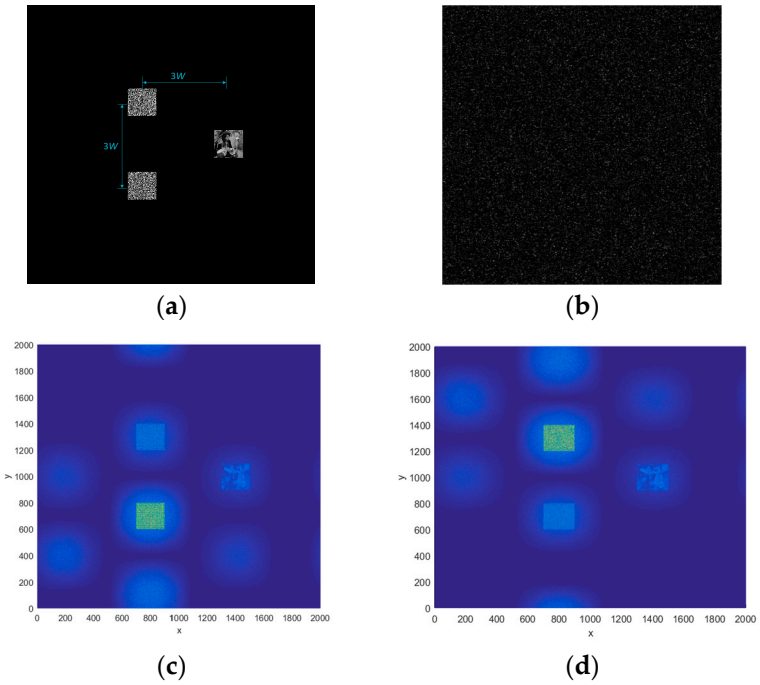


Figure 15. (**a**) The plain image and the keys, (**b**) the cipher-text, (**c**) the decrypted result by Oscar, and (**d**) the decrypted result by Alice and Bob together.

The plain image and the keys are placed at different positions on the input, respectively, as shown in Figure 15a. Here, the keys are on the left (above is Oscar's key, below is the product of Alice and Bob's key), and the plain image is on the right. The cipher-text is obtained as shown in Figure 15b. It should be noted that the size of the cipher-text is the same as that of the input surface (2000 × 2000 pixels). The result that Oscar decrypts alone is shown in Figure 15c, and the result that Alice and Bob decrypt together is shown in Figure 15d.

Next, the multi-user double image encryption scheme is analyzed. The keys are still used in Figure 14, so the distribution of the keys and plain images are shown in Figure 16a. Here, the keys are on the left (above is Oscar's key, below is the product of Alice and Bob's key), and the two plain-text images are on the right. In Figure 16b, the ciphertext is obtained (2000 × 2000 pixels). The result that Oscar's decrypt alone is shown in Figure 16c, and the result that Alice and Bob's decrypt together is shown in Figure 16d. Here, Figure 16c corresponds to Equation (24), because the same coordinate positions are merged, so we see that there are nine items. Similarly, Figure 16d corresponds to Equation (25), and there are also nine items.

Correlation is an important method to evaluate whether the system can resist statistical analysis attack. For a good encryption method, the cipher-text obtained should be fully confused; that is, the attacker cannot get any plain-text information from the cipher-text.

Figure 17 is the histogram of the ciphertext of the two encryption schemes (Figures 15b and 16b, respectively). The cipher-text obtained by the proposed scheme is the energy spectrum. From the histogram, the proposed scheme does not achieve the effect of chaotic encryption [44,45].

The impact of noise on the system should mainly come from two aspects: on the one hand, the impact of the fingerprint recognition; on the other hand, the cipher-text will be attacked by noise, which will affect the results of decryption [46].

When fingerprints are corrupted by noise, it will affect the authentication process. Here, the fingerprint is partially damaged, and the verification results obtained are shown in Figure 3. The decryption process is built in the optical system. Owing to the optical holography, the system is robust against interference. When the ciphertext is partially damaged, the decryption results are shown in Figure 18. Here, we give the mean square error and the correlation coefficient (MSE = 52; CC = 0.7538).

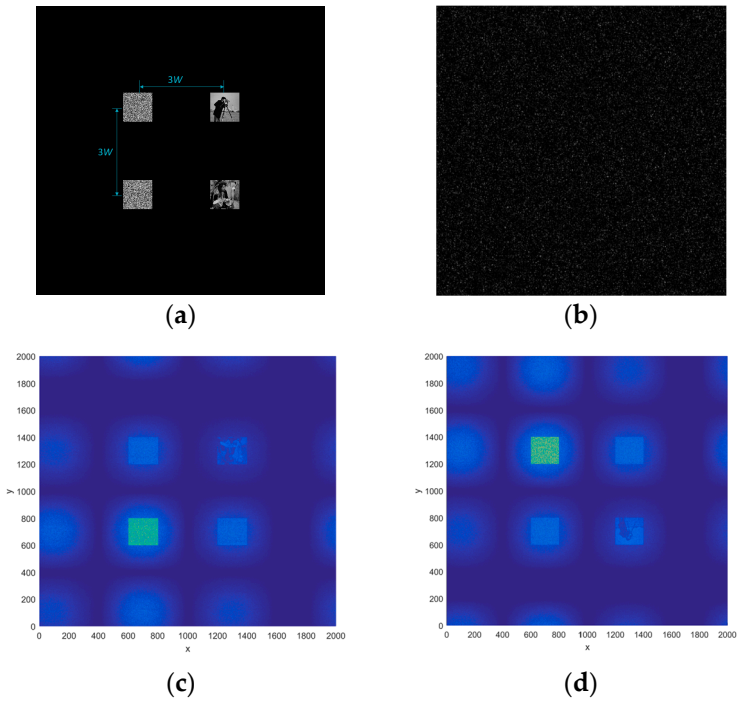


Figure 16. (**a**) The plain images and the keys, (**b**) the cipher-text, (**c**) the decrypted result by Oscar, and (**d**) the decrypted result by Alice and Bob together.

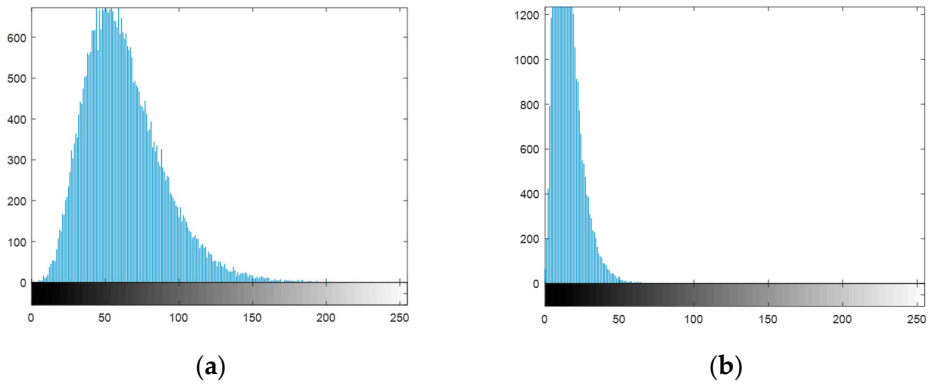


Figure 17. Histogram of the cipher-text: (**a**) histogram of Figure 15b; (**b**) histogram of Figure 16b.

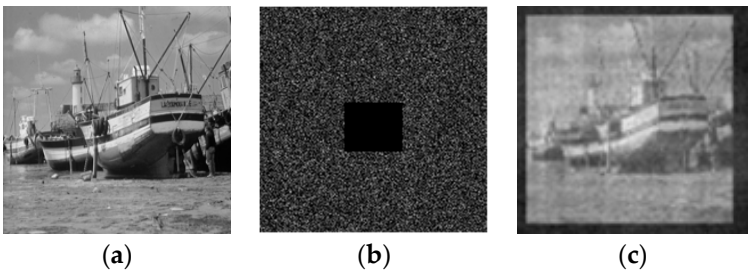


Figure 18. (**a**) The plain-text; (**b**) the cipher-text; (**c**) the decrypted image.

The simulation analysis not only verifies the effectiveness of the proposed scheme, but also proves that the image encryption system based on JTC can ensure that the output image cannot be overlapped when the distance between the input images is three times the edge length of the image. In the performance analysis, the system shows good anti-jamming ability. However, the obtained cipher-text is an energy spectrum, and its encryption process is not ideal for plain-text confusion.

5. Conclusions

This paper proposed a multi-user authentication image encryption scheme based on JTC. A user's fingerprint can not only be used as a key, but can also be authenticated. In order to protect user privacy, fingerprints are pre-processed and phase extracted as encryption/decryption keys stored in the computer. In the proposed scheme, two conditions must be met for the plain-text to be successfully restored: (1) before decryption, the user must be authenticated, and only those with legitimate identities can participate in decryption; and (2) each group of users must reach a specified number of users before they can be decrypted (users are grouped before encryption). As far as we know, this scheme is not involved in previous encryption methods. The feasibility and effectiveness of the proposed scheme were verified by mathematical derivation and numerical simulation. However, with the deepening of the research, we found that the scheme has the hidden danger of key leakage in the decryption process. Therefore, we further proposed a multi-user double image encryption scheme to overcome the hidden danger. The new scheme not only satisfies the above two security conditions, but also adds a hierarchical relationship between users. Only specific users have the right to access two images, while other users can only access one of them. At this point, considering the position of the restored image is particularly important. We analyzed and discussed the circumstances that can ensure that the output images are separated from each other. Finally, the performance of the proposed scheme is analyzed by numerical simulation.

In the future, we will study multi-user color image encryption, because color images contain more information [44]. At present, our research only applies to gray images. At the same time, the positions of the input images are symmetrical. If the positions of the images are irregularly arranged, the correlation between the output images will need to be further studied. As a stage study, this paper hopes to give some inspiration to researchers.

Author Contributions: Methodology, T.Z.; software, T.Z.; validation, T.Z. and Y.C.; writing—original draft preparation, Y.C.; writing—review and editing, T.Z.; supervision, T.Z.; funding acquisition, T.Z.

Funding: This study was supported by National Natural Science Foundation of China (No.61702088); Central University Basic Research Service Fees, China. (No.N172303014); School PhD Fund, Northeastern University, Qinhuangdao, China. (XNB201708).

Acknowledgments: The authors thank the reviewers for their valuable comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nomura, T.; Javidi, B. Optical encryption using a joint transform correlator architecture. *Opt. Eng.* **2000**, *39*, 2031–2035.
2. Abookasis, D.; Arazi, O.; Rosen, J.; Javidi, B. Security optical systems based on a joint transform correlator with significant output images. *Opt. Eng.* **2001**, *40*, 1584–1589. [CrossRef]
3. Nomura, T.; Mikan, S.; Morimoto, Y.; Javidi, B. Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator. *Appl. Optics* **2003**, *42*, 1508–1514. [CrossRef] [PubMed]
4. La Mela, C.; Iemmi, C. Optical encryption using phase-shifting interferometry in a joint transform correlator. *Opt. Lett.* **2006**, *31*, 2562–2564. [CrossRef] [PubMed]
5. Amaya, D.; Tebaldi, M.; Torroba, R.; Bolognini, N. Multichanneled encryption via a joint transform correlator architecture. *Appl. Optics* **2008**, *47*, 5903–5907. [CrossRef]
6. Amaya, D.; Tebaldi, M.; Torroba, R.; Bolognini, N. Wavelength multiplexing encryption using joint transform correlator architecture. *Appl. Optics* **2009**, *48*, 2099–2104. [CrossRef] [PubMed]
7. Islam, M.N.; Karim, M.A.; Alam, M.S.; Asari, K.V. Optical cryptographic system employing multiple reference-based joint transform correlation technique. *Opt. Eng.* **2011**, *50*, 068202.
8. Alsamman, A. Spatially efficient reference phase-encrypted joint transform correlator. *Appl. Optics* **2010**, *49*, B104–B110. [CrossRef]
9. Rueda, E.; Barrera, J.F.; Henao, R.; Torroba, R. Optical encryption with a reference wave in a joint transform correlator architecture. *Opt. Commun.* **2009**, *282*, 3243–3249. [CrossRef]

10. Rueda, E.; Tebaldi, M.; Torroba, R.; Bolognini, N. Three-dimensional key in a modified joint transform correlator encryption scheme. *Opt. Commun.* **2011**, *284*, 4321–4326. [CrossRef]
11. Shi, X.Y.; Zhao, D.M. Image hiding in Fourier domain by use of joint transform correlator architecture and holographic technique. *Appl. Optics* **2011**, *50*, 766–772. [CrossRef] [PubMed]
12. Li, J.; Zheng, T.; Liu, Q.Z.; Li, R. Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography. *Opt. Commun.* **2012**, *285*, 1704–1709. [CrossRef]
13. Vilardy, J.M.; Millan, M.S.; Perez-Cabre, E. Improved decryption quality and security of a joint transform correlator-based encryption system. *J. Optics-Uk* **2013**, *15*, 025401. [CrossRef]
14. Vilardy, J.M.; Millan, M.S.; Perez-Cabre, E. Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. *Appl. Optics* **2014**, *53*, 1674–1682. [CrossRef] [PubMed]
15. Vilardy, J.M.; Millan, M.S.; Perez-Cabre, E. Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain. *Opt. Laser. Eng.* **2017**, *89*, 88–94. [CrossRef]
16. Wang, Q.; Guo, Q.; Lei, L.; Zhou, J.Y. Optical image encryption based on joint fractional transform correlator architecture and digital holography. *Opt. Eng.* **2013**, *52*, 048201. [CrossRef]
17. Shen, X.J.; Liu, X.M.; Yin, J.L.; Lu, X.W.; Kong, D.Z.; Lin, C. Joint Fresnel transform correlator based on double optical wedges. *Opt. Commun.* **2015**, *339*, 243–246.
18. Saini, N.; Sinha, A. Video encryption using chaotic masks in joint transform correlator. *J. Optics-Uk* **2015**, *17*, 035701. [CrossRef]
19. Zhao, H.J.; Zhong, Z.; Fang, W.W.; Xie, H.; Zhang, Y.B.; Shan, M.G. Double-image encryption using chaotic maps and nonlinear non-DC joint fractional Fourier transform correlator. *Opt. Eng.* **2016**, *55*, 093109. [CrossRef]
20. Barrera, J.F.; Vargas, C.; Tebaldi, M.; Torroba, R. Chosen-plaintext attack on a joint transform correlator encrypting system. *Opt. Commun.* **2010**, *283*, 3917–3921. [CrossRef]
21. Barrera, J.F.; Vargas, C.; Tebaldi, M.; Torroba, R.; Bolognini, N. Known-plaintext attack on a joint transform correlator encrypting system. *Opt. Lett.* **2010**, *35*, 3553–3555. [CrossRef] [PubMed]
22. Qin, W.; Peng, X.A.; Meng, X.F. Cryptanalysis of optical encryption schemes based on joint transform correlator architecture. *Opt. Eng.* **2011**, *50*, 028201. [CrossRef]
23. Lin, C.; Shen, X.J. Analysis and design of impulse attack free generalized joint transform correlator optical encryption scheme. *Opt. Laser Technol.* **2012**, *44*, 2032–2036. [CrossRef]
24. Zhang, C.G.; Liao, M.H.; He, W.Q.; Peng, X. Ciphertext-only attack on a joint transform correlator encryption system. *Opt. Express* **2013**, *21*, 28523–28530. [CrossRef] [PubMed]
25. Liao, M.H.; He, W.Q.; Peng, X.; Liu, X.L.; Meng, X.F. Cryptanalysis of optical encryption with a reference wave in a joint transform correlator architecture. *Opt. Laser Technol.* **2013**, *45*, 763–767. [CrossRef]
26. Cai, J.J.; Shen, X.J.; Wu, H.L.; Lin, C. Ciphertext-only attack on the JTC-based cryptosystem with sizes and locations of the plaintext and the key code unknown. *Appl. Optics* **2015**, *54*, 4760–4764. [CrossRef] [PubMed]
27. Millan, M.S.; Perez-Cabr, E.; Javidi, B. Multifactor authentication reinforces optical security. *Opt. Lett.* **2006**, *31*, 721–723. [CrossRef] [PubMed]
28. Pérez-Cabré, E.; Millán, M.S.; Javidi, B. Near infrared multifactor identification tags. *Opt. Express* **2007**, *15*, 15615–15627. [CrossRef] [PubMed]
29. Mohammed, E.A.; Saadon, H.L. Optical double-image encryption and authentication by sparse representation. *Appl. Optics* **2016**, *55*, 9939–9944. [CrossRef]
30. Perez-Cabre, E.; Mohammed, E.A.; Millan, M.S.; Saadon, H.L. Photon-counting multifactor optical encryption and authentication. *J. Optics-Uk* **2015**, *17*, 025706. [CrossRef]
31. Zhao, T.Y.; Chi, Y.Y. A novel secret sharing with two users based on joint transform correlator and compressive sensing. *J. Mod. Optics* **2018**, *65*, 1072–1080. [CrossRef]
32. Yuan, S.; Zhang, T.; Zhou, X.; Liu, X.M.; Liu, M.T. An optical authentication system based on encryption technique and multimodal biometrics. *Opt. Laser Technol.* **2013**, *54*, 120–127. [CrossRef]
33. Saini, N.; Sinha, A. Optics based biohashing using joint transform correlator. *Opt. Commun.* **2010**, *283*, 894–902. [CrossRef]
34. Islam, M.N.; Karim, M.A.; Asari, K.V. Information security using multiple reference-based optical joint transform correlation and orthogonal code. *Opt. Laser Technol.* **2013**, *50*, 8–13. [CrossRef]
35. Diaz-Ramirez, V.H.; Kober, V.; Alvarez-Borrego, J. Pattern recognition with an adaptive joint transform correlator. *Appl. Optics* **2006**, *45*, 5929–5941. [CrossRef]

36. Kamal, H.A.; Cherri, A.K. Complementary-reference and complementary-scene for real-time fingerprint verification using joint transform correlator. *Opt. Laser Technol.* **2009**, *41*, 643–650. [CrossRef]
37. Wang, H.J.; Qin, Y.; Huang, Y.D.; Wang, Z.P.; Zhang, Y.Y. Multiple-image encryption and authentication in interference-based scheme by aid of space multiplexing. *Opt. Laser Technol.* **2017**, *95*, 63–71. [CrossRef]
38. Liu, W.; Xie, Z.W.; Liu, Z.J.; Zhang, Y.; Liu, S.T. Multiple-image encryption based on optical asymmetric key cryptosystem. *Opt. Commun.* **2015**, *335*, 205–211. [CrossRef]
39. Kong, D.Z.; Shen, X.J. Multiple-image encryption based on optical wavelet transform and multichannel fractional Fourier transform. *Opt. Laser Technol.* **2014**, *57*, 343–349. [CrossRef]
40. Zhao, T.Y.; Yuan, L.; Chi, Y.Y. Hierarchical secret image sharing using phase modulation based on the Fresnel transform. *J. Mod. Optic.* **2019**, *66*, 1491–1497. [CrossRef]
41. Goodman, J.W. *Introduction to Fourier Optics*; Roberts and Company Publishers: Devon, UK, 2005.
42. Angervaks, A.E.; Malyi, A.F.; Fedorov, I.U.; Shcheulin, A.S. Dynamic joint transform correlator of images. In *Lasers for Measurements and Information Transfer 2007*; International Society for Optics and Photonics: Bellingham, WA, USA, 2008; Volume 7006.
43. Fan, C. Design of compact joint transform correlator. *Ukr. J. Phys. Opt.* **2017**, *18*, 55–65.
44. Murillo-Escobar, M.A.; Cruz-Hernandez, C.; Abundiz-Perez, F.; Lopez-Gutierrez, R.M.; Del Campo, O.R.A. A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal. Process.* **2015**, *109*, 119–131. [CrossRef]
45. Han, C.Y. An image encryption algorithm based on modified logistic chaotic map. *Optik* **2019**, *181*, 779–785. [CrossRef]
46. Kumar, R.; Quan, C. Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform. *Opt. Laser Eng.* **2019**, *120*, 118–126. [CrossRef]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).