electronics

MDPI

Article

Thumbnail-Preserving Encryption Technology Based on Digital Processing

Dan Li, Ziming Zhang, Xu Dai and Erfu Wang *

School of Electronic Engineering, Heilongjiang University, Harbin 150080, China; 2221783@s.hlju.edu.cn (D.L.); 2211730@s.hlju.edu.cn (Z.Z.); 2221717@s.hlju.edu.cn (X.D.)
* Correspondence: wangerfu@hlju.edu.cn

Abstract: In recent years, the security of cloud storage has become a topic attracting significant attention due to a series of features such as large storage space, high availability, and low cost. Although traditional plain text images can withstand external attacks, the usability of images is completely lost. In order to balance the usability and privacy of images, some scholars have proposed the thumbnail-preserving encryption (TPE) scheme. The ideal TPE algorithm can keep the same thumbnail before and after encryption, which reduces the time cost and strengthens the resistance to attacks, but the existing schemes cannot fulfill the above criteria. In this paper, we propose a new TPE scheme that combines bit-transform encryption and improved hierarchical encryption. By constructing a chaotic system, both encryption and decryption times are shortened, while the randomness of the selected cells is enhanced. In addition, the Hamming distance is introduced to classify and scramble the binary encryption units. The experimental results show that when the number of thumbnail chunks is 16 × 16, the encryption and decryption time decreases to 4 s, and the SSIM value after encryption is close to 1, which indicates that the thumbnail before and after satisfying the encryption basically remains the same, and when the number of chunks is gradually increased, the success rate of the face detection tends to be close to 0. In addition, as the number of experimental iterations increases, the encryption effect improves with an increasing ability to resist attacks.

Keywords: visual usability; privacy; image encryption; pixel self-transforming; chaotic system

check for updates

Citation: Li, D.; Zhang, Z.; Dai, X.; Wang, E. Thumbnail-Preserving Encryption Technology Based on Digital Processing. *Electronics* **2024**, *13*, 2682. https://doi.org/10.3390/electronics13142682

Academic Editor: Stefanos Kollias

Received: 28 May 2024
Revised: 26 June 2024
Accepted: 1 July 2024
Published: 9 July 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the rapid development and wide application of the Internet and smartphones, people are increasingly relying on these technologies for information exchange. However, the convenience brought from the public transmission also brings a series of security problems, including data leakage, tampering and forgery [1,2]. The popularity of terminal devices and the rise of short video forms have brought cloud storage into the public's view, and more and more image data in different fields are stored and disseminated in the cloud due to the fact that storing files in the cloud space can realize the release of cell phone memory, provide a larger storage space, and reduce the characteristics of file damage and loss due to the damage of hardware equipment or improper placement [3–5]. According to data statistics, more than 1.8 billion photos are shared on social networking platforms every day [6]. However, there are some risks associated with storing data in the cloud. Attackers may use illegal tools to steal cloud data, and even secure websites labeled on the web cannot be fully trusted [7–9]. In 2014, hackers used phishing to trick celebrities into entering their iCloud account credentials into a fake secure website, which resulted in the acquisition of private photos and videos of more than 300 victims and their public dissemination on the web [10–12]. Since April 2022, the North Korean hacker group Lazarus used NukeSped to install additional console-based information-stealing malware to collect information stored on web browsers. Additionally, insiders may have illegally

accessed the data, resulting in a massive personal data breach [13,14]. On 18 February 2024, a misconfiguration incident on the cloud storage servers of automotive giant BMW resulted in the exposure of sensitive information such as private keys and internal data. Although timely modifications have been made, much of the information has been seen by many netizens [15]. It can be seen that cloud storage, despite its high availability, convenience, and a host of other features, poses certain privacy risks [16–18].

The ciphertext image generated by traditional image encryption is usually a noise-like image, which completely loses the details and structural features of the original image. Although it ensures the security of the image in the transmission process, the usability of the image is completely lost [19]. The encrypted image is not only inaccessible to the attacker but also makes it impossible for the user to extract useful information, which increases the time and cost of decryption. Therefore, while realizing image encryption to ensure security, a certain degree of usability of the image should be retained. As shown in Figure 1, some scholars proposed the thumbnail-preserving encryption (TPE) for the first time, i.e., the encrypted thumbnail and the original image have the same thumbnail attributes [20].

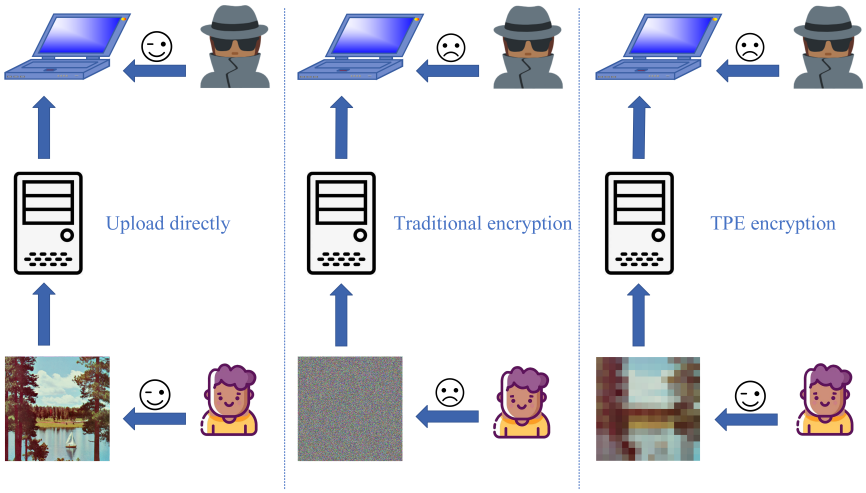


Figure 1. The left side is the original image uploaded to the cloud, which can be accessed directly by both the user and the outside; the center is the traditional encrypted image uploaded to the cloud, which cannot be accessed by the user or the outside; and the right side is the uploaded to the cloud after the TPE scheme, which can be accessed by the user but not by the outside.

1.1. Related Works

In 2015, Wright et al. [21] divided the image into equal blocks and implemented the pixel value substitution operation independently within each block so that only the pixel value position change occurs within the block after the operation, thus achieving encryption, but this approach has a significant drawback in that the encrypted image is easily decrypted. In 2017, Marohn et al. [22] proposed two approximate TPE schemes, namely dynamic range preserving encryption and least significant bit based embedding, but the thumbnail generated from the ciphertext image differs significantly from the thumbnail of the plain text image, which reduces the usability of the ciphertext image. In 2019, Tajik et al. [23] proposed a new scheme for constructing an ideal TPE, and for the first time proposed to transform the encryption unit by a rank function, but the experiment requires calling a large number of pseudo-random functions to enhance the resistance to resistance attacks, which leads to inefficient encryption. In 2022, Zhang et al. [24] proposed the first TPE scheme based on a chaotic system, which not only shortens the encryption and decryption time but also realizes lossless decryption, but the scheme takes the neighboring pixels as the encryption unit during the encryption process. These neighboring pixels lead to insufficient anti-attack ability, and they also need to be encrypted after several rounds to

achieve better security. A comparative analysis of the encryption performance metrics for the currently available schemes is presented in Table 1 [25].

Table 1. An analysis of the advantages and disadvantages of existing programs is warranted.

Scheme	Wright [21]	Marohn [22]	Tajik [23]	Zhang [24]
Robustness against attacks	No Ideal	No Ideal	Ideal	No Ideal
Time cost	Quick	Quick	Slow	Very Slow
Quality of encrypted image	Ideal	No Ideal	No Ideal	Ideal
Image availability	Ideal	No Ideal	Ideal	Ideal
Decryption success rate	100%	100%	100%	100%

1.2. Contribution and Motivation

Based on this, we propose a bit-transform encryption scheme combined with the improved RANK encryption algorithm for the following reasons: the encryption scheme needs to introduce enough randomness to resist the attack; the chaotic system has the characteristics of unpredictability, initial value sensitivity, etc., and the one-dimensional chaotic mapping contains fewer parameters and variables; and the capacity of the key space is small, which results in the system being easily cracked and the problem of lower security [26]. Multi-dimensional chaotic mapping contains more variables and parameters, more complex structures, and better chaotic performance, but there are problems such as high computational cost and complex performance analysis. Therefore, we choose to construct a two-dimensional chaotic system for testing in the experiments to ensure that the chaotic performance is improved while reducing certain computational costs. Through in-depth analysis of the connection between TPE and the 2D chaotic system, a chaotic random sequence is generated to enhance the randomness of the selected encryption unit. The number of encryption iteration rounds is effectively reduced to ensure the security of the encrypted image; the concept of Hamming distance is introduced, and the encrypted units are divided into two categories by judging the size of the Hamming distance, which are scrambled and encrypted using the above algorithm, respectively. After encryption, it is tested and proved that the scheme can guarantee the security of the ciphertext image and reduce the time cost.

The main contributions of this paper are as follows:

(1) Combining a chaotic system and TPE to design a 2D chaotic system, and realizing the random selection of encryption units through chaotic sequences to avoid insufficient resistance to attacks due to the formation of encryption units by neighboring pixels.
(2) Proposing the bit transform encryption scheme, introducing the Hamming distance for the first time, classifying the encryption unit by judging the size of the Hamming distance, and realizing the scrambled encryption, respectively. The ciphertext image after encryption has good resistance to attacks, the ciphertext image has the same pixel sum with the plain text image, and the thumbnails before and after encryption are the same, which has good usability.
(3) The traditional rank encryption algorithm is improved, and the randomness of the encryption process is enhanced by generating random numbers through chaos to realize the disarrayed encryption, which effectively reduces the number of encryption iterations, decreases the encryption and decryption time, and decrypts the encrypted image without loss.

2. TPE Description

In order to balance the availability and privacy in cloud images, scholars have researched and implemented TPE schemes, and the ensuing issue to be considered becomes whether the images are secure in cloud storage.

The essence of the TPE scheme is that the encrypted image and the original image share an identical thumbnail. Figure 2 illustrates the fundamental concept of thumbnail-preserving encryption, and its detailed structure is described as follows:

The specific operation is as follows:

(1) An RGB image of size $I_1 \times I_2$ is selected and divided into three channels, each containing a two-dimensional matrix composed of pixel values $[0, d](d \leq 255)$, which has a size of $I_1 \times I_2$.
(2) A two-dimensional matrix of size $I_1 \times I_2$ is divided into blocks of size $b \times b$, where I_1 and I_2 are divisible by b. Each channel contains $\frac{I_1}{b} \times \frac{I_2}{b}$ blocks.
(3) Calculate the average value within each pixel block denoted as $\{\overrightarrow{v_1}, \overrightarrow{v_2} \ldots \overrightarrow{v_{b \times b}}\}$. The encrypted thumbnail contains only $\frac{I_1}{b} \times \frac{I_2}{b}$. pixel values, and the pixel values in each block are replaced by the average value.

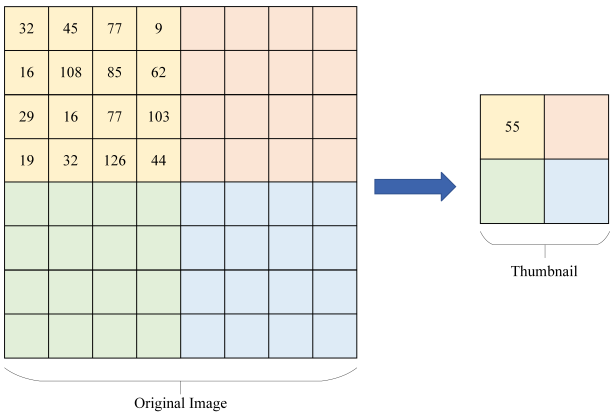


Figure 2. Core program for the generation of thumbnail images.

The above method shows that the original image is partitioned into blocks, and if the sum of pixel values within each block remains unchanged before and after encryption, the thumbnail will also be consistent with the original thumbnail, and this kind of encryption is a special case of format-preserving encryption (FPE) defined by Bellare et al. [20], which is recorded as the preserve and encrypt method.

Let M represent the plain text space. The function ϕ is defined arbitrarily to retain the attributes of M, resulting in a thumbnail image as the output. When the input picture P is provided, a key $K = \{0,1\}^{\lambda}$, $P \in M, \phi(P) = \phi(M)$ is utilized at this time. The encryption algorithm Enc_K is represented by Equation (1), the decryption algorithm Dec_K is represented by Equation (2), and the encryption scheme that preserves ϕ is represented by Equation (3).

$$Enc_K(P, M) \in M \tag{1}$$

$$Dec_K(P, Enc_K(P, M)) = M \tag{2}$$

$$\phi(Enc_K(P, M)) = \phi(M) \tag{3}$$

3. TPE Construction

In the encryption scheme proposed by Tajik et al., 2019 [23], adjacent pixel points are selected to form the encryption unit, but this scheme needs to call the random function several times to enhance the randomness to ensure that the encryption has a better resistance to attacks. However, calling the function increases the computational cost and leads to long and inefficient encryption time. Based on this, in the experiment, we classify the encryption unit by judging the Hamming distance of the selected encryption unit. We

design a two-dimensional chaotic system instead of the random function to enhance the randomness, reduce the number of encryption rounds required in the experiment, and combine the bit self-transform encryption with the sum-preserving encryption algorithm so that the thumbnails are the same before and after the encryption of the image. The specific encryption process is shown in Figure 3.

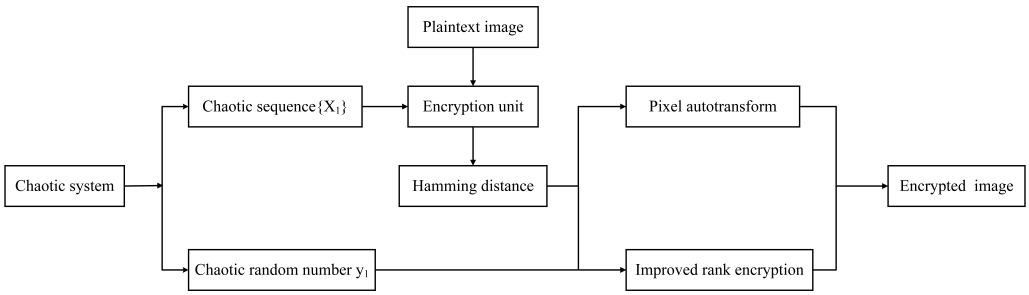


Figure 3. A scheme diagram for preserving thumbnail encryption.

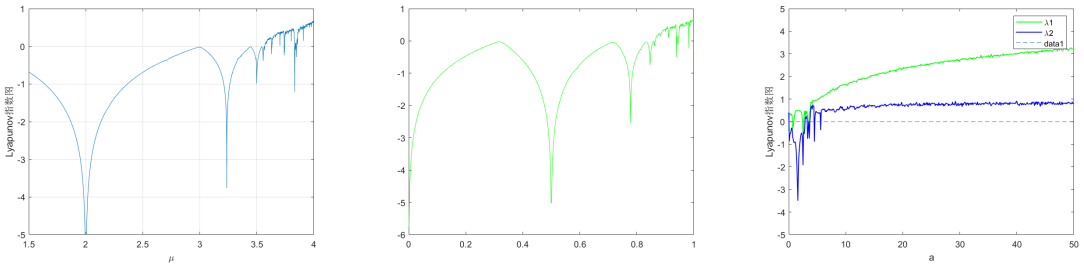
3.1. Chaotic System

One-dimensional chaotic systems exhibit simple chaotic orbits and a small chaos space, making them relatively straightforward to predict. This is in contrast to two-dimensional chaotic systems, which are more complex and difficult to predict [27,28]. Based on these observations, one-dimensional chaotic systems can be transformed into two-dimensional chaotic systems through the coupling of logistic mapping and sine mapping. The resulting chaotic system exhibits excellent dynamics characteristics.

$$\begin{cases} x_{n+1} = u_1 \sin[\pi x_n + a(y_n - x_n)] \\ y_{n+1} = u_2 \sin[\pi y_n + a(x_n - y_n)] \end{cases} \tag{4}$$

3.1.1. Lyapunov Exponent

The Lyapunov exponent is considered to be one of the most important metrics for evaluating the dynamic properties of chaotic systems. It is defined as the average exponential rate of convergence or divergence of neighboring orbits of the system in phase space. A system with a positive Lyapunov exponent is considered to have chaotic properties [29]. In Figure 4, the initial values of $u_1 = 0.80$ and $u_2 = 0.95$ are set, and the system remains hyperchaotic with a positive Lyapunov exponent for $a > 5.7$.



(**a**) Logistic. (**b**) Sine. (**c**) logistic-sine.

Figure 4. Lyapunov exponent map of chaotic systems before and after coupling.

3.1.2. Bifurcation Diagram

Bifurcation diagrams illustrate the manner in which the trajectory of a dynamic system varies with the control parameters. The greater the uniformity of the trajectory of the bifurcation diagram, the more stable the chaotic system will be. The distribution of the system's parameters across the bifurcation diagram is presented here. The bifurcation diagram for this chaotic system is depicted in Figure 5. It can be observed that the desired chaotic effect can be achieved when the system is within the parameter range.

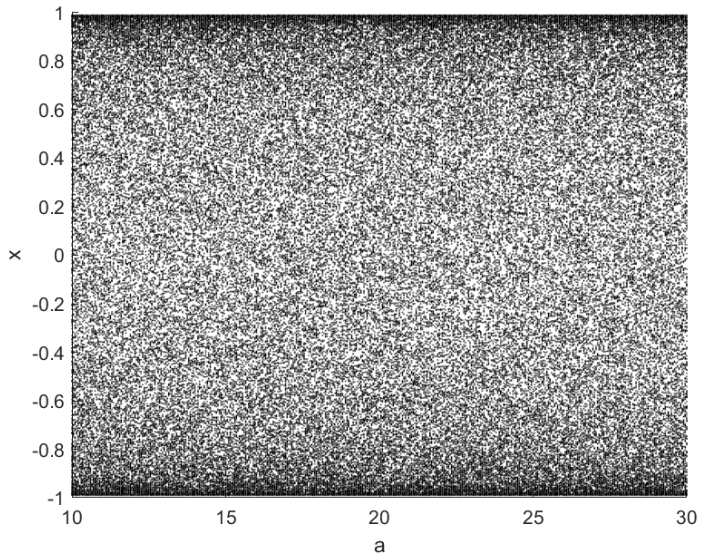


Figure 5. Bifurcation diagrams.

3.1.3. NIST SP-800-22 Statistical Tests

In order to further verify the randomness of chaotic sequences generated by chaotic systems, the randomness of chaotic sequences x_{n+1} and y_{n+1} is tested using SP800-22 given by NIST, using 100 binary sequences of 500,000 bits to complete 15 sub-items of the test, and it can be considered to pass the test when the value of test result P_{value} is greater than the threshold value a = 0.01. From the test results of x_{n+1} and y_{n+1} sequences in Table 2, it can be seen that the randomness of the chaotic sequences generated by the chaotic system meets the requirements, the periodicity is long enough, and the complexity is high enough, which can be applied to image encryption.

Table 2. NIST statistical test results for sequence x and sequence y.

Statistical Index	Passing Ratio (x)	*p*-Value (x)	Passing Ratio (y)	*p*-Value (y)
Frequency	0.98	0.7598	0.98	0.1088
Rank	0.99	0.5749	0.99	0.5955
FFT	0.98	0.0628	0.99	0.6579
Runs	0.98	0.0965	0.99	0.2493
Serial	0.99	0.9463	0.98	0.3838
Block frequency	0.99	0.1719	0.97	0.9943
Cumulative sums	0.99	0.3669	0.98	0.5749
Linear complexity	0.98	0.3191	0.99	0.4944
Longest runs of ones	0.99	0.8514	0.97	0.6579
Random excursions	0.98	0.8832	0.98	0.7565
Random excursions variant	0.98	0.7791	0.98	0.8195
Approximate entropy	0.99	0.5341	0.97	0.8977
Overlapping template of all ones	0.96	0.1538	0.97	0.3345
Block frequency	0.99	0.1719	0.97	0.9943
Universal statistical	0.98	0.4372	0.98	0.1719

3.1.4. Generate Random Sequence

A set of chaotic random sequences X_1 is generated by coupling the formed two-dimensional chaotic system, and the first 10,000 bits of the generated sequences are omitted due to the transient nature of chaotic systems. The generated random sequences are converted into integers between [1, $b \times b$], as shown in Equation (5). The generated X_{temp} is equal in length to $b \times b$, and during subsequent experiments, different encryptions are realized for each pixel block by the generated random decimal y_1:

$$X_{temp} = [fix(X_1 * 10^5) \bmod b^2] + 1 \tag{5}$$

In addition, the generated chaotic sequence is to ensure the randomness of the selected encryption unit, and its generated chaotic sequence is subject to the initial value and a change. The specific process is shown in Algorithm 1.

Algorithm 1 Chaotic selection of random sequences and random values.

Input: y_n, x_n and a
Output: X_{temp}, y_1
1: **for** $n = 1 : N - 1$ **do**
2: $x_{n+1} = u_1 \sin[\pi x_n + a(y_n - x_n)]$
3: $y_{n+1} = u_2 \sin[\pi y_n + a(x_n - y_n)]$
4: **end for**
5: $x_1 = x_{n+1}$
6: $x_{temp} = [\text{fix}(x_1 * 10^5) \bmod b^2] + 1$
7: $idx = \text{rand}(1, N)$
8: $y_1 = y_{n+1}[idx]$
9: **return** Outputs

3.2. Pixel Self-Transforming Encryption Scheme

Tajik et al. [23] proposed a perfect TPE scheme in their paper, in which the core of their scheme is to realize the sum-preserving encryption operation through a pair of encryption and decryption functions $rank(\cdot)$ and $rank^{-1}(\cdot)$, but the scheme only replaces the neighboring pixels, which is computationally expensive and inefficient, and it is poorly resistant to resisting attacks. Based on these issues, for the first time, it is proposed to group the randomly selected pixel units by using the Hamming distance in experiments, and the pixels are grouped through pixel grouping for multiple rounds of encryption of different pixel units. The following is the pixel bit transform encryption scheme:

(1) Input size is $w * h$ image P; first, determine the size of the thumbnail block as $b * b$; then, according to the random sequence X_{temp} generated by X_1, randomly select points within the pixel block of $b * b$; the selected pixel pairs are denoted as $\left\{L_1, L_2 \cdots L_{\frac{b*b}{2}}\right\}$; each pixel pair is denoted as an encrypted unit $\overrightarrow{e}$; and the selected pixel points are denoted as (p_1, p_2).

(2) The selected pixels can be expanded into 8-bit binary numbers, of which the order from left to right is a_7–a_0, i.e., the highest valid bit to the lowest valid bit. The Hamming distance between the encryption units is recorded as $d_{(p_1,p_2)}$ after the expansion.

(3) When $d_{(p_1,p_2)} \geq 2$, judge whether the highest different bit and the second highest different bit are equal; when the two are not the same, the highest bit and the second highest bit will be self-swapped to ensure that the sum of pixel values before and after the swap is unchanged. The encryption process is shown in Figure 6.

The encryption algorithm is subject to the constraints of the encryption unit $\overrightarrow{e}$ corresponding to the generation of the Hamming distance $d_{(p_1,p_2)}$. In both encryption and decryption processes, it is necessary to satisfy the two conditions of $d_{(p_1,p_2)} \geq 2$, and the highest bit of the second-highest bit is different, and its encryption algorithm flow is shown in Algorithm 2.

Algorithm 2 Bit transformation encryption algorithm.

Input: p_1, p_2 and P
Output: (p_1', p_2')

```
(w, h) = params(P)
for i = 1 : w do
    for j = 1 : h do
        d = HammingDistance(p1, p2)
        if d ≥ 2 and MSB is inequal to SMSB then
            Swap the highest and second highest different bits
        end if
    end for
end for
return Outputs
```

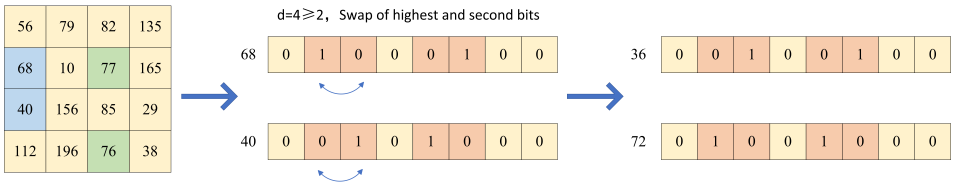


Figure 6. Pixel bit self-transformation encryption scheme.

3.3. Improved Rank Encryption Scheme

On this basis, this algorithm combines TPE with a 2D chaotic system, and it introduces the improved rank encryption algorithm when the Hamming distance $d_{(p_1,p_2)} \leq 2$ or the highest sub-high bit is the same. The encryption scheme is shown in Figure 7.

(1) When $d_{(p_1,p_2)} \leq 2$ or the highest bit of the next highest bit is the same, the selected pixel pair constitutes the encryption unit $\overrightarrow{e} = (p_1, p_2)$; $|\Omega_{sum(s)}|$ denotes the number of encryption units with the same pixel sum. The formula is shown in Equation (6), in which $|\Omega_{sum(s)}|$ and $(p_1, p_2) \neq (p_2, p_1)$ indicate that the encryption unit is ordered.

$$|\Omega_{sum(s)}| = \begin{cases} s+1 & s \leq \mathrm{d} \\ 2*d-s+1 & otherwise \end{cases} \tag{6}$$

(2) Define the $rank(\cdot)$ function, which corresponds to the output k_0 when the encryption unit $\overrightarrow{e}$ is input.

$$rank(p_1, p_2) = \begin{cases} p_1 & s \leq d \\ p_1 - s + d & otherwise \end{cases} \tag{7}$$

(3) k_e is encrypted by k_0.

$$k_e = k_0 + (y_1 * 10^5) \bmod \left|\Omega_{sum(s)}\right| \tag{8}$$

(4) Define the function $rank^{-1}(\cdot)$ as the inverse function of $rank(\cdot)$, and input the generated k_e value to generate the corresponding encryption unit.

$$rank^{-1}(k_e) = \begin{cases} (k_e, s-k_e) & s \leq d \\ (s-d+k_e, d-k_e) & otherwise \end{cases} \tag{9}$$

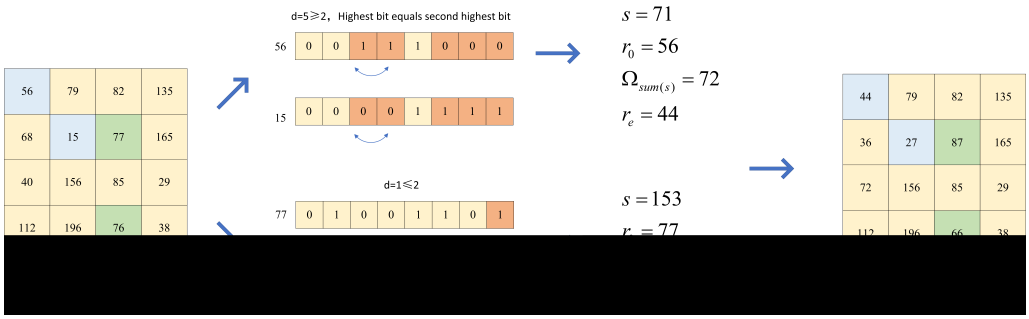


Figure 7. Rank encryption scheme after Hamming distance segmentation.

The improved rank encryption algorithm effectively combines the two-dimensional chaotic system. It generates random encryption units and determines their Hamming distance in step 1, defines the encryption process of the rank function in step 2, achieves different encryption in different blocks by combining the random values generated by the chaotic system in step 3, and iterates through all the pixel points in the pixel blocks during the encryption process. The encryption algorithm flow is shown in Algorithm 3. The image decryption operation is similar but opposite to the encryption operation.

Algorithm 3 Rank encryption algorithm.

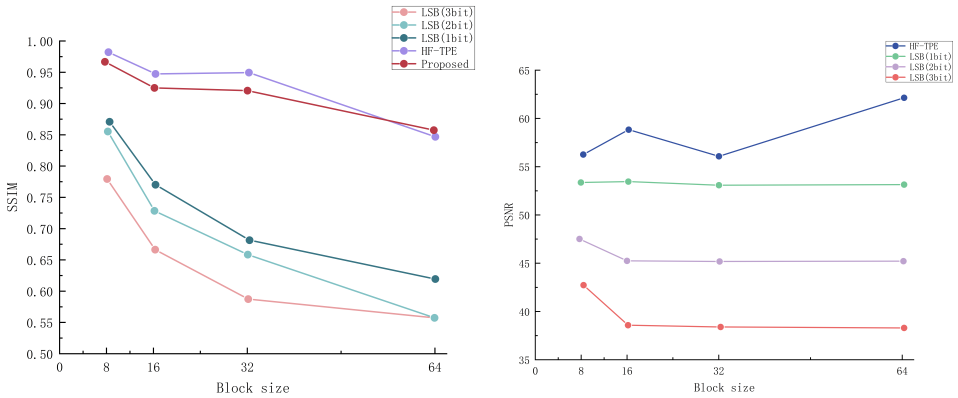
Input: p_1, p_2 and P
Output: $(p_1{}', p_2{}')$
1: $(w, h) = params(P)$
2: **for** $i = 1 : w$ **do**
3: **for** $j = 1 : h$ **do**
4: $d = HammingDistance(p_1, p_2)$
5: **if** $d \leq 2$ and MSB is inequal to SMSB **then**
6: The $\left|\Omega_{sum(s)}\right|$ is calculated as (6)
7: The output k_0 can be obtained by (7)
8: k_e can be further derived using (8)
9: $rank^{-1}(k_e)$ generated through (9)
10: **end if**
11: **end for**
12: **end for**
13: **return** Outputs

4. Experiment

In order to compare the performance metrics of the proposed scheme with the existing schemes, a series of experiments such as image quality analysis before and after encryption, expansion rate analysis, adjacent pixel correlation, histogram analysis, and resistance to attacks of the encrypted image are selected to evaluate the proposed scheme, and the images selected for the experiments are uniformly PNG images with a pixel size of 512 × 512.

4.1. Image Quality Analysis

In order to evaluate the quality of the images before and after encryption and decryption, the experiments utilize structural similarity (SSIM) to assess the encrypted image and the peak signal-to-noise ratio (PSNR) to evaluate the decrypted image for distortion. A larger SSIM value and PSNR value indicate a smaller degree of image distortion. The algorithm generates the same thumbnail image before and after encryption with an SSIM value close to 1, which is an ideal state. In contrast, although the encryption values of LSB-TPE and HF-TPE are greater than 0.94, the decrypted images are distorted. Since the scheme is lossless decryption, the PSNR value of the decrypted image is infinite, as shown in Figure 8 below.

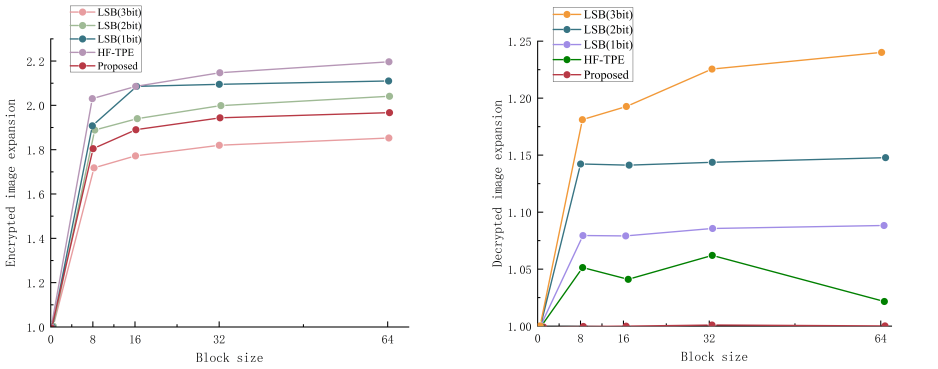


(**a**) The SSIM of encrypted image (**b**) The PSNR of decrypted image

Figure 8. Image quality analysis before and after encryption and decryption.

4.2. Image Size Expansion

Encrypted image size is very important for image storage in the cloud; when the encrypted image occupies too much space, it will affect the image transmission and preview time. In this section, we measure the degree of expansion by the ratio of the encrypted image size to the original image size. If the value is 1, it means the encrypted image is not expanded. The expansion rate of this scheme is between 1.8 and 1.9, which effectively reduces the expansion rate of the image compared to the currently existing schemes. Since the scheme is lossless decryption, no expansion occurs in the decrypted image, i.e., the expansion rate is always 1, as shown in Figure 9.



(**a**) The encrypted image expansion ratio (**b**) The decrypted image expansion ratio

Figure 9. Analysis of image expansion rate before and after encryption and decryption.

4.3. Correlation Analysis

The adjacent pixel correlation method was employed to assess the correlation between neighboring pixels in an image. For this analysis, a 512 × 512 image containing a 16 × 16 pixel thumbnail block was selected. From this image, 5000 pairs of adjacent pixels were randomly chosen for correlation analysis in three directions: horizontal, vertical, and diagonal. As illustrated in Figure 10, the R, G and B channels of the plain text image exhibit a high degree of correlation in all three directions with pixel pairs closely clustered along a line. In contrast, the pixel pairs in the encrypted image are widely dispersed, leading to a significant reduction in correlation coefficients in each direction. This effectively mitigates the risk of statistical attacks.

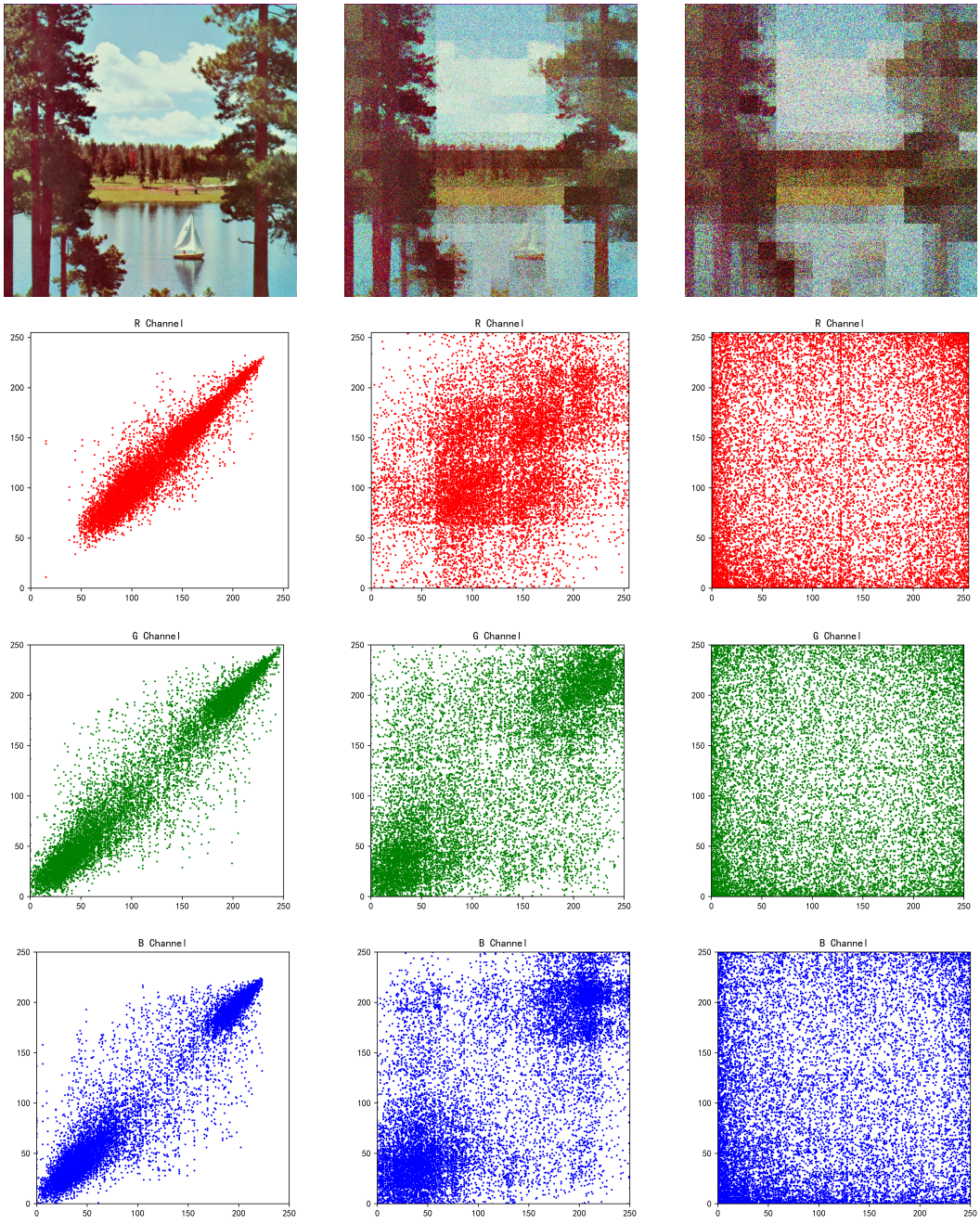
The calculation process of the correlation coefficient is shown in Formula (10). In the traditional encryption process, the correlation coefficients in the three directions after encryption should be close to 0 [30], while in the process of preserving thumbnail encryption, a certain correlation should be retained between the encrypted image pixels [31], as

shown in Table 3. where $\mathrm{cov}(x, y)$ and $D(x)$ represent the covariance and variance of pixel values, respectively.

$$R_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{10}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{11}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{12}$$



(**a**) plaintext image (**b**) Round 10 (**c**) Round 100

Figure 10. Correlation distribution of encrypted images with different number of rounds.

Table 3. Correlation analysis.

Image	Horizontal	Vertical	Diagonal
Plaintext	0.9651	0.9626	0.9501
Thumbnail	0.3438	0.3440	0.3481
Baboon	0.8926	0.8347	0.8047
Thumbnail	0.1486	0.1575	0.1480
Peppers	0.9668	0.9684	0.9599
Thumbnail	0.2153	0.2112	0.2189

4.4. Histogram Analysis

The histogram is a fundamental metric utilized to analyze the statistical properties of an image, and it has the objective of estimating the resistance of the image to a statistical analysis attack. This relates to the ability of the password to statistically break the statistical patterns of the cipher text and plain text. The experiment analyzes the histograms of the cipher text image and the plain text image, demonstrating how the distribution of each gray value in the image is visualized. The histogram of the plain text image exhibits a discernible statistical pattern and an uneven distribution across each channel. Upon statistical analysis of the intercepted cipher text image, the attacker identifies and compares the statistical patterns among them with those of the plain text. This process enables the extraction of a transformational relationship between the plain text image and the cipher text image, which is then leveraged to attack the encryption scheme and achieve the attack objective. This mode is known to not only make the histogram of a cipher text image in each channel gradually become uniform but also ensure a significant difference still exists between the cipher text and the plain text image. In order to analyze the resistance of the encryption scheme to an attack based on statistical analysis, the iterative graph variance must be considered. The histogram of the image after encryption must be as uniform as possible for statistical analysis attacks. The variance of a histogram can be employed to assess the resilience of an encryption algorithm to statistical analysis attacks. A lower variance indicates a more uniform distribution of pixels, which in turn implies reduced statistical information content in the image. This represents a more robust improvement in the secure image scheme encryption. During the experiments, we tested on a test set that included an image file with a pixel value size of 512 × 512. This is demonstrated in Figure 11, which presents the histograms of the distribution of the original image in R, G and B after both ten and one hundred iterations.

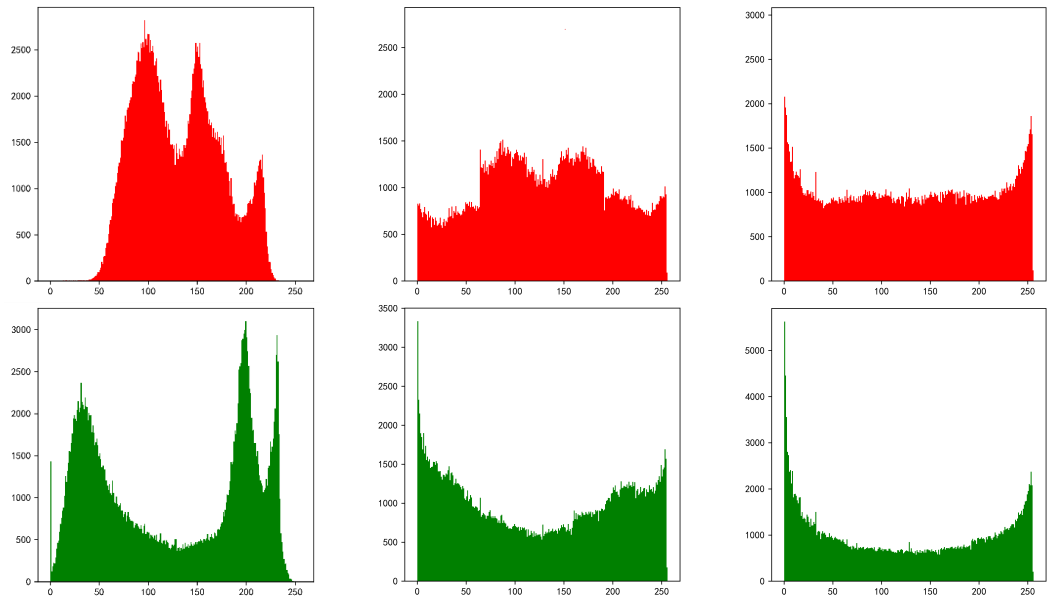
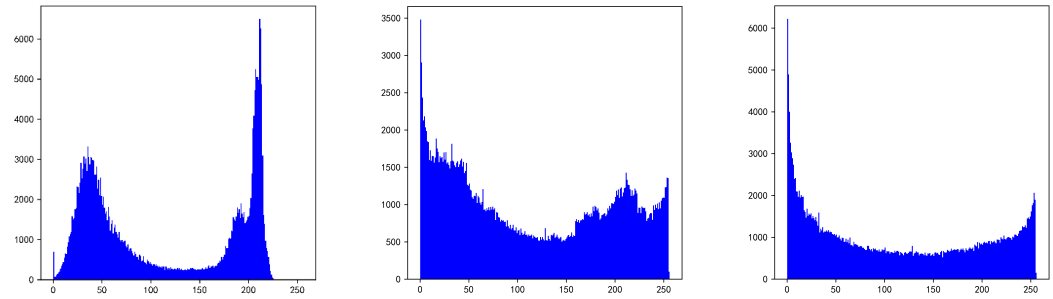


Figure 11. *Cont.*



(**d**) Plain text image (**e**) Round 10 (**f**) Round 100

Figure 11. Histogram analysis of R,G and B channels with different number of rounds

4.5. Face Detection

The TPE technique is a balance between availability and privacy, but the security of the images stored in the cloud is still a concern. In Figure 12, we encrypt the original images in different block sizes, and the images gradually lose their availability as the number of blocks increases. In our experiments, we select the first 500 images in the HELEN face dataset [32], use the face detection API algorithm in the Face++ platform to experiment on them, and compare them with the HF-TPE [24], TPE2 [33] scheme. The results of the experiments are shown in Figure 13, from which it can be concluded that the encryption scheme proposed in this paper has similar results to the above schemes, and with the increase in the chunks of the image, the success rate of the face detection decreases continuously, and when the image chunks are 32×32, the detection success rate tends to be close to 0.

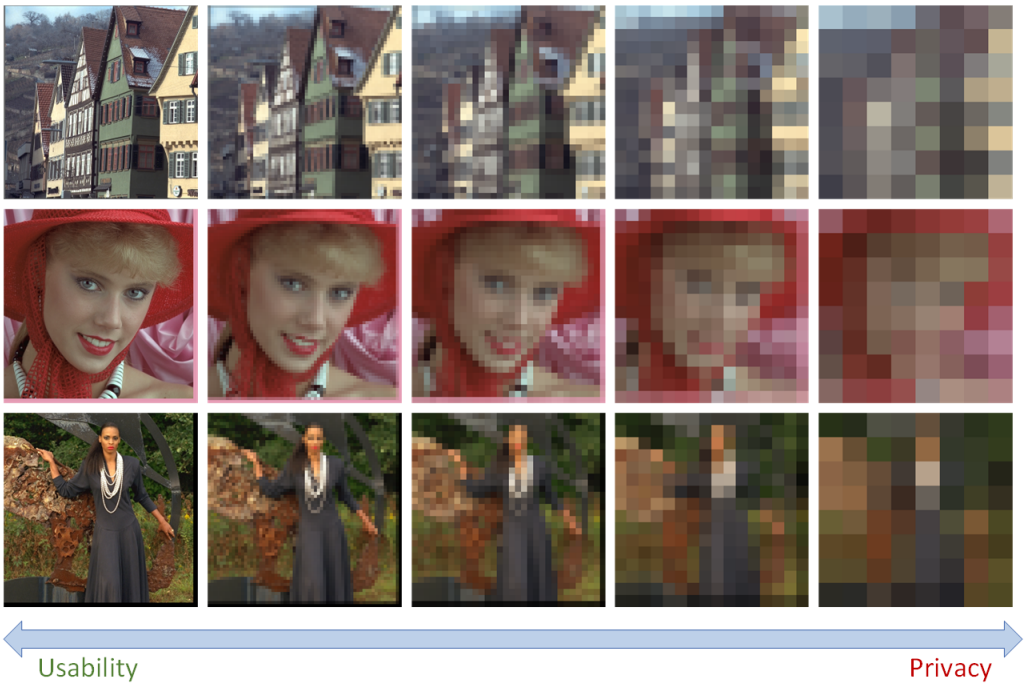


Figure 12. Analysis of availability and privacy after encryption with different block sizes.

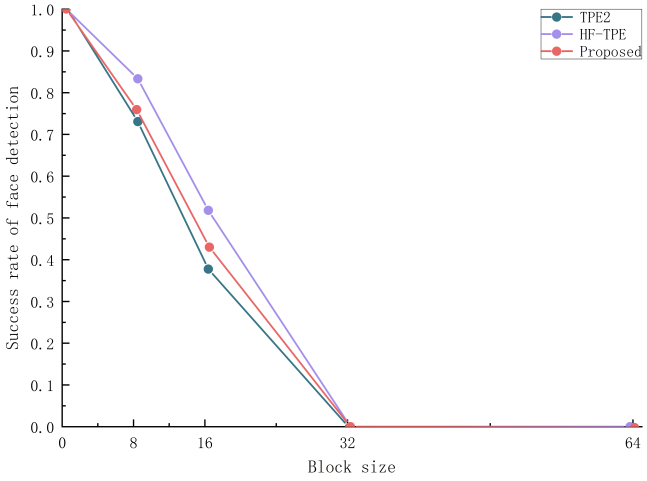
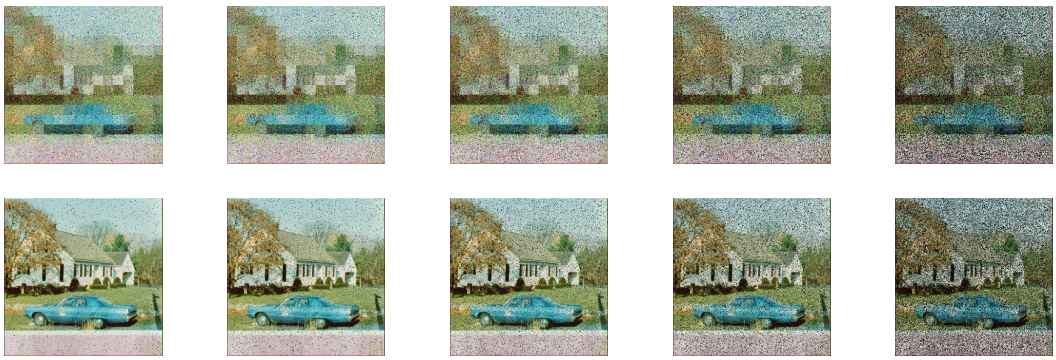


Figure 13. The success rate of face detection.

4.6. Robustness Analysis

Due to the inevitable influence of various factors during transmission, including noise, distortion, and those caused by noisy communication, degradation, and pollution, the encrypted images are subject to alteration. Consequently, the image encryption algorithm must be sufficiently robust to withstand attacks in real-world scenarios. In this experiment, the encrypted image was subjected to a loss of pixels at random with the percentage of loss ranging from 2% to 32%. The results are presented in Figure 14. The image demonstrates that the attacked TPE image and the decrypted image are darkened overall. However, the information contained in the image prior to the attack is still discernible, indicating that the scheme exhibits robust resilience.



(**a**) 2% (**b**) 4% (**c**) 8% (**d**) 16% (**e**) 32%

Figure 14. The example image of data loss.

4.7. Time Cost

The efficiency of image encryption in terms of time is a crucial metric, and this section will address it. We compare the results with those of Tajik [23] et al., the HF-TPE proposed by Zhang [24,34] et al., and the scheme of Zhu [35] et al., as they use the same encryption algorithm that was proposed in this paper, which uses two pixel points as a unit to achieve disambiguation encryption. Table 4 gives the time taken by the scheme proposed in this paper and the other schemes, and the test metrics contain four metrics: average time, maximum time taken, minimum time taken, and standard deviation. After comparison, the encryption time increases slightly as the number of chunks increases, and the encryption time is stable. The decryption time is not listed for any of the above schemes because the decryption time is approximately the same as the encryption time.

Table 4. Different methods of time cost.

		Average Time (s)	Standard Deviation (s)	Maximum Time (s)	Minimum Time (s)
Proposed	16 × 16	4.8695	0.0939	5.0763	4.7551
	32 × 32	5.3535	0.1411	5.7308	5.2091
	64 × 64	5.6904	0.2069	5.8256	5.4285
Tajik [23]	16 × 16	92.1738	0.1693	6.5912	6.1683
	32 × 32	93.9273	0.0499	5.664	5.5274
	64 × 64	93.3785	0.0528	5.8009	5.6521
HF-TPE [24]	16 × 16	107.9098	2.8809	115.7901	94.8455
	32 × 32	110.2784	3.0943	120.8373	94.4825
	64 × 64	107.4650	3.9875	127.3896	92.9793
Zhu [35]	16 × 16	6.3087	0.1693	6.5912	6.1683
	32 × 32	5.5833	0.0499	5.664	5.5274
	64 × 64	5.7314	0.0528	5.8009	5.6521

5. Conclusions

In this paper, a novel scheme that combines bit-transform encryption with improved back-rank encryption is proposed. The encryption core of the scheme is to realize the sum-preserving encryption by scrambling code and to design a two-dimensional chaotic system to reduce the encryption cost. In comparison to the outcomes of existing research, this scheme demonstrates that the encryption can generate the same thumbnail as the plain text image and achieve lossless decryption. Furthermore, the encrypted image expansion rate is reduced to within 1.9, effectively preventing the encrypted image from occupying the space of the cloud. The experiments have demonstrated that the three channels can be considered as three distinct parts, each of which can be encrypted independently. In future work, the three channels will be considered as a single entity, and the encryption will be further encrypted by vertical scrambling to break the correlation between the channels and realize cross-plane encryption.

Author Contributions: Conceptualization, D.L. and Z.Z.; methodology, D.L.; software, D.L.; validation, X.D., E.W. and D.L.; investigation, Z.Z., X.D. and E.W.; writing—original draft preparation, D.L.; writing—review and editing, D.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Science Foundation of China (No. 61571181), Heilongjiang Province Postdoctoral Science Foundation under Grant (No. LBH-Q14136), and Heilongjiang Natural Science Foundation (No. JJ2019LH1317).

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

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

References

1. Wang, B.; Zhang, F.; Liu, X.W. An image encryption approach on the basis of a time delay chaotic system. *Optik* **2021**, *225*, 165737–165741. [CrossRef]
2. Yassein, M.B.; Aljawarneh, S.; Wahsheh, Y.A. Survey of Online Social Networks Threats and Solutions. In Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 9–11 April 2019; pp. 375–380.
3. Wang, C.; Zhang, B.; Ren, K. Privacy-assured outsourcing of image reconstruction service in cloud. *IEEE Trans. Emerg. Top. Comput.* **2013**, *1*, 166–177. [CrossRef]

4. Li, S.; Xu, C.; Zhang, Y. CSED: Client-side encrypted deduplication scheme based on proofs of ownership for cloud storage. *J. Inf. Secur. Appl.* **2019**, *46*, 250–258. [CrossRef]
5. Lan, R.; He, J.; Wang, S.; Gu, T.; Luo, X. Integrated chaotic systems for image encryption. *Signal Process.* **2018**, *147*, 133–145. [CrossRef]
6. Chu, W.T.; Lee, K.T.; Luo, W. Predicting the Security Threats of Internet Rumors and Spread of False Information Based on Sociological Principle. *Comput. Stand. Interfaces* **2021**, *73*, 103454. [CrossRef]
7. Zhang, Y.; Xu, C.; Lin, X. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. *IEEE Trans. Cloud Comput.* **2019**, *9*, 923–937. [CrossRef]
8. Hong, J.; Xue, K.; Gai, N. Service Outsourcing in f2c architecture with attribute based anonymous access control and bounded service number. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 1051–1062. [CrossRef]
9. Shen, J.; Zhou, T.; Cao, Z. Protection methods for cloud data security. *J. Comput. Res. Dev.* **2021**, *58*, 20–79.
10. Fallon, R. Celebgate: Two methodological approaches to the 2014 celebrity photo hacks. *Int. Conf. Internet Sci.* **2015**, *32*, 49–60.
11. Yang, C.H.; Weng, C.Y.; Yang, Y.Z. TPEIP: Thumbnail preserving encryption based on sum preserving for image privacy. *J. Inf. Secur. Appl.* **2022**, *70*, 103352. [CrossRef]
12. Marwick, A.E. Scandal or sex crime? gendered privacy and the celebrity nude photo leaks. *Ethics Inf. Technol.* **2017**, *19*, 177–191. [CrossRef]
13. The Cyberspace Detection Engine Is Used to Track the Activities of the Lazarus Organization. Available online: https://www.ahnlab.com/cn/contents/content-center/35229 (accessed on 23 May 2022).
14. Mazzarolo, G.; Casas, J.C.F.; Jurcut, A.D.; Le-Khac, N.A. Protect against unintentional insider threats:The risk of an employee's cyber misconduct on a social media site. In *Cybercrime in Context*; Springer: Cham, Switzerland, 2021; pp. 79–101.
15. BMW Security Lapse Exposed Sensitive Company Information, Researcher Finds. Available online: https://techcrunch.com/2024/02/14/bmw-security-lapse-exposed-sensitive-company-information-researcher-finds/ (accessed on 14 February 2024).
16. Dong, Y.; Sun, L.; Liu, D.; Feng, M.; Miao, T. A survey on data integrity checking in cloud. In Proceedings of the 2018 1st International Cognitive Cities Conference (IC3), Okinawa, Japan, 7–9 August 2018; pp. 109–113.
17. Bian, G.; Fu, Y.; Shao, B.; Zhang, F. Data integrity audit based on data blinding for cloud and fog environment. *IEEE Access* **2022**, *10*, 39743–39751. [CrossRef]
18. Mauch, V.; Kunze, M.; Hillenbrand, M. High performance cloud computing. *Future Gener. Comput. Syst.* **2013**, *29*, 1408–1416. [CrossRef]
19. Qin, C.; Zhou, Q.; Cao, F. lexible lossy compression for selective encrypted image with image inpainting. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *29*, 3341–3355. [CrossRef]
20. Bellare, M.; Ristenpart, T.; Rogaway, P. Format-preserving encryption. In Proceedings of the International Workshop on Selected Areas in Cryptography, Calgary, AB, Canada, 13–14 August 2009; pp. 295–312.
21. Wright, C.V.; Feng W.C.; Liu, F. Thumbnail-preserving encryption for JPEG. In Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, Portland, OR, USA, 17–19 June 2015; pp. 141–146.
22. Marohn, B.; Wright, C.V.; Feng, W.C. Approximate thumbnail preserving encryption. In Proceedings of the Multimedia Privacy and Security, Dallas, TX, USA, 30 October 2017; pp. 33–43.
23. Tajik, K.; Gunasekaran, A.; Dutta, R. Balancing image privacy and usability with thumbnail-preserving encryption. In Proceedings of the Symposium of Network and Distributed Systems Security, San Diego, CA, USA, 27 February 2019.
24. Zhang, Y.; Zhao, R.; Xiao, X.; Lan, R.; Liu, Z.; Zhang, X. HF-TPE: High-fidelity thumbnail-preserving encryption. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 947–961. [CrossRef]
25. Abid, M.; Arslan, S.; Neeraj, K.; Muhammad, N.B. Data security in the Industrial Internet of Things (IIoT) through a triple-image encryption framework leveraging 3-D NEAT, 1DCJ, and 4DHCFO techniques. *Comput. Electr. Eng.* **2024**, *118*, 109354.
26. Ray, A.; Ghosh, D. Another new chaotic system: Bifurcation and chaos control. *Int. J. Bifurc. Chaos* **2020**, *30*, 2050161. [CrossRef]
27. Lazzús, J.A.; Rivera, M.; López-Caraballo, C.H. Parameter Estimation of Lorenz Chaotic System Using a Hybrid Swarm Intelligence Algorithm. *Phys. Lett.* **2016**, *380*, 1164–1171. [CrossRef]
28. Liu, M.; Zhang, S.; Fan, Z. Exponential H ∞ Synchronization and State Estimation for Chaotic Systems Via A Unified Model. *IEEE Trans. Neural Netw. Learn. Syst.* **2013**, *24*, 1114–1126. [PubMed]
29. Jain, A.; Rajpal, N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimed. Tools Appl.* **2016**, *75*, 5455–5472. [CrossRef]
30. Abid, M.; Arslan, S.; Shehzad, A.C.; Moatsum, A.; Abdul, N.K.; Neeraj, K. A time-efficient and noise-resistant cryptosystem based on discrete wavelet transform and chaos theory:An application in image encryption. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 10167–10179.
31. Chang, H.P.; Wang, E.F.; Liu, J. Research on Image Encryption Based on Fractional Seed Chaos Generator and Fractal Theory. *Fractal Fract.* **2023**, *78*, 103590. [CrossRef]
32. Le, V.; Brandt, J.; Lin, Z.; Bourdev, L.; Huang, T.S. Interactive facial feature localization. *Comput. Vis.* **2012**, *183*, 679-692.
33. Zhao, R.; Zhang, Y.; Xiao, X. TPE2: Three-pixel exact thumbnail preserving image encryption. *Signal Process.* **2021**, *183*, 108019. [CrossRef]

34. Zhang, Y.; Zhao, R.; Zhang, Y. High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 2993–3010. [CrossRef]
35. Zhu, Z.W.; Liu, L.F. Thumbnail-preserving encryption based on improved logistic system. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 10167–10179. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.