applied sciences

MDPI

Article

A Novel Signature and Authentication Cryptosystem for Hyperspectral Image by Using Triangular Association Encryption Algorithm in Gyrator Domains

Zhonglin Yang [1], Yanhua Cao [1], Shutian Liu [2], Camel Tanougast [3], Walter Blondel [3], Zhengjun Liu [2] and Hang Chen [1,3,*]

[1] School of Space Information, Space Engineering University, Beijing 101416, China; feifeiliu1999@163.com (Z.Y.); yanhuacao1997@163.com (Y.C.)
[2] Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China; stliu@hit.edu.cn (S.L.); zjliu@hit.edu.cn (Z.L.)
[3] Centre National de la Recherche Scientifique, Centre de Recherche en Automatique de Nancy, UMR 7039, Universitéde Lorraine, 54000 Nancy, France; camel.tanougast@univ-lorraine.fr (C.T.); walter.blondel@univ-lorraine.fr (W.B.)
* Correspondence: hitchenhang@foxmail.com

Abstract: A novel optical signature and authentication cryptosystem is proposed by applying triangular association encryption algorithm (TAEA) and 3D Arnold transform in Gyrator domains. Firstly, a triangular association encryption algorithm (TAEA) is designed, which makes it possible to turn the diffusion of pixel values within bands into the diffusion within and between bands. Besides, the image signature function is considered and utilized in the proposed cryptosystem. Without the image signature, the original image cannot be restored even if all of the keys are obtained. Moreover, the image integrity authentication function is provided to prevent pixel values from being tampered with. Through the numerical simulation of various types of attacks, the effectiveness and capability of the proposed hyperspectral data signature and authentication cryptosystem is verified.

Keywords: optical hyperspectral image cryptosystem; 3D Arnold; image signature; image integrity authentication; gyrator; TAEA

Citation: Yang, Z.; Cao, Y.; Liu, S.; Tanougast, C.; Blondel, W.; Liu, Z.; Chen, H. A Novel Signature and Authentication Cryptosystem for Hyperspectral Image by Using Triangular Association Encryption Algorithm in Gyrator Domains. *Appl. Sci.* **2022**, *12*, 7649. https://doi.org/10.3390/app12157649

Academic Editor: Juan Francisco De Paz Santana

Received: 13 July 2022
Accepted: 26 July 2022
Published: 29 July 2022

1. Introduction

The explosion of information has brought the development of the information society, which has also brought threats to information security. As the mainstream information carrier, the security of images is faced with many challenges and threats. The security of an image can be achieved through traditional mathematical and non-traditional methods. Because digital images have the characteristics of strong pixel correlation, large data capacity and high redundancy, images are more suitable to be encrypted by non-traditional cryptographic algorithms, such as optical [1] and chaotic mapping [2].

Because of its ability to arbitrarily select optical parameters, such as amplitude, phase, polarization and wavelength, to construct multidimensional data in different ways, as well as the inherently high parallel processing speed, optical information encryption technology has an important potential for secure applications of increased security for information [3,4]. Since the double random phase encoding (DRPE) system was first proposed by Refregier and Javidi in 1995 [1], optical encryption opened up a new era of information security and promoted the development of cryptography. Optics were greatly developed in various transform domains, such as the fractional Fourier domain, discrete cosine transform domains and the Gyrator domain [5–11], besides, a variety of optical processing systems using random phase coding schemes were proposed to protect, store and decrypt information [12–18].

The optical techniques mentioned above [2–18] are usually applied to single image coding and are perfectly suitable for grayscale and color images. Compared with single band and few bands, hyperspectral images have more bands. The information of the image is stored in each band, and the different bands are closely related. This puts forward higher requirements for the confidentiality of the hyperspectral images. It needs not only to keep a single image confidential, but also to pay attention to the relationship between the bands. Some problems may occur when the single image encryption method is directly used in hyperspectral image encryption. For hyperspectral images with multiple bands, the same encryption method and key parameters are used repeatedly, which is equivalent to providing the corresponding ciphertext of different plaintext. This means that the attacker will be provided with a lot of known plaintext attack materials [19,20], which is a great threat to the encryption system.

Because hyperspectral images are applicable to many scenarios, especially in the field of remote sensing, hyperspectral image encryption has attracted attention at home and abroad. In recent decades, based on the sensitivity of the optical parameters, many researchers have proposed the technology of optical multiplexing to realize optical multiple image coding [21–26]. However, these multi-image encryption techniques based on multiplexing strategies are severely limited by optical calibration problems and the limited number of secret images that need to be hidden.

The application of chaos can help disrupt the connections between the pixels in an hyperspectral image. For example, Hang Chen presents an optical hyperspectral image cryptosystem using improved Chirikov mapping in the gyrator transform domains [27]. The improved Chirikov mapping can help the optical encryption scheme to simultaneously hide the spatial and spectrum information. However, the original hyperspectral image needs to be converted into a binary format and then extended into a one dimensional array, which will be a waste of time. Chaotic/hyperchaotic systems have been studied deeply in the field of hyperspectral image encryption, due to their high randomness, sensitivity of parameters and speed of multi-dimensional parallel processing. In the same way as the methods in other literature [13,28–34], using chaos or high-dimensional chaos for hyperspectral image encryption is also a scheme that uses chaos to generate sequences and then encrypts the pixels one by one, which is quite complicated.

The 3D Arnold transform can operate directly on the pixels, eliminating the need to convert the image formats. This paper draws lessons from the integer nonlinear coupled chaos model [35]. In this paper, an optical hyperspectral image cryptosystem is proposed by using the triangular association encryption algorithm(TAEA) model with signature and authentication based on 3D Arnold in the Gyrator domains. Limitations on the dimension of encrypted objects can be overcome by using the block mobile method. The triangular association encryption algorithm is developed, based on 3D Arnold in the Gyrator domains. Only in this way can the advantages of optical encryption be exploited, and the scrambling and diffusion within the bands can be extended to the ones within and between bands. On the basis of these, the algorithm also adds a signature and integrity authentication. It not only improves the security of the algorithm, but also confirms the identity of the other party and prevents tampering attacks. This algorithm is suitable for the transmission of important hyperspectral data, when such transmission needs to confirm the identity of the sender and prevent intermediate attackers from tampering.

Compared with the other hyperspectral encryption algorithms, the biggest advantage of the algorithm designed in this paper is that it is not limited to the size of the hyperspectral images. Almost all of the sizes of hyperspectral images can be directly processed by this algorithm without preprocessing. In addition, it adds the functions of signature and digital authentication.

The rest of this article is organized as follows. In Section 2, the proposed encryption/decryption algorithm is described in detail. In Section 3, the numerical simulation results are presented to verify the effectiveness and robustness of the proposed algorithm. Finally, the conclusion is summarized.

2. Optical Hyperspectral Image Cryptosystem

This section will discuss the whole optical hyperspectral image cryptosystem in detail first.

The flowchart of the optical signature and authentication cryptosystem by using the triangular association encryption algorithm (TAEA) and 3D Arnold transform in the Gyrator domains is illustrated in Figure 1. The intact encryption approach is completed by using 3D Arnold mapping, triangular association, Gyrator transform, and integrity authentication, respectively. The specific process is as follows:

1. The image as the signature formed by the identity information of the sender 'Lena' or another one is attached to the hyperspectral data as the $(N+1)$th layer;
2. Set the side length to be equal to N in the block mobile method of 3D Arnold. Except the $(N+1)$th layer, the N-layer hyperspectral data are scrambled by using the block mobile method of 3D Arnold (see Figure 1);
3. Except the $N+1$th layer, the N-layer hyperspectral data are encrypted by using the triangular association encryption algorithm (see (4)–(7));
4. Then perform the Gyrator transform for the first N layers;
5. Get the encrypted image with the signature. The signature is still the original identity image, which will not be transmitted to the receiver directly. The signature information is communicated in advance and is known only to the sender and receiver;
6. Take real integers from the first N layers. Let the side length be equal to N + 1 in the block mobile method of 3D Arnold. The N + 1 layers hyperspectral data are performed, using the block mobile method of 3D Arnold (see Figure 1). Then, the algorithm of image integrity authentication is performed for every layer (see (8));
7. Add the single-layer secret information obtained in step-6 to the first N layers encryption information obtained in step-5 to form the ciphertext of N + 1 layers;
8. The encrypted image information of N + 1 layers obtained in step-7, which has the function of signature and integrity authentication, can be transmitted to the recipient.

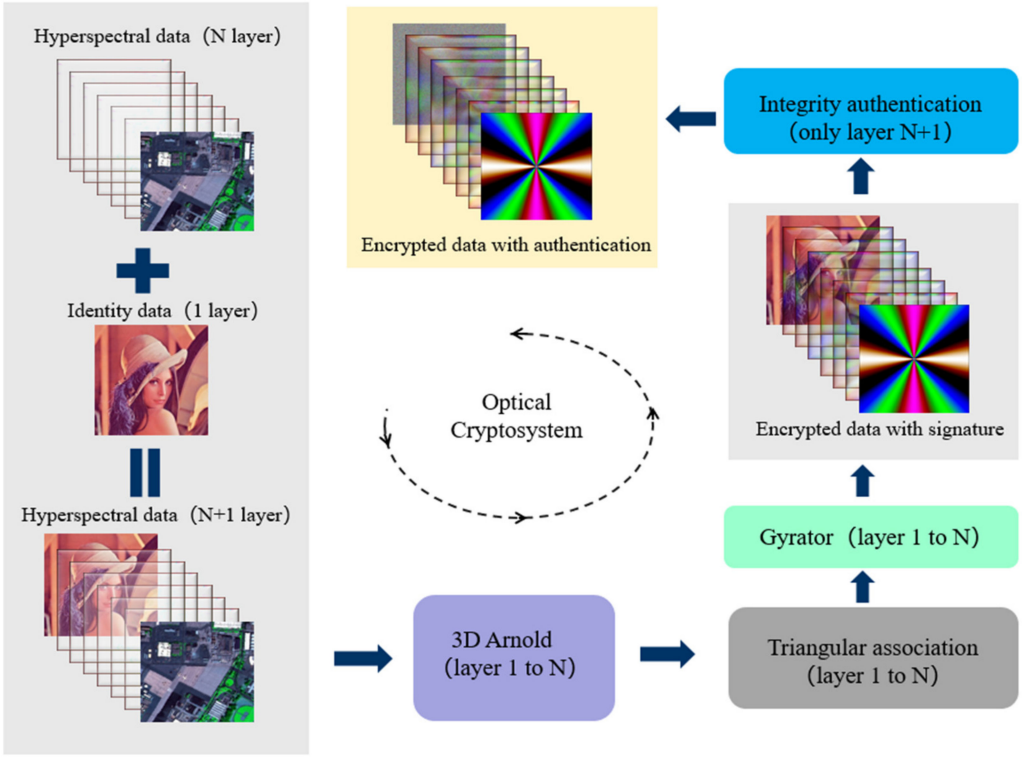


Figure 1. The flowchart of the hyperspectral image encryption algorithm.

Next, the 3D Arnold map and block mobile method, triangular association encryption algorithm, image signature, image integrity authentication and Gyrator transform are briefly introduced in this section.

2.1. D Arnold Map and Block Mobile Method

Arnold transform, called cat mapping, is a nonlinear discrete system often used in image encryption. The 3D Arnold transform evolves from the 2D Arnold in order to meet the higher security requirements as encrypted objects change from lower to higher dimensions. The mathematical definition [36,37] of a 3D Arnold map is as follows:

$$B = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \tag{1}$$

$$\begin{cases} a_{11} = 1 + ace, \ \ a_{12} = c, \quad a_{13} = c + ac + abce \\ a_{21} = f + ae + acef, \quad a_{22} = cf + 1 \\ a_{23} = bf + abcef + acf + abe + a \\ a_{31} = ade + e, \ \ a_{32} = d \\ a_{33} = abde + ad + be + 1 \end{cases} \tag{2}$$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ h_{n+1} \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ h_n \end{bmatrix} (\mathrm{mod} L) \tag{3}$$

As shown in Equation (1), B is the coefficient matrix of 3D Arnold and the parameters must satisfy the relationship in Equation (2). The variation range of these variables is a positive integer in Equation (2). As shown in Equation (3), the period of the transformation is dependent on L, which is the size of image; before the transformation, the position coordinates of the pixels is (x_n, y_n, h_n) and $(x_{n+1}, y_{n+1}, h_{n+1})$ is the position coordinates of pixels after the transformation. The pixel value of the image changes according to the position.

However, in the specific application, the premise of using 3D is that the object of the transformation has to be a square matrix, such as $256 \times 256 \times 256$. To solve this problem, the block mobile method, as an innovative use of 3D Arnold, is proposed in this paper.

$$a = \left\lceil {}^{x}\!/_{h} \right\rceil \tag{4}$$

In Figure 2a, the hyperspectral images have three dimensions. In Equation (4), x and y are the side length of a single band image, then the minimum number of square moves is a^2. Then, follow a certain rule to move the square horizontally, longitudinally and diagonally until the entire image area is covered, as shown in Figure 2b. Firstly, set the side length of the spatial mobile module as h. From the x–y plane, there is a square moving with a side length of h, and it can cover the whole plane at least four times. In this article, the step length we take is long enough to make the moving module move twice along the x axis and twice along the y axis, so that the whole hyperspectral image can be covered. From the perspective of permutation and combination, there are 24 kinds of this movement mode. The schematic diagram shows that the module moves to $(0, 0)$ points first, and then to $(256, 0)$, then to $(0, 256)$, then to $(256, 256)$ finally. After moving four times, in order to avoid periodic cycles, the 3D Arnold scrambling blocks can also be selected to be executed 2^{108} times in different positions.

The process and results of the block mobile method are shown in Figure 2b,c. As the block steps, the overlapping areas will appear. The end result is that 3D Arnold performs different times in different areas of the image, so that a higher level of security is achieved. More importantly, this method is easy to implement and can be applied to the vast majority of hyperspectral images.

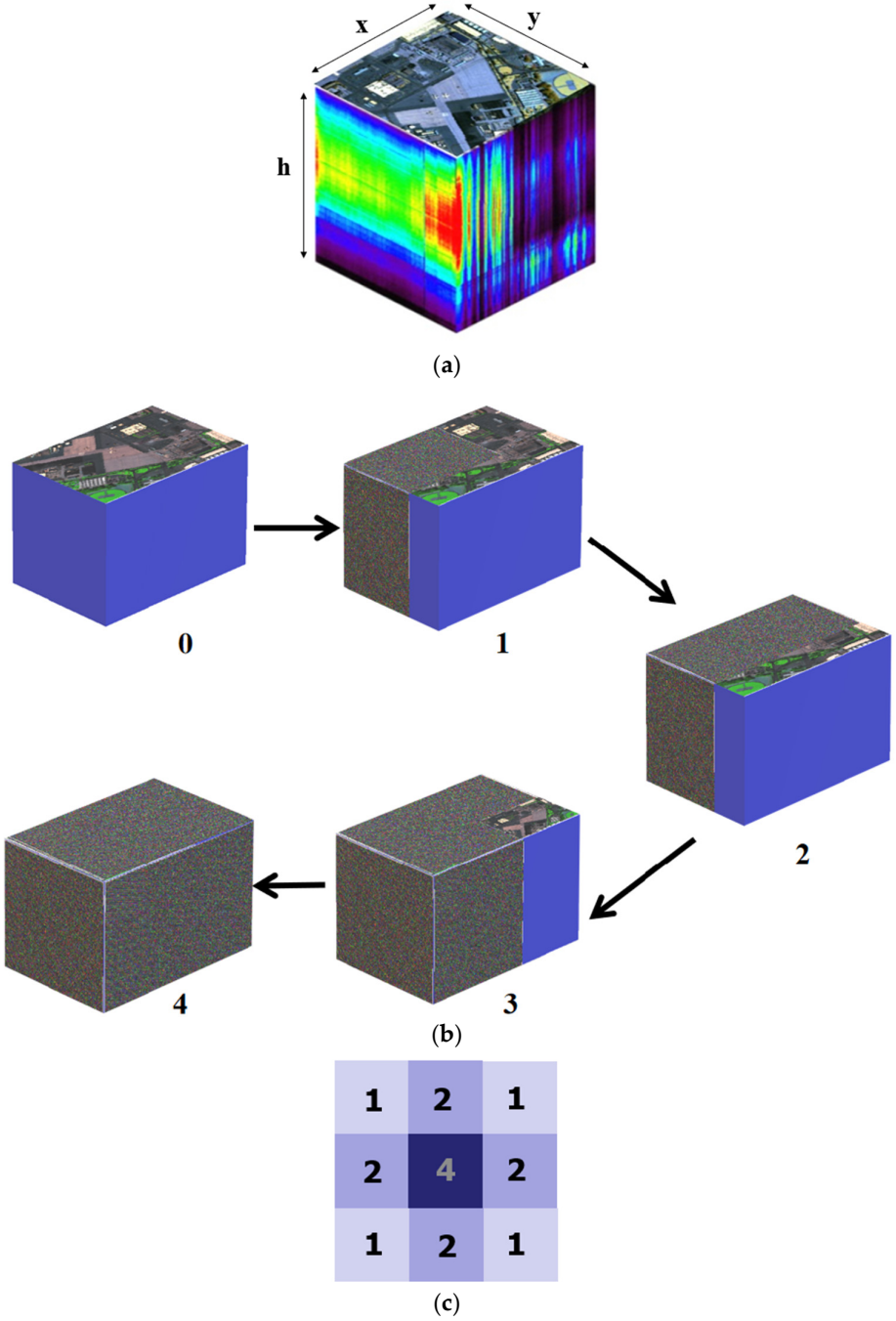


Figure 2. The block mobile method of 3D Arnold. (**a**) 3D model of hyperspectral image; (**b**) The movement schematic diagram of 3D Arnold transform; (**c**) The result of transformation and the number of transformations in different regions.

2.2. Triangular Association Encryption Algorithm (TAEA)

For grayscale and color images, as a key part of the image encryption diffusion, the diffusion is often used in-band. However, for hyperspectral images, the realization of diffusion in-band and inter-band can not only improve the efficiency, but also improve the security level. The TAEA designed in this paper can achieve the above goals and requirements perfectly. The model is as follows:

$$\begin{aligned} &I[x_{n+1}(i), y_{n+1}(i), h_{n+1}(i)] \\ &= g\{I[x_n(i), y_n(i), h_n(i)]\} + g\{I[x_n(i+a_0), y_n(i+a_0), h_n(i+a_0)]\} \\ &+ g\{I[x_n(i), y_n(i), N+1]\} \mod N \end{aligned} \tag{5}$$

where, $[x_{n+1}(i), y_{n+1}(i), h_{n+1}(i)]$ is the pixel coordinates after transformation; and $I[x_{n+1}(i), y_{n+1}(i), h_{n+1}(i)]$ is the corresponding pixel value; $[x_n(i), y_n(i), h_n(i)]$ is the pixel coordinates before transformation; and $I[x_n(i), y_n(i), h_n(i)]$ is the corresponding pixel value; $[x_n(i), y_n(i), N+1]$ is the pixel coordinates at layer $N+1$ corresponding to $[x_n(i), y_n(i), h_n(i)]$, and $I[x_n(i), y_n(i), N+1]$ is the corresponding pixel value; n is steps of iteration; $i = 1, 2, \cdots, N$ is number of transformation; N is system grid points. $[x_n(i+a_0), y_n(i+a_0), h_n(i+a_0)]$ are determined by the model as follows:

$$\begin{pmatrix} x_n(i+a_0) \\ y_n(i+a_0) \\ h_n(i+a_0) \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}^{a_0} \begin{bmatrix} x_n(i) \\ y_n(i) \\ h_n(i) \end{bmatrix} (\mathrm{mod} N) \tag{6}$$

where a_0 is a positive integer. According to the reference [36], the period of 3D Arnold is related to the size of image, and the period of the $64 \times 64 \times 64$ image is 112. The object size of this study is $256 \times 256 \times 189$, and the period is much larger than 112. Therefore, to be on the safe side, we set the variation range of a_0 as 112.

The mathematical form of function g, called dynamic integer tent mapping [38], is as follows. The tent map has good ergodic uniformity and can improve the optimization speed of the algorithm. Moreover, it can be used together with Arnold transform to give better play to the chaotic characteristics of the system:

$$g(x_k) = \begin{cases} \mu(f_k + \frac{1}{2}), & f_k \in [0, 2^{b-1}) \\ \mu(2^b - 1 - f_k), & f_k \in [2^{b-1}, 2^b - 1] \end{cases} \tag{7}$$

$$f_k = (x_k + j_k) \mathrm{mod}(2^b) \tag{8}$$

where $\mu \in (0, 2]$ and b is digit of the system; and j_k represents the displacement of the mapping. Multi-dimensional chaotic integer sequences with good pseudo randomness can be generated in this model rapidly and in parallel.

In space, three points $[x_n(i), y_n(i), h_n(i)]$, $[x_n(i), y_n(i), N+1]$ and $[x_n(i+a_0), y_n(i+a_0), h_n(i+a_0)]$ form a triangle, as shown in Figure 3, so the algorithm model is called the triangular association encryption algorithm (TAEA).

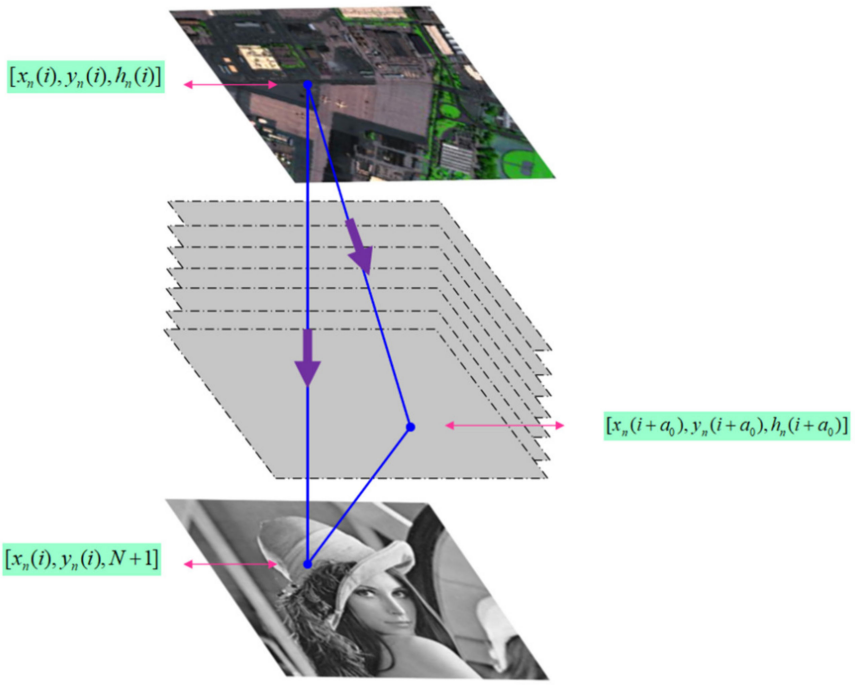


Figure 3. A triangle in space formed by three points of the image from the algorithm (TAEA).

2.3. Image Signature

The image signature can confirm that an image message is indeed sent by a sender, no one can forge the message, and the sender cannot deny. When the text message is digitally signed, the message's digest is calculated and then signed. The image signature method proposed in this paper can be implemented in the process of encryption, which is secure, convenient and fast.

The $N+1$th layer is the additional signature layer, which could be information about identity, or could be an image. We can also adopt a more convenient method, select a band of hyperspectral image as the signature layer, and attach it at the end. Thus, the transmission of the signature data means to transport only one band position. In Equation (4), the pixel values on the $N+1$th layer are used in each operation. So, in the decryption process, you cannot decrypt the message without the $N+1$th layer; similarly, the signature information of the other party can be used as the $N+1$th layer to decrypt the message and confirm the identity of the sender.

As shown in Figure 4, Bobo use the identity information as a signature for encryption; only Tom can restore the message correctly because he has Bobo's signature.

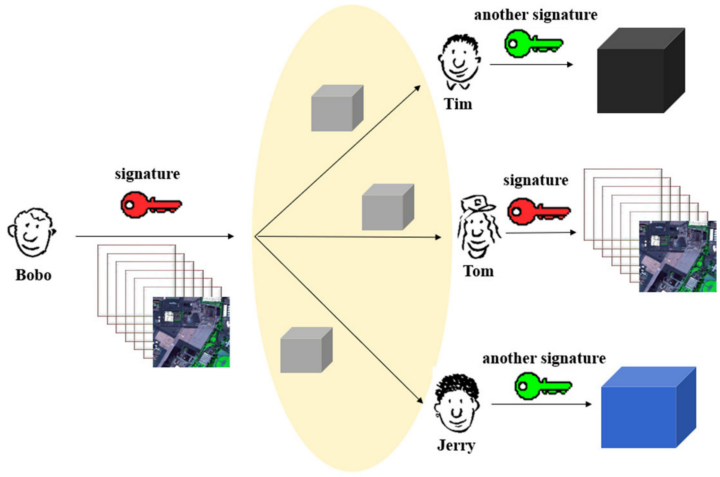


Figure 4. Flowchart of signature authentication.

2.4. Image Integrity Authentication

Images can also be tampered with during transmission. If the information is tampered with, the algorithm of image integrity authentication proposed in this paper will detect it.

$$\begin{aligned} &I[x_{n+1}(i), y_{n+1}(i), h_{n+1}(i)] \\ &= g\{I[x_n(i), y_n(i), h_n(i)]\} \\ &+g\{I[x_n(i+1), y_n(i+1), h_n(i+1)]\} \\ &+g\{I[x_n(i+2), y_n(i+2), h_n(i+2)]\} \\ &+g\{I[x_n(i+3), y_n(i+3), h_n(i+3)]\} \\ &+g\{I[x_n(i+4), y_n(i+4), h_n(i+4)]\} \quad \mathrm{mod} N \end{aligned} \tag{9}$$

After the signature encryption is performed, the authentication algorithm is performed separately for every layer. However, only the $N+1$th layer is attached to the secret information sent. In this algorithm, if the original information is changed as little as one pixel, the SSIM value will also drop below 0.6 (see numerical simulation).

2.5. Gyrator Transform

The Gyrator transform is both a generalized Fourier transform and a special linear regular transform. This optical transform only has a two dimensional format, thus it is suitable for digital image processing and image encryption applications, and has attracted

more and more attention in recent years. The mathematical definition of the Gyrator transformation [39] can be described as:

$$\begin{aligned} G(u,v) &= \xi^{\alpha}[g(x,y)](u,v) \\ &= \frac{1}{|\sin\theta|}\iint g(x,y)\exp\left[i2\pi\frac{(xy+uv)\cos\theta - xv - yu}{\sin\theta}\right]dxdy \end{aligned} \tag{10}$$

where (x, y) is the input spatial position coordinate and (u, v) is the frequency coordinate of the transformation domain; $g(x, y)$ represents the original image and $G(u, v)$ represents the image output by the Gyrator transformation. In which the parameter α is the fractional order of the Gyrator transformation, that is, the rotation angle. Besides, the Gyrator transform becomes a Fourier transform when $\alpha = \pi/2$.

Two important properties are often used when using Gyrator transformation in optical encryption systems. As shown in (10), the transformation is invertible, and the Gyrator transformation for which the fractional order is α, followed by the Gyrator transformation for which the fractional order is $-\alpha$ yields 1. It can be seen from (11) that its period is 2π:

$$R^{-\alpha}\{R^{\alpha}\{f(r)\}\} = R^{0}\{f(r)\} = f(r) \tag{11}$$

$$R^{\alpha+2\pi}\{f(r)\}(r_0) = R^{\alpha}\{f(r)\}(r) \tag{12}$$

3. Numerical Simulation

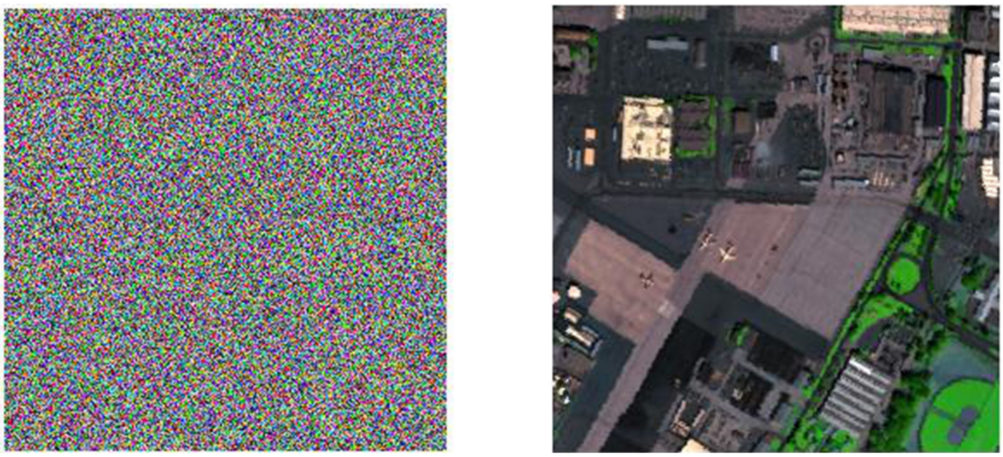
Various numerical simulations are performed to verify the feasibility and effectiveness of the optical signature and authentication cryptosystem by using a triangular association encryption algorithm (TAEA) and 3D Arnold transform in the Gyrator domains. Numerical experiments consider a hyperspectral image 'airport', which has 256 × 256 × 189 pixels as the secret information needed to be encrypted in the following experiments. A grayscale image of the color image 'Lena' having 256 × 256 × 3 pixels is considered as the image signature. The pseudo color composites combined of the 30th, 70th and 100th band and the image signature 'Lena' are depicted in Figure 5a,b.

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

Figure 5. Experimental data: (**a**) pseudo color composites combined of 30th, 70th and 100th band; (**b**) 'Lena' test image.

In the following tests, matrix B (see (1)) is used for the transformation, and we set $a = b = c = d = e = f = 1$. The number of 3D Arnold transformation is k = 3, and the number of triangular association encryptions is a_0 = 3. The parameters θ in the Gyrator transform is set as 0.5. What is more, in the block mobile method of 3D Arnold, set "upper left" as "1", "lower left" as "2", "upper right" as "3" and "lower right" as "4". In the experiment, the normal order of movement is "1234".

The computer environment for the experiment is the Windows 10 system, Intel (R) Core (TM) i7-10700 CPU @ 2.90GHz, and 8.00 GB of RAM. Then, we obtain the final encrypted and decrypted images shown as Figure 6a,b. The time required for the encryption and decryption is respectively 15.391 s and 13.283 s.



(**a**) encrypted image (**b**) restored image from (**a**)

Figure 6. Experimental data: (**a**) final encrypted image combined of 30th, 70th and 100th band; (**b**) decrypted image combined of 30th, 70th and 100th band.

The decrypted image (see Figure 6b) and the original image (see Figure 5a) are visually similar. This paper introduced a structural similarity index (SSIM) function in order to numerically measure the difference between the original image and the decrypted image. The SSIM value of two same images is equal to 1. If two images are very different, then the SSIM value is near to 0. The mathematical expression of the SSIM [40] is as follows:

$$\mathrm{SSIM}(A,B) = \frac{(2v_Av_B + r_1)(2\partial_{AB} + r_2)}{(v_A^2 + v_B^2 + r_1)(\partial_A^2 + \partial_B^2 + r_2)} \tag{13}$$

where, v_A and v_B are the average of A and B; ∂_A^2 is the variance of A; ∂_B^2 is the variance of B; ∂_{AB} is the covariance of A and B; N is the value variation range of pixels, $r_1 = (i_1L)^2$, $r_2 = (i_2L)^2$, $i_1 = 0.01$, $i_2 = 0.03$.

The following experiments were quantitatively analyzed in detail. Note that, since the output of the Gyrator transform is complex, the simulation appears to be a real function.

3.1. Theoretical Analysis and Algebraic Attack

The image encryption system is based on optical and chaos theory. To prove its security, we must first test whether it can withstand the theoretical analysis against the weakness of the chaotic linear transformation and algebraic attack [41].

In the triangle correlation algorithm (TAEA) used in this paper, although the Arnold transform is linear, the Tent map is nonlinear, and the two are not a simple cascade, so the whole encryption system is not linear. Therefore, the theoretical analysis method for the weakness of the linear chaotic encryption system described in the "Cryptanalysis of Chaotic Ciphers" [41] is not applicable. We can also assume that the system is secure in this respect.

Algebraic attack methods are implemented based on key space or cycle, so we now analyze the key space of the encryption system. The 3D Arnold has six parameters a, b, c, d, e, f, and they're all eight bits, and there are $4 \times 3 \times 2$ types of module movement methods. The variation range of a_0 is set as 112. μ and θ are the double-precision floating point data, and the computer used for the simulation is 64-bit. So, the key space is $2^{108} \times 2^8 \times 2^8 \times 2^8 \times 2^8 \times 2^8 \times 2^8 \times 24 \times 112 \times 2^{64} \times 2^{64} > 2^{294} > 10^{87}$. The encryption

system is computationally secure and can withstand violent attacks [42,43] and algebraic attacks based on key space analysis.

According to Kerckhoff's criterion [44], a good encryption algorithm should have enough key space. The key space comparison of several encryption algorithms is shown in Table 1. Compared with the encryption algorithm in literature [27,45–48], the key space of the encryption algorithm in this paper is larger, which can better resist the exhaustive attack.

Table 1. Comparison of key space among several algorithms.

Algorithm	Key Space
Ref. [41]	3.41×10^{38}
Ref. [42]	10^{45}
Ref. [43]	10^{56}
Ref. [44]	$>10^{77}$
Our cryptosystem	$>10^{87}$

3.2. Test the Sensitivity of Keys

This paper will firstly test the sensitivity of some of the keys in protecting the secret images. Some attackers are designed to have a complete encryption and decryption system, but with partial keys which are incorrect.

Suppose the attackers wants to gain the three keys, one is the number of the 3D Arnold transformation ($k = 3$), one is the number of the triangular association encryptions ($a = 3$) and one is the order of the block mobile method ($O =$ "1234").

First, attacker-1 has obtained all of the keys, except the number of the 3D Arnold transformations. He assumes that $k = 2$ and Figure 7 shows the decrypted image. Attacker-1 cannot obtain any information about the original text from Figure 7d–g.

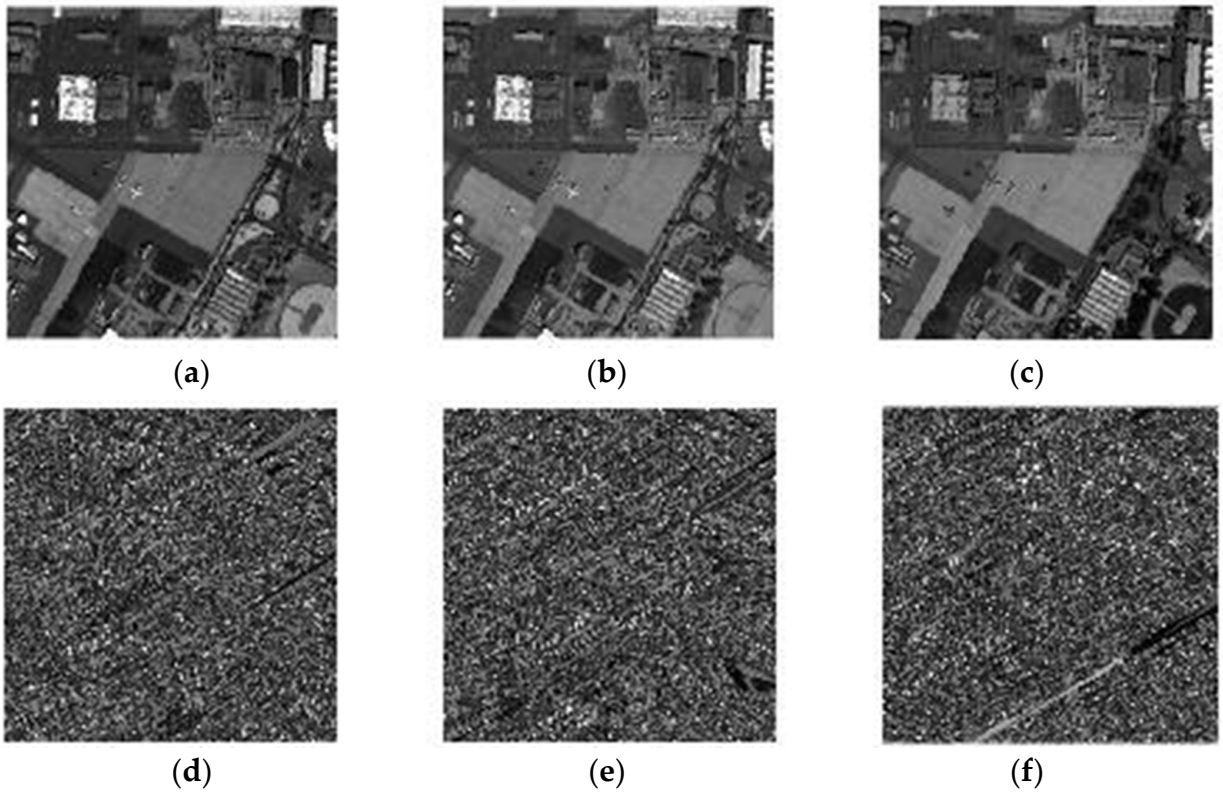
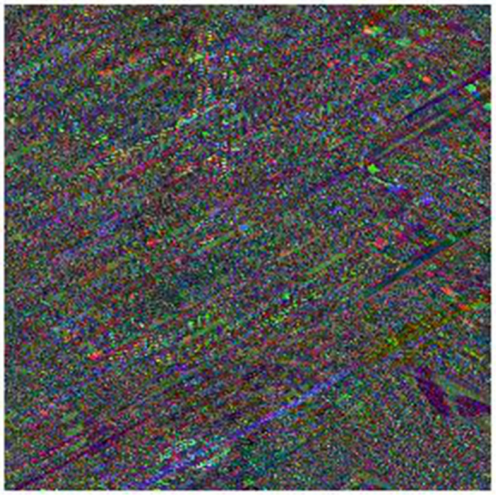


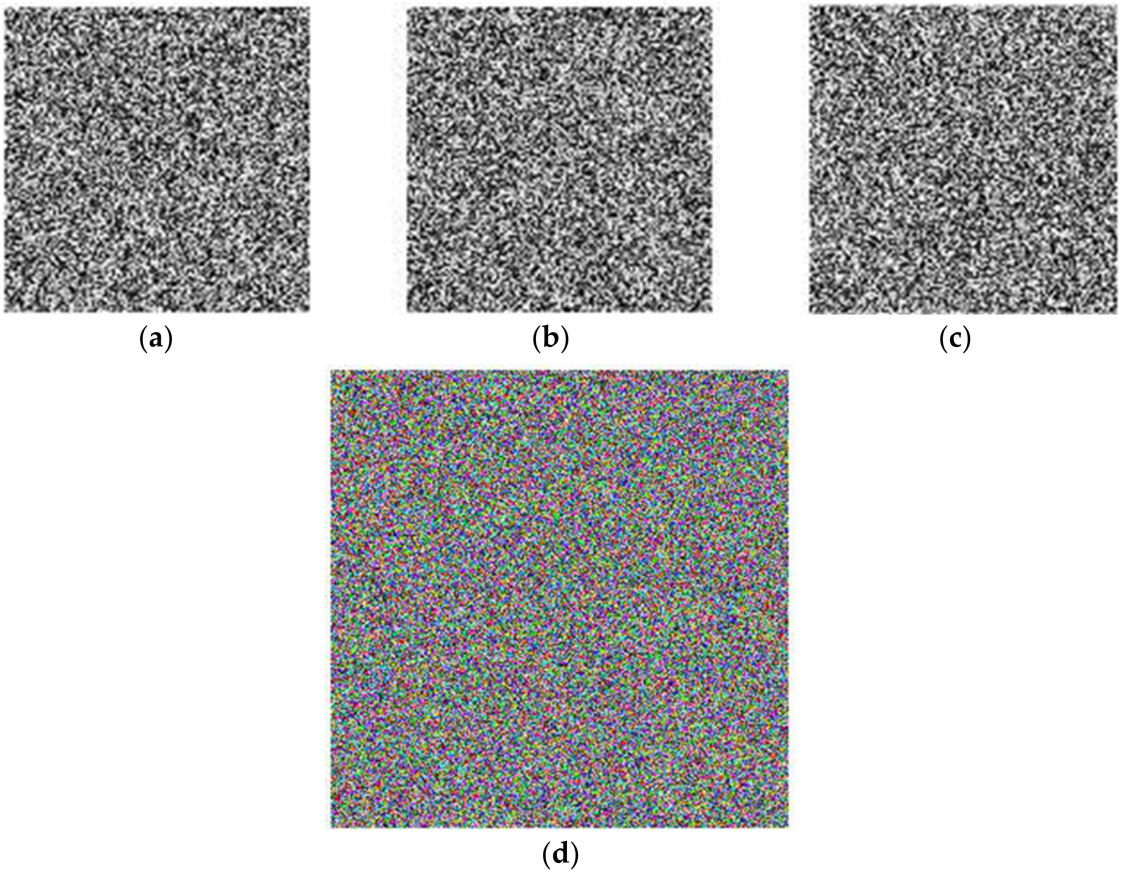
Figure 7. *Cont.*



(**g**)

Figure 7. Experimental data: (**a**–**c**) original image of 30th, 70th and 100th band; (**d**–**f**) corresponding decrypted image with k = 2; (**g**) decrypted image combined of (**d**–**f**).

Attacker-2 has obtained all of the keys, except the number of triangular association encryptions. He assumes that a = 2 and Figure 8 shows the decrypted image. Attacker-2 cannot obtain any information about the original text from the Figure 8a–d.



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

(**d**)

Figure 8. Experimental data: (**a**–**c**) corresponding decrypted image of 30th, 70th and 100th band with a = 2; (**d**) decrypted image combined of (**a**–**c**).

Attacker-3 has obtained all of the keys, except the order of the block mobile method. He assumes that O = "1324" and Figure 9 shows the decrypted image. Attacker-3 cannot obtain any information about the original text from the Figure 9a–d.

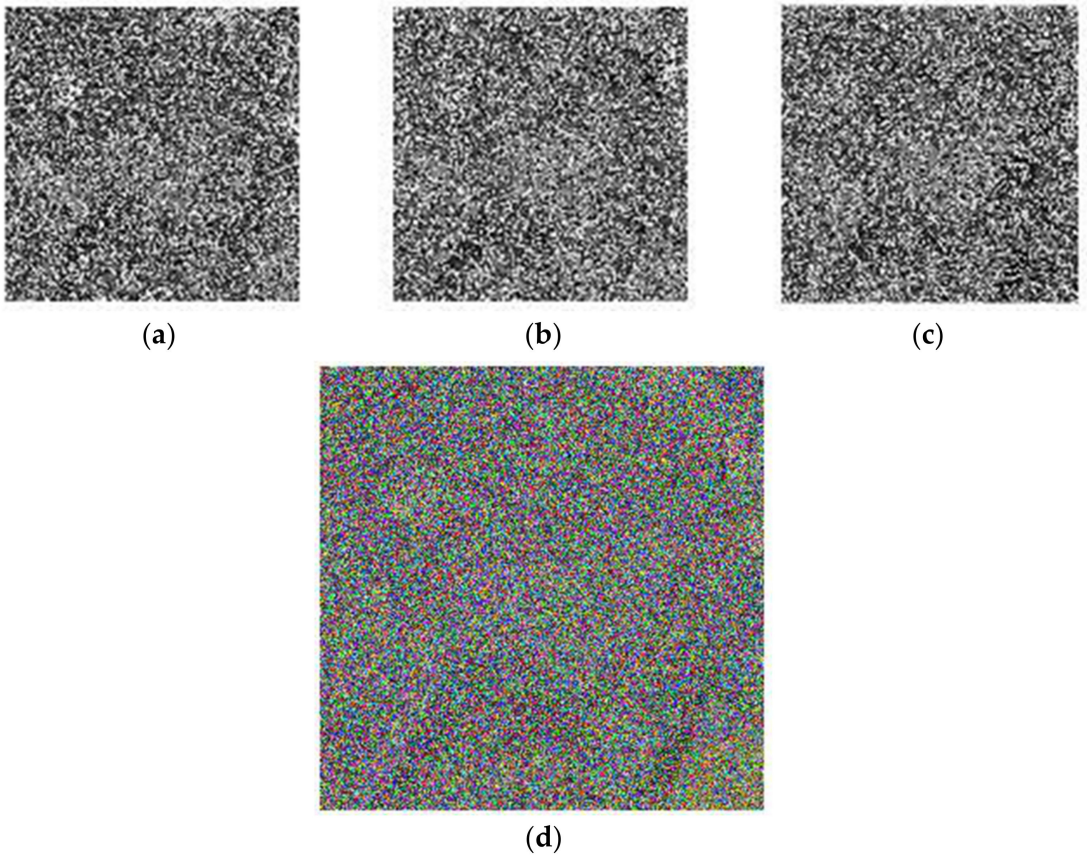


Figure 9. Experimental data: (**a**–**c**) corresponding decrypted image of 30th, 70th and 100th band with O = "1324"; (**d**) decrypted image combined of (**a**–**c**).

Besides, the keys held by the recipient and the three attackers are listed in Table 2, with the SSIM values by calculating the difference between the original and the tampered value. The results in Table 2 show that any small change in the keys can make a huge difference in the results, demonstrating the high sensitivity and ability of the keys to protect information.

Table 2. The results by using different initial conditions.

k	a	O	SSIM–30th	SSIM–70th	SSIM–100th
3	3	1234	1	1	1
2	3	1234	0.0387	0.0371	0.0355
3	2	1234	0.0091	0.0109	0.0086
3	3	1324	0.0286	0.0308	0.0268

The keys above can only be integers, then this paper will further test the sensitivity of the angle of the Gyrator transformation, whose range of change is real. Figure 10 shows the corresponding SSIM curve with the angle of the Gyrator transformation changing near the right value, under the condition that the correct key and decryption method are known. In this test, the correct angle and the sampling step are set to 0.5 and 0.005. When the step is +1 or −1, that is, when the angle is 0.495 and 0.505, two decrypted images are completely unrecognizable. In fact, it would be worse if the angle value deviates more from the set value. Therefore, in terms of the effect of protecting secret images, the angle is a good additional key.

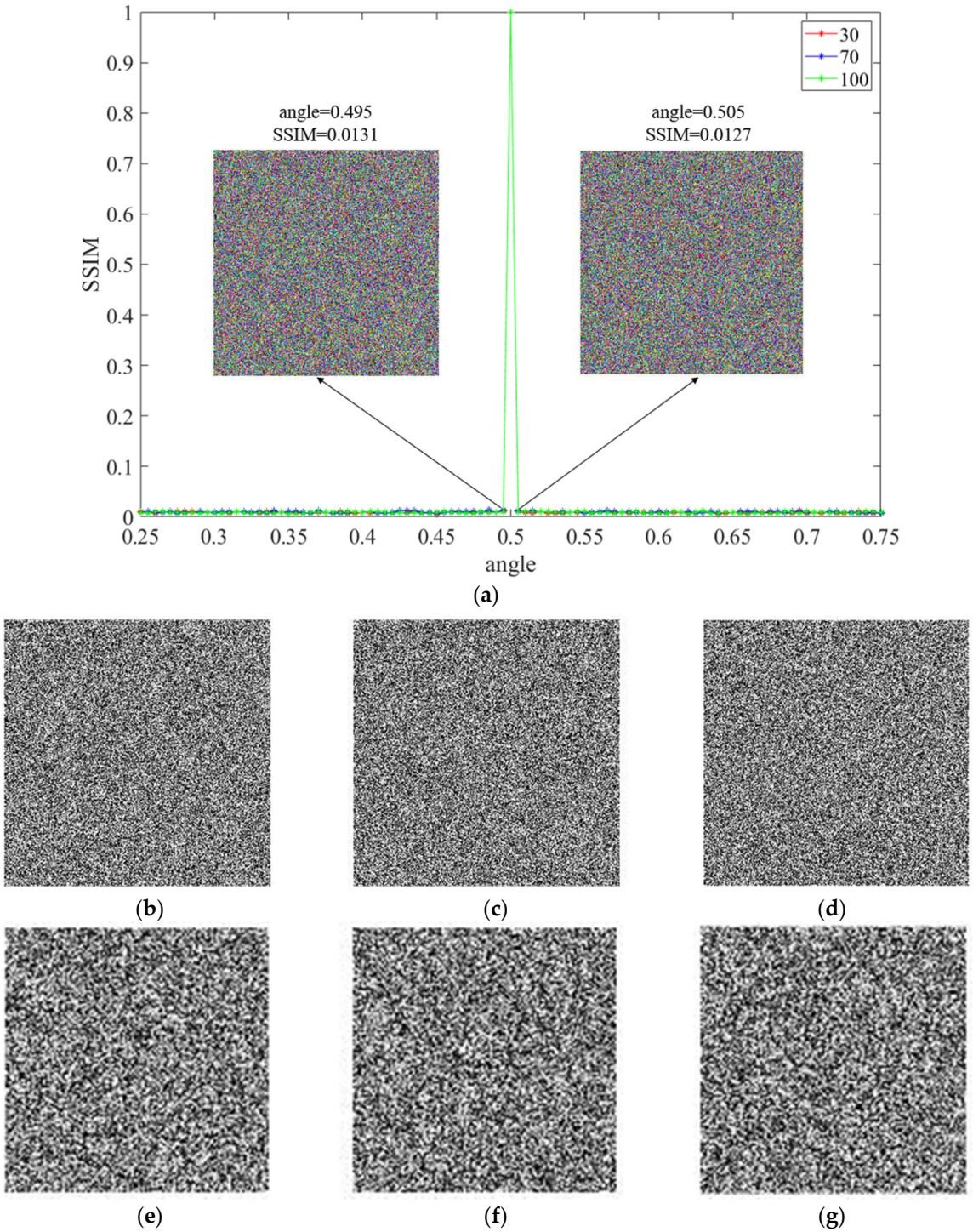


Figure 10. (**a**) the SSIM curve calculated by the different values of the parameter of the Gyrator (**b**–**d**) corresponding decrypted image of 30th, 70th and 100th band with angle = 0.495; (**e**–**g**) corresponding decrypted image of 30th, 70th and 100th band with angle = 0.505.

3.3. Test Resistance to the Noise Attack

The next analysis of robustness will perform a noise attack on the hyperspectral image encryption system. In order to complete the noise attack robustness experiments [49], this paper introduces the following noise model:

$$H'(x,y) = H(x,y)[1 + p \cdot \xi_{0,1}(x,y)] \tag{14}$$

where $H(x,y)$ represents the test image before adding noise and $H'(x,y)$ represents the test image after adding noise respectively. The symbol p represents the intensity factor of the noise. In addition, the size of the test image is same as random data $\xi_{0,1}(x,y)$, of which the mean value is 0 and standard deviation is 1.

Thus, different ciphertexts are obtained by adding different intensities of noise, which are decrypted and compared with the original text to obtain the SSIM change diagram, as shown in the Figure 11. In the calculation, the variation range of noise intensity is 0 to 1, and the variation step is 0.01, that is, the number of the decryption is 101. Note that when the noise intensity is 0.5 and 1, the main information of the decrypted image can be recognized, as shown in the figure. So, we can say that this system can resist the noise attack effectively.

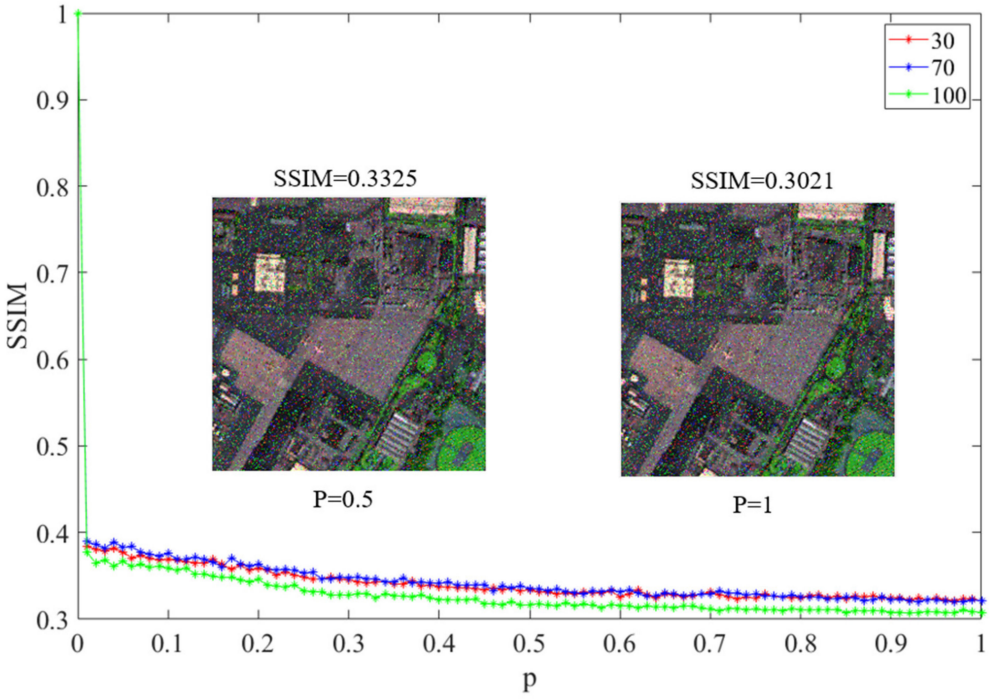


Figure 11. The SSIM curve of noise attack including decrypted image obtained with p = 0.5, and decrypted image obtained with p = 1.

3.4. Test Resistance to the Occlusion Attack

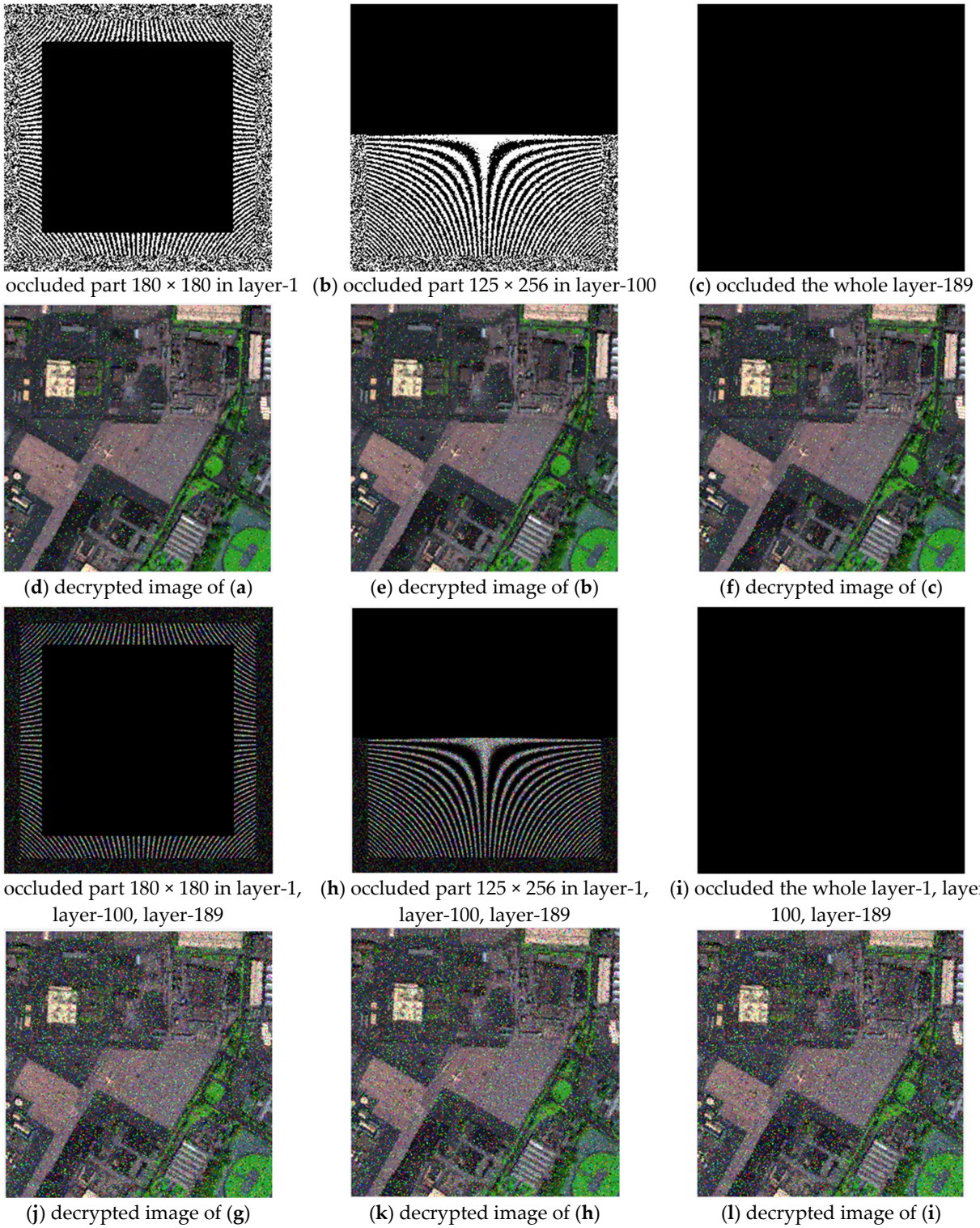
Next, the occlusion attack experiment is carried out. It is assumed that the attacker intercepts and captures the transmitted secret information in the transmission channel. In order to simplify the process, 0 was used in the experiment to represent the obscured pixel in this experiment. The receiver partly decrypts the occluded information with the known decryption scheme and keys.

In Figure 12, the occluded secret information is up there and the corresponding decryption information is down there. To improve persuasion, cover the middle half, the upper half and the whole of the single layer first. Then cover the middle half, the upper half and the whole of the three layers.

As shown in Figure 12a, the middle half of the layer-1 is obscured; in Figure 12b, the upper half of the layer-100 is obscured; in Figure 12c, the whole layer-189 is obscured. The corresponding decrypted information is shown in Figure 12d–f, and the primary information of the original image can be identified well.

As shown in Figure 12g, the middle half of the layer-1, layer-100 and layer-189 are obscured; in Figure 12h, the upper half of the three layers are obscured; in Figure 12i, the whole of the three layers are obscured. The corresponding decrypted images are shown in Figure 12j–l, and the main information can be identified from the image.

The experimental results show that the occlusion attack has a poor effect on the cryptographic system.



(**a**) occluded part 180 × 180 in layer-1 (**b**) occluded part 125 × 256 in layer-100 (**c**) occluded the whole layer-189

(**d**) decrypted image of (**a**) (**e**) decrypted image of (**b**) (**f**) decrypted image of (**c**)

(**g**) occluded part 180 × 180 in layer-1, layer-100, layer-189 (**h**) occluded part 125 × 256 in layer-1, layer-100, layer-189 (**i**) occluded the whole layer-1, layer-100, layer-189

(**j**) decrypted image of (**g**) (**k**) decrypted image of (**h**) (**l**) decrypted image of (**i**)

Figure 12. The test of occlusion attack: (**a**–**c**) the occluded cipher text of layer-1, layer-100 and layer-189 respectively; and (**d**–**f**) corresponding decrypted image; (**g**–**i**) the occluded cipher text of the three layers; and (**j**–**l**) corresponding decrypted image.

3.5. Test Resistance to the Known and Chosen Plaintext Attack

Among the existing attack schemes which are used to verify the security of cryptosystem, the most widely used and effective schemes are the known plaintext attack and the chosen plaintext attack. Firstly, a model for encryption is expressed as follows [19,50]:

$$\mathrm{E}(x,y) = GN^{\alpha}\{\exp[i\cdot\xi_1(x,y)]\times IM(x,y)\}\exp[i\cdot\xi_2(x',y')] \tag{15}$$

where the symbol GN^{α} represents that the Gyrator transform is performed with rotation angle α. The two random phase masks are indicated by functions $\xi_1(x,y)$ and $\xi_2(x',y')$. In this paper, the function $E(x,y)$ is used to represent the components of the ciphertexts.

Accordingly, the iterative phase retrieval algorithm and the impulse function can be used as the known plaintext attack and chosen plaintext attack, respectively.

Here, the new layer-100 and layer-120 of 'sandiegou' having $256\times256\times60$ pixels are displayed in Figure 13a,b, which are encrypted by using the proposed cryptosystem. Figure 13c,d represents the results of encryption. As shown in Figure 13a, to perform the attack experiment, the original color image and its encrypted data are assumed to have been stolen by the attacker. Then, in simulation, the attacker tries their best to obtain the decrypted data of the layer-120 of 'sandiegou'. In the known plaintext attack, the phase retrieval algorithm is performed 500 times. The attack results are shown in Figure 13e,f, from which it can be seen that the recovery results are in random mode.

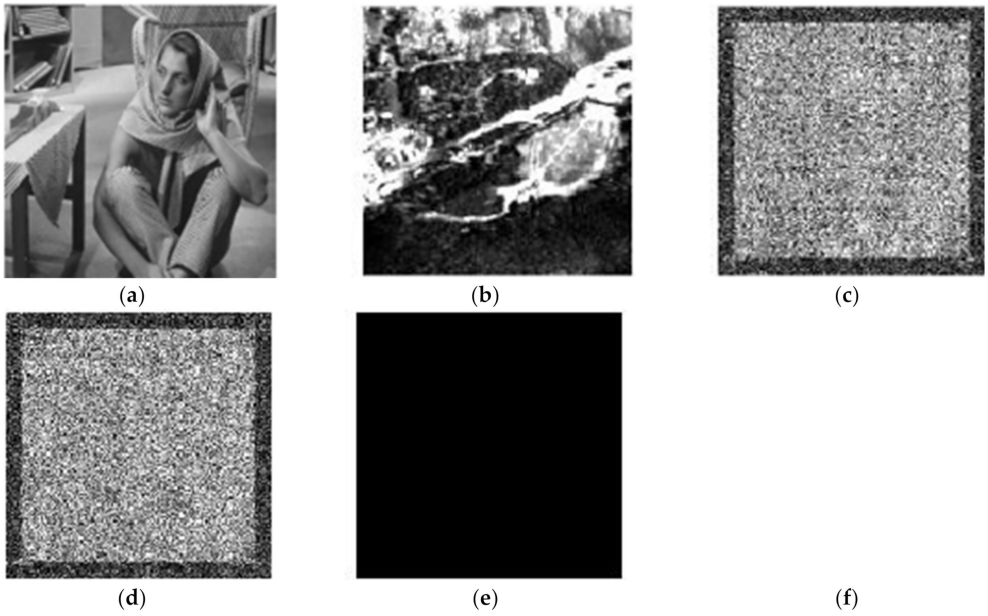


Figure 13. The test of known plaintext attack and chosen plaintext: (**a**) the secret image; (**b**) the secret image; (**c**) the encrypted data of (**a**); (**d**) the encrypted data of (**b**); (**e**) the result of known plaintext attack; and (**f**) the result of chosen plaintext attack.

3.6. Test Validity of the Image Signature

The function of the signature is to confirm the identity of the sender party, and in the absence of a signature, the secret information cannot be decrypted. Next, the decryption algorithm is performed with a correct signature and a fake signature, as shown in Figure 14. If the attacker uses a fake signature or other data as the signature, he will not obtain the right original information, just as shown in Figure 14b–f. It can only be completely decrypted only if the signature of 'Lena' is used for the decryption. The sender can also be identified as 'Lena'. So, the validity of the signature algorithm is well provided.

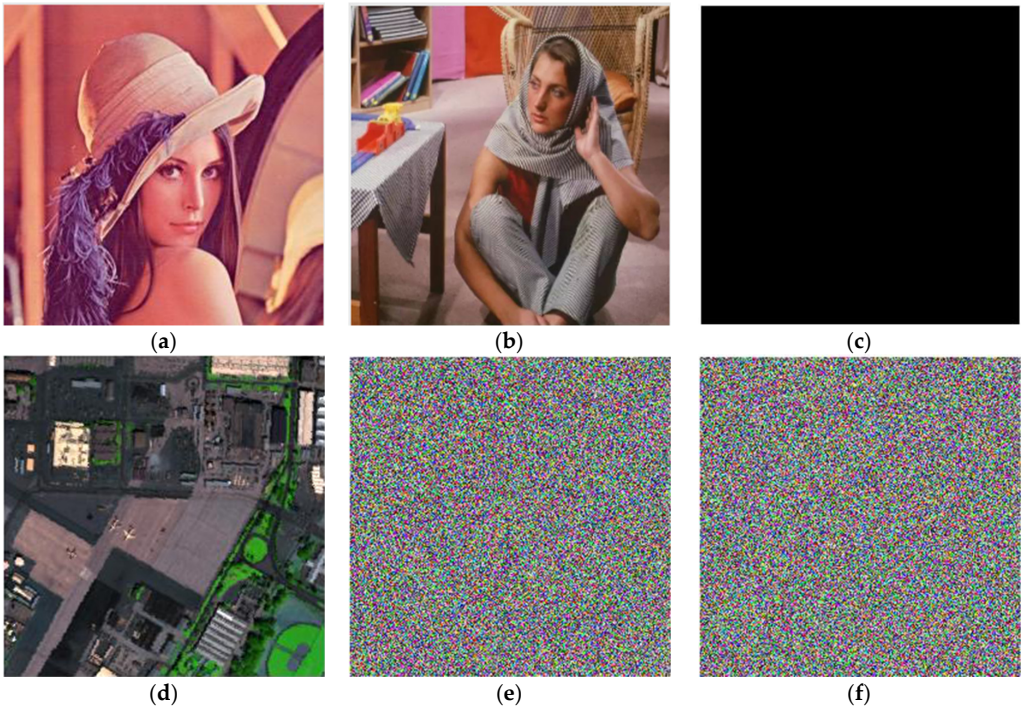


Figure 14. (**a**) image signature of 'Lena'; (**b**) image signature of 'Barbara'; (**c**) image signature of all zero; (**d**–**f**) the corresponding encrypted data.

3.7. Test Validity of the Image Integrity Authentication

After obtaining the signature and the key, the attacker can obtain the original text. Then the attacker can tamper with the original text and use the same encryption techniques to obtain the ciphertext and send it to the recipient. The integrity authentication algorithm can prevent the tampering attacks by checking whether the original message has been tampered with. The receiver performs the image integrity authentication algorithm to obtain $N + 1$ layers, and compares the calculated $(N + 1)$th layer with the $(N + 1)$th layer in the ciphertext to calculate the SSIM value. As shown in Table 3, this algorithm is very sensitive to tampering, even if one pixel value is changed, the SSIM value greatly changes. The SSIM value decreases to below 0.08 when nine elements are changed. It shows that the algorithm can effectively resist a tamper attack.

Table 3. The results with different numbers of pixels changed.

x	y	h	$Pixels'Number-Changed$	$SSIM-Authentication$
0	0	0	0	1
75:75	75:75	99	1	0.5835
75:76	75:76	99	4	0.5276
75:77	75:77	99	9	0.0585
100:100	100:100	99	1	0.5934
100:101	100:101	99	4	0.1045
100:102	100:102	99	9	0.0706
75:75	75:75	189	1	0.5508
75:76	75:76	189	4	0.0764
75:77	75:77	189	9	0.0495
100:100	100:100	189	1	0.5680
100:101	100:101	189	4	0.0854
100:102	100:102	189	9	0.0719

4. Conclusions

In summary, an optical hyperspectral image cryptosystem is proposed, using a triangular association encryption algorithm model with signature and authentication in Gyrator domains (TASA). The number of the hyperspectral bands is not unique, and the proposed cryptographic system can be implemented in different multi-band images. The block mobile method makes the 3D Arnold more suitable for hyperspectral images with a different number of bands, and increases the difficulty of deciphering the images. The triangular association encryption algorithm model makes diffusion expand from within the band to within and between the bands, avoiding the repeated operation of a single encryption algorithm on different bands. The image signature not only provides a large number of additional keys, but also enables the receiver to verify the identity of the originator. Moreover, the image integrity authentication enables the receiver to verify the integrity of the received message. By using numerical simulation, including various potential attack experiments, the optical hyperspectral image cryptosystem is proved to have the characteristics of effectiveness, security and robustness, and the functions of image signature and image integrity authentication.

Author Contributions: Formal analysis, Z.Y., Y.C., S.L., Z.L. and H.C.; Funding acquisition, Z.L. and H.C.; Investigation, C.T., W.B., Z.L. and H.C.; Writing—original draft, Z.Y. and H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant 62005320, 61975044 and 12074094).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets generated and/or analyzed during the current study are available from the corresponding author on reasonable request.

Acknowledgments: The authors are indebted to the two anonymous reviewers for their professional comments to improve the manuscript.

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

References

1. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
2. Ye, H.S.; Zhou, N.R.; Gong, L.H. Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion. *Signal Process.* **2020**, *175*, 107652. [CrossRef]
3. Alfalou, A.; Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photon.* **2009**, *1*, 589–636. [CrossRef]
4. Liu, S.; Guo, C.; Sheridan, J.T. A review of optical image encryption techniques. *Opt. Laser Technol.* **2014**, *57*, 327–342. [CrossRef]
5. Chen, H.; Liu, Z.; Tanougast, C.; Liu, F.; Blondel, W. A novel chaos based optical cryptosystem for multiple images using DNA-blend and gyrator transform. *Opt. Lasers Eng.* **2021**, *138*, 106448. [CrossRef]
6. Zhou, J.; Zhou, N.; Gong, L. Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix. *Opt. Laser Technol.* **2020**, *131*, 106437. [CrossRef]
7. Rakheja, P.; Singh, P.; Vig, R.; Kumar, R. Double image encryption scheme for iris template protection using 3D Lorenz system and modified equal modulus decomposition in hybrid transform domain. *J. Mod. Opt.* **2020**, *67*, 592–605. [CrossRef]
8. Qu, G.; Meng, X.; Yin, Y.; Wu, H.; Yang, X.; Peng, X.; He, W. Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation. *Opt. Lasers Eng.* **2021**, *137*, 106392. [CrossRef]
9. Yang, X.; Wu, H.; Yin, Y.; Meng, X.; Peng, X. Multiple-image encryption base on compressed coded aperture imaging. *Opt. Lasers Eng.* **2020**, *127*, 105976.
10. Duan, C.F.; Zhou, J.; Gong, L.; Wu, J.; Zhou, N. New color image encryption scheme based on multi-parameter fractional discrete Tchebyshev moments and nonlinear fractal permutation method. *Opt. Lasers Eng.* **2022**, *150*, 106881. [CrossRef]
11. Liu, Z.; Xu, L.; Lin, C.; Dai, J.; Liu, S. Image encryption scheme by using iterative random phase encoding in gyrator transform domains. *Opt. Lasers Eng.* **2011**, *49*, 542–546. [CrossRef]
12. Li, H.; Bai, X.; Shan, M.; Zhong, Z.; Liu, L.; Liu, B. Optical encryption of hyperspectral images using improved binary tree structure and phase-truncated discrete multiple-parameter fractional Fourier transform. *J. Opt.* **2020**, *22*, 055701. [CrossRef]

13. Chen, H.; Liu, Z.; Tanougast, C.; Blondel, W. Optical cryptosystem scheme for hyperspectral image based on random spiral transform in gyrator domains. *Opt. Lasers Eng.* **2021**, *137*, 106375. [CrossRef]
14. Situ, G.; Zhang, J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586. [CrossRef]
15. Abuturab, R.M. Color image security system using double random-structured phase encoding in gyrator transform domain. *Appl. Opt.* **2012**, *51*, 3006. [CrossRef]
16. Liu, Z.; Li, S.; Liu, W.; Liu, W.; Liu, S. Image hiding scheme by use of rotating squared sub-image in the gyrator transform domains. *Opt. Laser Technol.* **2013**, *45*, 198–203. [CrossRef]
17. He, W.; Meng, X.; Peng, X. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm: Comment. *Opt. Lett.* **2013**, *38*, 4044. [CrossRef]
18. Liu, Z.; Zhang, Y.; Li, S.; Liu, W.; Liu, W.; Wang, Y.; Liu, S. Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains. *Opt. Laser Technol.* **2013**, *47*, 152–158. [CrossRef]
19. Peng, X.; Zhang, P.; Wei, H.; Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **2006**, *31*, 1044–1046. [CrossRef]
20. Qin, W.; Peng, X.; Meng, X.; He, W. Improved Known-Plaintext Attack on Optical Encryption Based on Double Random Phase Encoding. In Proceedings of the 2010 Symposium on Photonics and Optoelectronics, Chengdu, China, 19–21 June 2010; pp. 1–4.
21. Situ, G.; Zhang, J. Multiple-image encryption by wavelength multiplexing. *Opt. Lett.* **2005**, *30*, 1306–1308. [CrossRef]
22. Situ, G.; Zhang, J. Position multiplexing for multiple-image encryption. *J. Opt. A Pure Appl. Opt.* **2006**, *8*, 391. [CrossRef]
23. Alfalou, A.; Brosseau, C.; Abdallah, N.; Jridi, M. Simultaneous fusion, compression, and encryption of multiple images. *Opt. Express* **2011**, *19*, 24023–24029. [CrossRef]
24. Shi, Y.; Situ, G.; Zhang, J. Multiple-image hiding by information prechoosing. *Opt. Lett.* **2008**, *33*, 542–544. [CrossRef]
25. He, W.; Peng, X.; Meng, X. Optical multiple-image hiding based on interference and grating modulation. *J. Opt.* **2012**, *14*, 565–570. [CrossRef]
26. Shi, Y.; Situ, G.; Zhang, J. Multiple-image hiding in the Fresnel domain. *Opt. Lett.* **2007**, *32*, 1914–1916. [CrossRef]
27. Zhu, C. A novel image encryption scheme based on improved hyperchaotic sequences. *Opt. Commun.* **2012**, *285*, 29–37. [CrossRef]
28. Chen, H.; Tanougast, C.; Liu, Z.; Blondel, W.; Hao, B. Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform. *Opt. Lasers Eng.* **2018**, *107*, 62–70. [CrossRef]
29. Chen, H.; Xiao, P.; Liu, Z. Optical spectrum encryption in associated fractional Fourier transform and gyrator transform domain. *Opt. Quantum Electron.* **2016**, *48*, 1–16. [CrossRef]
30. Ozkaynak, F.; Ahmet, B.; Yavuz, S. Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences. *Opt. Commun.* **2012**, *285*, 4946–4948. [CrossRef]
31. Huang, Z.W.; Zhou, N.R. Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion. *Opt. Laser Technol.* **2022**, *149*, 107879. [CrossRef]
32. Ye, G.; Jiao, K.; Pan, C.; Huang, X. An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map. *Secur. Commun. Netw.* **2018**, *21*, 8402578. [CrossRef]
33. Ye, G.D.; Wu, H.S.; Liu, M.; Shi, Y. Image encryption scheme based on blind signature and an improved Lorenz system. *Expert Syst. Appl.* **2022**, *205*, 117709. [CrossRef]
34. Kurunandan, J.; Aravind, A.; Prabhakar, K. Medical Image Encryption Scheme Using Multiple Chaotic Maps. *Pattern Recognit. Lett.* **2021**, *152*, 356–364.
35. Yang, Z.L.; Cao, Y.H.; Ji, Y.; Liu, Z.; Chen, H. Securing color image by using bit-level modified integer nonlinear coupled chaos model in Fresnel diffraction domains. *Opt. Lasers Eng.* **2022**, *152*, 106969. [CrossRef]
36. Dyson, F.J.; Falk, H. Period of a discrete cat mapping. *Am. Math. Mon.* **1992**, *99*, 603–614. [CrossRef]
37. Deng, X.; Zhao, D. Color component 3D Arnold transform for polychromatic pattern recognition. *Opt. Commun.* **2011**, *284*, 5623–5629. [CrossRef]
38. Zhang, X.; Wen, S.; Li, H. A Chaotic Particle Swarm Optimization Algorithm Based on Tent Mapping. *J. Taiyuan Univ. Sci. Technol.* **2011**, *19*, 2108–2112.
39. Rodrigo, J.A.; Alieva, T.; Calvo, M.L. Gyrator transform: Properties and applications. *Opt. Express* **2007**, *15*, 2190–2203. [CrossRef]
40. Hore, A.; Ziou, D. Image Quality Metrics: PSNR vs. SSIM. In Proceedings of the 20th International Conference on Pattern Recognition, ICPR 2010, Istanbul, Turkey, 23–26 August 2010; IEEE Computer Society: Washington, DC, USA, 2010.
41. Li, Y.; Zhang, R.; Ge, J.; Sun, Z. Periods of the 3-Arnold Transformation and Its Application in Image Encryption. *J. Univ. Electron. Sci. Technol. China* **2015**, *44*, 6.
42. Ljupco, K.; Shiguo, L. (Eds.) *Chaos-Based Cryptography: Theory, Algorithms and Applications*; Springer: Berlin/Heidelberg, Germany, 2011.
43. Patro, K.; Acharya, B. Secure multi-level permutation operation based multiple colour image encryption. *J. Inf. Secur. Appl.* **2018**, *40*, 111–133. [CrossRef]
44. Kulsoom, A.; Xiao, D.; Aqeel, R. efficient and noise re- sistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. *Media Tools Appl.* **2016**, *75*, 1–23. [CrossRef]
45. Kerckhoffs, A. La cryptographie militaire. *J. Sci. Mil.* **1883**, *9*, 5–38.
46. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solut. Fractals* **2004**, *21*, 749–761. [CrossRef]

47. Zhu, C.; Chen, Z.; Ouyang, W. A new image encryption algorithm based on general Chen's chaotic system. *J. Cent. South Univ. Sci. Technol.* **2006**, *37*, 1142–1148.
48. Akhshani, A.; Akhavan, A.; Lim, S.-C.; Hassan, Z. An image encryption scheme based on quantum logistic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 4653–4661. [CrossRef]
49. Loubaton, P.; Vallet, P. Almost sure localization of the eigenvalues in a gaussian information plus noise model. Applications to the spiked models. *Electron. J. Probab.* **2011**, *16*, 1934–1959. [CrossRef]
50. Peng, X.; Wei, H.; Zhang, P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Opt. Lett.* **2006**, *31*, 3261–3263. [CrossRef]