symmetry

Article

3D Copyright Protection Based on Binarized Computational Ghost Imaging Encryption and Cellular Automata Transform

Meng Wang [1], Mengli Chen [1], Jianzhong Li [2] and Chuying Yu [3,*]

[1] School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China; wangmeng3@stu.scu.edu.cn (M.W.); chenmengli20212021@163.com (M.C.)
[2] School of Computer and Information Engineering, Hanshan Normal University, Chaozhou 521041, China; lizj@hstc.edu.cn
[3] School of Physics and Electronic Engineering, Hanshan Normal University, Chaozhou 521041, China
* Correspondence: chyyu@hstc.edu.cn

Abstract: In this paper, a watermark embedding scheme based on ghost image encryption and cellular automata transformation is proposed. In this scheme, the watermark forms speckle through different light intensities into a key, and the cellular automata transformation algorithm is embedded into the 3D image. Compared with the traditional watermarking encryption method, this scheme combines ghost imaging and the cellular automata transformation algorithm, which double guarantees and increases the confidentiality of the watermark. The binary computing ghost imaging discussed in this paper saves the storage space of password text and makes the transmission of password text more convenient and faster. Experiments on this method also verify that the watermark-embedded image has higher imperceptibility and higher robustness against attacks, and that the extracted watermark has good integrity.

Keywords: ghost imaging encryption; cellular automata transform; 3D image security; watermark embedding and extraction

Citation: Wang, M.; Chen, M.; Li, J.; Yu, C. 3D Copyright Protection Based on Binarized Computational Ghost Imaging Encryption and Cellular Automata Transform. *Symmetry* **2022**, *14*, 595. https://doi.org/10.3390/sym14030595

Academic Editor: Gianluca Vinti

Received: 27 January 2022
Accepted: 11 March 2022
Published: 17 March 2022

1. Introduction

With the rapid development of information technology, image encryption techniques have gained a high level of interest. In recent years, images have been maliciously modified or destroyed by criminals, which not only loses the original value of the image, but also may cause copyright disputes. Therefore, copyright protection for images is of great significance. Digital watermark is a kind of copyright protection technology [1], whose basic idea is to embed the copyright watermark logo in the carrier image by an embedding algorithm. When a copyright dispute occurs, the copyright holder can extract the copyright logo by watermark extraction algorithm, and then compare it with the registered watermark image in the copyright protection center to complete the copyright authentication process.

Compared with traditional 2D images, 3D images have attracted more and more attention because of their stereoscopic nature, excellent experience and ability to truly reproduce life scenes. Integral imaging (InI) is a practical light-field [2] three-dimensional imaging method; it originated from the integral photography(IP) [3] proposed by Lippmann in 1908 and has become one of the cutting-edge 3D display methods in the international arena. InI uses a microlens array (MLA) to capture a set of element images (EIs) [4]. Each element image shows an incoherent illuminated 3D scene of different perspectives. The InI system can obtain the direction and spatial information of the light ray from the scene [5] and project this information on a 2D display to produce a 3D image visible to the naked eye without any special glasses. There have been many research results on copyright protection of 2D images, and its watermarking algorithms can be implemented either by spatial domain algorithms or by frequency domain algorithms [6,7]. In 2008, a digital museum copyright protection method based on the discrete wavelet transform (DWT) was proposed in [8], where the Fresnel hologram of the watermarked image is embedded in the protected object by the discrete wavelet transform (DWT). After watermark detection, the copyright information appears in the reconstructed hologram. In [9], the authors proposed discrete cosine transform (DCT) as a method for embedding watermarks with high accuracy in extracting watermarks, and it is less affected by image compression. In [10], the authors proposed a cellular automata (CA)-based watermarking method for copyright protection of 2D images with better results than the traditional transform methods (DWT, DFT, etc.)-based watermarking techniques. In 2019, Li and Wang [11] proposed using a 3D CA filter to embed 3D watermark-converted data (QR codes) into cellular automata (CA) domains instead of 2D watermarks. This approach protects the copyright of holographic videos from malicious copying and is robust to noise and compression attacks. In 2020, Valandar et al. [12] proposed a robust watermarking scheme using different transformations (i.e., DWT, IWT and CT) and segmentation by block. In the embedding process, the image is segmented into uniform blocks and the blocks are transformed. Finally, the watermarked bits are embedded using the LL band. The method achieves significant invisibility results, but the robustness to various signal processing attacks needs to be improved. In 2021, Li and Ren [13] proposed a method for protecting the ownership of light-field images based on high-dimensional color transform (HDCT) watermarking, which outperformed existing light-field watermarking algorithms in terms of both imperceptibility and robustness. Mohamed Hamidi [14] proposed a robust hybrid watermarking method based on discrete cosine transform (DCT), discrete wavelet transform (DWT) and scale invariant feature transform (SIFT). SIFT is used to protect the watermark from geometric attacks while the watermark is embedded in the DWT-DCT domain to resist image processing operations. Medical images contain a lot of patient information and have a high demand for privacy. In [15], Wu et al. proposed a robust medical image watermarking algorithm based on contourlet transform and DCT, using contourlet transform to extract multi-scale texture information and DCT to extract feature vectors in low-frequency directional subbands. In the area of industrial image copyright protection [16], Asra Kamili et al. [17] proposed 'DWFCAT', a dual watermarking framework for industrial image content authentication using discrete cosine transform coefficients and exploiting their energy compression properties to achieve robust watermark embedding. At present, the research results of copyright protection for 3D images are relatively few. With the rapid development of 3D display technology based on integrated imaging [18], 3D images are increasingly being transmitted and used, and if these 3D images are not effectively protected, they can easily be illegally stolen without permission and cause losses. Therefore, the research on the copyright protection technology of 3D images is very necessary.

Watermarking technology has become a hot research topic in the field of optical information security as a method to effectively protect the copyright of images and video works [19,20]. Since some watermarking techniques do not take encryption measures or have simple encryption methods, unauthorized persons can easily detect or extract the embedded digital watermark and tamper with it through some computational operations, thus affecting the security of the watermark. Therefore, encryption pre-processing of watermarked images before watermark embedding has an important role. Existing encryption methods can be divided into two categories: symmetric and asymmetric encryption. It involves a secret key, or a symmetric key, used at the encryption and decryption sides, as in [21]. In symmetric encryption, the secret key used for encryption and decryption is the same. The process of encrypting and decrypting a message in asymmetric encryption requires the use of a set of key pairs, called a public key and a private key. If the public key is used to encrypt a message, only the private key can be used to decrypt it, and if the private key is used to encrypt it, only the public key can be used to decrypt it. The public key is required to be made public to others, and the private key must be kept by the user and kept secret. Symmetric encryption and decryption is faster, while asymmetric encryption and decryption takes longer and is relatively slower. The encryption method based on optical 4f system double random phase coding [22] is a classical optical encryption method, but it encrypts the real plaintext image as a complex-valued image, and it brings inconvenience to the transmission of the ciphertext. Computational ghost imaging encryption, which has emerged in recent years, has attracted the research interest of many scientists because of its small ciphertext data size, simple experimental setup and good encryption effect. Clemente et al. proposed optical encryption based on computational ghost imaging [23], which encodes the information of an object as a light intensity value. Duran et al. combined computational ghost imaging (CGI) with compressed sampling (CS) [24]. Zhang, Leihong et al. proposed an optical encryption method based on double random phase encoding compressed ghost imaging [25], which further improved the effect of ghost imaging encryption.

In this paper, we propose a copyright protection method for 3D light-field images based on binarized computational ghost imaging encryption and cellular automata transform watermarking algorithms. First, we generate an elemental image array (EIA) of hexagonal lens arrays from three-dimensional (3D) objects, which has a higher fill factor compared with the rectangular lens array case, and thus the hexagonal lens arrays are more effective. Secondly, we extract the carrier image from EIA and encrypt the watermarked image by ghost imaging system and binarize the encrypted data. Compared with the traditional optical encryption method, computational ghost imaging encryption is more suitable to be used because of its small amount of ciphertext data, simple experimental setup and good encryption effect. We embed the encrypted watermarked image into the carrier image by cellular automata transformation (CAT) and test the imperceptibility of the embedded watermarked image with peak signal-to-noise ratio (PSNR). The watermark is extracted using the inverse transform of the cellular automaton, which extracts the encrypted image. We associate the extracted image to be decrypted with the scattered field intensity in all iterations one by one and add up each consecutive frame with a suitable weight factor to reproduce the initially embedded watermarked image. The simulation results indicate that the embedded information has good imperceptibility when the PSNR of the embedded watermark reaches above 38 dB [26], the quality of the reproduced image is good and it can resist attacks such as noise, filtering and compression, which demonstrates robustness. The results show that it is a general method for copyright protection of 3D light-field images.

The main contributions of this scheme to the copyright protection of images are as follows:

1. Ghost imaging optical encryption generates ciphertext through different light intensities. By controlling the initial phase, it saves key space and improves the security performance of the system.
2. Ghost imaging generates a key through different light intensities, and the speckle is embedded into the original image through meta-cellular automata watermark. The embedding effect of the speckle key is better than that of traditional watermark embedding.
3. Ghost image encryption embeds the original image through the speckle key. The extracted speckle still has irregular light intensity distribution. Without the key, the correct watermark cannot be restored, which strengthens the security of the system.
4. The key is embedded into the original image through meta-cellular automata, and the algorithm has strong confidentiality. In extracting the watermark, the same sort as that in embedding should be used, otherwise it will be extracted incorrectly, which makes the encryption of the scheme have a double guarantee.

2. Theoretical Analysis

2.1. Image Encryption Based on Binarized Computational Ghost Imaging (BCGI)

To secure watermark information, the watermark image is encrypted before embedding. In this paper, we adopt the image encryption method based on binarized computational ghost imaging (BCGI). Compared with other traditional optical encryption methods, BCGI encrypts the image into an intensity vector instead of a complex-valued matrix, which reduces the storage space of the ciphertext and also brings convenience to the subsequent processing and transmission of the ciphertext, while the binarization of the ciphertext makes it easier to hide.

The schematic diagram of computational ghost imaging is shown in Figure 1. Random scatter patterns are generated by computational devices such as spatial light modulators, digital micromirror devices, or projectors [27,28], and different scatter patterns are converted into different light spots to interact with the target object under the irradiation of a stable laser light source. This beam, which carries information about the object, is called the signal beam, and it is detected by single-pixel camera. The other beam, which contains only the computer-generated scatter pattern information and does not contain object information, is called the reference beam. We correspond the signal beam and the reference beam one by one and calculate them using the correlation algorithm, which can reconstruct the pattern of the target object. The process can be expressed as follow,

$$C_r = \iint I_r(x,y)m(x,y)dxdy \tag{1}$$

where $\{C_r\}$ is the data detected by a single pixel camera, $m(x,y)$ is the distribution function of the target object and $I_r(x,y)$ is the intensity of light projected onto an object after the beam has been modulated by a random scatter pattern.

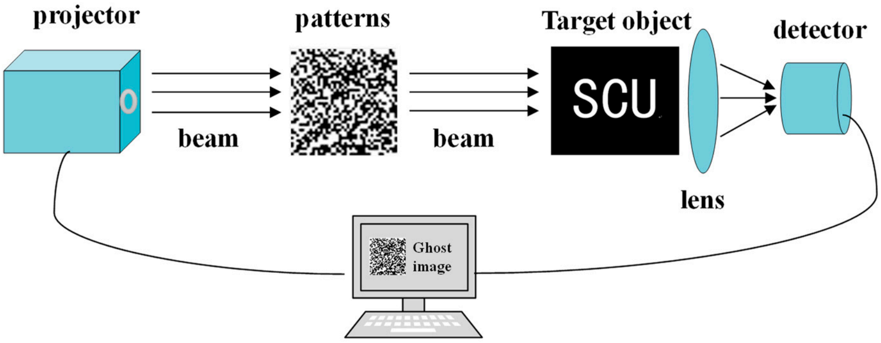


Figure 1. The schematic diagram of computational ghost imaging.

In the image encryption scheme based on binarized computational ghost imaging, we use the watermarked image as the target object, the random scatter pattern $\{\delta_i(x,y)\}$ $i = 1,2,\ldots,N$ generated by the spatial light modulator as the encryption key, where N is the maximum number of random scatters generated and the light intensity data detected by single-pixel camera as the ciphertext.

In the decryption process, after the ciphertext watermark is extracted and associated with speckle one by one, the watermark pattern can be solved completely. The encryption process is shown in Figure 2. Since the secret key used for encryption and decryption is the same, the ghost imaging encryption in this paper is a symmetric encryption. The computational ghost imaging-based image encryption system has a fast parallel data processing capability unique to optical systems [29], which encrypts the image into an intensity vector rather than a complex-valued matrix, reducing the storage space for the ciphertext. To facilitate concealment, the ciphertext $\{C_r\}$ is binarized as follows,

$$D_r = \left\{ \begin{array}{cc} 1 & C_r > V \\ 0 & C_r \leq V \end{array} \right\} \tag{2}$$

where $V = [max(C) + min(C)]/2$ is the critical value, $max(C)$ is the maximum of $\{C_r\}$ and $min(C)$ is the minimum of $\{C_r\}$. In the decryption process, we associate the binarized ciphertext $\{D_r\}$ with the light intensity $I_r(x,y)$ projected onto the object after the beam has been modulated with a random scattering pattern. The core operation of the association algorithm is formulated as follows,

$$T(x,y) = \frac{1}{N}\sum_{i=1}^{N}(D_r - \langle D\rangle)(I_r(x,y) - \langle I(x,y)\rangle) = \langle DI(x,y)\rangle - \langle D\rangle\langle I(x,y)\rangle \quad (3)$$

where $T(x,y)$ represents the decrypted image and $\langle D\rangle$ is the average value of D.

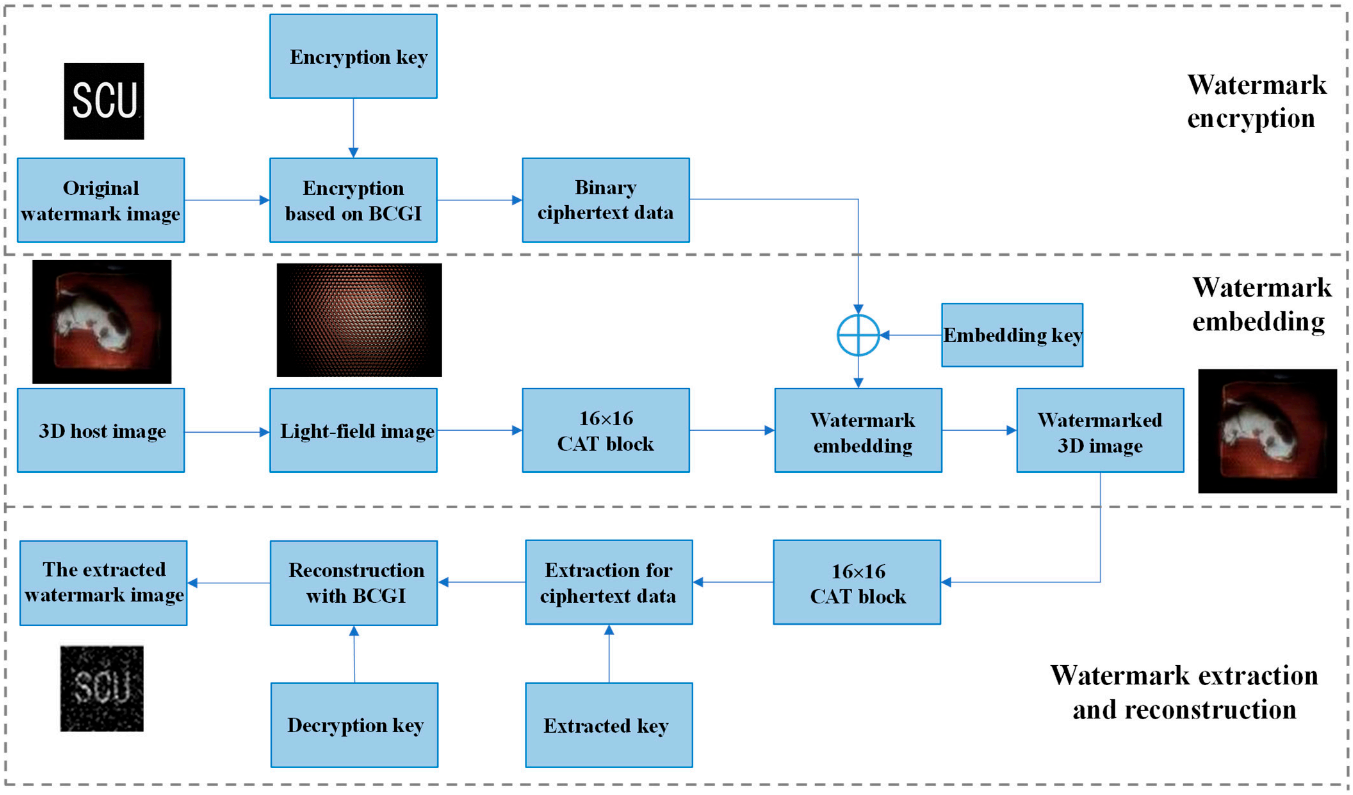


Figure 2. Flowchart of the watermarking method based on binarized computational ghost imaging.

The detail of encryption and decryption process [30–35] is as follows:

Step 1: The laser beam is transmitted via a spatial light modulator (SLM). The spatial light modulator contains a random phase matrix $\{\delta_i(x,y)\}$ $i = 1,2,\ldots,N$ and a spatially incoherent beam is generated after SLM. When we know the random phase and the incident light field $I(x,y)$, the intensity of the light field after SLM can be calculated as $I_i(x,y)$.

$$I_i(x,y) = I(x,y)e^{\delta_i(x,y)} \quad (4)$$

Step 2: After Fresnel diffraction, light transmits to the object plane. Assume that the distance between the object plane and the spatial modulator is z and the intensity of light projected onto the object after random phase modulation is $I_r(x,y)$.

$$I_r(x,y) = |I_i(x,y) \otimes h_z(x,y)|^2 \quad (5)$$

where $h_z(x,y)$ is the optical transfer function at distance z in the spatial domain and $\otimes$ represents the convolution operation.

Step 3: Data detected by single pixel cameras $\{C_r\}$ is as follows:

$$C_r = \iint I_r(x,y)m(x,y)dxdy \quad (6)$$

where $m(x,y)$ represents distribution function of the target object.

Step 4: To facilitate concealment, the ciphertext $\{C_r\}$ is binarized as follows:

$$D_r = \left\{ \begin{array}{ll} 1 & C_r > V \\ 0 & C_r \le V \end{array} \right\} \tag{7}$$

where $V = [max(C) + min(C)]/2$ is the critical value, $max(C)$ is the maximum of $\{C_r\}$ and $min(C)$ is the minimum of $\{C_r\}$.

Step 5: The purpose of the decryption process is to reconstruct the distribution function $m(x,y)$ of the target object. We associate the binarized $\{D_r\}$ with the light intensity $I_r(x,y)$ projected onto the object. The core arithmetic formula for correlation is as follows:

$$T(x,y) = \frac{1}{N}\sum_{i=1}^{N}(B_r - \langle B\rangle)(I_r(x,y) - \langle I(x,y)\rangle) = \langle BI(x,y)\rangle - \langle B\rangle\langle I(x,y)\rangle \tag{8}$$

where $T(x,y)$ is the distribution function of the object obtained after decryption and $\langle B\rangle$ is the average value of B.

2.2. Watermark Embedding and Extraction Based on Cellular Automata Transform (CAT)

2.2.1. Cellular Automata

Cellular automata is a dynamic model with discrete time, space and state. It is composed of cell units arranged according to certain rules. The state of each unit is synchronized with the cell state of the previous time and kept updated. The current moment is related to the evolution of cellular automata. The one-dimensional formula of CAT and the two-dimensional formula of CAT are defined as follows:

$$f = \sum_k c_k A_{ik_i} \tag{9}$$

$$\sum_{k=0}^{N-1}\sum_{k=0}^{N-1} c_u A_{ijkl} \tag{10}$$

Among *i*,*j*,*k*,*l* = 0,1,2, ... , $N-1$, f_i and f_{ij} represent one-dimensional and two-dimensional data sequences, respectively, A_{ik} and A_{ijkl} represent basis functions (also known as a transformation bases), c_k and c_{kl} represent the transformation coefficients. The above formula takes the basis function as the transfer function and the data sequence from the physical domain to map transformation coefficients in the CA domain. A_{ik} is called one dimension generated by one-dimensional CA; the basis function (*i*,*k* = 0,1, ... , $N-1$) of one-dimensional CA with N cells is a function of cell state (*i*,*t* = 0,1,2, ... , $N-1$), there are an infinite number of such function representations. Lafe lists the sub categories β Class ρ Seven orthogonal wiki functions of class and class R (type1~type7), the orthogonal basis can find the transformation system (*i*,*j*,*k*,*l* = 0,1, ... , $N-1$) in a recursive way, which is called bivariate, it can be generated by the evolution of a two-dimensional CA containing N ∗ N cells.

It can be seen that generating the basis function with CA is the prerequisite for cat. The construction of CA is realized by setting the parameters of the dynamic system according to its dynamic model. The typical system parameters of CA are different, the constructed CA is different, the basis functions generated by different CA are different and the CAT transformation coefficients obtained by different basis functions are different. Using the base key can generate a second wiki as shown in Figure 3. Lafe's research shows that CAT can produce thousands of orthogonal bases, semi orthogonal bases, biorthogonal bases and non-orthogonal bases with different properties, some of which have similar properties to the bases of known transforms (such as Walsh transform, wavelet transform, etc.). Some bases reflect the self-organization of data sets or functions, which are the rich and complex transformation properties of CA and cat. The main function of the transformation of cellular automata is to obtain a large number of basis functions with different properties.

The nature of the self-generating function shown by some basis functions is unmatched by other transformations.

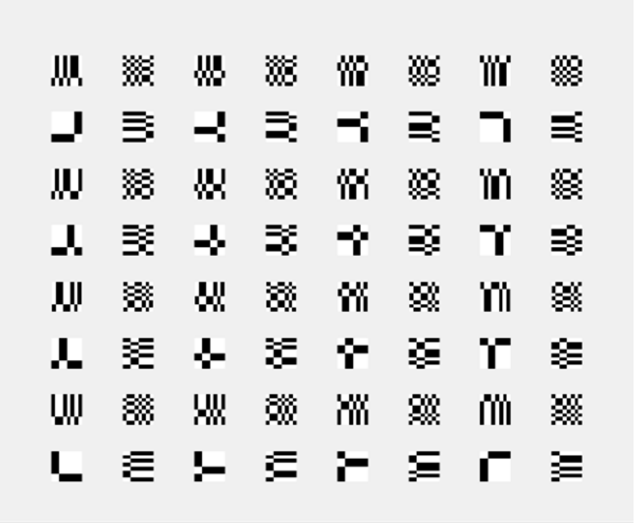


Figure 3. Two-dimensional CAT base function.

2.2.2. Cellular Automata Transform

Set the size of the given image to among

$$w = 2^n, h = 2^m \tag{11}$$

where m and n are positive integers. If the size of a given image does not satisfy Equation (11), it is processed by filling 0. According to the above assumptions, the original image is divided into B sub blocks, each of which is composed of 8 sub blocks × 8 = 64 pixels. Implement cellular automata change for each sub block (using type 8 bivariate function):

$$C_{kl} = \left(\sum_{i=0}^{7} \sum_{j=0}^{7} f_{ij} A_{ijkl} \right) \backslash 8(CAT) \tag{12}$$

$$f_{ij} = \left(\sum_{i=0}^{7} \sum_{j=0}^{7} C_{kl} A_{ijkl} \right) \backslash 8\,(ICAT) \tag{13}$$

Then, the transformation coefficient c_{kl} falls in four different subbands, and the coefficient (I) at the position where k and l are even numbers is the low-frequency part of the transformation coefficient of cellular automata. These coefficients are separated to form a new low-resolution image with size $2^{(m-1)}2^{(n-1)}$; the other coefficients (II: k is even, l is odd; III: k is odd, l is even and IV: k is odd, l is odd) are the high-frequency part of the transformation coefficients of cellular automata. The high-frequency part can provide the edge information of the image, and the low-resolution image formed by the low-frequency part can be further transformed by cellular automata and then divided into $2^{(m+n-2)}/64$ sub blocks.

2.2.3. Logistic Chaotic Mapping

Logistic map is a commonly used discrete chaotic map for generating pseudo-random sequences. The simplest one-dimensional logistic map is:

$$x_{n+1} = \mu x_n(1 - x_n),\ x_n \in (0, 1),\ \mu \in [3.5699456, 4] \tag{14}$$

x_n can be transformed into an integer chaotic sequence between [1, n] through a positive integer N, and different elements are taken out to obtain a non-repetitive positive integer chaotic sequence: $y_n \in [1, M]$, $m \leq n$. There is another form of logistic mapping:

$$x_{n+1} = 1 - \mu x_n^2,\ x_n \in (-1,1),\ \mu \in (0,2) \tag{15}$$

It can also be transformed into an integer chaotic sequence by the above method: $y_n \in [-T, T]$, where t is a positive integer. Logistic chaotic mapping is extremely sensitive to the initial value. Given two slightly different initial values, two completely different pseudo-random sequences are obtained after multiple iterations. Therefore, the initial value of the mapping can be used as the key to improve the security of the watermarking algorithm.

2.2.4. Watermark Embedding and Extraction

Divide the image into m non overlapping 16 × 16 according to the base key base. The key generates a two-dimensional foundation and two levels of CAT transformation are performed on each sub block. Calculate the mean value of high-rise low-frequency coefficient f_j = mean{f_i, 1 < i < 44}, a logistic mapping function in the form of Equation (15) with an initial value of X is transformed into a non-repeating positive integer chaotic sequence OPF = {opf_i | I opf_i ∈ [1, 16], $1 \leq i \leq 8$}, the OPF selects 8 coefficients from the high-level low-frequency coefficients. An initial configuration C = {c_h, $1 \leq h \leq 8$} is obtained by comparing with a_v one by one.

$$c_h = \begin{cases} 0 & f_{opt} > av \\ 1 & f_{opt} < av \end{cases} \tag{16}$$

Another logistic mapping function in the form of Equation (7) with an initial value of f_i is transformed into an integer chaotic sequence OPK = {opk | opk; ∈[−T, T], $1 \leq i \leq$ m | TI ≤ Lm/2jf~1}; each OPK determines a local rule number for the corresponding sub block: f = [($m/2j$) + f_i], which indicates rounding down. Taking C as seed and using local rules as the binary watermark, W = {w, $1 \leq i \leq 8 \times 8$} is generated by ECA evolution of f_j, Quantify the low-frequency coefficient f ($1 \leq J \leq 8 \times 8$) embedded in the lower layer. Calculate the quantization step f_j = βy; among β is the variance of the low-frequency subgraph at the lower level, y is the adjustment factor and f is quantized by an integer multiple of first. Then, the quantization value is adjusted according to the watermark bit. If w = 1, take the quantized value λ as the nearest odd number. If w = 0, take λ as the nearest even number. Finally, modify the coefficient F = λ × △ and perform the ICAT transformation with F to obtain the water bearing imprint block. After completing the watermark generation and embedding of all sub blocks, the watermarked image is obtained.

The watermarked image is divided into m 16 × 16, using the same base key. The key generates two layers of A_{ijkl}, and performs two-layer CAT transformation on each sub block. the initial configuration C′ is generated by selecting the high-level low-frequency coefficients with the non-repeating positive integer chaotic sequence OPF with the initial value of x_1. The local rule number f of the corresponding sub block is calculated from the integer chaotic sequence OPK with the initial value of x_2, the watermark W′ is evolved from the ECA with the local rule of f and the watermark WT is extracted from the low-frequency coefficient of the lower layer. The extraction method is as follows: the quantization step Δ′ is determined in the above process, pair coefficient quantizes the integer multiple of O′ and then extracts the watermark bit according to the quantized value; if quantized value λ′ is an odd number = 1 and if λ′ is even = 0.

Comparing the generated watermark W′ with the extracted watermark WT, a tamper detection matrix D is defined to reflect the difference between the two and the tamper location: D = w′ wt. If the value is between [0, 1], the greater the value, the greater the degree of image tampering. Otherwise, the smaller the degree of tampering. However, directly authenticating the image content with the above tamper detection matrix determines good faith processing such as JPEG compression as tampering with the image in order to better distinguish good faith processing of the image from the malicious tampering with the content.

3. Experiment Result and Discussion

3.1. Experiental Setup

In this experiment, we used a desktop 3D display device to verify the validity of the experimental method. The device mainly consists of three parts: an optical diffuser, a composite lens array and a liquid crystal display (LCD), as shown in Figure 4a. We generate elemental image arrays (EIA) of hexagonal lens arrays from three-dimensional (3D) objects, as shown in Figure 4b. Compared with rectangular lens arrays, hexagonal lens arrays have a higher fill factor and are better for use in desktop 3D displays. The size of the optical diffuser screen is 76,804,320, so we use 76,804,320 light-field images for the experiment.

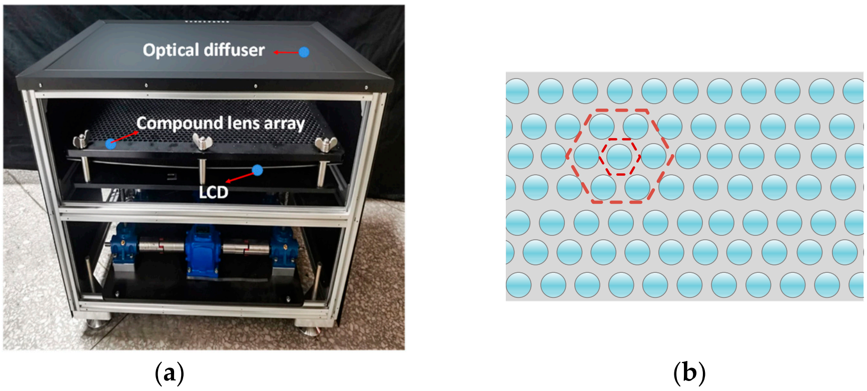


Figure 4. The structure of the 3D integrated display: (**a**) the desktop 3D integrated display device; (**b**) diagram of the hexagonal compound lens array.

3.2. Performance Analysis

We analyze the imperceptibility of the watermark after embedding the ghost imaging encrypted watermark into the carrier light-field image using the cellular automata transformation (CAT) algorithm. We evaluate the imperceptibility of the image from both subjective and objective aspects. First, in our experiments, we compare the 3D images before and after embedding the watermark displayed by the desktop 3D-integrated display from five viewpoints: top, middle, bottom, left and right, as shown in Figures 5 and 6.

Figures 5 and 6 show the 3D images before and after embedding the watermark; they are so similar that they cannot be distinguished with human eyes. Therefore, we evaluate the imperceptibility of the embedded watermark by calculating the peak signal to noise ratio (PSNR). PSNR is one of the most common and widely used metrics for the objective evaluation of images, however, it is based on the error between corresponding pixel points, with larger values indicating less distortion.

$$\mathrm{MSE} = \frac{1}{\mathrm{H} \times \mathrm{W}} \sum_{i=1}^{\mathrm{H}} \sum_{j=1}^{\mathrm{W}} (\mathrm{X}(i,j) - \mathrm{Y}(i,j))^{2} \tag{17}$$

$$\mathrm{PSNR} = 10 \log_{10}\left(\frac{(2^{n}-1)^{2}}{\mathrm{MSE}}\right) \tag{18}$$

The MSE is the mean square error (MSE) of the current image X and the reference image Y. H and W are the height and width of the image, respectively; n is the number of bits per pixel, generally taken as 8, which means the number of grey levels of the pixel is 256.

In our experiments, we calculate the PSNR values for several different methods separately at the embedding degree of 0.1. As shown in Table 1, when using the CAT embedding algorithm, the PSNR value reaches 40.12, indicating that the quality of the image after embedding the watermark is extremely good and very close to the original image. We have confirmed the validity of the watermark embedding algorithm through both subjective and objective aspects.

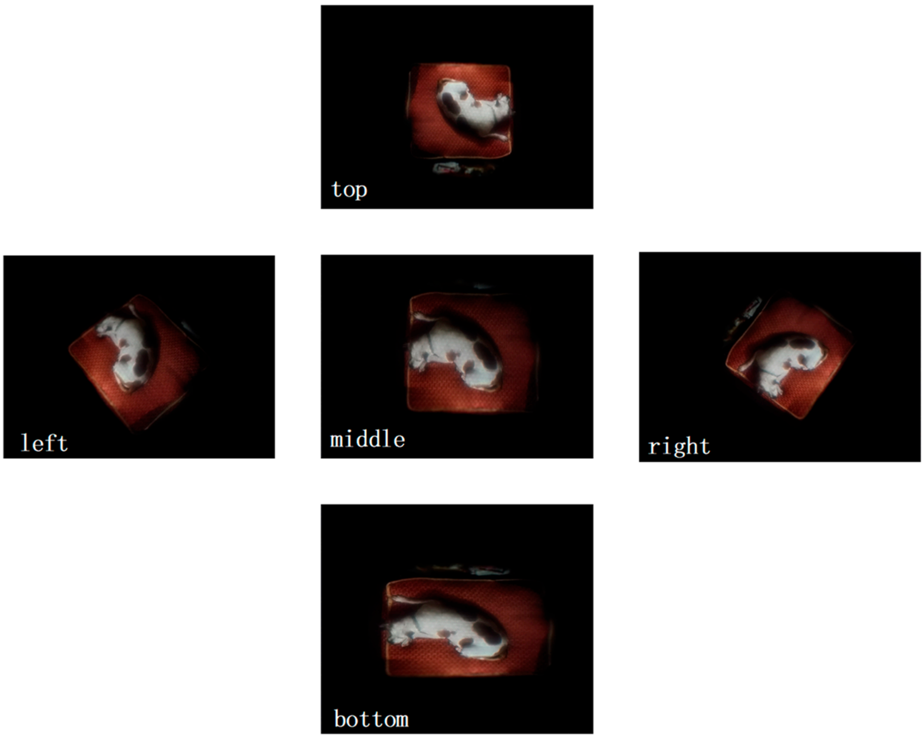


Figure 5. Different perspectives of the 3D scene 'dog' before the watermark is embedded.

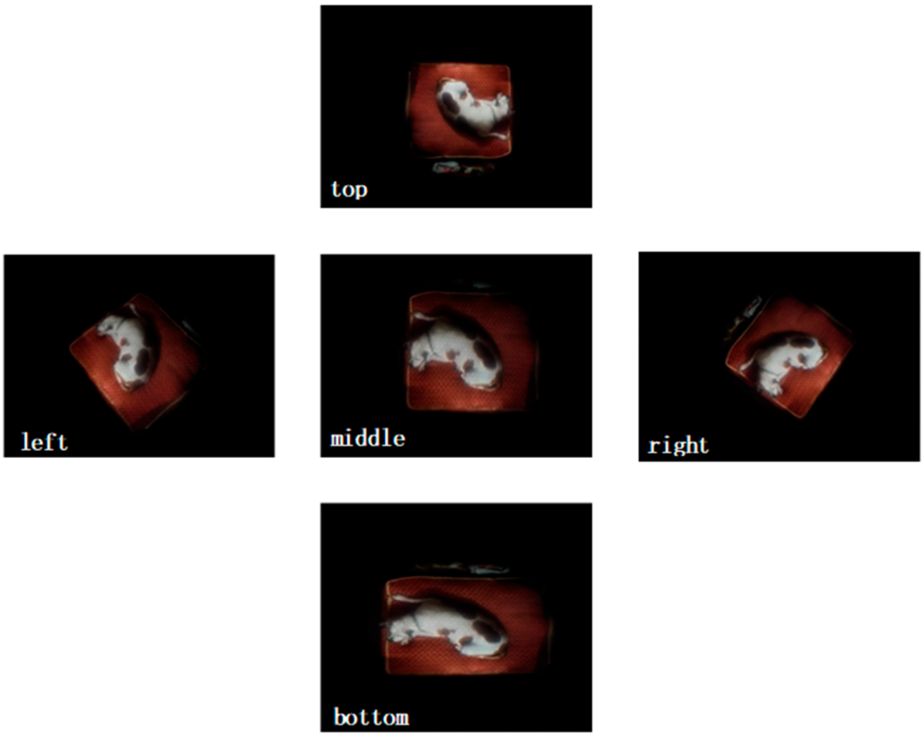


Figure 6. Different perspectives of the 3D scene 'dog' after the watermark is embedded.

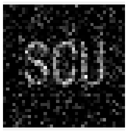
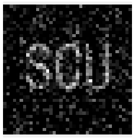
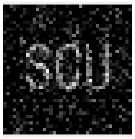
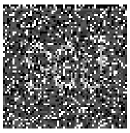
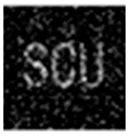
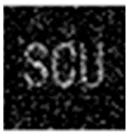
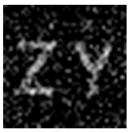
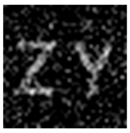
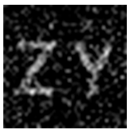
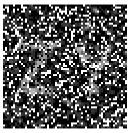
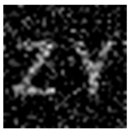
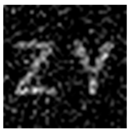
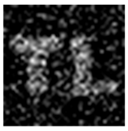
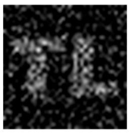
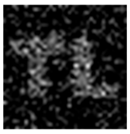
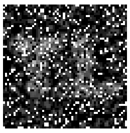
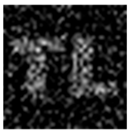
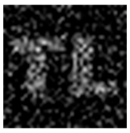
Table 1. Comparison of the imperceptibility of different watermark embedding methods.

Method	PSNR (dB)
Our method	40.12
Method [36]	35.63
Method [37]	36.09
Method [38]	35.04

Next, we experimentally verify that the watermarking algorithm used in this paper is robust to some attacks. A practical watermarking algorithm should be robust to signal processing, usual geometric distortions and malicious attacks. A highly robust watermarking algorithm should be able to embed and extract properly after attacks such as image compression and noise addition, and the extracted watermark results should be minimally affected. As shown in Figure 7, we verify the robustness of the watermarking algorithm by adding five attacks: Gaussian noise (v = 0.1), white noise, JPEG compression (QF50), Gaussian filtering and rotation by 10°.

As shown in Table 2, the above results show that the watermark can be extracted correctly and with good results for the case of added Gaussian noise and white noise. When the embedded carrier image is rotated, the extracted 2D watermark is distorted and corrupted by the noise.

Table 2. Watermark extraction result after adding attacks.

Attacks	No Attacks	Gaussian Noise (v = 0.1)	White Noise	Rotation by 10°	JPEG Compression	Gaussian Filtering
Extracted 'SCU' watermark						
Extracted 'ZY' watermark						
Extracted 'TL' watermark						

As we can see from the experimental results above, The cellular automata transform (CAT) algorithm has certain disadvantages, although it is more resistant to compression, filtering and noise attacks. The CAT watermarking method we use is a transform domain watermarking method; it is vulnerable to rotation attacks. The transformed domain method refers to some invertible mathematical transformation of the image followed by some modification of the coefficients of the transformed domain. We then perform an inverse transformation to obtain the image. Rotation attacks can disrupt synchronization so that watermark embedding and watermark detection position no longer match. The difficulty in combating this attack lies in the search for the original watermark reference point in the carrier data. Therefore, the rotation of only ten degrees destroys the embedded watermark.

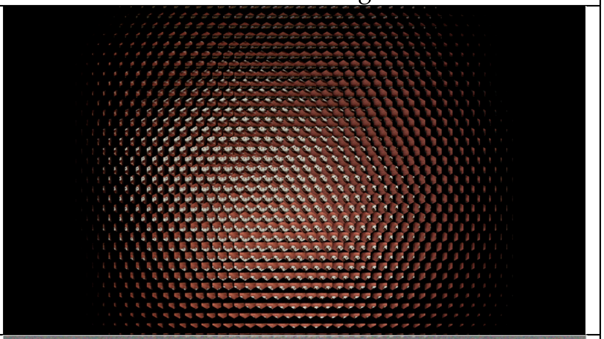
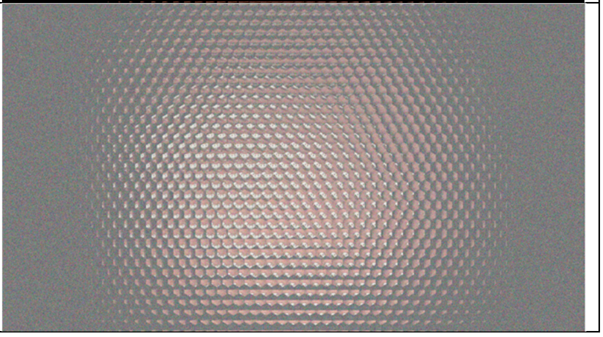
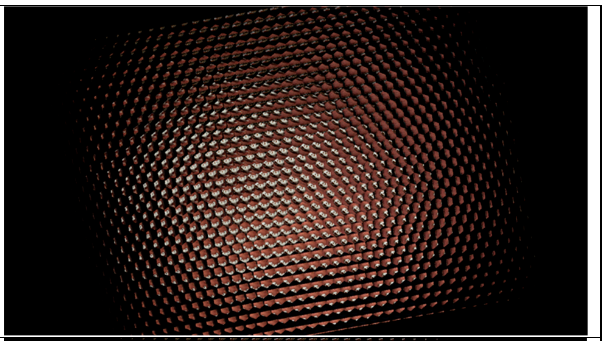
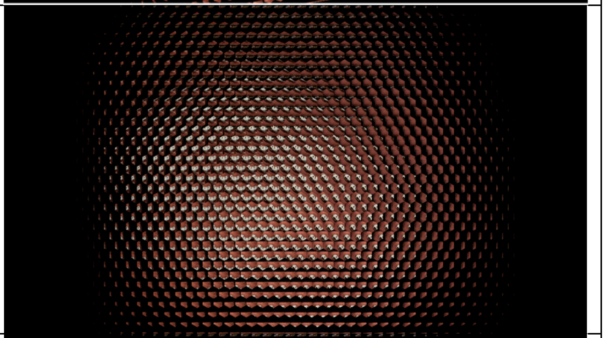
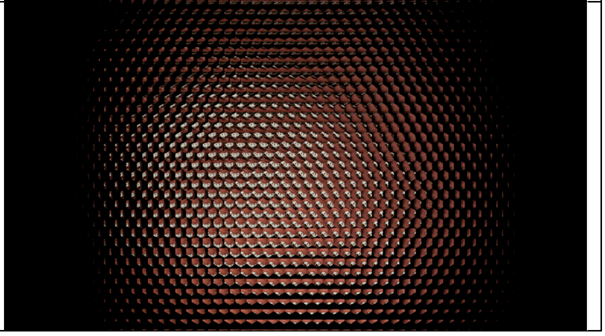
Types of attacks	Watermarked carrier image after attack
Gaussian noise (v = 0.1)	
white noise	
rotation by 10°	
JPEG compression (QF50)	
Gaussian filtering	

Figure 7. Image of the carrier after the attack.

The robustness of a watermarking algorithm refers to the high similarity between the extracted watermark and the original watermark after various attacks on the embedded watermarked image. Normalized correlation coefficient (NC) and bit error rate (BER) are common measures of robustness. They are defined as shown below.

$$NC = \frac{\sum\limits_{p=1}^{p}(m_p - u_m)\left(m_p^* - u_{m^*}\right)}{\sqrt{\sum\limits_{p=1}^{p}(m_p - u_m)^2}\sqrt{\sum\limits_{p=1}^{p}\left(m_p^* - u_{m^*}\right)^2}} \tag{19}$$

$$BER = \frac{\sum\limits_{p=1}^{p}\left(m_p \oplus m_p^*\right)}{P}$$

m_p and m_p^* are the original watermark and the extracted watermark, respectively. u_m and u_m^* are the average of the original watermark and the extracted watermark.

In order to verify that the proposed watermarking algorithm has better performance compared with existing ones, similar algorithms [36,37] are selected for comparison with it in this paper. We compare the robustness by calculating the NC and BER values as shown in Table 3.

Table 3. Robustness comparison against attacks.

Attack	**Our Method**		**Method [36]**		**Method [37]**	
	NC	**BER**	**NC**	**BER**	**NC**	**BER**
Gaussian noise (v = 0.1)	0.9610	0.0162	0.9513	0.0185	0.9605	0.0184
white noise	0.9602	0.0184	0.9510	0.0195	0.9593	0.0189
JPEG compression (QF50)	0.9510	0.0194	0.9502	0.0204	0.9418	0.0264
Gaussian filtering	0.9692	0.0153	0.9508	0.0197	0.9684	0.0178

4. Conclusions

In this paper, a 3D object copyright protection method based on ghost imaging encryption and cellular automata transform (CAT) watermarking algorithm is proposed. The watermark is first encrypted by ghost imaging and then embedded in the light-field image by CAT algorithm. The watermark is extracted by CAT inverse algorithm and decrypted by using the generated scatter intensity in ghost imaging as the key, and the decrypted watermarked image is of high quality. Through a series of experimental operations, the experimental results show that the imperceptibility of the watermark embedding algorithm is higher than that of the traditional DCT and DWT algorithms, and it is more robust and has better resistance to added Gaussian noise, etc. The ghost imaging encryption process before embedding improves the security of the carrier image in use and plays an important role in identity authentication and copyright protection.

Author Contributions: Conceptualization, M.W., M.C. and C.Y.; methodology, M.W. and C.Y.; software, M.C. and M.W.; validation, M.W., M.C. and C.Y.; formal analysis, M.W., M.C. and C.Y.; investigation, M.W. and M.C.; resources, M.W., M.C. and C.Y.; data curation, M.W., M.C. and C.Y.; writing—original draft preparation, M.W. and M.C.; writing—review and editing, M.W., M.C. and C.Y.; visualization, M.W. and M.C.; supervision, M.W., M.C. and C.Y.; project administration, M.W., M.C., C.Y. and J.L.; funding acquisition, C.Y. and J.L. All authors have read and agreed to the published version of the manuscript.

Funding: The funding from Sichuan University (2020SCUNG205); National Natural Science Foundation of China (61775151, 61975138); Natural Science Foundation of Guangdong Province (2018A0303070009, 2021A1515011091); Educational Commission of Guangdong Province (2018KTSCX143, 2020ZDZX3056).

Institutional Review Board Statement: Not applicable.

Acknowledgments: The authors are grateful for the reviewers' careful, unbiased and constructive suggestions.

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

References

1. Lacy, J.; Quackenbush, S.R.; Reibman, A.R.; Snyder, J.H. Intellectual property protection systems and digital watermarking. *Opt. Express* **1998**, *3*, 478–484. [CrossRef] [PubMed]
2. Kim, J.; Jung, J.-H.; Jeong, Y.; Hong, K.; Lee, B. Real-time integral imaging system for light field microscopy. *Opt. Express* **2014**, *22*, 10210–10220. [CrossRef] [PubMed]
3. Lippmann, G. Epreuves reversibles donnant la sensation du relief. *J. Phys.* **1908**, *7*, 821–825. [CrossRef]
4. Llavador, A.; Sánchez-Ortiga, E.; Saavedra, G.; Javidi, B.; Martínez-Corral, M. Free-depths reconstruction with synthetic impulse response in integral imaging. *Opt. Express* **2015**, *23*, 30127–30135. [CrossRef]
5. Burckhardt, C.B. Optimum Parameters and Resolution Limitation of Integral Photography. *J. Opt. Soc. Am.* **1968**, *58*, 71–74. [CrossRef]
6. Nikolaidis, N.; Pitas, I. Robust image watermarking in the spatial domain. *Signal Process.* **1998**, *66*, 385–403. [CrossRef]
7. Chen, W.; Chen, X.; Stern, A.; Javidi, B. Phase-Modulated Optical System with Sparse Representation for Information Encoding and Authentication. *IEEE Photonics J.* **2013**, *5*, 6900113. [CrossRef]
8. Li, Z.; Xia, F.; Zheng, G.; Zhang, J. Copyright protection in digital museum based on digital holography and discrete wavelet transform. *Chin. Opt. Lett.* **2008**, *6*, 251–254.
9. Ishikawa, Y.; Uehira, K.; Yanaka, K. Practical Evaluation of Illumination Watermarking Technique Using Orthogonal Transforms. *J. Disp. Technol.* **2010**, *6*, 351–358. [CrossRef]
10. Li, X.; Lee, I.-K. Robust copyright protection using multiple ownership watermarks. *Opt. Express* **2015**, *23*, 3035–3046. [CrossRef]
11. Li, X.; Wang, Y.; Wang, Q.-H.; Kim, S.-T.; Zhou, X. Copyright Protection for Holographic Video Using Spatiotemporal Consistent Embedding Strategy. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6187–6197. [CrossRef]
12. Valandar, M.Y.; Barani, M.J.; Ayubi, P. A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map. *Soft Comput.* **2019**, *24*, 771–794. [CrossRef]
13. Li, X.; Ren, Z.; Wang, T.; Deng, H. Ownership protection for light-field 3D images: HDCT watermarking. *Opt. Express* **2021**, *29*, 43256–43269. [CrossRef]
14. Hamidi, M.; El Haziti, M.; Cherifi, H.; El Hassouni, M. A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection. *J. Imaging* **2021**, *7*, 218. [CrossRef]
15. Wu, X.; Li, J.; Tu, R.; Cheng, J.; Bhatti, U.A.; Ma, J. Contourlet-DCT based multiple robust watermarkings for medical images. *Multimedia Tools Appl.* **2018**, *78*, 8463–8480. [CrossRef]
16. Hurrah, N.N.; Loan, N.A.; Parah, S.A.; Sheikh, J.A.; Muhammad, K.; de Macedo, A.R.L.; de Albuquerque, V.H.C. INDFORG: Industrial Forgery Detection Using Automatic Rotation Angle Detection and Correction. *IEEE Trans. Ind. Inform.* **2020**, *17*, 3630–3639. [CrossRef]
17. Kamili, A.; Hurrah, N.N.; Parah, S.A.; Bhat, G.M.; Muhammad, K. DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization. *IEEE Trans. Ind. Inform.* **2020**, *17*, 5108–5117. [CrossRef]
18. Wang, Y.; Ren, Z.; Zhang, L.; Li, D.; Li, X. 3D image hiding using deep demosaicking and computational integral imaging. *Opt. Lasers Eng.* **2021**, *148*, 106772. [CrossRef]
19. Kishk, S.; Javidi, B. Information hiding technique with double phase encoding. *Appl. Opt.* **2002**, *41*, 5462–5470. [CrossRef]
20. Wang, X.; Chen, W.; Chen, X. Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding. *Opt. Express* **2014**, *22*, 22981–22995. [CrossRef]
21. Rajanbabu, D.T.; Raj, C. Multi level encryption and decryption tool for secure administrator login over the network. *Indian J. Sci. Technol.* **2014**, *7*, 8. [CrossRef]
22. Rrfregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
23. Clemente, P.; Durán, V.; Torres-Company, V.; Tajahuerce, E.; Lancis, J. Optical encryption based on computational ghost imaging. *Opt. Lett.* **2010**, *35*, 2391–2393. [CrossRef] [PubMed]
24. Duran, V.; Clemente, P.; Torres-Company, V.; Tajahuerce, E.; Lancis, J.; Andrés, P. Optical encryption with compressive ghost imaging. In Proceedings of the 2011 Conference on Lasers and Electro-Optics Europe and 12th European Quantum Electronics Conference (CLEO EUROPE/EQEC), Munich, Germany, 22–26 May 2011; p. 1. [CrossRef]
25. Zhang, L.; Pan, Z.; Liang, D.; Ma, X.; Zhang, D. Study on the key technology of optical encryption based on compressive ghost imaging with double random-phase encoding. *Opt. Eng.* **2015**, *54*, 125104. [CrossRef]
26. Zhang, X.; Meng, X.; Yin, Y.; Yang, X.; Wang, Y.; Li, X.; Peng, X.; He, W.; Dong, G.; Chen, H. Two-level image authentication by two-step phase-shifting interferometry and compressive sensing. *Opt. Lasers Eng.* **2018**, *100*, 118–123. [CrossRef]
27. Zheng, P.; Tan, Q.; Liu, H.-C. Inverse computational ghost imaging for image encryption. *Opt. Express* **2021**, *29*, 21290–21299. [CrossRef]

28. Zhang, L.; Wang, Y.; Zhang, D. Research on multiple-image encryption mechanism based on Radon transform and ghost imaging. *Opt. Commun.* **2021**, *504*, 127494. [CrossRef]
29. Bromberg, Y.; Katz, O.; Silberberg, Y. Ghost imaging with a single detector. *Phys. Rev. A* **2009**, *79*, 053840. [CrossRef]
30. Yang, Y.G.; Wang, B.P.; Pei, S.K.; Zhou, Y.H.; Shi, W.M.; Liao, X. Using M-ary decomposition and virtual bits for visually meaningful image encryption. *Inf. Sci.* **2021**, *580*, 174–201. [CrossRef]
31. Erkan, U.; Toktas, A.; Toktas, F.; Alenezi, F. 2D eπ-map for image encryption. *Inf. Sci.* **2022**, *589*, 770–789. [CrossRef]
32. Dong, Y.; Zhao, G.; Ma, Y.; Pan, Z.; Wu, R. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. *Inf. Sci.* **2022**, *593*, 121–154. [CrossRef]
33. Jiang, D.; Liu, L.; Zhu, L.; Wang, X.; Rong, X.; Chai, H. Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. *Signal Process.* **2021**, *188*, 108220. [CrossRef]
34. Huang, W.; Jiang, D.; An, Y.; Liu, L.; Wang, X. A novel double-image encryption algorithm based on rossler hyperchaotic system and compressive sensing. *IEEE Access* **2021**, *9*, 41704–41716. [CrossRef]
35. Toktas, A.; Erkan, U. 2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm. *Neural Comput. Appl.* **2021**, *34*, 4295–4319. [CrossRef]
36. Agarwal, N.; Singh, P.K. Discrete cosine transforms and genetic algorithm based watermarking method for robustness and imperceptibility of color images for intelligent multimedia applications. *Multimed. Tools Appl.* **2022**, 1–27. [CrossRef]
37. Vaidya, S.P. Fingerprint-based robust medical image watermarking in hybrid transform. *Vis. Comput.* **2022**, 1–16. [CrossRef]
38. Hussain, M.; Riaz, Q.; Saleem, S.; Ghafoor, A.; Jung, K.H. Enhanced adaptive data hiding method using LSB and pixel value differencing. *Multimed. Tools Appl.* **2021**, *80*, 20381–20401. [CrossRef]