Hindawi
Security and Communication Networks
Volume 2020, Article ID 8842376, 13 pages
https://doi.org/10.1155/2020/8842376

Research Article

An Unequal Image Privacy Protection Method Based on Saliency Detection

Rongxin Tu, Wenying Wen, and Changsheng Hua

School of Information Management, Jiangxi University of Finance and Economics, Nanchang 330013, China

Correspondence should be addressed to Wenying Wen; wenyingwen@sina.cn

Received 26 August 2020; Revised 5 October 2020; Accepted 20 November 2020; Published 3 December 2020

Academic Editor: Guodong Ye

Cloud platforms provide a good stage for storing and sharing big image data for users, although some privacy issues arise. Image encryption technology can prevent privacy leakage and can ensure secure image data sharing on cloud platforms. Hence, in this paper, an unequal encryption scheme based on saliency detection is proposed. First, based on the mechanism of visual perception and the theory of feature integration, the visual attention model is employed to realize the recognition of significant regions and insignificant regions. Then, a dynamic DNA encryption algorithm is proposed to exploit heavyweight encryption for significant regions, while semi-tensor product compressed sensing is introduced to exploit lightweight encryption and compression for insignificant regions. Experimental results demonstrate that the proposed framework can serve to secure big image data services.

1. Introduction

The Internet of Things is entering the lives of people. Combined with various information sensing devices, a huge network is formed and realizes the interconnection of people, machines, and things at any time and any place. In the real-time process of interconnection, a huge amount of image data is produced [1]. Since these images are acquired in daily life, they are relevant to us and contain significant personal information. The privacy security of image data becomes a concern and an urgent problem to be solved.

There are many encryption methods to provide security to the privacy of image data. Among them, dynamic DNA encoding and compressed sensing are the most useful encryption methods. Dynamic DNA encoding has been infiltrated into the field of cryptography, which has lots of characteristics, such as massive parallelism, huge storage, and ultra-low power consumption. In these DNA-based cryptosystems, DNA is used as information carrier, and the DNA sequences coding and operational rules are employed to encrypt images. Compressive sensing is a novel signal acquisition theory that the signal can be sampled at a much lower sampling rate than Nyquist–Shannon sampling theorem. Under certain conditions, the original signal can still be accurately recovered by these small amounts of sampled data. When the image data is sampled by compressive sensing, a small amount of sampled data will be obtained from which one cannot obtain any useful information. Therefore, compressive sensing can achieve both compression and encryption of image data.

Image encryption technology can prevent privacy leakage and can ensure secure image data sharing on cloud platforms. Conventional image encryption technology can be divided into two categories: full encryption [2–6] and selective encryption [7–12]. Full encryption serves to encrypt the complete image data, which not only causes high complexity and low efficiency but also cannot satisfy the rapid expansion of image data demand.

Selective encryption mainly focuses on a part of the image data, which can trade security for computational complexity. In [7], Bhatnagar et al. proposed a selective encryption scheme based on pixels of interest and singular value decomposition. In [13], an edge-based lightweight encryption scheme was proposed by Zhang et al. using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. In [10], Wen et al. proposed a selective scheme to encrypt the objects of infrared images by using chaotic maps. Furthermore, they protected the salient image regions by embedding them into a visually meaningful image [11]. Selective encryption is suitable for protecting important image regions, but not entire images. Applying a selective encryption scheme to encrypt private images would still expose a considerable amount of information.

However, with the exponential growth of the data volume, a large amount of data needs to be encrypted, and the present encryption methods have obvious disadvantages. In selective encryption schemes, the data of important regions are still huge, and the computation of encryption algorithms is complex. Selective encryption algorithms only protect the important regions, while the unimportant regions are not protected. On the other hand, selective encryption techniques are not considered further image compression, which is very important for big image data. Therefore, the existing selective encryption algorithms have limitations regarding the protection of big image data.

Based on the above statement, we propose an unequal protection scheme for big image data. Firstly, significant regions and insignificant regions are identified by the visual attention model. Then, a dynamic DNA encryption algorithm is proposed to exploit heavyweight encryption for significant regions, while semi-tensor product compressed sensing is introduced to exploit lightweight encryption and compression for insignificant regions, achieving unequal protection. The final resulting image is obtained when the two regions are processed. Our contributions can be summarized as follows:

(1) An unequal privacy protection method for big image data is proposed. A saliency detection model in the compressed domain is employed to realize the hierarchical recognition of significant regions and insignificant regions. According to the characteristics of regions, heavyweight encryption is proposed for significant regions, while lightweight encryption and compression are applied for insignificant regions.

(2) For significant regions, dynamic DNA random encoding is proposed to achieve heavyweight encryption. For insignificant regions, semi-tensor product compressed sensing is introduced to implement lightweight encryption and compression.

(3) The proposed unequal privacy protection method can save storage and computational resources for society by combining the advantages of a heavyweight encryption algorithm and a lightweight encryption method.

The rest of the paper is organized as follows. In section 2, the related work on image encryption techniques is introduced. In section 3, the framework of the proposed scheme is depicted in detail, including the recognition of significant regions and insignificant regions, heavyweight encryption for significant regions, and lightweight encryption and compression for insignificant regions. An analysis of experimental results is presented in section 4. Finally, the conclusions are given in section 5.

2. Related Work

Because images contain much sensitive information, they are easy to attack, leading to the disclosure of privacy. Image encryption has become a hot topic, and many encryption techniques have been developed, such as chaotic system theory [14, 15], DNA encoding [16, 17], optical transform [18, 19], and compressed sensing [20, 21]. Different encryption techniques have different encryption effects and computation. According to the characteristics of encryption, these techniques can be divided into spatial domain encryption and transform domain encryption.

The main ideas of spatial domain encryption are permutation, which primarily changes the pixel values, and diffusion, which disorganizes the positions of the pixel values. In [22], Fridrich put forward pioneering permutation-diffusion architecture to encrypt images. Then, Bao and Zhou [23] extended the technique of the permutation-diffusion architecture, which further increased the encryption effect. In [24], Hua et al. proposed a scheme using a 2D logistic-adjusted-sine map to encrypt images. To enhance the encryption efficiency, a high speed scrambling and pixel adaptive diffusion scheme was proposed for medical images [25]. In further exploration of image encryption, Zhou et al. [26] proposed a scheme for a new 1D chaotic system for image encryption and noted that the sine map also offers effective performance with respect to chaotic behaviour. The above encryption technologies also offer good encryption effects to encrypt images, although they are not suitable for some important data because of the need for strong security assurance. To enhance the security guarantee of encryption schemes, multidimensional chaotic systems have been employed for image encryption. In [27], Chen et al. proposed an image encryption algorithm based on a combined multidimensional chaotic system. On the other hand, DNA coding exhibits the characteristics of massive parallelism, ultra-high storage capacity, and ultra-low energy consumption, but the design is not flexible enough and cannot be used independently. At present, many researchers have proposed encryption algorithms based on DNA coding and chaos theory [28]. To further enhance the security, DNA coding combined with a multidimensional chaotic system has been proposed. In [29], Zhou and Wang proposed a scheme in which hyperchaotic systems were introduced into DNA coding to encrypt images. The experimental results demonstrated that the encryption algorithm offered high security and a strong encryption effect.

3. Framework of the Proposed Unequal Privacy Protection Method

The aforementioned encryption methods mainly focus on the security and encryption performance, and they do not consider image compression [30, 31]. Compressed sensing is a new information acquisition guidance theory. Its basic idea is to use random projection to obtain the observed value, realize the purpose of compression at the same time as sampling, then transmit to the receiver to acquire the observed value, and use the sparse prior of the image to reconstruct the original signal by solving the convex optimization problem. This theory provides a new idea for image security research, that is, carrying out simultaneous compression and encryption of images. In [32], Rachlin and Baron proved that CS can guarantee relative security in calculation. However, CS technology cannot be applied to encrypt important data due to the fact that the method is not yet sufficiently secure. Therefore, some conventional encryption methods are employed in CS. In [33], Zhang et al. combined a chaotic system and CS and proposed a scheme that can accomplish low-cost acquisition and confidentiality preservation of data for the Internet of Multimedia Things, realizing high security. With further enhancement of the security, the compression properties in CS have been considered. In [34], a secure and energy-efficient data transmission scheme was proposed by Peng et al., which can greatly reduce the storage space.

The aforementioned encryption algorithms have their own specific purposes, such as enhancing the security, reducing the complexity, and compression. However, they are not suitable for massive amounts of image data. The storage and transmission as well as the computational power required to handle a large quantity of image data bring about great pressure on social resources. Handling big image data with limited resources is an issue of concern. On the premise of ensuring image security, reducing both the computing power and storage of big image data is a problem we need to solve. Since the current heavyweight encryption algorithms [16, 17] require enormous computation, they are not suitable for handling large image data. The lightweight encryption methods [30, 32, 35] are insufficiently secure, but they do not require much computation and offer a rapid encryption speed.

Based on the above statement, we propose an unequal protection scheme that combines the advantages of heavyweight encryption algorithms and lightweight encryption methods. The visual attention model based on the mechanism of visual perception and the theory of feature integration is employed to realize the recognition of significant regions and insignificant regions. Then, the significant regions are encrypted by the dynamic DNA encryption algorithm, while the insignificant regions are encrypted by semi-tensor product compressed sensing. The final resulting image is obtained after the significant regions and insignificant regions are processed. When a user requires an image, assembling the recovery of the two parts can produce the original image.

On the other hand, the partitioning of significant regions is not stationary and depends on the image itself. To identify the significant regions, we design an adaptive rectangular box to cover them. The size of the significant regions is adaptive according to the image. After the recognition of significant regions and insignificant regions, an unequal privacy protection method is applied to process the two types of regions. In terms of computation and security, the proposed scheme is very suitable for encrypting large amounts of image data.

In the following, we provide specific operations for the recognition of significant regions and insignificant regions: heavyweight encryption for significant regions and lightweight encryption and compression for insignificant regions. The framework of the proposed scheme is depicted in Figure 1.

3.1. Recognition of Significant Regions and Insignificant Regions. There are many main techniques for image data recognition. In this paper, we focus on the saliency detection model, which was first proposed by Itti et al. [36]. In the model, according to the multiscale centre-surrounding differences, three features are calculated for the saliency map: intensity, colour, and orientation. Then, the final saliency map is obtained by combining these three feature maps. In the proposed scheme, saliency detection in the compressed domain [37] is adopted. The specific algorithm steps are shown as follows:

(i) Step 1: The DCT coefficients are obtained from the image bitstream. Based on the DCT coefficients of each 8×8 block, four features, including intensity, colour, and texture (T, C_{rg}, C_{by}, and U), are extracted to build the feature maps.

(ii) Step 2: The feature differences between DCT blocks are computed. The feature differences between DCT blocks m and n can be calculated as follows:

$$D^r_{m,n} = \zeta^r_m - \zeta^r_n, \tag{1}$$

where $r = 1, 2, 3$ indicates the intensity and two colour features and $\zeta^r \in \{T, C_{\mathrm{rg}}, C_{\mathrm{by}}\}$. The texture difference $D_{m,n}$ between blocks m and n can be calculated as follows:

$$D^4_{m,n} = \max\left(P\left(U_m, U_n\right), P\left(U_m, U_n\right)\right), \tag{2}$$

where U_m and U_n represent the vectors of texture features for blocks m and n, respectively. $P(U_m, U_n)$ is calculated as follows:

$$P\left(U_m, U_n\right) = \max_{u_m \in U_m} \min_{u_n \in U_n} \left\| U_m - U_n \right\|, \tag{3}$$

where is the L_2 norm.

(i) Step 3: To determine the weighting for these DCT blocks, the Gaussian model of the Euclidean distances is used between DCT blocks. The feature map for the r^{th} feature can be obtained as follows:

$$G^r_m = \sum_{m \neq n} \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(d^2_{m,n}/2\sigma^2\right)} D^r_{m,n}, \tag{4}$$

where G^r_m represents the saliency value calculated from the r^{th} feature. σ is a parameter for the Gaussian model; set $\sigma = 5$. $d_{m,n}$ is the Euclidean distance between DCT blocks m and n, and $D^r_{m,n}$ is calculated as in (2) and (3).

(i) Step 4: By using the coherent normalization-based fusion method, these four feature maps are combined

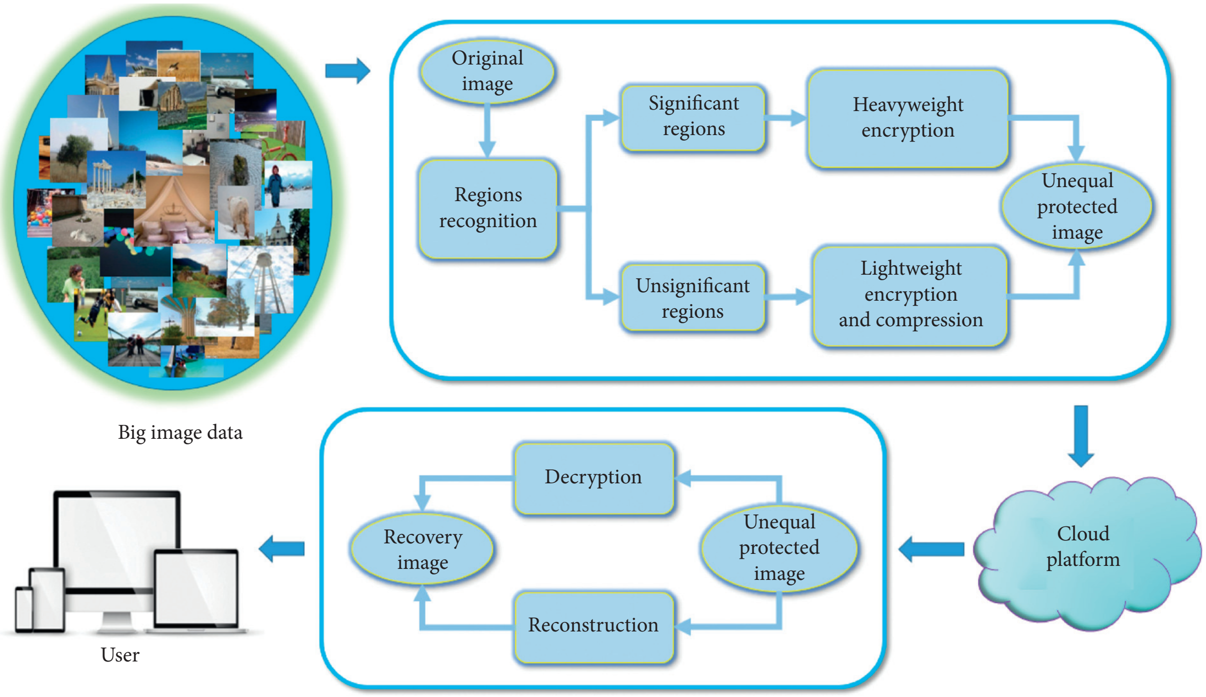


FIGURE 1: Framework of the proposed scheme.

to obtain the saliency map. The saliency map $\mathbb{G}$ is calculated as follows:

$$\mathbb{G} = \sum \varphi_{\vartheta} L(\vartheta) + \omega \prod L(\vartheta), \tag{5}$$

where L is the normalization operation, $\vartheta \in G^r$, and the parameters of φ_{ϑ} and ω are the weights for each of the components, which are set as $\varphi_{\vartheta} = \omega = 1/5$. The second term in (5) corresponds to all four feature maps G^r detected as significant regions.

After these four steps, the saliency map can be obtained. More details of the saliency detection in the compressed domain are shown in [37].

3.2. Heavyweight Encryption for Significant Regions.

Generally speaking, the amount of important data of an image is small. Considering the importance of data, we design dynamic DNA encoding combined with a chaotic system algorithm to realize heavyweight encryption for significant regions. The details of the method are as follows.

TABLE 1: DNA encoding rules.

	1	2	3	4	5	6	7	8
A	00	01	10	11	00	01	10	11
C	10	00	11	01	01	11	00	10
G	01	11	00	10	10	00	11	01
T	11	10	01	00	11	10	01	00

There are four nucleic acids in DNA sequences, called A, T, C, and G. The DNA encoding rules are shown in Table 1. We use DNA sequences to encode the image. For instance, when the value of a pixel is 68, the binary number is [01000100]. We use rule 1 to encode the binary number [01000100] into a DNA sequence (GAGA). Then, we use rule 2 to decode the DNA sequence (GAGA) into a binary number [11011101], and the decimal number is 221. Encryption of the image can be achieved by disordering the coded DNA sequences for each pixel. To enhance the effect of the encryption, some algebraic operations for DNA sequences are introduced. The DNA XOR operation is shown in Table 2, the DNA ADD operation is represented in Table 3, and the DNA SUB operation is depicted in Table 4. In the encoding and algebraic operation processing, we need to select the code rules and operations by obtaining key sequences. In this paper, we employ a chaotic system to generate pseudorandom sequences.

The key sequences are generated by the method of chaotic system, which is a long pseudorandom sequence. It can be expressed as follows:

$$\begin{cases} \dot{x} = a(y - x) + w, \\ \dot{y} = cx - y - 2xz, \\ \dot{z} = 2x^2 - bz, \\ \dot{w} = yz - dw, \end{cases} \tag{6}$$

where x, y, z, and w are state variables. The values of a, b, c, and d are parameters of the system. When $a = 10$, $b = 8/3$, $c = 28$, and $d = 2$, the system is in hyperchaos.

Additionally, the significant regions are encrypted by the following steps:

(i) Step 1: By iterating a logistic map, a random matrix that has the same size of significant regions is generated. The logistic map is depicted as follows:

Table 2: DNA XOR operation.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
T	T	C	G	A
C	C	T	A	G

Table 3: DNA addition operation.

ADD	A	G	C	T
A	A	G	C	T
G	G	A	T	C
T	T	C	A	G
C	C	T	G	A

Table 4: DNA subtraction operation.

SUB	A	G	C	T
A	A	G	T	C
G	G	A	C	T
T	T	C	G	A
C	C	T	A	G

$$\mu_{n+1} = \lambda\mu_n\left(1 - \mu_n\right), \tag{7}$$

where λ is a parameter, and μ_0 based on the plain image is defined as follows:

$$\mu_0 = \frac{1}{I \times J \times 255}\sum_{m=1,n=1}^{I,J} P(m, n), \tag{8}$$

where $I \times J$ is the size of P and P is the plain image, (m, n) is the position of the pixel in the plain image, and $P(m, n)$ is the value of the pixel.

(i) Step 2: The values of the random matrix $\varphi(x)$ and significant region $G(x)$ pixels are transformed from decimal into binary form. Then, both the random matrix and significant regions are encoded by the DNA encoding rules in Table 1.

(ii) Step 3: According to the hyperchaotic system, four secret key sequences x_n, y_n, z_n, and w_n are generated. Due to the rules of DNA coding including eight possibilities, the key of x_n and y_n must deal with the following formula:

$$\begin{cases} x_n = \operatorname{mod}\left(\lceil x_n \times 10^5 \rceil, 8\right), \\ y_n = \operatorname{mod}\left(\lceil y_n \times 10^5 \rceil, 8\right), \end{cases} \tag{9}$$

where both x_n and y_n have eight possibilities from 0 to 7. Through the sequences of x_n and y_n, both the random matrix values and significant region pixels are transformed into DNA sequences.

(i) Step 4: The three DNA operations, including XOR, addition, and subtraction, are shown in Tables 2, 3, and 4, respectively. The calculation of z_n is expressed as follows:

$$z_n = \operatorname{mod}\left(\lceil z_n \times 10^5 \rceil, 3\right). \tag{10}$$

where z_n has three possibilities from 0 to 2, with each number representing a kind of DNA operation. Through the DNA operation, a cipher DNA sequence is obtained.

(i) Step 5: The key sequences of w_n need to deal with the following formula:

$$w_n = \operatorname{mod}\left(\lceil w_n \times 10^5 \rceil, 8\right). \tag{11}$$

The key sequences w_n are used to choose the DNA coding rules to decode the cipher DNA sequences into binary sequences. When the binary sequences turn into decimal form, encryption blocks corresponding to significant regions are obtained. The decryption process is the reverse operation of the encryption process.

3.3. Lightweight Encryption and Compression for Insignificant Regions. As mentioned earlier, the significant regions contain a small amount of data, whereas the insignificant regions include a large amount of data. Therefore, a compression encryption mechanism is adopted for insignificant regions. In particular, for a huge amount of data, compressed sensing is a suitable algorithm that can carry out simultaneous compression and encryption of images [38, 39].

Compressed sensing (CS) is a theory that signals can be sampled at a much lower sampling rate than possible according to the Nyquist–Shannon sampling theorem. Under some circumstances, these small amounts of sampled data can still enable accurate recovery of the original signal. For a one-dimensional length Q discrete-time real signal ω, the compressed projection observation of signal w is multiplied by a measurement matrix $P \times Q (P \ll Q)$ constructed from a Gaussian random matrix, a Bernoulli random matrix, or a partial Hadamard matrix. This can be expressed as follows:

$$v = \theta\omega, \tag{12}$$

where v is a dimension of the $P \times 1$ compressed measurement vector. When the signal ω is not sparse, it will be expressed as a $Q \times Q$ size sparse orthogonal basis ξ multiplied by a sparse vector x, shown as follows:

$$\omega = \xi x. \tag{13}$$

In this way, the sampling process of CS can be depicted as

$$v = \theta\xi x = \Psi x, \tag{14}$$

where the matrix $\Psi = \xi x$ is called the sensing matrix of CS. The size of Ψ is $P \times Q (P \ll Q)$.

As for the sampling process of CS, it is easy to obtain the measured value v from the original signal ω. However, it seems impossible to recover the original ω from the measured value v because this is an ill-posed equation that possesses infinitely many solutions.

However, if the matrix Ψ and the measured value satisfy certain conditions [40] and the vector x is sufficiently sparse, then the task becomes solving an optimization problem to accurately recover the original signal ω.

$$\text{Minimize } \|x\|_0 \text{ subject to } v = \Psi x, \tag{15}$$

where $\| \|_0$ represents the L_0 norm of x.

By solving the optimization problem, the original signal can be reconstructed as $\widehat{\omega} = \xi \widehat{x}$. To break through the limitation of dimension in conventional matrix multiplication operation, the semi-tensor product is introduced into the compressed sensing. It is assumed that $M \in R^{a \times b}$, $N \in R^{c \times d}$ semi-tensor product can be defined as

$$S = M \times N, \tag{16}$$

where S represents the STP of M and N. Let b be a factor of c $(c = bt)$, $m_{ab} \in M$, $n_{ab} \in N$. The extensional formula is then

$$\begin{aligned} T &= \begin{bmatrix} m_{11} & \cdots & m_{1b} \\ \vdots & \ddots & \vdots \\ m_{a1} & \cdots & m_{ab} \end{bmatrix} \times \begin{bmatrix} n_{11} & \cdots & n_{1d} \\ \vdots & \ddots & \vdots \\ n_{c1} & \cdots & n_{cd} \end{bmatrix} \\ &= \begin{bmatrix} m_{11} & \cdots & m_{1b} \\ \vdots & \ddots & \vdots \\ m_{a1} & \cdots & m_{ab} \end{bmatrix} \times \begin{bmatrix} N^{11} & \cdots & N^{1d} \\ \vdots & \ddots & \vdots \\ N^{b1} & \cdots & N^{bd} \end{bmatrix}, \end{aligned} \tag{17}$$

where N_{ab} $(a = 1, 2, \ldots, c;\ b = 1, 2, \ldots, d)$ represents the result of dividing the jth column in matrix N into b blocks and N^{ab} is a column vector of length t. When $b = c$, $M \times N = MN$; that is, the STP degenerates into the conventional matrix product.

The size of the measured measurement matrix in conventional CS is $P \times Q$. The size of the original image matrix is $Q \times Q$. The size of the secret image in CS is $P \times Q$. The compression ratio (CR) of CS is (P/Q). If the CR is low, then the image storage is small. This can save storage resources when it is necessary to handle big image data. It is difficult to recover the original image when the CR is too low. Therefore, a good balance must be maintained between the CR and image recovery. In another aspect, employing the STP to the measurement matrix $(P \times Q)$ can reduce the size to $(P/q) \times (Q/q)$, which can greatly reduce the computing resources. The following steps accomplish the compressive process for insignificant regions.

(i) Step 1: Use discrete wavelet transform for sparse original image. The sparse image matrix is called N.

(ii) Step 2: Employ a chaotic system to generate a random matrix as the measurement matrix.

(iii) Step 3: Apply the STP strategy for the sparse matrix N and the measurement matrix. After CS, the insignificant regions are compressed and encrypted.

4. Experimental Results

In this section, the performance of the proposed unequal encryption is analysed. A series of images to which the encryption operation was applied are depicted in Figure 2. Numerous experiments were performed by employing a personal computer configured with an Intel (R) Core (TM) i5-4200 U CPU @ 1.60 GHz with an 8 GB RAM, 64 bit operating system with Windows 10 and MATLAB 2018a.

Figure 3 depicts the effect of privacy protection of the significant regions and insignificant regions in the plain image. Figure 3(b) shows the effect of heavyweight encryption for significant regions, and Figure 3(c) reveals the effect of lightweight encryption and compression for insignificant regions. Figure 3(d) shows the recovered image, which demonstrates good recovery. One cannot obtain any useful information from the cipher image-blocks corresponding to significant regions, which indicates the effective performance of heavyweight encryption in visual security. Comparing the two encryption images, the encryption effects for significant regions are better than those for insignificant regions since the former appear to be more smooth and intensive than the latter with respect to the texture feature. In Table 5, the advantages and limitations of different encryption algorithms are summarized and compared. Due to the use of heavyweight encryption for the important parts of the image, which contain the main information, the experimental analysis is primarily centred around the dynamic DNA encryption algorithm.

4.1. Analysis of Subjective Vision.

The basic security requirements of an encryption system are the subjective vision performance and then other security requirements. An encryption algorithm should guarantee that no visual information can be obtained from the encrypted image. The experimental results of heavyweight encryption are shown in Figure 2, demonstrating the efficacy of the encryption algorithm for the significant regions. One cannot obtain any visual information from the cipher image-blocks corresponding to the significant regions. Thus, the more important information in an image has stronger encryption, which corresponds to the idea of the proposed scheme.

4.2. Correlation Analysis.

The adjacent pixels in a meaningful visual image gradually change. The correlation between them is generally very high, as their values are similar, so the visual image can easily be attacked by statistical analysis. When an image is encrypted, the correlation between adjacent pixels is significantly reduced. The correlation analysis result is an important index to evaluate the encryption performance for an image. The following operations realize correlation analysis. From the significant regions and corresponding cipher image-blocks, 3000 pixels are randomly selected. Then, the correlation coefficient is

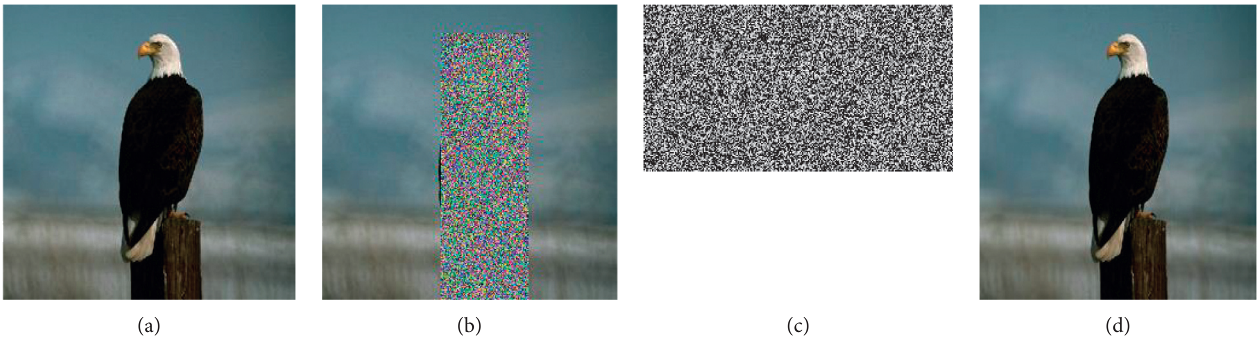


Figure 2: (a) Original image. (b) Significant regions protection. (c) Compressed sensing applied to insignificant regions. (d) Recovery image.

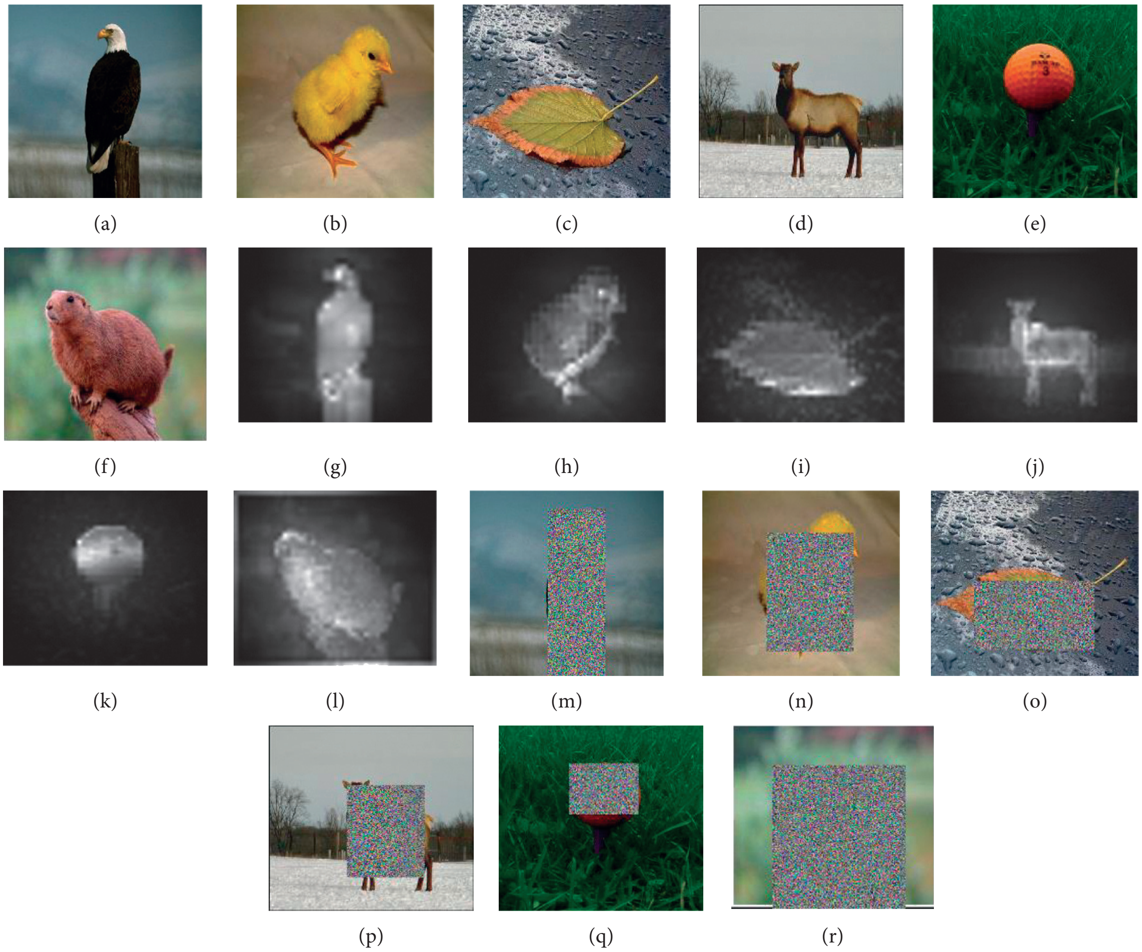


Figure 3: The algorithm of dynamic DNA implemented on significant image. The first row includes (a) eagle, (b) chicken, (c) leaf, (d) deer, (e) ball, and (f) squirrel. The second row presents the salient regions from the model in the compressed domains. The third row presents the cipher image-blocks corresponding to significant regions.

calculated between two adjacent pixels in horizontal, vertical, and diagonal directions. The correlation coefficient is depicted as follows:

$$\mathrm{Cor} = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \overline{x})^2 \sum_{i=1}^{N}(y_i - \overline{y})^2}}, \quad (18)$$

where x_i and y_i are adjacent pixel values, $\overline{x}$ and $\overline{y}$ are the average of x_i and y_i, and N represents the selected pixels. The correlation coefficients of three channels are listed in Table 6, and the correlation plots of the R-channel are shown in Figure 4. It can be found that the correlation coefficient is high in the original image and low in the encrypted image. Furthermore, the distribution of pixels in a cipher image

Table 5: Summary and comparison of the current encryption algorithms.

Algorithms	Encryption types	Algorithms used	Advantages	Limitations
Chen et al. [17]	Full encryption	Self-adaptive permutation-diffusion and DNA random encoding	Enhancing the plaintext attack resistance	Consuming much time and requiring high computation
Wen et al. [41]	Full encryption	DNA sequences and chaotic systems	Enough security to protect image	Complexity and requiring high computation
Wang et al. [42]	Selective encryption	Compressed sensing and data hiding	Degrading the visual quality level and saving computation	The visual information in image may have security issue
Khan and Ahmad [43]	Selective encryption	Chaotic system	Lower overhead and more efficiency	2D map system may not get enough security
Proposed	Unequal encryption	DNA sequences and compressed sensing	Saving computation and storage	Increasing the execution speed

Table 6: The correlation coefficients of three channels.

Original image	Channel	Significant regions				Cipher blocks			
		Horizontal	Vertical	Diagonal	Average	Horizontal	Vertical	Diagonal	Average
Eagle	*R*	0.9400	0.9740	0.9240	0.9460	−0.0035	−0.0045	−0.0033	0.0016
	G	0.9477	0.9785	0.9335	0.9532	−0.0095	0.0602	−0.0351	0.0156
	B	0.9533	0.9817	0.9411	0.9587	0.0488	0.0417	0.0230	0.0378
Chicken	*R*	0.9871	0.9799	0.9766	0.9812	0.0346	0.0019	−0.0055	0.0103
	G	0.9851	0.9773	0.9764	0.9796	−0.0129	−0.0250	−0.0460	0.0280
	B	0.9894	0.9845	0.9813	0.9851	−0.0010	−0.0195	0.0026	−0.0060
Leaf	*R*	0.8959	0.8406	0.7803	0.8389	0.0068	−0.0243	0.0427	0.0084
	G	0.8759	0.8088	0.7357	0.8068	−0.0136	0.0166	0.0253	0.0094
	B	0.8057	0.7121	0.6175	0.7118	−0.0562	0.0424	−0.0103	0.0089
Dear	*R*	0.9704	0.9852	0.9598	0.9718	0.0348	0.0450	−0.0138	0.0220
	G	0.9733	0.9865	0.9635	0.9744	0.0384	0.0252	0.0138	0.0258
	B	0.9778	0.9876	0.9691	0.9781	0.0183	−0.0391	−0.0164	−0.0124
Ball	*R*	0.9819	0.9733	0.9548	0.9700	0.0526	−0.0506	−0.0028	−0.0003
	G	0.9765	0.9577	0.9387	0.9576	−0.0218	−0.0083	−0.0329	−0.0210
	B	0.9610	0.9180	0.8859	0.9216	−0.0484	0.0597	0.0078	0.0064
Squirrel	*R*	0.9377	0.9256	0.9105	0.9246	0.0170	−0.0213	−0.0131	−0.0058
	G	0.9611	0.9527	0.9457	0.9532	0.0088	−0.0061	0.0007	0.0011
	B	0.9526	0.9421	0.9341	0.9429	−0.0066	0.0244	0.0129	0.0102

exhibits good uniformity. Both of these factors mean that the proposed unequal protection scheme exhibits high security and resistance against statistical analysis.

4.3. Peak Signal to Noise Ratio. The proposed scheme uses the peak signal to noise ratio to effectively measure the performance of the encryption. PSNR is employed to measure image distortion. Suppose that $I_1(m,n)$ and $I_2(m,n)$ are $(m,n)^{\text{th}}$ pixels of two images I_1 and I_2 . The mean squared error (MSE) between the original image and encryption image is defined as follows:

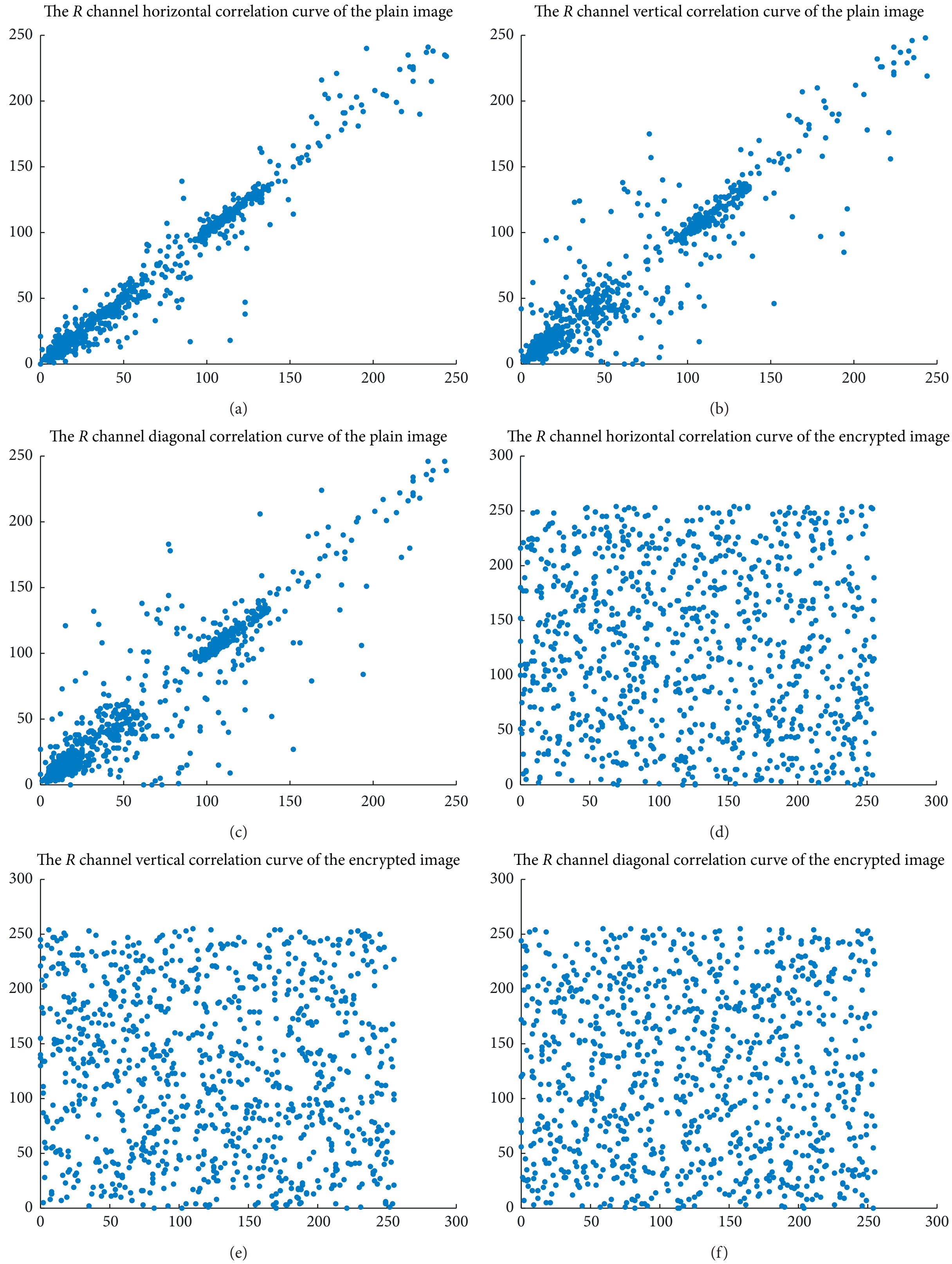
$$\mathrm{MSE} = \frac{\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}\left(I_1(m,n) - I_2(m,n)\right)^2}{mn}. \tag{19}$$

The formula of PSNR is shown as follows:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{\mathrm{MSE}}\right). \tag{20}$$

The smaller the values of the indicators are, the higher the distortion of the image is, which also means that there is less visual information of the image. Table 7 shows the values of PSNR on six images. One can find that the values of the significant regions are small. The results therefore demonstrate that the heavyweight encryption has good encryption performance.

4.4. Information Entropy Analysis. Information entropy is generally used to describe the uncertainty of information. Here, it is applied to measure the randomness of the distribution of pixels of a whole image. A larger information entropy value represents higher randomness of an image. To



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 4: The R-channel correlation distribution of adjacent pixels in horizontal, vertical, and diagonal directions: (a), (b), (c) Significant regions. (d), (e), (f) Corresponding cipher image-blocks.

Table 7: PSNR analysis between original and encryption images.

Image	Eagle	Chicken	Leaf	Dear	Ball	Squirrel
PSNR	14.7992	18.7725	20.3600	18.8665	22.2202	15.5835

Table 8: Entropy analysis of three channels.

Original image	Channel	Entropy	
		Significant regions	Cipher blocks
Eagle	R	6.7955	7.9883
	G	6.6199	7.9883
	B	5.8452	7.9883
Chicken	R	7.1462	7.9951
	G	6.9712	7.9951
	B	6.9004	7.9951
Leaf	R	7.2890	7.9921
	G	7.1148	7.9921
	B	6.9236	7.9921
Dear	R	7.2562	7.9919
	G	7.2000	7.9919
	B	6.9812	7.9919
Ball	R	7.7168	7.9891
	G	7.2286	7.9891
	B	5.1497	7.9891
Squirrel	R	7.2491	7.9973
	G	7.5227	7.9973
	B	7.3945	7.9973

some extent, it can indicate the security of an encryption algorithm. The formula of the information entropy $H(I)$ is as follows:

$$H(I) = -\sum_{j=0}^{2^L-1} P(I_j)\log_{10} P(I_j), \tag{21}$$

where L represents the number of possible values, I_j is the pixel value $(0 < I_j < 255)$, and $P(j)$ represents the probability of the pixel value. The information entropy is larger when the distribution of pixel values is more uniform. The ideal limit value of the image entropy is 8 if all of the pixel values have the same probabilities. Thus, the closer the value of the encryption image entropy is to 8, the better the performance of the encryption algorithm is. The entropy values of the cipher image-blocks corresponding to significant regions are listed in Table 8. It can be found that the values of the significant regions vary, whereas the values of the corresponding cipher image-blocks are very similar and close to 8. The results therefore demonstrate that the heavyweight encryption has good encryption performance.

4.5. Histogram of the Cipher Image. The histogram of an image reflects the frequency distribution of pixels. When the histogram of an image is smooth, the performance in resisting statistical attacks is strong. The histogram of the encryption image is shown in Figure 5. The histogram of the cipher image-blocks corresponding to significant regions is smooth, which demonstrates that the dynamic DNA encryption algorithm exhibits good performance in resisting statistical analysis.

4.6. Key Sensitivity Analysis. Generally, the goal of a differential attack is to make a slight change in the original image and then compare the corresponding encrypted image to obtain clues regarding the secret key. The number of pixels change rate NPCR and the uniform average change intensity UACI are used to test whether the encryption algorithm can resist a differential attack. Suppose that $I_1(m,n)$ and $I_2(m,n)$ are the $(m,n)^{\text{th}}$ pixels of two images I_1 and I_2. Two indicators are defined as follows:

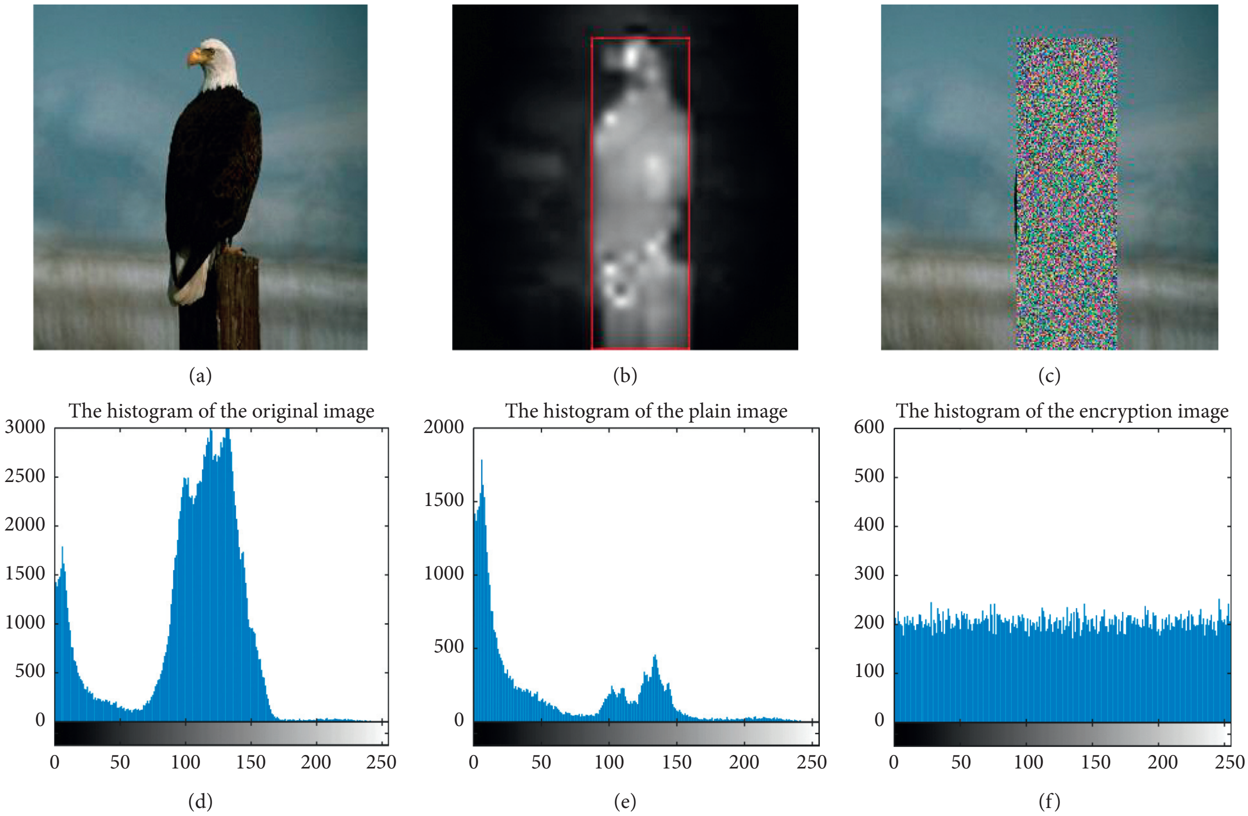
$$\begin{aligned} \text{NPCR}(I_1, I_2) &= \sum_{n,m}\left(\frac{P(n,m)}{T}\right) \times 100\%, \\ (m,n) &= \begin{cases} 0, \text{ if } I_1(m,n) = I_2(m,n) \\ \\ 1, \text{ if } I_1(m,n) \neq I_2(m,n) \end{cases}, \\ \text{UACI}(I_1, I_2) &= \sum_{m,n} \frac{|I_1(m,n) - I_2(m,n)|}{(L-1) \times T} \times 100\%, \end{aligned} \tag{22}$$

where T indicates the total number of pixels in an image.

The expected values of NPCR and UACI for a good encryption scheme are given as the following equations:

$$\begin{aligned} \text{NPCR}_{\text{expected}} &= \left(1 - \frac{1}{2^{\log_2 L}}\right) \times 100\%, \\ \text{UACI}_{\text{expected}} &= \frac{1}{L^2}\, \frac{\sum_{v=1}^{L-1} v(v+1)}{L-1} \times 100\%. \end{aligned} \tag{23}$$

As the test frames are the length of 8 bit pixel value image, the expected values of NPCR and UACI are 0.9961 and 0.3346, respectively. When the NPCR and UACI values of an image are closer to the expected values, the attack resistance ability of the encryption algorithm is stronger. The NPCR and UACI results of the cipher image-blocks corresponding to significant regions are shown in Table 9. It can be found that the values are close to the expected values,



(a) (b) (c)

(d) (e) (f)

Figure 5: Histogram analysis. (a) Original image of eagle. (b) Significant regions of eagle. (c) Cipher image. (d) Histogram of eagle. (e) Histogram of significant regions. (f) Histogram of cipher block corresponding to significant regions.

which demonstrates that the heavyweight encryption exhibits a strong ability to resist differential attacks.

Table 9: The average NPCR and UACI of three channels.

Original image	Channel	NPCR	UACI
Eagle	R	0.9964	0.3755
	G	0.9966	0.3904
	B	0.9959	0.4023
Chicken	R	0.9960	0.3116
	G	0.9960	0.2798
	B	0.9963	0.3615
Leaf	R	0.9962	0.2867
	G	0.9960	0.2754
	B	0.9962	0.3079
Dear	R	0.9964	0.3017
	G	0.9965	0.3088
	B	0.9968	0.3305
Ball	R	0.9959	0.3425
	G	0.9945	0.3232
	B	0.9957	0.4426
Squirrel	R	0.9962	0.2767
	G	0.9965	0.2951
	B	0.9960	0.3012

4.7. Known-Plaintext and Chosen-Plaintext Attack Analyses. Ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack are four classical types of attacks. In those attacks, known-plaintext and chosen-plaintext attacks are the more powerful. When the selected plaintext image data information is input into the system, it would output the corresponding ciphertext image information. According to the relationship between the plaintext image and the ciphertext image data, the encryption analyst may find a part of the key or even all the keys to attack the encryption system. In this paper, the keys are used in the DNA encoding steps, and the DNA operation rules are selected by the chaotic system, which reaches a key change each time. In addition, the proposed encryption system depends on the plain image, making it difficult for an attacker to obtain key information. Therefore, the proposed method can resist known-plaintext and chosen-plaintext attacks. We fully consider the results of the security analysis and the difficulty of being attacked and have a well experimental result.

4.8. Key Space Analysis. The total number of different keys that can be used in the encryption algorithm represents the key space. To resist brute-force attack, the key space should be sufficiently large. Generally, if the key space is larger than 2^{100}, then the encryption algorithm can be regarded as a secure one [44]. In the proposed scheme, the secret keys are provided by the initial values of the hyperchaotic Lorenz system (x, y, z, w). The computational precision of a 64 bit double-precision number is approximately 10^{-15}, according to the IEEE floating-point standard. Therefore, the key space of the proposed scheme is key $= 10^{-15} \times 4 \approx 2^{-199}$. It can be found that the proposed scheme exhibits sufficient security against brute-force attack.

5. Conclusions

This paper proposes an unequal protection scheme that combines the relative advantages of heavyweight and lightweight encryption algorithms. The basic idea of this method is to implement different intensity protection methods by distinguishing the different importance of image data. First, significant regions and insignificant regions are identified by a visual attention model based on the mechanism of visual perception and the theory of feature integration. Then, the significant regions are encrypted by a dynamic DNA encryption algorithm, while the insignificant regions are protected by semi-tensor product compressed sensing, achieving unequal protection. The final resulting image is obtained when the two parts of the image are processed. This method can save storage and computational resources for society and can offer high security for transmission and sharing of images with others. The experimental results verified that the proposed scheme can provide sufficient security for huge amounts of image data.

Data Availability

The data used to support the findings of this study have not been made available.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Authors' Contributions

R. T. proposed the methodology. W. Y. conceived the conceptualization. R. T. and W. Y. collected the resources. R. T. wrote the manuscript under the supervision of W. Y. who provided valuable suggestions on the original draft.

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant 61961022 and the Natural Science Foundation of Jiangxi Province under Grant 2020BAB202022.

References

[1] Y. Zhang, Q. He, G. Chen, X. Zhang, and Y. Xiang, "A low-overhead, confidentiality-assured, and authenticated data acquisition framework for IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7566–7578, 2020.

[2] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[3] T. Kim, Y. Oh, and H. Kim, "Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption," *Security and Communication Networks*, vol. 2020, Article ID 4195852, 11 pages, 2020.

[4] N. Zhou, Y. Hu, L. Gong, and G. Li, "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations," *Quantum Information Processing*, vol. 16, p. 164, 2017.

[5] G. Ye, K. Jiao, C. Pan, and X. Huang, "An effective framework for chaotic image encryption based on 3D logistic map," *Security and Communication Networks*, vol. 2018, Article ID 8402578, 11 pages, 2018.

[6] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, Article ID 105816, 2020.

[7] B. Gaurav, M. Qing, and W. Jonathan, "Selective image encryption based on pixels of interest and singular value decomposition," *Digital Signal Processing*, vol. 22, pp. 648–663, 2012.

[8] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 01, Article ID 1850010, 2018.

[9] W. Wen, R. Tu, and K. Wei, "Video frames encryption based on DNA sequences and chaos. Eleventh international conference on digital image processing (ICDIP 2019)," *International Society for Optics and Photonics*, vol. 11179, Article ID 111792T, 2019.

[10] W. Wen, Y. Zhang, Z. Fang, and J.-x. Chen, "Infrared target-based selective encryption by chaotic maps," *Optics Communications*, vol. 341, pp. 131–139, 2015.

[11] W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "Image salient regions encryption for generating visually meaningful ciphertext image," *Neural Computing and Applications*, vol. 29, no. 3, pp. 653–663, 2018.

[12] J. W. Byun, "A generic multifactor Authenticated key exchange with physical unclonable function," *Security and Communication Networks*, vol. 2019, Article ID 5935292, 15 pages, 2019.

[13] Y. Zhang, D. Xiao, W. Wen, and Y. Tian, "Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform," *Optics & Laser Technology*, vol. 54, pp. 1–6, 2013.

[14] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[15] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[16] R. Enayatifar, F. G. Guimarães, and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," *Optics and Lasers in Engineering*, vol. 115, pp. 131–140, 2019.

[17] J. Chen, Z.-l. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 2018.

[18] A. Engelmann and A. Jukan, "Toward all-optical layered encryption: a feasibility analysis of optical stream cipher," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2689–2704, 2019.

[19] H. Chen, C. Tanougast, Z. Liu, W. Blondel, and B. Hao, "Optical hyperspectral image encryption based on improved

Chirikov mapping and gyrator transform," *Optics and Lasers in Engineering*, vol. 107, pp. 62–70, 2018.

[20] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, Article ID 107563, 2020.

[21] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding," *Optics and Lasers in Engineering*, vol. 124, Article ID 105837, 2020.

[22] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 08, no. 06, pp. 1259–1284, 1998.

[23] L. Bao and Y. Zhou, "Image encryption: generating visually meaningful encrypted images," *Information Sciences*, vol. 324, pp. 197–207, 2015.

[24] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[25] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[26] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[27] Y. Chen, Y. Huang, Y. Han et al., "Multi wings chaotic encryption for physical layer security in optical PAM4-DMT System," in *Proceedings of the 2019 Asia Communications and Photonics Conference (ACP)*, pp. 1–3, Chengdu, China, November 2019.

[28] T. Hu, Y. Liu, L.-H. Gong, S.-F. Guo, and H.-M. Yuan, "Chaotic image cryptosystem using DNA deletion and DNA insertion," *Signal Processing*, vol. 134, pp. 234–243, 2017.

[29] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Article ID 107484, 2020.

[30] Y. Zhang, P. Wang, L. Fang, X. He, H. Han, and B. Chen, "Secure transmission of compressed sampling data using edge clouds," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6641–6651, 2020.

[31] W. Shen, J. Qin, and J. Ma, "A lightweight identity-based cloud storage auditing supporting proxy update and workload-based payment," *Security and Communication Networks*, vol. 2019, Article ID 8275074, 15 pages, 2019.

[32] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proceedings of the 2008 46th Annual Allerton IEEE Conference on Communication, Control, and Computing*, pp. 813–817, Monticello, IL, USA, October 2008.

[33] Y. Zhang, Q. He, Y. Xiang et al., "Low-cost and confidentiality-preserving data acquisition for internet of multimedia things," *IEEE Internet of Things Journal*, vol. 5, pp. 3442–3451, 2017.

[34] H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, and D. Wang, "Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 11, no. 3, pp. 558–573, 2017.

[35] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Optics and Lasers in Engineering*, vol. 82, pp. 79–86, 2016.

[36] L. Itti, C. Koch, and E. Niebur, "A model of saliency-based visual attention for rapid scene analysis," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 11, pp. 1254–1259, 1998.

[37] Y. Fang, Z. Chen, W. Lin, and C.-W. Lin, "Saliency detection in the compressed domain for adaptive image retargeting," *IEEE Transactions on Image Processing*, vol. 21, no. 9, pp. 3888–3901, 2012.

[38] W. Wen, Y. Hong, Y. Fang, M. Li, and M. Li, "A visually secure image encryption scheme based on semi-tensor product compressed sensing," *Signal Processing*, vol. 173, Article ID 107580, 2020.

[39] Y. Yang, X. Qin, and B. Wu, "Median filter based compressed sensing model with application to MR image reconstruction," *Mathematical Problems in Engineering*, vol. 2018, Article ID 8316194, 9 pages, 2018.

[40] Y. Zhang, J. Zhou, F. Chen et al., "A block compressive sensing based scalable encryption framework for protecting significant image regions," *International Journal of Bifurcation and Chaos*, vol. 26, no. 11, Article ID 1650191, 2016.

[41] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, "Colour light field image encryption based on DNA sequences and chaotic systems," *Nonlinear Dynamics*, vol. 99, no. 2, pp. 1587–1600, 2020.

[42] J. Wang, L. Y. Zhang, J. Chen, G. Hua, Y. Zhang, and Y. Xiang, "Compressed sensing based selective encryption with data hiding capability," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6560–6571, 2019.

[43] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.

[44] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.