symmetry

MDPI

Article

Information Hiding Based on Two-Level Mechanism and Look-Up Table Approach

Jeng-Shyang Pan [1], Xiao-Xue Sun [1], Hongmei Yang [1], Václav Snášel [2] and Shu-Chuan Chu [1,*]

[1] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China; jengshyangpan@gmail.com (J.-S.P.); xues1123@163.com (X.-X.S.); yanghongmei@sdust.edu.cn (H.Y.)
[2] Faculty of Electrical Engineering and Computer Science, VŠB-Technical University of Ostrava, 70032 Ostrava, Czech Republic; vaclav.snasel@vsb.cz
* Correspondence: scchu0803@gmail.com

Abstract: Information hiding can be seen everywhere in our daily life, and this technology improves the security of information. The requirements for information security are becoming higher and higher. The coverless information hiding with the help of mapping relationship has high capacity, but there is still a problem in which the secret message cannot find the mapping relationship and the process requires extra storage burden during the transmission. Therefore, on the basis of symmetric reversible watermarking, the paper introduces the two-level mechanism and novel arrangements to solve the problem of sufficient diversity of features and has better capacity and image quality as a whole. Besides, for the security of secret message, this paper designs a new encryption model based on Logistic mapping. This method only employs coverless information hiding of one carrier image to transmit secret message with the help of the two-level mechanism and look-up table. Reversible information hiding is applied to embed the generated location table on the original image so that ensures storage and security. The experiment certifies that the diversity of hash code is increased by using the two-level image mechanism and the quality of the image is excellent, which proves the advantages of the proposed symmetric method over the previous algorithm.

Keywords: logistic mapping; two-level mechanism; look-up table; reversible information hiding

Citation: Pan, J.-S.; Sun, X.-X.; Yang, H.; Snášel, V.; Chu, S.-C. Information Hiding Based on Two-Level Mechanism and Look-Up Table Approach. *Symmetry* **2022**, *14*, 315. https://doi.org/10.3390/sym14020315

Academic Editor: José Carlos R. Alcantud

Received: 2 January 2022
Accepted: 28 January 2022
Published: 3 February 2022

1. Introduction

The development of network technology has greatly promoted the security need in daily life [1,2]. Our daily life is inseparable from the application of network transmission, so there are many technologies used to solve the problem of network transmission security. The digital media transmitted by the network mainly includes video, audio, pictures, and text. As the main form of multimedia, the acquisition and tampering of digital images are quite easy. At present, the most commonly used methods to protect digital media are mainly grouped by encryption and information hiding. The former is that the sender applies the encryption algorithm to directly encrypt the multimedia information, and the receiver with the key can obtain the secret information in view of the encryption method. Generally speaking, the garbled state formed after encryption can easily arouse the suspicion and attention of others. The information hiding needs to conceal the existence of the secret message with the help of the carrier, that is, it is hidden in multimedia data. The secret is transmitted depending on multimedia data. The receiver exploits the corresponding extraction method to extract the secret message.

The information hiding technology is a key technology and is widely utilized in many fields such as copyright protection and digital signature [3,4]. Information hiding technology changes the carrier to hide information, which can be implemented in the spatial domain or frequency domain. Some techniques even permanently damage the original carrier image. Sahu et al. apply a two-level LSB replacement technique [5].

Muhuri et al. implement image steganography on Integer Wavelet Transformation (IWT) using Particle Swarm Optimization (PSO) algorithm in 2020 [6–8]. Digital watermarking focuses on protecting the secret message. The digital watermarking methods commonly used inevitably cause irreversible effects on the original carrier [9]. Therefore, the emergence of reversible information hiding technology satisfies the dual recovery of the carrier and secret message [10–12]. Reversible information hiding means that when the receiver receives the watermarked image not only the secret message can be extracted but also the original image can be recovered according to the embedding and extraction rules [13,14]. It not only satisfies the confidentiality of secrets but also does not permanently destroy the image, which can be widely applied to medical image transmission.

Reversible information hiding was first proposed by Honsinger et al. in 1999 [15]. There are three types of algorithms on the spatial domain most commonly used by reversible information hiding techniques: lossless compression, difference expansion [16], and histogram shifting [17,18]. Difference expansion uses the correlation characteristics between pixels to expand the pixel difference through integer transformation to embed secret [19,20]. The prediction error algorithm predicts the target pixel through the prediction model [21–23]. Weng et al. combine difference expansion and prediction error to improve the quality of the image embedded with data [24]. According to whether the parameters used for embedding and extraction are the same, the information hiding can be divided into symmetric and asymmetric. The symmetric mechanism is efficient and simple so most of the current information hiding technologies are symmetric [25–27].

Steganalysis is a technique that tries to find the secret message. Although the secret message is difficult to be found by Human Visual System (HVS) on the carrier, the existence of the secret message can still be found through the traces of these modifications [28]. Coverless information hiding is one of the means to avoid steganalysis. This method directly expresses the secret message utilizing the characteristics of the carrier [29]. Zhou et al. use faster-RCNN for training to find the labels of images to express the secret message [30]. The network architecture based on deep learning has a large transmission overhead and requires a long training time. Zou et al. come up with a novel coverless information hiding based on the average pixel value of the image, which hides the information through mapping relation and multi-level index structure [31]. Cao et al. propose an approach based on the molecular structure images of material [32]. Wang et al. construct an intelligent search algorithm for mapping relationships to implement coverless information hiding [33]. Although this method solves the problems of transmission overhead and training, it inevitably adopts the mapping relationship. Information hiding techniques based on mapping relationships still have the limitation that increases the number of mapping relationships with the extension of secret information, resulting in a large cost or even being impractical.

The coverless information hiding approach proposed by Fatimah Shamsulddin Abdulsattar well improves the efficiency of feature extraction and explores the effect of block size on image hiding [34]. However, the features generated by analysis may not satisfy the secret message embedding due to lacking diversity in the obtained hash code. To improve the success rate of secret hiding, we combine the two-level mechanism and design novel arrangements to increase the diversity of hash codes.

During the hiding process, a location table is generated, so additional storage space and transmission process are required to ensure the recovery of secret data. The hidden framework proposed in this paper combines coverless information hiding and reversible information hiding techniques [35]. This process not only satisfies the hiding capacity of the secret message but also ensures the recovery of the original image. To better solve the problem of additional information storage and the security of secret data, the newly proposed encryption model is employed to encrypt the data first, then generate eigenvalues, calculate the hash code, and establish a look-up table on the original image [36]. The generated location table is embedded taking advantage of reversible information hiding technology, and the whole process is symmetric.

Since the secret message is hidden adopting a coverless way, this method will not produce any changes to the image, and then the pivotal information is embedded using the prediction error expansion (PEE) algorithm. Of course, other outstanding PEE algorithms could also be combined. Finally, the image can be recovered. The main contributions of this work are as follows.

1. A more secure encryption model based on Logistic mapping is devised;
2. The hash code based on the two-level image mechanism is more diverse and reduces the unconcealable rate of the secret message;
3. A new combination of reversible information hiding and coverless information hiding is designed, which greatly improves capacity and the image quality;
4. The proposed method solves the additional storage of location table without sacrificing hiding capacity and no large image database is required;
5. Compared with other similar algorithms, our method has more security and better image quality and higher storage capacity.

The remainder of the paper is formed as follows. Section 2 reviews the basic Logistic mapping and previous coverless information method. The proposed model is presented in Section 3. Section 4 displays experiment results and comparative analysis. Finally, Section 5 gives a conclusion and future directions.

2. Related Works

To further improve the security of secret message, the paper designs a novel encryption model to encrypt it based on logistic mapping. This part also introduces the previous coverless information hiding algorithm proposed by [34].

2.1. Logistic Mapping

Chaos refers to the seemingly random and irregular movement that occurs in a non-deterministic system. It originates from nonlinear dynamic systems. Logistic mapping is one of the most famous chaotic mappings due to its simple expression and excellent performance [37–39]. Its expression form is as Equation (1).

$$y_{n+1} = \mu \times y_n \times (1 - y_n), \tag{1}$$

where $n = 0, 1, 2, 3, \ldots$ and y belongs to 0 and 1. The system control parameter μ is the constant and $\mu \in (0, 4]$. When $3.569945672 \cdots < \mu \leq 4$ and the final sequence value belongs to $[0, 1]$, the logistic sequence y_n is in the state of chaos. The function has the characteristics of aperiodic and sensitive dependence to the initial condition. Logistic mapping is simple without losing the complex characteristics of the chaos, so it is usually used on image encryption.

2.2. Previous Method

The main idea is to form a mapping relationship between the carrier and the secret message, and then realize the coverless hiding of the secret data. The construction of the look-up table is based on the generation of hash code. Fatimah Shamsulddin Abdulsattar generates eigenvalues based on feature decomposition, and then calculates the hash code of the image block and builds a look-up table [34]. The look-up table contains the hash code and its location information. In the image, the main feature vector represents the direction of the maximum change between image pixels, and the largest feature value is related to the foremost feature vector. The hash code is calculated by the largest eigenvalue obtained by feature decomposition which is Equation (2).

$$max\_e_{jl} = max\{e_{jl1}, e_{jl2}, e_{jl3}, \ldots, e_{jlk}\}, \tag{2}$$

where max_e_{jl} denotes the largest value in the l-th sub-block and the block $\mathbf{B_{jl}}$ has k eigenvalues. The largest eigenvalue of adjacent image sub-blocks is arranged and combined in

light of the specific arrangements to obtain an 8-bit binary hash code. The arrangements in this method are displayed in Figure 1. If the arrangement Arr.1, as shown in Figure 1a, is selected in the process, the hash code is acquired by Equation (3). When another arrangement (Arr.2 or Arr.3 or Arr.4) is selected, the function is calculated according to Equation (4).

$$h_c = \begin{cases} 0, & \text{if } max\_e_{jl} > max\_e_{j5} \\ 1, & \text{if } otherwise \end{cases} \tag{3}$$

where the max_e_{jl} is the largest value in the l-th sub-block and $l \in [1, 8]$.

$$h_c = \begin{cases} 0, & \text{if } max\_e_{jl} < max\_e_{jl+1} \\ 1, & \text{if } otherwise \end{cases} \tag{4}$$

where $l \in [1, 8]$ and $l \neq 5$.

The hash code of each sub-block can be converted into the corresponding ASCII-code value [40]. The range of the ASCII code is $[0, 255]$. The look-up table is created by putting the positions of the hash code and the hash code into the same table. When the sender hides the secret message, they can map the table with the data and record the location of the hash code, that is, by creating a location table to achieve coverless hiding. After receiving the location table and the original image, the receiver can establish the same look-up table and then extract the hidden secret from the look-up table in the light of the mapping relationship.

According to the above description, Fatimah Shamsulddin Abdulsattar uses eigenvalue decomposition to establish the hash code as the feature of the image and then establish the look-up table. The secret message is hidden according to the mapping relationship. Although their method does not require a large database and achieves a high hidden capacity, when the image block is set to a large size, the number of hash codes generated is less. There is a problem that the secret message has no mapping relationship. When the size of the secret message increases, the corresponding location table requires more space. In other words, there is room for improvement. Our method for this problem is increasing the diversity of hash code and further improving the hiding rate.

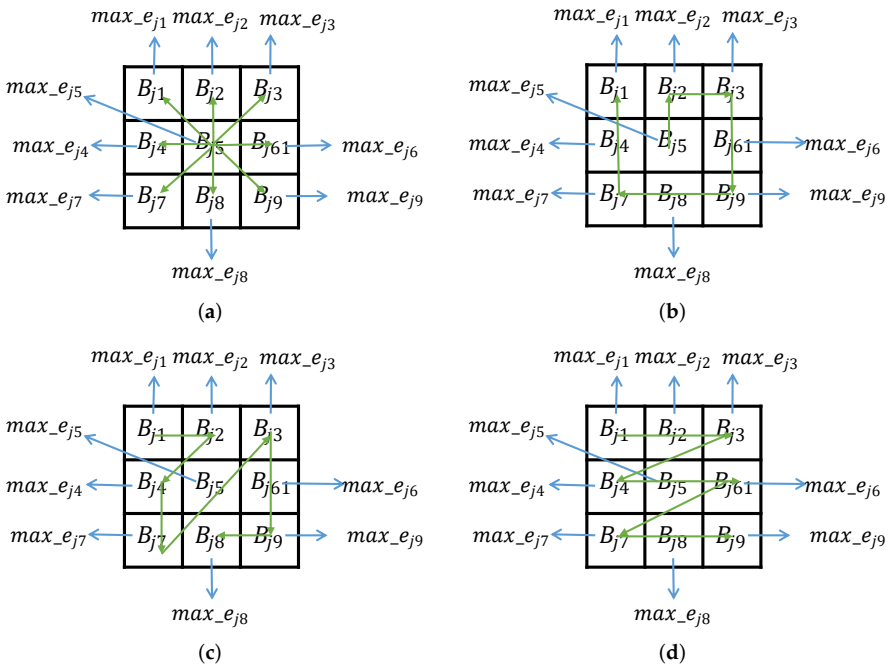


Figure 1. The four arrangements are used in [34]. (**a**) Arr.1, (**b**) Arr.2, (**c**) Arr.3, and (**d**) Arr.4.

3. Proposed Method

The information hiding technology proposed in the paper is mainly divided into two, secret message hiding and secret message extraction. The whole process is divided into two stages. The first stage takes advantage of the coverless information hiding to hide the secret message. The stage generates a vital location table. The second stage embeds the location table using the PEE algorithm. The main idea of our model is to combine coverless information hiding and PEE during hiding the secret message.

Before the secret message is hidden, the new encryption model is designed to enhance the security of secret data first. To increase the diversity of hash codes, the original image is divided into two sub-images using the two-level mechanism, and the mapping relationship formed by the look-up table established by the image blocks of the sub-image and the secret message is formed to realize the coverless hiding of the secret data. Although the hiding process does not change the original image, it needs to generate a corresponding location table. Considering that the location table needs additional storage and transmission, the paper adopts PEE to realize the second embedding of the location table. After receiving the watermarked image, the receiver can extract the location table and recover the original image. After obtaining the original image, the same look-up table can be established, and the encrypted secret information can be extracted according to the mapping relationship. The secret message can be recovered through decryption model with the same key. Figure 2 shows the framework model of the proposed algorithm. Due to the parameters used in the sender and receiver are the same, the designed model is symmetric.

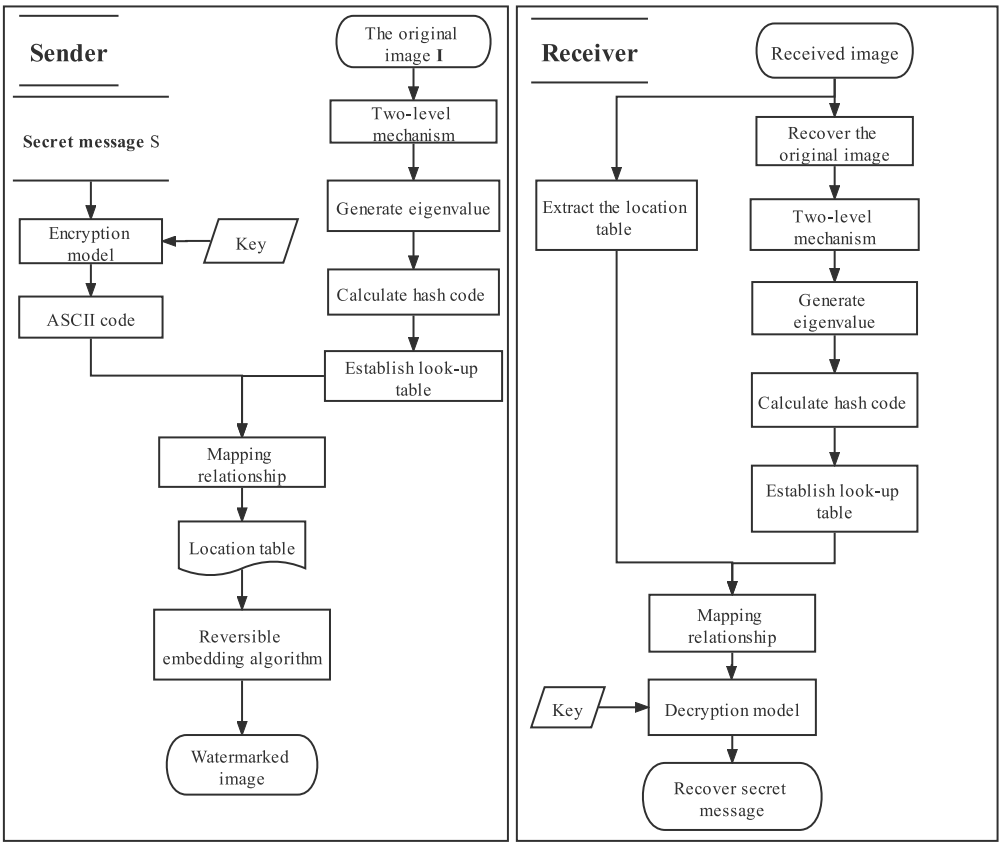


Figure 2. The framework of the proposed model.

3.1. Encrypt the Secret Message

Logistic mapping is an encryption algorithm with a simple structure and good encryption effect. However, it is sensitive and periodic to the initial value, and its structure is relatively simple. Once the initial value is known, it is easy to be cracked. Therefore,

we adopt a dual logistic mapping, and the function of the model can be described as Equation (5).

$$\begin{cases} y_{i+1} = \mu \times y_i \times (1 - y_i),\ i = 1, 2, 3, \ldots, n/2 - 1 \\ y_{i+1} = \mu \times sin(\pi/2 \times y_i) \times (1 - sin(\pi/2 \times y_i)),\ i = n/2, n/2 + 1, \ldots, n - 1 \end{cases} \tag{5}$$

By combining the original logistic mapping and sin-logistic mapping, the final sequence is more chaotic. It is less easy to traverse to the secret message after encryption. If the initial value is not set, ten bits of secret information will be randomly selected to calculate the mean value as the initial value, see as Equation (6).

$$\begin{cases} r = randperm(sum, 10), \\ y_1 = \dfrac{\sum S(r)}{10}, \end{cases} \tag{6}$$

where S is the one-dimensional secret message sequence and the length is sum.

3.2. Hiding the Secret Message

The two-level mechanism splits the image into two sub-images, and two sub-images can be restored to the original image. Each pixel value of the image is composed of an 8-bit binary value, and the image can be divided into 8-bit planes. The image is split into two images according to the 8-bit planes of the image. The pixel value of the image is represented as Equation (7).

$$p = p_h \times 2^w + p_l, \tag{7}$$

where p represents the pixel value in the image, p_h represents the high-level plane, w represents the number of bits divided, and p_l is the low-level plane. According to Equation (8), the high-level plane is divided into two parts p_{h1} and p_{h2}, where a is the constant ranging from 0 to 1.

$$\begin{cases} p_{h1} = a \times p_h, \\ p_{h2} = p_h - p_{h1} \end{cases} \tag{8}$$

Equation (9) is the method of dividing the low-level plane, that is, dividing the low-level plane into two sub-planes p_{l1} and p_{l2}. The parameter c is the number of bits during the division.

$$\begin{cases} p_{l1} = \dfrac{(p_l - p_{l1})}{2^c}, \\ p_{l2} = p_l \% 2^c \end{cases} \tag{9}$$

The two sub-planes of the high plane are combined with the two sub-planes of the low plane, respectively, according to Equation (10). Thus, two sub-images can be obtained by splitting one image according to the above-mentioned division mechanism.

$$\begin{cases} p_1 = p_{h1} \times 2^w + p_{l1} \times 2^c, \\ p_2 = p_{h2} \times 2^w + p_{l2} \end{cases} \tag{10}$$

The hiding stage is mainly divided into two parts; one is coverless information hiding based on the look-up table approach, and the other embeds the location table into the original image by PEE. Firstly, the image is split into two sub-images and divided into image blocks. Secondly, the 8-bits hash code of the image block is calculated according to the designed arrangements, and each group of hash code is converted into ASCII code. The ASCII code of all image blocks and their location are combined to form a look-up table. Then the secret message is hidden without changing depending on the mapping relationship. Finally, the key location table is embedded into the image by PEE. The specific embedding steps are as follows:

Step 1. Predict the pixel value $p_{r,i}$ by Equation (11) according to the predictor as shown in Figure 3.

$$\hat{p}_{r,i} = \frac{p_{r+1,i-1} + p_{r+1,i} + p_{r+1,i+1}}{3}, \tag{11}$$

where $\hat{p}_{r,i}$ is the predicted value.

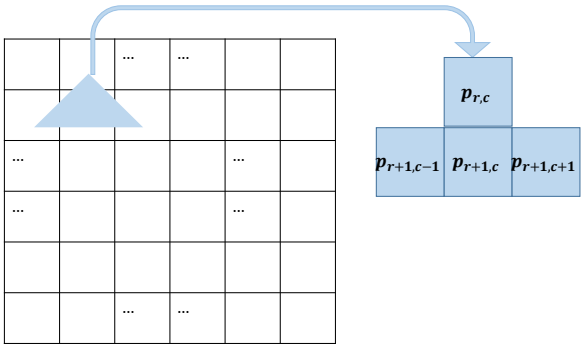


Figure 3. The predictor used in our algorithm.

Step 2. Calculate the prediction error of the pixel $p_{r,i}$ according to Equation (12).

$$e_{r,i} = p_{r,i} - \hat{p}_{r,i} \tag{12}$$

Step 3. Expand the prediction error and embed the secret message by Equation (13) where T is a threshold. The prediction error in $[-T, T)$ will be used to embed the secret message.

$$e'_{r,i} = \begin{cases} 2 \times e_{r,i} + s_i & \text{if } e_{r,i} \in [-T, T) \\ e_{r,i} + T & \text{if } e_{r,i} \in [T, \infty) \\ e_{r,i} - T & \text{if } e_{r,i} \in (-\infty, -T) \end{cases} \tag{13}$$

Step 4. Modify the corresponding pixel value according to the extended prediction error referring to Equation (14).

$$p'_{r,i} = \hat{p}_{r,i} + e'_{r,i} \tag{14}$$

After the secret message is embedded into the original and is transmitted to the receiver, the receiver could extract the message and recover the original image by the inverse process. Our method designs three novel arrangements as seen in Figure 4 to increase the diversity of hash codes. In Figure 4c, the nine values of the sub-block are scrambled randomly to generate the hash code so that each hiding process will have different results. The paper adopts the two-level mechanism and selects three arrangements from seven ways in Figures 1 and 4 randomly to generate features. The random approach adopted can elevate the security of the architecture. This mode increases the diversity of hash code and can further allow the secret message to be successfully hidden. To understand the whole hiding process, the specific steps can be seen as Algorithm 1.

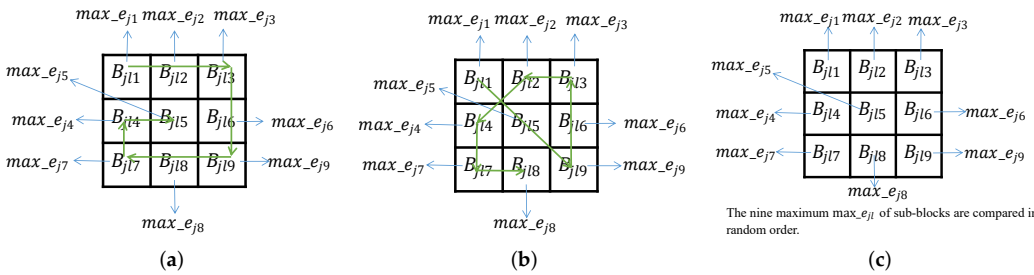


Figure 4. The remaining three arrangements we designed. (**a**) Arr.5 (**b**) Arr.6, (**c**) Arr.7.

Algorithm 1 Pseudo-code of the hiding model.

Require: Original image **I**, secret message S, the initial key $Init_k$, parameter μ, w, c, b, b_s
Ensure: Watermarked image $\mathbf{I}'$
Step 1. Generate one-dimensional sequence Y that the length is as same as the secret message using Equations (5) and (6) with the initial key $Init_k$.
Step 2. Encrypt the secret message S by exclusive-or operation with Y and obtain the encrypted sequence S'.
Step 3. Divide host image **I** into two sub-images $\mathbf{I_1}$ and $\mathbf{I_2}$ based on the two-level mechanism by Equations (8)–(10).
Step 4. Split two sub-images into image block $\mathbf{B_j}$ with fixed-size b.
Step 5. Further split $\mathbf{B_j}$ into nine sub-blocks $\mathbf{B_{jl}}$ with the small size b_s where l denotes the l-th sub-block in the image block $\mathbf{B_j}$.
Step 6. Calculate the eigenvalue of all sub-blocks $\mathbf{B_{jl}}$ and find the largest value max_e_{jl} by Equation (2).
Step 7. Acquire the hash code by arranging the eigenvalues of the sub-blocks in every image block where uses three arrangements of seven arrangements randomly.
Step 8. Generate the ASCII code with every 8-bit hash code and an ASCII code corresponding to a block.
Step 9. Establish look-up table including ASCII codes and their location.
Step 10. Convert the encrypted message S' to ASCII code S'_a.
Step 11. Match S'_a with the equal image block and record the location of the corresponding image block in order in the position table.
Step 12. Embed the location table and additional information into the original image **I** using above PEE. The additional information includes the encryption key, parameter w, c, b, b_s, the arrangements selected, and the size of the secret message.

3.3. Extract the Secret Message and Recover the Original Image

The symmetric framework of requiring secret data is the inverse process of embedding. After receiving the watermarked image, the receiver first performs the inverse operation of the prediction error expansion to extract the location table and additional information. Then, the original image is recovered, and the same look-up table is established. Finally, the key and encrypted secret data are extracted according to the mapping relationship. The secret can be recovered by decrypting the encrypted message with the key. The pseudo-code is displayed in Algorithm 2 which includes the whole process of extracting the secret message and recovering the original image.

Algorithm 2 Pseudo-code of the extraction and recover model.

Require: Watermarked image
Ensure: Recovered host image $\mathbf{I_o}$ and the secret message S''
Step 1. Extract the location table, additional information, and recover the original image $\mathbf{I_o}$.
Step 2. Divide the recovered image using the same method.
Step 3. Calculate the corresponding eigenvalue and hash code.
Step 4. Convert the hash codes to ASCII code.
Step 5. Establish the look-up table.
Step 6. Acquire the encrypted secret sequence from the look-up table and the location table by the mapping relation.
Step 7. Generate one-dimensional sequence Y_2 that the length is as same as the secret message using Equations (5) and (6) with the initial key $Init_k$.
Step 8. Decrypt the secret message S'' by executing exclusive or operation between Y_2 and the encrypted sequence.

4. Experiment and Results

The computer configuration used in this article is: Intel(R) Core(TM) i5-8500 CPU @ 3.00 GHz, 16.0 GB memory, and Windows 10 (64 bits), and the experimental codes are all running on the MATLAB R2018a.

To prove the effectiveness of the encryption method, we take an example for the encryption test and compare with other encryption methods. Both methods use the same initial value to iteratively generate the sequence. Information entropy is one of the crucial indicators to measure the performance of encryption models. It is the average of the information and is expressed as Equation (15).

$$\begin{cases} I_H(p) = -\sum_{i=1}^{ps} q(p_i) \times log_2 q(p_i), \\ \sum_{i=1}^{n} q(p_i) = 1, \end{cases} \tag{15}$$

where $q(p_i)$ satisfies $0 \leq q(p_i) \leqslant 1$.

For the digital image, the information entropy can reflect the distribution of gray values. If the gray pixel value distribution is uniform, the maximum value of information entropy will be 8, which is a proportional relationship. When the information entropy is larger, the more average the gray value distribution is, the smaller the correlation degree is.

The experimental results are shown in Table 1. It can be concluded from the data that the information entropy of the original image is 7.2081, and the information entropy after encryption can exceed 7.99; more than 7.99, in theory, means that encryption is considered successful.

Table 1. Information entropy and correlation coefficient compared with other encryption model.

Index\Image	Original Image	Encrypted Image		
		Logistic Mapping [38]	Sin-Logistic Mapping	Our Model
Entropy	7.2081	7.9945	7.9623	**7.9954**
Horizontal	0.9687	−0.0868	0.0620	**0.0352**
Vertical	0.9372	−0.0934	−0.1215	**−0.0391**
Diagonal	0.9057	0.0722	0.0514	**0.0188**

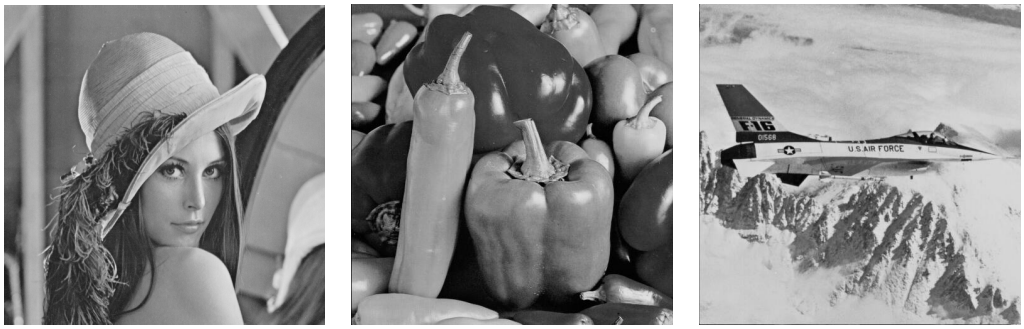
In Table 1, the information entropy of the encrypted image is 7.9954, which is closer to 8 than the other two algorithms, which proves that the method can have a more average gray value distribution after application. Our algorithm achieves the maximum information entropy, which means it performs excellently compared with other methods.

Each digital image is not independent, and the correlation between adjacent pixels is crucial. The calculation function is as Equation (16). One purpose of the image encryption is reducing the correlation between pixels, making correlation analysis invalid. The smaller the correlation value between pixels, the better the encryption effect and the safer the information. A strong correlation must be broken to avoid the statistical attack. So, we design correlation analysis experiments in three different directions and the directions include horizontal, vertical, and diagonal direction. The data are in Table 1.

$$\begin{cases} C_R(p, p_x) = \frac{cov(p,p_x)}{\sigma_p \times \sigma_{p_x}}, \\ cov(p, p_x) = \frac{\sum_{j=1}^{M}(p_j - E(p)) \times (p_{x_j} - E(p_x))}{M}, \\ \sigma_p = \frac{\sum_{j=1}^{M}(p_j - E(p))^2}{M}, \\ E(p) = \frac{\sum_{j=1}^{M} p_j}{M} \end{cases} \tag{16}$$

So, we design correlation analysis experiments in three different directions where 2000 pairs of adjacent pixels are randomly selected for testing. The correlation coefficients in the original image and the encrypted image are calculated in the horizontal, vertical, and diagonal directions according to the above definition of the correlation coefficient. The data are in Table 1. According to Equation (16), it can be known that the coefficient may be positive or negative. When $|C_R| \leq 0.3$, it means that the correlation between the two variables is extremely weak and can be regarded as irrelevant. From Table 1, we can see that the correlation coefficient of the original image is close to 1, which means that there is a high correlation between pixels. On the contrary, the correlation coefficient of the encrypted image is close to 0, which means that the statistical characteristics of the encrypted image are successfully disrupted. As shown, our method achieves better dispersion than other algorithms in the horizontal, vertical, and diagonal direction and holds higher security.

Information hiding should realize the complete hiding of the secret message under the premise of ensuring the quality of the original image. In [34], the experimental results prove that there will be cases where secret message cannot be found to match it in the look-up table. Hash codes are important features used in coverless information hiding. When the range of generated features is large and different enough, hash codes are more diverse. The paper designs new arrangements, and there are seven arrangements now. In addition, we employ the two-level mechanism. Comparative experiments are performed on three different images, as shown in Figure 5. In the same figure, the experiment compares the generated types of hash codes by seven arrangements.



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

Figure 5. The three test images. (**a**) Lena, (**b**) Pepper, (**c**) Plane.

The results are put in Table 2 which has only one arrangement. From the data in Table 2, we see that the types of hash codes generated under the two-level mechanism become larger, that is, the designed model can find more different hash codes. The diversity of the hash code is enhanced. However, the types of hash codes generated under a single arrangement still cannot reach 256. Therefore, the paper increases the formation range of hash codes and increases the diversity of hash code through the two-level mechanism and three new arrangements to achieve 256 different hash codes. The method can generate enough unique features in a non-overlapping way. To prove the effectiveness, a comparative experiment is carried out on Figure 5 when hiding the same secret message.

From the data, we can see that the hash code value generated under the two-level mechanism is larger, that is, the designed model can find more different hash codes. The diversity of the hash code is enhanced. However, the types of hash codes generated when a single arrangement is adopted still cannot reach 256. Therefore, the paper increases the formation range of hash codes and increases the diversity of hash code through the two-level mechanism and three new arrangements to achieve 256 different hash codes. The method can generate enough unique features in a non-overlapping way. To prove the effectiveness, a comparative experiment is carried out on Figure 5 when hiding the same secret message. The size of the secret message is set as 6272 bits. The test and comparison experiment results are shown in Table 3.

Table 2. Types of different hash codes generated under different arrangements.

Hash Codes	[34]			Two-Level Mechanism		
	Lena	Pepper	Plane	Lena	Pepper	Plane
Arr.1	148	139	158	186	161	198
Arr.2	179	180	214	186	182	207
Arr.3	155	163	169	170	161	186
Arr.4	208	188	158	251	166	248
Arr.5	192	191	201	217	210	227
Arr.6	171	160	195	170	166	191
Arr.7	143	123	170	183	176	210

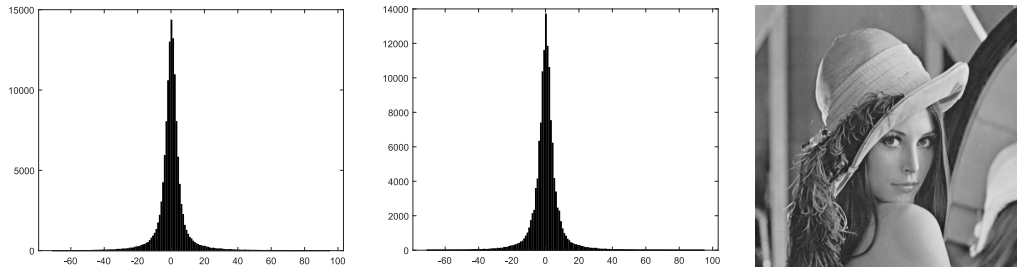
In the experiment, the size of the secret message is set as 6272 bits. The test and comparison experiment results are shown in Table 3. Arr.4 is used in [34] and our method selected three arrangements including Arr.2, Arr.4, and Arr.5. In Table 3, "Hash code(types)" denotes the types of hash code generated, and "No-find(bits)" is that the secret message cannot find the corresponding hash code. Since every 8 bits of secret information are converted into ASCII code for embedding, the ASCII-code range is between 0 and 255. Therefore, the hash code generated should be converted into ASCII code in 256 cases. It can be seen from the test data that the previous method cannot produce enough types of hash code. There is some message that cannot find the mapping relationship in the look-up table. Our algorithm obtains more different hash codes, that is, the diversity of hash code is increased by adding arrangements and the two-level mechanism. Due to the diversity of hash code increasing, the number of no-find cases will decrease accordingly. We increase the concealment rate of secret message through adding the two-level mechanism and designing new arrangements. As the results in Table 3, when the same number of bits is hidden in the same image, we can hide all secret message compared with the previous method.

Table 3. Comparison of the types of hash code and the number of the secret message cannot find.

Hiding Capability	[34]		Our Method	
	Hash Code (Types)	No-Find (Bits)	Hash Code (Types)	No-Find (Bits)
Lena	208	156	**256**	**0**
Pepper	188	219	**256**	**0**
Plane	158	305	**256**	**0**

Our coverless information hiding method can store an infinite amount of secret information, but for ensuring the security and transmission space of the location table, we also use reversible information hiding technology to embed the location table into the original image. Therefore, the embedding capacity depends on the method of reversible information hiding technology used. This paper adopts a simple PPE algorithm. After hiding the secret data, the image carrying the secret message is put in Figure 6. The secret message cannot be detected from Figure 6c by our eyes.

Reference [34] realizes the high capacity. The high hiding capacity is one of our goals in the paper. The experiment of the capacity in the paper is compared with other methods in Figure 5a, "Lena". The test results are stored in Table 4, where the different image has the different capacity with different embedding algorithms. The capacity represents the largest length of secret message that can be hidden under the algorithm model. From the data in Table 4, our method has the highest capacity to hide the secret message. Regarding reversible information hiding technology, it can also be combined with technologies with higher hiding ability. In the future, different reversible information hiding technologies can be selected according to the size of secret data.



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

Figure 6. The image with the secret message applying our method. (**a**) The histogram of the predict error; (**b**) the histogram of predict error after embedding message; (**c**) the image carrying the secret message.

Table 4. Comparison of the hiding capacity with other papers.

Approaches	Capacity (bits)
HOGs [41]	8
DCT+LDA [42]	1–15
faster-RCNN [43]	20 and 25
[34] (non-overlapping)	6272
[34] (overlapping)	55,112
Our proposed method	**84,005**

In view of analyzing the image quality, this experiment is compared with several methods. This paper still uses the standard Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM) to measure the quality of several methods. PSNR is one of the criteria for measuring the invisibility of images embedded with watermarks in information hiding, calculated by Equation (17).

$$\begin{cases} \text{PSNR} = 10 \times log_{10}(\frac{\text{MAX}_I^2}{\text{ME}}), \\ \text{MAX}_I = 2^8 - 1, \\ \text{ME} = \frac{\sum_{u=1}^{rol}\sum_{v=1}^{col}(p_{uv} - p'_{uv})^2}{rol \times col}, \end{cases} \tag{17}$$

where p_{uv} and p'_{uv}, respectively, are the pixel value in the original host and the stego image. rol and col denote the total number of image rows and columns.

SSIM is an index to judge the similarity between two images, and the calculation function can be seen in Equation (18). Here, SSIM is used to measure the extraction quality of secret information.

$$\text{SSIM}(\mathbf{I}, \mathbf{I}') = \frac{(2 \times \mu_I \times \mu_{I'} + c_{a1})(2 \times \sigma_{II'} + c_{a2})}{(\mu_I^2 + \mu_{I'}^2 + c_{a1})(\sigma_I^2 + \sigma_{I'}^2 + c_{a2})}, \tag{18}$$

where μ_I and $\mu_{I'}$ represent the average of I and I'. $\sigma_{I'}$ and $\sigma_{I'}^2$ is the variance of $\mathbf{I}$ and $\mathbf{I}'$. $\sigma_{II'}$ is the covariance. c_{a1} and c_{a2} are two constants to avoid dividing by zero.

Table 5 shows PSNR and SSIM for different methods without suffering any attacks. From the calculation results, we can see that our method is the best performance of these methods. This algorithm achieves excellent image quality when it has the same capacity and can obtain the original secret message.

Table 5. PSNR and SSIM about our proposed method and other papers.

Methods	PSNR	SSIM
Sahu and Swain [5]	51.25	0.999
Muhuri et al. [6]	51.668	0.998
Sahu and Swain [43]	48.2	0.997
[34]	∞	**1**
Our method	52.024	**1**

In the network transmission, images may be intercepted or tampered with, so the information hiding algorithm needs to have the ability to resist attacks, which we call robustness. The robustness refers to the nature of an image with the secret message that can still extract information after suffering the attack. To reflect the robustness of the model designed, we compare it with the previous model. The experimental results are shown in Table 6.

Table 6. The extraction rate using different methods under different attacks.

Attacks	[34]	Our Hiding Method
No attack	80.10%	**100%**
Median (3 × 3)	65.90%	**72.60%**
Median (5 × 5)	59.60%	**68.20%**
Gaussian low-pass filter (w = 3)	69%	**75.80%**
Gaussian noise (r = 0.001)	**39.30%**	6.90%
Salt and pepper noise	**3.70%**	1%
Speckle noise	**39.90%**	10.60%
Sharpening attack (r = 0.05)	**88.50%**	78.80%
Histogram equalization	0.80%	0.80%
Average filter	69%	**77.30%**
Motion blur	58.50%	**59.70%**

It can be seen from the extraction rate that under the same hidden capacity, our algorithm has higher value, which means that our model has better robustness.

Pixel Difference Histogram (PDH) is an important indicator to measure security [44,45]. The PDH graph reveals the relationship between the pixel difference and the number of occurrences of the difference. The X-axis represents the pixel difference between two consecutive pixels, and the Y-axis is the frequency of the difference. The zig-zag phenomenon that appears in the PDH curve is called the undesired step effect. If this effect appears in the curve, it is considered that the image hides the secret message. The greater the distortion of the image containing the secret message, the corresponding PDH curve shows undesired steps; conversely, when the distortion is very small, the PDH curve would look as smooth as the original image.

The same secret message is hidden in three test images located in Figure 5. Figure 7a,d,g are the curves using [34]. In this experiment, the first stage (coverless information hiding) and the final image that carries the location table of our algorithm are represented in the analysis, respectively. Figure 7b,e,f are the first stage and Figure 7c,f,i denote the results in the final image.

It can be seen that these PDH curves are still as smooth as the original image after hiding the secret message and they do not show the effects of any steps. Therefore, this algorithm is undetectable by PDH analysis and is considered to have a certain degree of security.

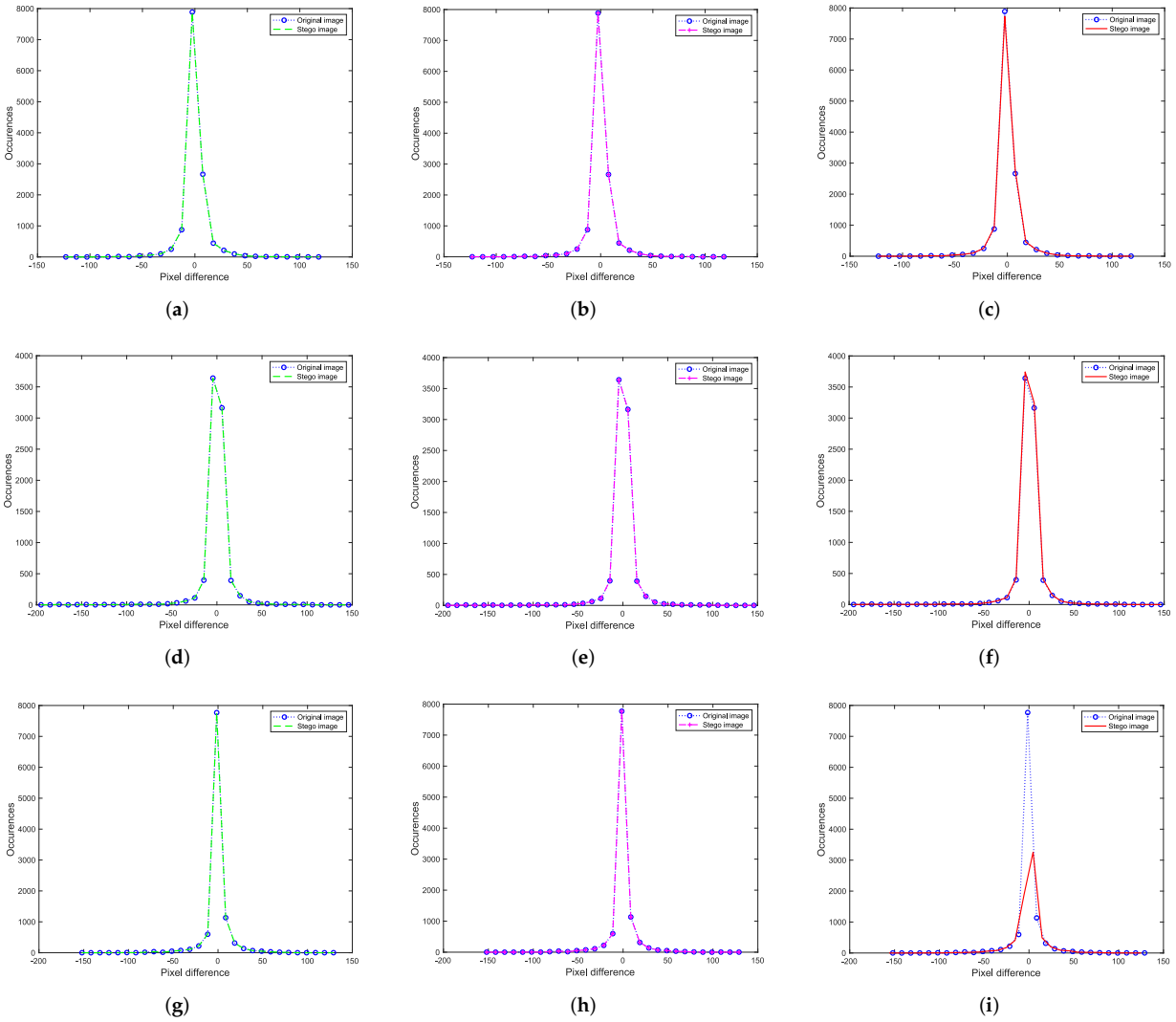


Figure 7. The PDH analysis with different images: (**a**–**c**) are the results in "Lena", (**d**–**f**) are the results in "Pepper", and (**g**–**i**) are the results in "Plane".

5. Conclusions

Network transmission is a vital part of our modern life. With the convenience it brings, information security issues follow. Information hiding has made great progress. Considering the problems of the previous work requires a large number of training databases, has the low hiding rate, and occupies a big space. This work adopts a two-level mechanism, look-up table, and reversible information hiding technology based on high-quality information hiding. Through reversible information hiding, the additional storage and transmission burden is solved. In addition, to further improve the security of the secret message, a new encryption model is designed. Compared with different methods in the experiment, our proposed model achieves high capacity and perfect hiding rate under the premise of ensuring image quality. The robustness is achieved in the attack tests. To verify the security, the PDH analysis is also performed. The test results prove that the method is undetectable by PDH. Therefore, our algorithm can achieve better results in terms of image quality, capacity, and security compared with other methods. The proposed symmetry model is outstanding and efficient.

Furthermore, we can combine different methods with higher capacity and better robustness in future work. In addition, more diverse hash codes or other feature values can be designed to hide the secret message. The method is efficient in the paper, but once an attacker masters our model, hidden information can be extracted or even tampered with.

So, to further improve the security of secret messages, asymmetric mechanisms are also the focus of our future research.

Author Contributions: Conceptualization, X.-X.S. and J.-S.P.; formal analysis, J.-S.P., X.-X.S., V.S. and S.-C.C.; methodology, J.-S.P., X.-X.S., S.-C.C. and H.Y.; validation, J.-S.P., H.Y. and V.S.; writing—original draft preparation, X.-X.S.; writing—review and editing, J.-S.P., X.-X.S., S.-C.C., V.S. and H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

$\mathbf{I}$	Original image
$\mathbf{I}'$	Watermarked image
$\mathbf{S}$	Secret message
$Init_k$	Initial key on the encryption algorithm
Y	One-dimensional sequence used for encryption
y_n	n-th value in Y
μ	System control parameter
e_{jlk}	The k-th eigenvalue in the l-th sub-block
max_e_{jl}	The largest value in all eigenvalues of the l-th sub-block
$\mathbf{B}_{jl}$	The l-th sub-block of j-th block
h_c	Hash code
sum	The length of secret message
p	The pixel value in the image
p_h	The high-level plane
p_l	The low-level plane
w	The number of bits divided in the plane
$\hat{p}_{r,i}$	The predicted pixel value
$p_{r,i}$	The pixel value of the original image at row r and column i
$e_{r,i}$	The error value between the pixel value and the predicted value
T	Threshold
$e'_{r,i}$	The modified error value
$p'_{r,i}$	The modified pixel value
s_i	One bit in secret message S
$I_H(p)$	The average of the information
$C_R(p, p_x)$	Correlation coefficient between p and p_x
p_{uv}	The pixel value in the original image
p'_{uv}	The pixel value in the stego image
rol	The total rows of image
col	the total columns of image
PSO	Particle Swarm Optimization
IWT	Integer Wavelet Transformation
PEE	Prediction Error Expansion
PDH	Pixel Difference Histogram

References

1. Pfleeger, C.P. The fundamentals of information security. *IEEE Softw.* **1997**, *14*, 15–16. [CrossRef]
2. Shelupanov, A.; Evsyutin, O.; Konev, A.; Kostyuchenko, E.; Kruchinin, D.; Nikiforov, D. Information Security Methods—Modern Research Directions. *Symmetry* **2019**, *11*, 150. [CrossRef]
3. Mei, X.S.; Chen, H.T.; Fan, H.Y.; Lu, Z.M.; Yeh, J.h. A Robust Digital Image Watermarking Scheme for Content Protection. *J. Netw. Intell.* **2020**, *5*, 54–61.
4. Zhang, Z.; Chen, S.; Sun, X.; Liang, Y. Trajectory privacy protection based on spatial-time constraints in mobile social networks. *J. Netw. Intell.* **2021**, *6*, 485–499.
5. Sahu, A.K.; Swain, G. A novel n-rightmost bit replacement image steganography technique. *3D Res.* **2019**, *10*, 2. [CrossRef]

6. Muhuri, P.K.; Ashraf, Z.; Goel, S. A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. *Appl. Soft Comput.* **2020**, *92*, 106257. [CrossRef]
7. Song, P.C.; Chu, S.C.; Pan, J.S.; Yang, H. Simplified Phasmatodea population evolution algorithm for optimization. *Complex Intell. Syst.* **2021**, 1–19. [CrossRef]
8. Pan, J.S.; Song, P.C.; Pan, C.A.; Abraham, A. The Phasmatodea Population Evolution Algorithm and Its Application in 5G Heterogeneous Network Downlink Power Allocation Problem. *J. Internet Technol.* **2021**, *22*, 1199–1213.
9. Pan, J.S.; Sun, X.X.; Chu, S.C.; Abraham, A.; Yan, B. Digital watermarking with improved SMS applied for QR code. *Eng. Appl. Artif. Intell.* **2021**, *97*, 104049. [CrossRef]
10. Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 354–362.
11. Luo, H.; Chu, S.C.; Lu, Z.M. Self embedding watermarking using halftoning technique. *Circuits Syst. Signal Process.* **2008**, *27*, 155–170. [CrossRef]
12. Shi, Y.Q.; Li, X.; Zhang, X.; Wu, H.T.; Ma, B. Reversible data hiding: Advances in the past two decades. *IEEE Access* **2016**, *4*, 3210–3237. [CrossRef]
13. Nguyen, T.D.; Le, H.D. A reversible data hiding scheme based on (5, 3) Hamming code using extra information on overlapped pixel blocks of grayscale images. *Multimed. Tools Appl.* **2021**, *80*, 13099–13120. [CrossRef]
14. Linb, C.Y.Y.C.H.; Hua, W.C. Reversible data hiding for high-quality images based on integer wavelet transform. *J. Inf. Hiding Multimed. Signal Process.* **2012**, *3*, 142–150.
15. Honsinger, C.W.; Jones, P.W.; Rabbani, M.; Stoffel, J.C. Lossless Recovery of an Original Image Containing Embedded Data. U.S. Patent 6,278,791, 21 August 2001.
16. Hu, Y.; Lee, H.K.; Li, J. DE-based reversible data hiding with improved overflow location map. *IEEE Trans. Circuits Syst. Video Technol.* **2008**, *19*, 250–260.
17. Faragallah, O.S.; Elaskily, M.A.; Alenezi, A.F.; El-sayed, H.S.; Kelash, H.M. Quadruple histogram shifting-based reversible information hiding approach for digital images. *Multimed. Tools Appl.* **2021**, *80*, 26297–26317. [CrossRef]
18. Weng, S.; Zhao, Y.; Pan, J.S.; Ni, R. A novel reversible watermarking based on an integer transform. In Proceedings of the 2007 IEEE International Conference on Image Processing, San Antonio, TX, USA, 16 September–19 October 2007; Volume 3, p. III-241.
19. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [CrossRef]
20. Alattar, A.M. Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Trans. Image Process.* **2004**, *13*, 1147–1156. [CrossRef] [PubMed]
21. Thodi, D.M.; Rodriguez, J.J. Prediction-error based reversible watermarking. In Proceedings of the 2004 International Conference on Image Processing, ICIP'04, Singapore, 24–27 October 2004; Volume 3, pp. 1549–1552.
22. Tseng, H.W.; Hsieh, C.P. Prediction-based reversible data hiding. *Inf. Sci.* **2009**, *179*, 2460–2469. [CrossRef]
23. Weng, S.; Chu, S.C.; Cai, N.; Zhan, R. Invariability of Mean Value Based Reversible Watermarking. *J. Inf. Hiding Multim. Signal Process.* **2013**, *4*, 90–98.
24. Weng, S.; Zhao, Y.; Ni, R.; Pan, J.S. Lossless data hiding based on prediction-error adjustment. *Sci. China Ser. F Inf. Sci.* **2009**, *52*, 269–275. [CrossRef]
25. Yu, Y.; Lei, M.; Liu, X.; Qu, Z.; Wang, C. Novel zero-watermarking scheme based on DWT-DCT. *China Commun.* **2016**, *13*, 122–126. [CrossRef]
26. Weng, S.; Chen, Y.; Hong, W.; Pan, J.S.; Chang, C.C.; Liu, Y. An improved integer transform combining with an irregular block partition. *Symmetry* **2019**, *11*, 49. [CrossRef]
27. Yan, Y.S.; Cai, H.L.; Yan, B. Data Hiding in Symmetric Circular String Art. *Symmetry* **2020**, *12*, 1227. [CrossRef]
28. Pan, J.S.; Luo, H.; Lu, Z.M. Look-up table based reversible data hiding for error diffused halftone images. *Informatica* **2007**, *18*, 615–628. [CrossRef]
29. Zhou, Z.; Su, Y.; Zhang, Y.; Xia, Z.; Du, S.; Gupta, B.B.; Qi, L. Coverless Information Hiding Based on Probability Graph Learning for Secure Communication in IoT Environment. *IEEE Internet Things J.* **2021**. [CrossRef]
30. Zhou, Z.; Cao, Y.; Wang, M.; Fan, E.; Wu, Q.J. Faster-RCNN Based Robust Coverless Information Hiding System in Cloud Environment. *IEEE Access* **2019**, *7*, 179891. [CrossRef]
31. Zou, L.; Sun, J.; Gao, M.; Wan, W.; Gupta, B.B. A novel coverless information hiding method based on the average pixel value of the sub-images. *Multimed. Tools Appl.* **2019**, *78*, 7965–7980. [CrossRef]
32. Cao, Y.; Zhou, Z.; Sun, X.; Gao, C. Coverless information hiding based on the molecular structure images of material. *Comput. Mater. Contin.* **2018**, *54*, 197–207.
33. Wang, Y.; Wu, B. An intelligent search method of mapping relation for coverless information hiding. *J. Cyber Secur.* **2020**, *5*, 48–61.
34. Abdulsattar, F.S. Towards a high capacity coverless information hiding approach. *Multimed. Tools Appl.* **2021**, *80*, 18821–18837. [CrossRef]
35. Weng, S.; Pan, J.s.; Li, L. Reversible data hiding based on an adaptive pixel-embedding strategy and two-layer embedding. *Inf. Sci.* **2016**, *369*, 144–159. [CrossRef]
36. Wu, T.Y.; Chen, C.M.; Wang, K.H.; Pan, J.S.; Zheng, W.; Chu, S.C.; Roddick, J.F. Security Analysis of Rhee et al.'s Public Encryption with Keyword Search Schemes: A Review. *J. Netw. Intell.* **2018**, *3*, 16–25.
37. Andrecut, M. Logistic map as a random number generator. *Int. J. Mod. Phys. B* **1998**, *12*, 921–930. [CrossRef]

38. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [CrossRef]
39. Li, C.; Xie, T.; Liu, Q.; Cheng, G. Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dyn.* **2014**, *78*, 1545–1551.
40. Elshoush, H.T.; Ali, I.A.; Mahmoud, M.M.; Altigani, A. A novel approach to information hiding technique using ASCII mapping based image steganography. *J. Inf. Hiding Multimed. Signal Process.* **2021**, *12*, 65–82.
41. Zhou, Z.; Wu, Q.J.; Yang, C.N.; Sun, X.; Pan, Z. Coverless image steganography using histograms of oriented gradients-based hashing algorithm. *J. Internet Technol.* **2017**, *18*, 1177–1184.
42. Zhang, X.; Peng, F.; Long, M. Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Trans. Multimed.* **2018**, *20*, 3223–3238. [CrossRef]
43. Sahu, A.K.; Swain, G. Reversible image steganography using dual-layer LSB matching. *Sens. Imaging* **2020**, *21*, 1–21. [CrossRef]
44. Pradhan, A.; Sahu, A.K.; Swain, G.; Sekhar, K.R. Performance evaluation parameters of image steganography techniques. In Proceedings of the 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), Bangalore, India, 6–7 May 2016; pp. 1–8.
45. Swain, G. Very high capacity image steganography technique using quotient value differencing and LSB substitution. *Arab. J. Sci. Eng.* **2019**, *44*, 2995–3004. [CrossRef]