

Research Article

A Novel Selective Encryption Method Based on Skin Lesion Detection

Dezhi An , Jun Lu, Shengcai Zhang, and Yan Li

School of Cyber Security, Gansu University of Political Science and Law, Lanzhou 730070, China

Correspondence should be addressed to Dezhi An; adz6199@gsli.edu.cn

Received 1 May 2020; Revised 24 July 2020; Accepted 24 July 2020; Published 28 September 2020

Academic Editor: António M. Lopes

Copyright © 2020 Dezhi An et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Due to the semitrusted cloud, privacy protection of medical images in medical imaging clouds has become a precondition. For the privacy of patients and the security of medical images in the cloud, this paper proposes a selective encryption based on DNA sequence and chaotic maps for skin lesion image. Initially, we design a transition region-based level set evolution functional which is merged into a variational level set expression with two extra energy functionals, to segment skin lesion image. Once skin lesion detection has been performed, the detected skin lesion pixels are encrypted by employing chaotic systems and DNA sequences. We apply 2D-LASM and 1D-LSS to produce the pseudorandom sequences and use the hash function of the plaintext image to calculate the secret keys of the encryption system. Results demonstrate that the proposed segmentation method is particularly suitable for the detection of skin lesion images with strong noise and complex background. Meanwhile, security analysis also reveals that this selective encryption has a large security key space and high sensitivity to the plaintext image and the secret key.

1. Introduction

Medical image processing has developed for many years, and there are more and more powerful tools to help dermatologists identify and classify skin lesions [1–6]. Among all kinds of skin lesions, melanoma is the most aggressive skin cancer and the one leading to the most deaths. However, in the transmission and storage, there are potential threats to the important content of these images, which makes the protection of important content a challenging problem [7–11].

To achieve confidentiality, encryption as an effective technology includes full encryption [12–15] and selective encryption [3, 16–20]. Full encryption involves encrypting complete image information, while selective encryption mainly focuses on the encryption of part of the image data. In recent years, selective encryption has been widely studied because of its tradeoff between computational complexity and security. Based on pixels of interest and singular value decomposition, Bhatnagar et al. proposed a selective image encryption scheme [16]. In [17], an edge-based lightweight image encryption scheme is proposed by Zhang et al. which employs chaos-based reversible hidden transform and

multiple-order discrete fractional cosine transform. Wen et al. [18] proposed a selective method to encrypt the object of infrared images by using chaotic maps. Furthermore, they protected the salient regions of image by embedding them into a visually meaningful image in the work [19]. Actually, selective encryption is suitable for protecting the important areas of the image, but not the entire image. Most of the existing detection schemes do not have the ability to handle the skin lesions image [20].

In recent years, there are many techniques used for skin lesion detection, such as active contour model [21, 22], thresholding [23], fuzzy c-means [24], and neural network [25], and local binary patterns clustering [2]. Rajab et al. [25] introduce the thresholding algorithm and neural network to realize the skin lesion detection. This technique can obtain the efficient result. However, the technique based on neural networks cannot deal with noisy images as the details of the edge were broken. Motivated by these problems, Barcelos et al. [26] posed a detection model for skin lesion image starting from nonlinear diffusion equations. However, in the case of strong noise and complex background, this model has some limitations.

So far, various techniques have been proposed for object detection. The level set method is an important segmentation method which has the advantages of allowing variable topological transformation and flexible numerical implementation. However, this method has the problem of contour initialization and reinitialization. To overcome these problems, Li et al. put forward a segmentation model without reinitialization [27] and distance regularized level set evolution (DRLSE) [28]. The two models employ the corresponding deviation penalty energy to force the level set function approach sign distance function and finally eliminate reinitialization. However, these two models need to initialize the contour. Recently, He et al. [29] proposed a weighted region-scalable fitting (WRSF) model which can handle well on medical images with intensity inhomogeneity, but fails to segment these with strong noises. In a partial differential equation (PDE) formulation, two geometric active contour models are, respectively, proposed by Wen et al. [22, 30]. The two models have the ability to segment skin lesion images with blurred boundaries.

Inspired by the works of Wen et al. [22, 30], but different from these works, this paper proposes a transition region- (TR-) based energy functional which can compel the level set function to have opposite different inside and outside image target. And then this energy functional is introduced into a variational level set expression with two extra energy functionals. According to the characteristics of significant regions, chaotic systems and DNA are combined to design suitable sensitive encryption algorithms.

The main contributions of this paper include the following points:

- (1) A novel skin lesion detection-based selective encryption method is proposed. This method consists

of the detection process of skin lesion image and selective encryption for privacy protection of skin lesion data.

- (2) In the skin lesion detection scheme, we propose a transition region- (TR-) based energy functional which compels this function to have a different sign inside and outside the image target. And the TR-based functional is introduced into a variational level set expression.
- (3) In the selective encryption for skin lesion data, we employ chaotic systems and DNA sequence operations. 2D-LASM and 1D-LSS are chosen to generate pseudorandom sequences and determine DNA encoding/decoding rules of the skin lesion region and the key matrix.

The structure of this article is described as follows. The DRLSE model and DNA encoding/decoding rules are introduced in Section 2. Section 3 describes the proposed skin lesion detection-based selective encryption algorithm which contains skin lesion detection based on TR-based energy functional model and selective encryption algorithm. The experimental results and security analysis are depicted in Section 4. The conclusions are given in Section 5.

2. Related Works

2.1. The DRLSE Model. Li et al. [27] extended distance regularized level set evolution (DRLSE) and proposed a variational level set model for image segmentation. In a variational framework, this model is formulated about the level set function ϕ as follows:

$$\begin{aligned} E(\phi) &= \mu R_p(\phi) + E_{\text{ext}}(\phi) \\ &= \mu R_p(\phi) + \lambda L_g(\phi) + \alpha A_g(\phi), \\ &= \mu \int_{\Omega} p(|\nabla\phi|) dx + \lambda \int_{\Omega} g(|\nabla I_{\sigma}|) |\nabla H(\phi)| dx dy + \alpha \int_{\Omega} g(|\nabla I_{\sigma}|) H(-\phi) dx dy, \end{aligned} \quad (1)$$

where $\mu > 0$, $\lambda > 0$, $\alpha \in \mathbb{R}$ are constants, $R_p(\phi)$ is the level set smooth term, and $E_{\text{ext}}(\phi)$ is a certain external energy term. p is a potential (or energy density) function $p: [0, \infty] \rightarrow \mathbb{R}$, $g(|\nabla I_{\sigma}|) = (1/(1 + |\nabla I_{\sigma}|^2))$ is an edge indicator function, and $I_{\sigma} = G_{\sigma} * I$ is the convolution of the image I and the Gaussian kernel G_{σ} with standard deviation σ . The function H is the one-dimensional Heaviside function.

The term $L_g(\phi)$ computes the length of the zero level set of ϕ in the conformal metric $d(s) = g(C(p)) |C'(p)| dp$ where $C(p)$ is a parameterized representation of the zero level set of ϕ . The term $A_g(\phi)$ can be viewed as the weighted area of the region $\{x \mid \phi(x) < 0\}$, which forces the zero level

set of ϕ to expand or shrink faster during the evolutionary process. Whether the parameter α of $A_g(\phi)$ can be positive or negative depends on the relative position of the object's initial contour.

The level set evolution equation corresponding to equation (1) is obtained by the following equation:

$$\frac{\partial \phi}{\partial t} = \mu \operatorname{div}(d_p(|\nabla\phi|) \nabla\phi) + \lambda \delta(\phi) \operatorname{div}\left(g \frac{\nabla\phi}{|\nabla\phi|}\right) + \alpha g \delta(\phi), \quad (2)$$

with initial condition $\phi(x, 0) = \phi_0(x)$, where $d_p(s)$ and $p(s)$ are, respectively, defined by

$$d_p(s) \triangleq \frac{p'(s)}{s}, \quad (3)$$

$$p(s) = \begin{cases} \frac{1}{2\pi} (1 - \cos(2\pi s)), & \text{if } s \leq 1, \\ \frac{1}{2}(s-1)^2, & \text{if } s \geq 1. \end{cases} \quad (4)$$

2.2. DNA Encoding/Decoding Rules. A DNA sequence consists of A (adenine), T (thymine), C (cytosine), and G (guanine), where A and T, G, and C are complementary pairs. Further, 0 and 1 are complementary, so the DNA sequence is similar to the binary data. According to the principle of complementary pairing, Table 1 shows eight types of encoding rules by the Watson–Crick complement regulation [31–33].

There introduce algebraic computation operators for DNA sequences to spread DNA computing, such as XOR. On the basis of traditional rule, the XOR operation is manipulated on DNA sequences. There exist 8 types of DNA XOR rules corresponding to 8 types of DNA encoding rules, and Table 2 shows DNA XOR under Rule 1.

3. Skin Lesion Detection-Based Selective Encryption Algorithm

This paper proposes a secure and privacy-preserving technique to protect patients' privacy and improve the security of skin lesion images. There have four stages of the proposed technique, as shown in Figure 1: TR-based energy functional based on adaptive function, skin lesion detection model, selective encryption based on skin lesion detection, and decryption.

3.1. Skin Lesion Detection Based on TR-Based Energy Functional Model. Because of the variation of the shape and appearance of the skin lesions, the detection of the edge of the skin lesions is a very important problem. This paper proposes a TR-based energy functional model to segment the skin lesion image.

3.1.1. TR-Based Energy Functional. Introduce an adaptive function via the gray mean of the transition region, which will serve as the weight of the proposed TR-based energy functional.

For an image $I: \Omega \subset \mathbb{R}^2 \rightarrow \mathbb{R}$ and function $\phi: \Omega \subset \mathbb{R}^2 \rightarrow \mathbb{R}$, we design

$$\nu(x, y) = M - I(x, y), \quad (5)$$

$$E(\phi) = E_v(\phi) + \lambda E_{\text{reg}}(\phi) + \mu R_p(\phi),$$

$$= \int_{\Omega} \nu(x, y) g(|\nabla I_{\sigma}|) H(-\phi) dx dy + \lambda \int_{\Omega} g(|\nabla I_{\sigma}|) \delta(\phi) |\nabla \phi| dx dy + \mu \int_{\Omega} p(|\nabla \phi|) dx dy, \quad (7)$$

TABLE 1: DNA encoding scheme.

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

TABLE 2: DNA XOR rule.

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

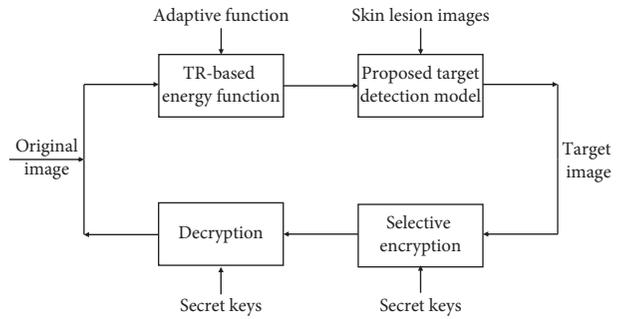


FIGURE 1: The framework of the proposed technique.

where M is mean value of the transition region drawn by LETREM algorithms [22, 30]. As shown in the works [22, 30], we observe that the function $\nu(x, y)$ has opposite sign inside and outside the transition region. A binary image is displayed in Figure 2(a), and the corresponding 3D plot of $\nu(x, y)$ is described in Figure 2(b). From Figure 2(b), we can really reveal that the function $\nu(x, y)$ has opposite sign inside and outside the transition region.

Now we pose a novel energy (TR-based energy) based on the function $\nu(x, y)$ defined by (5). Given a level set function $\phi: \Omega \subset \mathbb{R}^2 \rightarrow \mathbb{R}$, we design this external energy as follows:

$$E_v(\phi) = \int_{\Omega} \nu(x, y) g(|\nabla I_{\sigma}|) H_{\varepsilon}(-\phi) dx dy, \quad (6)$$

where $H_{\varepsilon}(\phi)$ is the one-dimensional smoothed Heaviside function and g is the edge indicator given by $g(s) = e^{-s/4}$.

3.1.2. The Proposed Detection Model. Following the DRLSE model, the energy functional $E_v(\phi)$ is introduced into a variational level set expression. The energy functional for the proposed model is defined as follows:

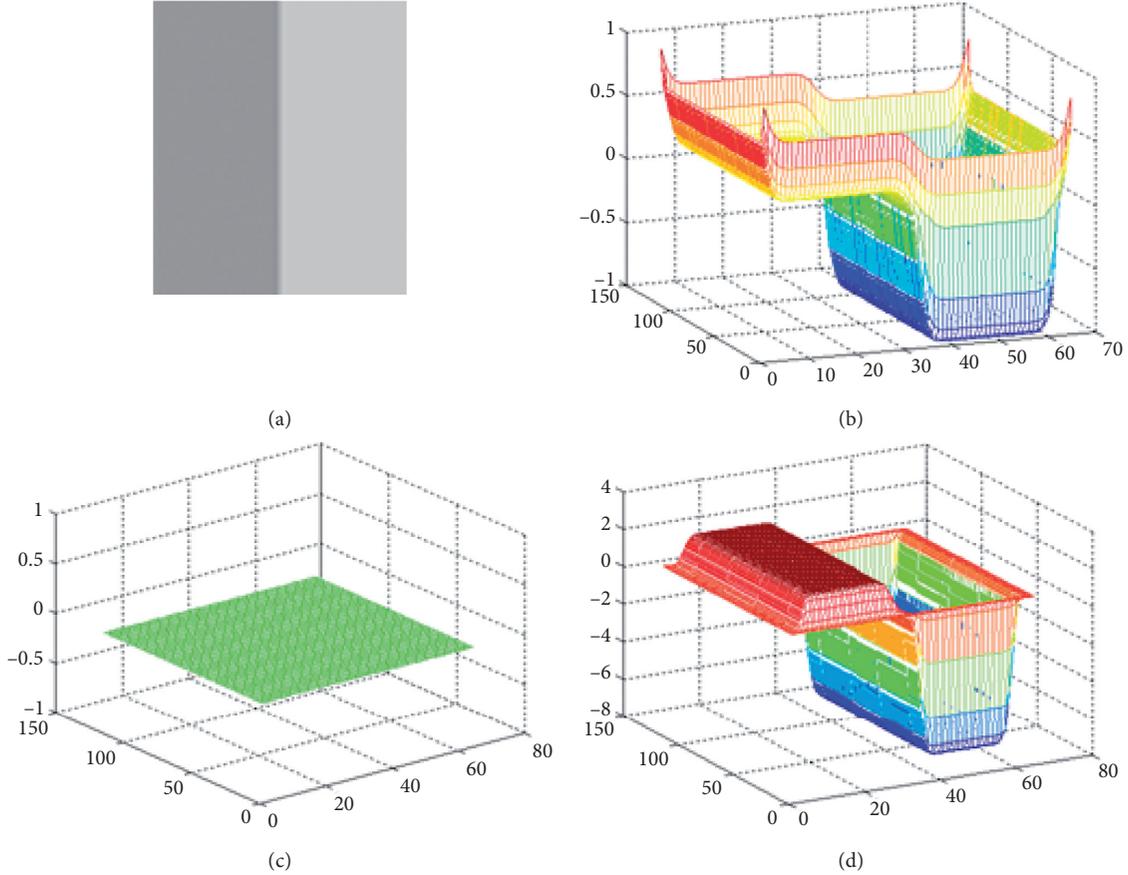


FIGURE 2: The 3D plot of $v(x, y)$ and its contribution to level set evolution driven by equation (14). (a) The binary image with two disjoint regions separated by a vertical edge. (b) 3D plot of $v(x, y)$. (c) 3D plot of the initial level set function ($\phi_0 = 0$). (d) 3D plot of the level set function after one iteration.

where the function p is given by (4) and $g(s) = e^{(-s/4)}$ is the edge indicator function, which is different from that used in the DRLSE model.

We employ the gradient descent method to minimize energy functional (7) with respect to ϕ and obtain the associated level set evolution equation:

$$\begin{aligned} \frac{\partial \phi}{\partial t} = & \mu \operatorname{div}(d_p(|\nabla \phi|) \nabla \phi) + \lambda \delta(\phi) \operatorname{div}\left(g(|\nabla I_\sigma|) \frac{\nabla \phi}{|\nabla \phi|}\right) \\ & + v(x, y) g(|\nabla I_\sigma|) \delta(\phi), \end{aligned} \quad (8)$$

where $d_p(s)$ is defined by equation (3).

3.2. Selective Encryption Based on Skin Lesion Detection. In our encryption method, the proposed TR-based energy functional model can be chosen to detect skin lesion images. Further, the extracted significant region is encrypted by employed chaotic maps and DNA sequences.

3.2.1. Encryption and Decryption Process. Chaotic encryption technology has strong sensitivity. DNA computing has many advantages, such as massive parallelism, huge storage, and ultra-low power consumption. Image encryption

method based on DNA encoding integrates biological characteristics, but its encryption principle is closely related to chaotic encryption technology.

Step 1. Construct 1D logistic-sine system (LSS) and 2D logistic-adjusted-sine map (LASM) and by chaotic maps.

Logistic map has high sensitivity and chaotic behavior. The sine map has a similar chaotic behavior with the logistic map. We employ 1D logistic-sine system (LSS) [34] and 2D logistic-adjusted-sine map (2D-LASM) [35] by the logistic and sine maps as seed maps:

$$x_{n+1} = \left(r x_n (1 - x_n) + \frac{(4-r) \sin(\pi x_n)}{4} \right) \bmod 1, \quad (9)$$

$$\begin{cases} y_{i+1} = \sin(\pi \mu (z_i + 3) y_i (1 - y_i)), \\ z_{i+1} = \sin(\pi \mu (y_{i+1} + 3) z_i (1 - z_i)). \end{cases} \quad (10)$$

In the LSS system, the parameter $r \in (0, 4]$, and \bmod function is the remainder used to return the division of two numbers. In 2D-LASM system, $\mu \in (0, 1)$, and y and z are state variables, $y, z \in (0, 1)$.

Step 2. Generate the initial values and parameter for 1D-LSS and 2D-LASM.

We employ the SHA 256 hash of the plaintext image to generate a 256-bit external secret key. Then the 256-bit secret key K is divided into 8-bit blocks (k_i), so K can also be described as follows:

$$K = k_1, k_2, \dots, k_{32}. \quad (11)$$

Then, the initial values can be produced as follows:

$$\left\{ \begin{array}{l} x_0 = \left(x'_0 + \frac{\text{mod}\left(\left(k_1 \oplus k_2 \oplus k_3 + k_4 + \sum_{i=1}^{32} k_i\right), 2^8\right)}{256} \right) \text{mod}1, \\ r_0 = \left(r'_0 + \frac{\text{mod}\left(\left(k_5 \oplus k_6 \oplus k_7 + k_8 + \sum_{i=1}^{32} k_i\right), 2^8\right)}{256} \right) \text{mod}1, \\ y_0 = \left(y'_0 + \frac{\text{mod}\left(\left(k_9 \oplus k_{10} \oplus \dots \oplus k_{14} + k_{15} \oplus k_{16} + \sum_{i=1}^{32} k_i\right), 2^8\right)}{256} \right) \text{mod}1, \\ z_0 = \left(z'_0 + \frac{\text{mod}\left(\left(k_{17} \oplus k_{18} \oplus \dots \oplus k_{22} + k_{23} \oplus k_{24} + \sum_{i=1}^{32} k_i\right), 2^8\right)}{256} \right) \text{mod}1, \\ \mu_0 = \left(\mu'_0 + \frac{\text{mod}\left(\left(k_{25} \oplus k_{26} \oplus \dots \oplus k_{30} + k_{31} \oplus k_{32} + \sum_{i=1}^{32} k_i\right), 2^8\right)}{256} \right) \text{mod}1, \end{array} \right. \quad (12)$$

where mod is the modular operation, μ_0 and r_0 are the system parameters, x_0 , y_0 , and z_0 are initial values, and μ'_0, r'_0, x'_0, y'_0 , and z'_0 are the given values used as secret keys.

Step 3. Perform DNA dynamic encoding process of the significant region.

Let I be an original skin lesion image, and detect the skin lesion region of image I using the proposed method as described in Section 3.1. Design an appropriate rectangle with the size of $m \times n$ to cover the skin lesion region.

- (1) Convert each pixel in the rectangle block to its binary form, and obtain a binary matrix p of $m \times 8n$.
- (2) Use x_0, r_0 produced in Step 1 for 1D-LSS system to iterate $(2000+4mn)$ times, then abandon the former 2000 values, and get chaotic sequences X to perform a matrix U of $m \times 4n$.
- (3) Generate dynamic encoding mode for every element of the significant region as follows:

$$R(i, j) = \left\{ \begin{array}{l} 1, 0 \leq U(i, j) < 0.125, \\ 2, 0.125 \leq U(i, j) < 0.25, \\ 3, 0.25 \leq U(i, j) < 0.375, \\ 4, 0.375 \leq U(i, j) < 0.5, \\ 5, 0.5 \leq U(i, j) < 0.625, \\ 6, 0.625 \leq U(i, j) < 0.75, \\ 7, 0.75 \leq U(i, j) < 0.875, \\ 8, 0.875 \leq U(i, j) \leq 1. \end{array} \right. \quad (13)$$

- (4) Group every element of the matrix p , then employ the corresponding encoding scheme in equation (13) to encode these elements, and finally form the encoded DNA a matrix $p1$ of $m \times 4n$.

Step 4. Generate the key matrix K .

- (1) Use μ_0 , y_0 , and z_0 produced in Step 1 for 2D-LASM map to iterate $(2000 + q)$ times, where $q = \max\{m, 4n\}$, and abandon the former 2000 values to avoid the transient effect. Pick up the former m values from Y to construct matrix $Y1$ of size $m \times 1$, and use the former $4n$ values from Z to produce a matrix $Z1$ of size $1 \times 4n$. Manipulate matrix multiplying operation for $Y1$ and $Z1$ to get a matrix V with $m \times 4n$.
- (2) Employ the matrix V to produce the key matrix K by the following formula:

$$K(i, j) = \begin{cases} A, 0 < V(i, j) < 0.25, \\ T, 0.25 \leq V(i, j) < 0.5, \\ C, 0.5 \leq V(i, j) < 0.75, \\ G, 0.75 \leq V(i, j) < 1. \end{cases} \quad (14)$$

Step 5. Implement DNA XOR between the $p1$ and the key matrix K by equation (13):

$$C(i, j) = p1(i, j) \oplus K(i, j), \quad (15)$$

where C denote the ciphertext DNA matrix.

Step 6. Decode the matrix C by equation (13) to get the cipher block E .

Step 7. Employ the Arnold transform to make cipher block E have more secure encryption effect.

Arnold scrambling is an image encryption technology which disturbs the original image by changing the position of image pixels. In our method, Arnold transform is applied to further disturb the pixel of ciphertext image E , and its definition is represented as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1 + ab \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N, \quad (16)$$

where a and b are positive integers, randomly selected scrambling parameters from the positive integers that affect the output value, and usually 1 is selected. N denotes the order of the image matrix.

The decryption process is the reverse operation of the encryption process.

4. Experimental Result and Discussion

In this section, a series of skin lesion images are applied to analyze the performance of the proposed detection. From Table 3, the strengths and limitations of different DNA sequence encryption algorithms are summarized and compared. Therefore, the proposed method is superior to other compared encryption schemes in some aspects.

4.1. Experimental Results of Skin Lesion Detection. Without loss of generality, we set default parameters: $\tau = 1$, $\Delta t = 5$, $\mu = 0.04$, $\lambda = 20$, $c = 10$, and $\varepsilon = 1$ (for $\delta_\varepsilon(z)$). The values of σ and α are provided in the following figure. In all the experiments, we simply initialize level set functions to zero function, i.e., $\phi_0 = 0$.

The following two experiments demonstrate that the diffusion model [26] and our model are applied to extract the lesion areas in several skin lesion images. It is a very important task to extract lesion regions from the background in the field of computer vision. Because of the variation in the shape and appearance of the skin lesions, the detection of the edge of the skin lesions is a very important problem. Other factors such as strong noise and hair, dim edges, or strong asymmetry, or complex texture background also make the segmentation process more difficult.

Figure 3 describes that the proposed model can handle well for four skin lesion images and is compared with the diffusion model [26] through the detective results and computing times. For a fair comparison, we select the best scale parameter K and the most suitable high threshold t_H (given in the caption of Figure 3) for the diffusion method. Our level set evolution starts with $\phi_0 = 0$, so there are no initial contours in the top row of Figure 3. It is clearly seen from the bottom that our model (with parameters $\sigma = 2.4, 2.3, 2, \alpha = 0.99, 0.9, 0.78$ for the first three images) obtains the satisfactory segmentation results for four images, which are almost the same as the diffusion model visually, but the important improvement of the proposed method is that computation complexity is lower than that in the diffusion method. Iteration umbers and CPU times of the two methods are exhibited in Table 4. It can be surveyed that iteration numbers and CPU times of the proposed method are all less than those of the diffusion model.

Figure 4 shows detective results of our model for ten skin lesions image with blurry boundaries and/or asymmetric lesions areas, as shown in the first and third rows. It is difficult to extract the lesion areas in such images. Here, we do not show the detective results of the diffusion model [26], as the model cannot achieve satisfactory detective results. It can be observed from the second and fourth rows of Figure 4 that our method ($\sigma = 6, 6, 2.3, 2, 2, \alpha = 0.83, 0.81, 0.9, 0.85, 0.99$ for images in the first row; and $\sigma = 2, \alpha = 0.85, 0.75, 0.95, 0.85, 0.85$ for images in the third row), and for the last two images), stating with a constant function $\phi_0 = 0$, accurately extracts the lesion area boundaries.

We conclude this section by simply describing about parameters α and σ ; for our model, the parameters α and σ are very important for the function $v(x, y)$. By experiments, our observations are as follows: for skin lesions images, σ is typically about 2, and α is in the range between 0.75 and 0.99.

4.2. Experimental Results of Skin Lesion Region Protection.

In this section, we, respectively, exhibit the subjective visual effect and objective data to prove the performance of plaintext encryption. We take four skin lesion images from

TABLE 3: Summary and comparison with the existing DNA encryption algorithm.

Algorithms	Encryption types	Image types	Advantages	Limitations
[36]	Full encryption	General image	Increases the strength of encryptions	High computational complexity
[37]	Full encryption	General image	Strong key sensitivity and security	Few experiments to resist security attacks
[33]	Full encryption	Colour light field image	Suitable for colour light field image	Complexity and need high computation
Proposed	Selective encryption	Skin lesion image	Sufficient experimental analysis and applied to skin lesion image	Increase the execution speed

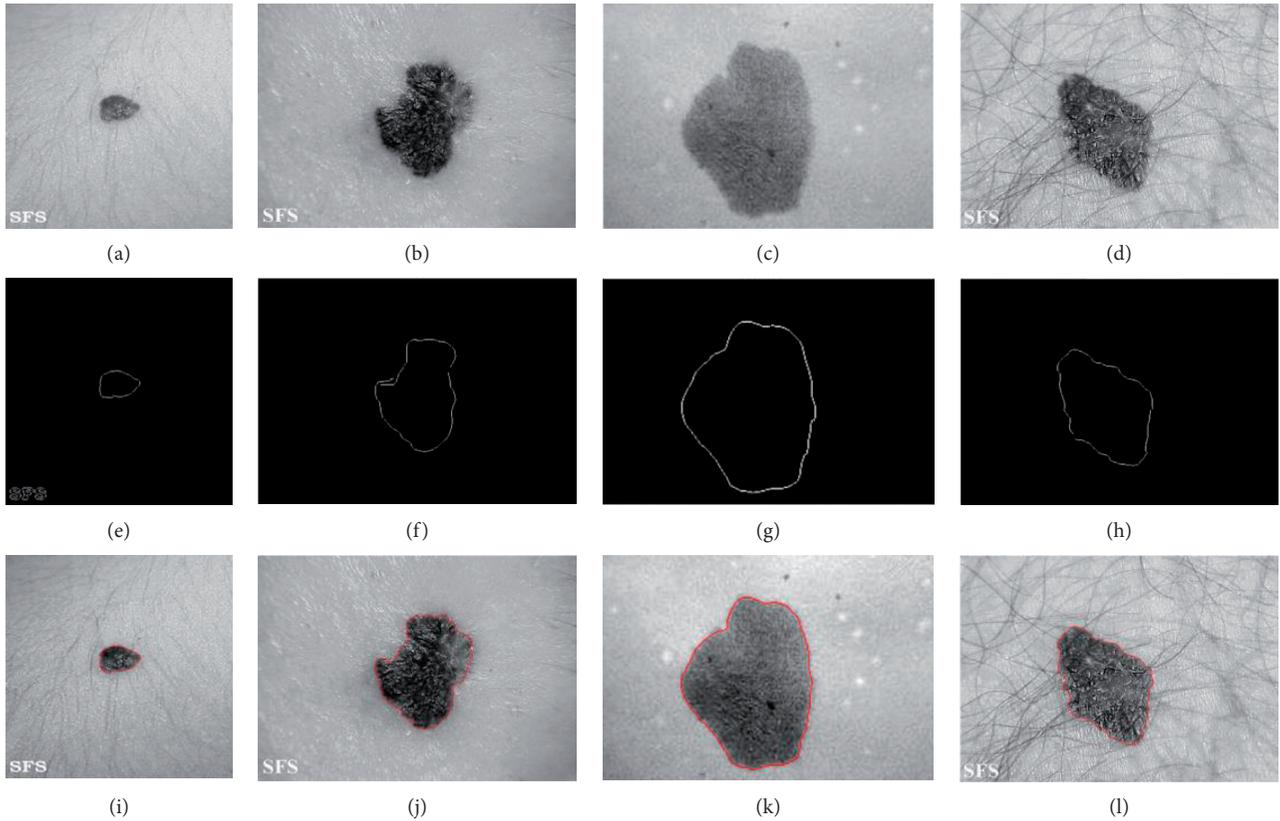


FIGURE 3: Comparison of both models. Middle row: diffusion model ($K = 0.002, 0.00025, 0.0004, 0.0004; t_H = 0.8, 0.55, 0.35, 0.6$). Bottom row: our model.

Figures 3 and 4, as examples using the initial values x_0, r and x_0, y_0, z_0, μ for the 1D-LSS system and 2D-LASM system. It can be seen from Figure 5 that the proposed method can protect significant regions.

4.2.1. Key Space Analysis. In the proposed encryption method, the key includes (i) the given initial values and the parameters of 1D LSS and 2D-LASM, $\mu'_0, r'_0, x'_0, y'_0,$ and $z'_0,$ and (ii) the 256-bit external secret key. If the accuracy of the float is 10^{-16} , then $\mu'_0, r'_0, x'_0, y'_0,$ and z'_0 can be any one among 10^{16} possible values. The whole key space is $10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 2^{128} = 10^{80} \times 2^{128}$, which is larger than 2^{100} . Therefore, the proposed encryption

method has a large key space to defend against brute force attacks.

4.2.2. Key Sensitivity Analysis. The encryption scheme expects a slight change in the key to result in completely different results. Key sensitivity guarantees the uniqueness of the key. The encryption algorithm contains multiple secret keys, and the value contributed by each key is different in the encryption process. The original clear image can be decrypted only when all the keys are correct.

To verify the sensitivity of the encryption algorithm for each key, the key sensitivity is performed by changing just one key in 10^{-15} position and keeping the rest same. The

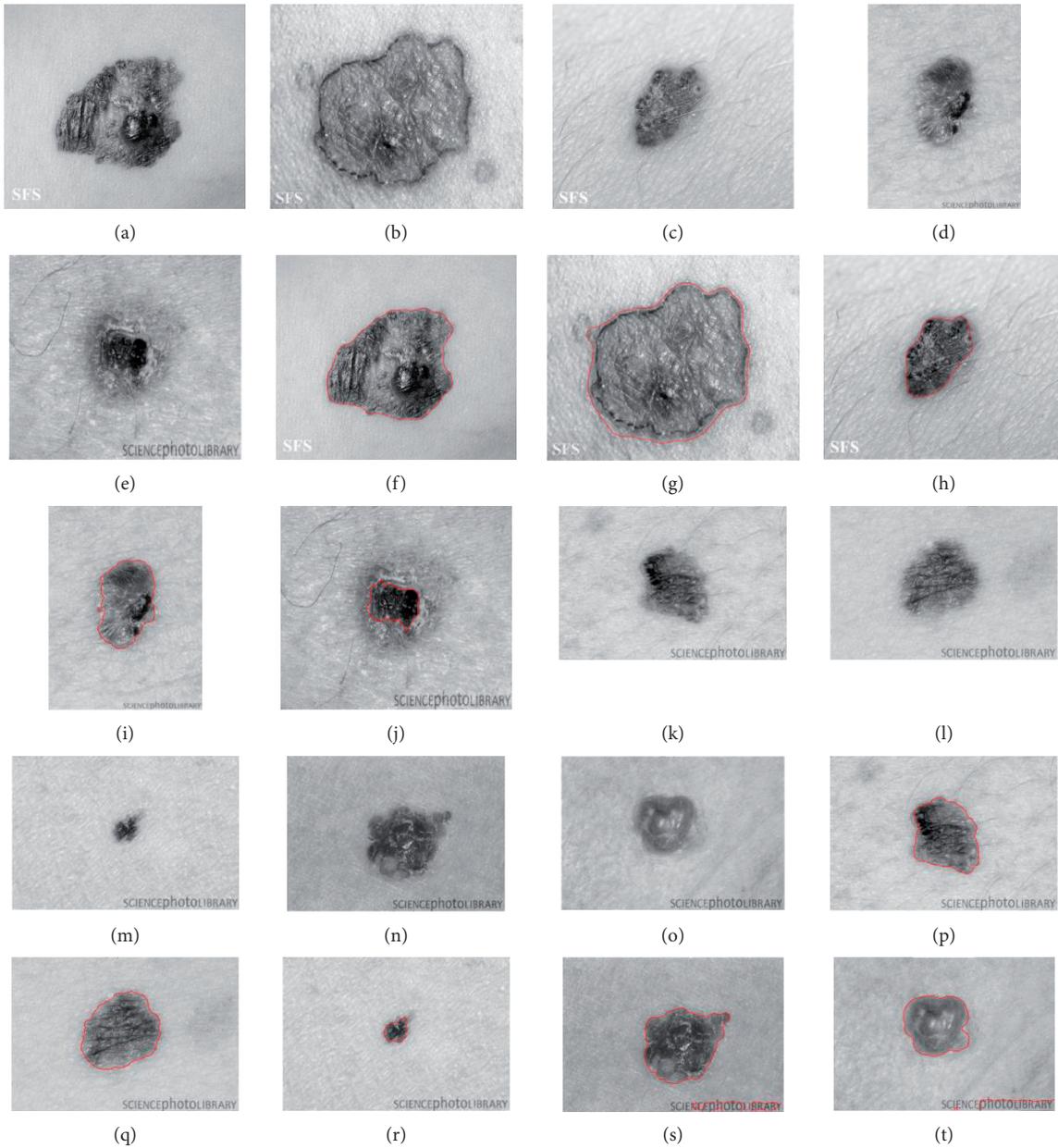


FIGURE 4: Detective results of our model for ten skin lesion images with blurred boundaries and asymmetric areas. The first and third rows: original images; the second and fourth rows: final detective results (left to right: 95, 150, 18, 10, 20 iterations for the second row; 10, 20, 10, 10, 25 iterations for the fourth row).

TABLE 4: Number of iterations and CPU times in seconds of Figure 3.

Model	(a)	(b)	(c)	(d)
Diffusion [26]	100	200	100	300
	69.5	195.2	20.2	366.7
Ours	25	20	30	13
	12.6	11.1	6.1	7.3

NPCR of the original target and changed cipher image-blocks for the keys of the proposed algorithm are listed in Table 5. It can be obviously seen from this table that when

the key has a trivial change, the encrypted image-blocks have a complete change, and more than 99% pixels are modified compared with Figure 5(i), which implies the proposed scheme is highly key sensitive to all the keys.

4.2.3. Histogram of Analysis. Histogram describes the distribution of pixel values in an image. A secure cipher image encryption method should have a uniform histogram [38–41]. Generally speaking, a natural image should follow a regular distribution, while the secure encryption method should force the cipher image to follow a consistent distribution. Figure 6 reveals that our method can effectively

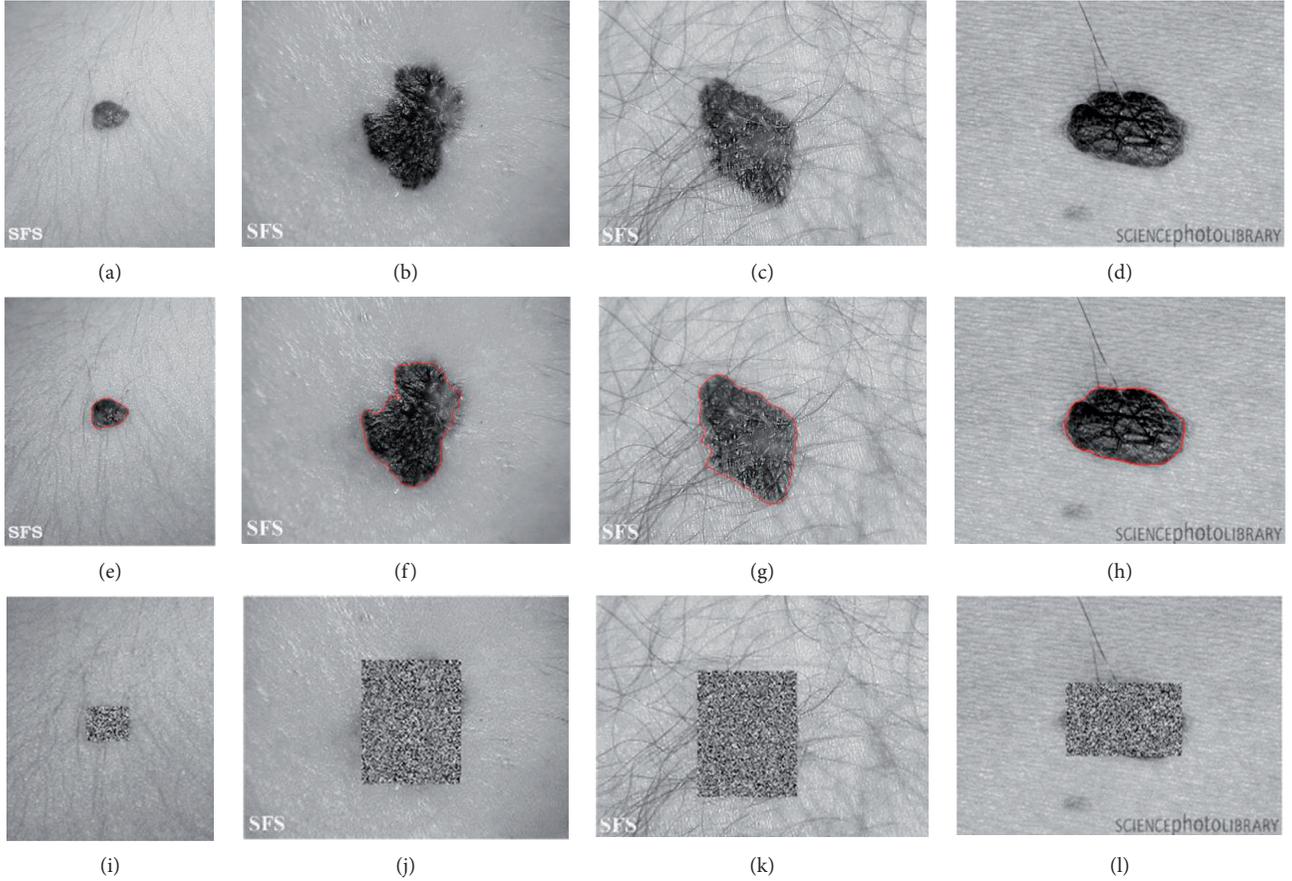


FIGURE 5: The first row: plain images. The second row: final detective results. The third row: cipher images.

TABLE 5: Difference between decrypted image-blocks and target with changed decryption key.

Decryption key	$\mu'_0 + 10^{-15}$	$r'_0 + 10^{-15}$	$x'_0 + 10^{-15}$	$y'_0 + 10^{-15}$	$z'_0 + 10^{-15}$
Comparison with Figure 5(i)	99.605%	99.623%	99.615%	99.634%	99.616%

prevent significant regions from being attacked by statistical attack opponents.

Furthermore, the variances of histograms and chi-square test are used to evaluate the uniformity of the pixel value distribution. The variances of histograms and chi-square values can be calculated as follows [42]:

$$\text{var}(Z) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (z_i - z_j)^2, \quad (17)$$

$$\chi^2 = \sum_{i=0}^{255} \frac{(n_i - n/256)^2}{(n/256)}, \quad (18)$$

where n_i is the occurrence frequency of gray level i , $(n/256)$ is the expected occurrence frequency of each of gray level, and n is the number of all the pixels. $Z = \{z_1, z_2, \dots, z_{256}\}$ is the vector of the histogram values, and z_i and z_j are the numbers of pixels in which gray values are equal to i and j , respectively.

As shown in ref. [42], according to the chi-square distribution table, at 255 degrees of freedom and 0.05 significance level, $\chi_{255,0.05}^2 = 293.2478$. With a significance level of 0.05, the chi-square test results are listed in Table 6. The results indicate that the null hypothesis that the distribution is uniform cannot be rejected at 0.05 significance level. In this circumstance, redundancy of the plain images has successfully been concealed and consequently does not provide any clue to apply statistical attacks. Besides, Table 7 lists the comparison of histogram variance among image encryption schemes. From this table, we can observe that the average histogram variance of the proposed method is less than the schemes in ref. [37, 42].

4.2.4. Correlation Analysis. We arbitrarily pick up 2,500 pairs of adjacent pixels in three directions which include horizontal, vertical, and diagonal from the skin lesion region of the plain image and the corresponding cipher image. The correlation coefficients r_{xy} of two adjacent pixels are computed through the following formulas:

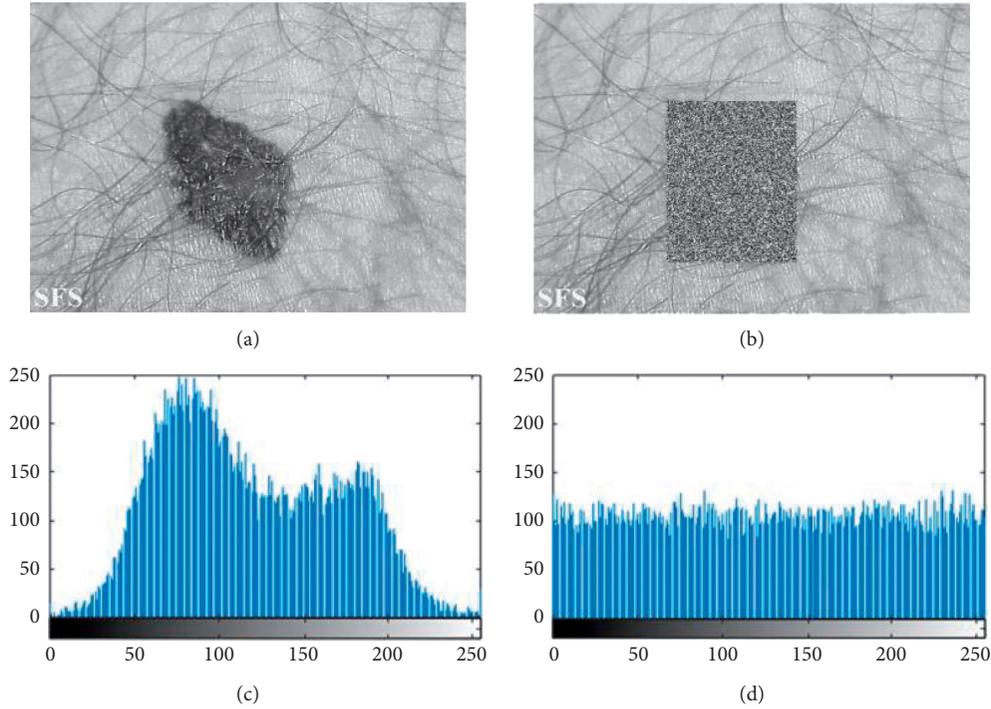


FIGURE 6: Skin lesion image, cipher image, the corresponding target, and cipher image-block histograms.

TABLE 6: Chi-square test results of the cipher image-blocks.

Test images	Figure 5(a)	Figure 5(b)	Figure 5(c)	Figure 5(d)
$\chi^2_{255,0.05}$	293	293	293	293
χ^2	258	272	219	237
Results	Pass	Pass	Pass	Pass

TABLE 7: Comparison of histogram variance among different image encryption schemes.

Test images	Proposed	[42]	[37]
Figure 5(a)	1051	1134	1230
Figure 5(b)	980	1022	1010
Figure 5(c)	1154	1205	1180
Figure 5(d)	947	1020	1035
Average	1033	1095	1114

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)], \quad (19)$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (20)$$

where x and y are values of the two adjacent pixels in the image. $E(x)$ and $D(x)$ are given by

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i, \quad (21)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2. \quad (22)$$

Figure 7 illustrates the correlations of two horizontally, vertically, and diagonally adjacent pixels in the skin lesion region of plaintext image and its cipher image. Besides, Table 8 describes the correlation coefficients of adjacent pixels of the skin lesion region in the plaintext image and cipher image. We can clearly observe from these results that the correlations between adjacent pixels in each direction of cipher image-block are much lower than the corresponding plaintext blocks.

4.2.5. Information Entropy Analysis. Information entropy $H(m)$ is employed to measure the uniform distribution of pixel grayscale, and its definition is given as follows:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)}, \quad (23)$$

where m_i denotes the pixel value and the $p(m_i)$ is the probability of m_i .

If the pixel values are distributed more uniformly, the information entropy is larger. For a gray image in the range of $[0, 255]$, ideally, if all pixel values have an equal probability of occurrence, the upper limit value of image entropy H is 8. From Table 9, we can observe that the entropies of the cipher image-blocks are closed to 8, which have been added to the corresponding plaintexts. Therefore, this reveals that our method can defend the entropy cryptanalysis.

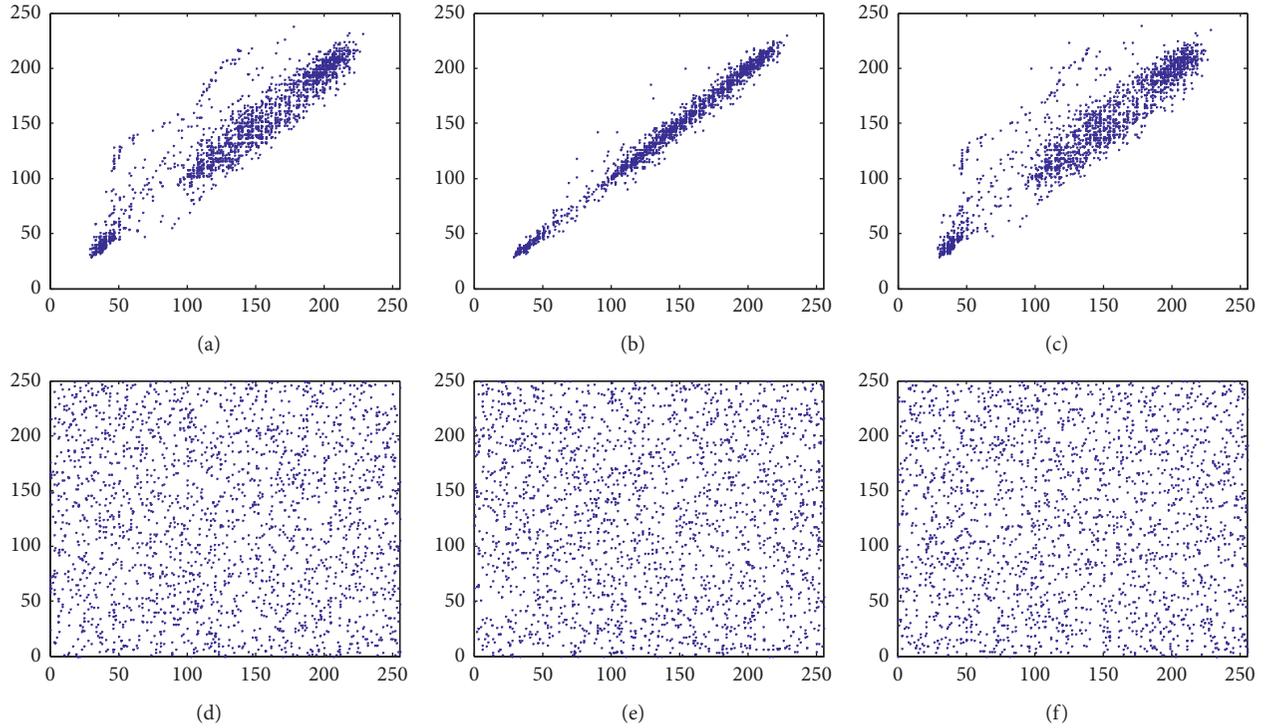


FIGURE 7: Correlations of horizontally, vertically, and diagonally adjacent pixels: (a–c) skin lesion region; (d–f) the corresponding cipher image-block.

TABLE 8: Correlation coefficients of adjacent pixels.

Direction	Target	Cipher image-block
Horizontal	0.8846	-0.0105
Vertical	0.9041	0.0338
Diagonal	0.9174	0.0023

TABLE 9: Information entropy analysis.

Skin lesion image	Target	Cipher image-block
Figure 5(a)	6.9755	7.8860
Figure 5(b)	7.4671	7.9939
Figure 5(c)	7.5990	7.9937
Figure 5(d)	7.5354	7.9799

4.2.6. Computational and Complexity Analyses. Algorithmic complexity is an important reference standard for algorithm performance. We analyze the computational complexity of the proposed scheme and compare it with ref. [36].

For the proposed scheme, the computational complexity has two parts: target extraction and target encryption. In the target extraction process, the main source of time complexity is the numerical solution of level set evolution equation (2). In this paper, we employ a simple explicit finite difference scheme to solve this equation. Its time complexity is $O(m \times n)$. The encryption process contains the DNA level diffusion part and the Arnold scrambling further disturbs the pixel of cipher image-block. For the DNA level diffusion part, the complexity of the time-consuming includes

generating chaotic sequences and DNA encoding and decoding operations. We, respectively, adopt 1D LSS and 2D-LASM to produce the chaotic sequences for the encoded DNA matrix and the key matrix K in the diffusion steps. The time complexity of generating LSS system-based sequence is $O(8)$, and the time complexity of generating the 2D-LASM system-based sequence is $O(2 \times m \times n)$. So the total time complexity of generating chaotic sequences is $O(2 \times m \times n)$. The time complexity of DNA encoding and decoding operation is $O(4 \times (m \times n)/8) = O((m \times n)/2)$. The time complexity of Arnold scrambling is no more than $O(m \times n)$. So the total time complexity of the proposed algorithm is $O(2 \times m \times n)$.

For ref. [36], there are three stages of encryption steps, that is shuffling, diffusion, and shuffling. The authors employ the complex hyperchaotic system to generate the chaotic sequences for increasing the strength of encryptions and decryptions, whereas low-dimensional chaotic systems are adopted in our algorithm, and the low-dimensional system is easy to implement and can run faster. As mentioned in ref. [36], the time complexity of the algorithm is $O(4 \times m \times n)$. Therefore, the time complexity of our algorithm is lower than that of ref. [36].

5. Conclusion

A novel approach for skin lesion detection and privacy protection is presented in this paper. Firstly, a transition region-based level set evolution method is proposed to detect skin lesion image. This idea of the proposed method is to construct the energy functional that compels the level set

function to have a different sign inside and outside the image target. Then this functional is introduced into a variational level set expression with the other two functionals. Then, once skin lesion detection has been performed, the detected skin lesion pixels are encrypted by utilizing DNA sequences and chaotic systems. We employ 2D-LASM and 1D-LSS to make the pseudorandom sequences and use the 256-bit hash value of the plaintext image to generate the initial values and system parameters. Different from these existing encryption algorithms based on DNA computing, the DNA encoding/decoding rules of the skin lesion region and the key matrix are generated by the skin lesion region, and this may increase resilience to statistical attacks. Experimental results of skin lesions detection show that the proposed method is particularly suitable for the detection of skin lesion images with strong noise and complex background. Meanwhile, security analyses reveal that our selective encryption method has a good encryption effect.

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

D.A. conceptualized the study, was responsible for methodology, and was involved in funding acquisition; J.L. was responsible for software and was involved in visualization; S.Z. validated and investigated the data; Y.L. performed formal analysis, reviewed and edited the manuscript, and supervised the study; J.L. and S.Z. prepared the original draft.

Acknowledgments

This research was funded by the Team Project of Collaborative Innovation in Universities of Gansu Province (no. 2017C-16) and the Major Project of Gansu University of Political Science and Law (no. 2016XZD12).

References

- [1] H. Kaufman, *The Melanoma Book: a Complete Guide to Prevention and Treatment*, Vol. 1, Gotham Books, New York, NY, USA, 2005.
- [2] P. Pereira, R. Fonseca-Pinto, R. Paiva et al., "Dermoscopic skin lesion image segmentation based on local binary pattern clustering: comparative study," *Biomedical Signal Processing and Control*, vol. 59, Article ID 101924, 2020.
- [3] Y. Zhang, H. Huang, Y. Xiang, L. Y. Zhang, and X. He, "Harnessing the hybrid cloud for secure big image data service," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1380–1388, 2017.
- [4] Y. Zhang, P. Wang, H. Huang, Y. Zu, D. Xiao, and Y. Xiang, "Privacy-assured FogCS: chaotic compressive sensing for secure industrial big image data processing in fog computing," *IEEE Transactions on Industrial Informatics*, 2020, In press.
- [5] 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.
- [6] J. Chen, L. Chen, L. Y. Zhang, and Z.-L. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 301–322, 2019.
- [7] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: a survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1093–1111, 2019.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] 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, 2019.
- [12] T. Zhao and Q. Ran, "The weighted fractional fourier transform and its application in image encryption," *Mathematical Problems in Engineering*, vol. 2019, Article ID 4789194, 10 pages, 2019.
- [13] 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.
- [14] H. Fan and M. Li, "Cryptanalysis and improvement of chaos-based image encryption scheme with circular inter-intra-pixels bit-level permutation," *Mathematical Problems in Engineering*, vol. 2017, Article ID 8124912, 11 pages, 2017.
- [15] Y. Niu, X. Sun, C. Zhang, and H. Liu, "Anticontrol of a fractional-order chaotic system and its application in color image encryption," *Mathematical Problems in Engineering*, vol. 2020, Article ID 6795964, 12 pages, 2020.
- [16] G. Bhatnagar and Q. M. Jonathan Wu, "Selective image encryption based on pixels of interest and singular value decomposition," *Digital Signal Processing*, vol. 22, no. 4, pp. 648–663, 2012.
- [17] 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.
- [18] 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.
- [19] 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.

- [20] D. Xiao, Q. Fu, T. Xiang, and Y. Zhang, "Chaotic image encryption of regions of interest," *International Journal of Bifurcation and Chaos*, vol. 26, no. 11, Article ID 1650193, 2016.
- [21] D. Chung and G. Sapiro, "Segmenting skin lesions with partial-differential-equations-based image processing algorithms," *IEEE Transaction on Medical Imaging*, vol. 19, no. 7, pp. 763–767, 2000.
- [22] W. Wen, C. He, and M. Li, "Transition region-based active contour model for image segmentation," *Journal of Electronic Imaging*, vol. 22, no. 1, pp. 1–12, 2013.
- [23] I. Maglogiannis, S. Pavlopoulos, and D. Koutsouris, "An integrated computer supported acquisition, handling, and characterization system for pigmented skin lesions in dermatological images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 9, no. 1, pp. 86–98, 2005.
- [24] Y. Lim and S. Lee, "On the color image segmentation algorithm based on the thresholding and the fuzzy c-means techniques," *Pattern Recognition*, vol. 23, no. 9, pp. 935–952, 1990.
- [25] M. I. Rajab, M. S. Woolfson, and S. P. Morgan, "Application of region-based segmentation and neural network edge detection to skin lesions," *Computerized Medical Imaging and Graphics*, vol. 28, no. 1-2, pp. 61–68, 2004.
- [26] C. A. Z. Barcelos and V. B. Pires, "An automatic based nonlinear diffusion equations scheme for skin lesion segmentation," *Applied Mathematics and Computation*, vol. 215, no. 1, pp. 251–261, 2009.
- [27] C. Li, C. Xu, C. Gui, and M. Fox, "Level set evolution without re-initialization: a new variational formulation," in *Proceedings of the 2005 IEEE CVPR*, pp. 430–436, San Diego, CA, USA, June 2005.
- [28] C. Li, C. Xu, C. Gui, and M. Fox, "Distance regularized level set evolution and its application to image segmentation," *IEEE Transactions on Image Processing*, vol. 19, no. 12, pp. 3243–3254, 2010.
- [29] C. He, Y. Wang, and Q. Chen, "Active contours driven by weighted region-scalable fitting energy based on local entropy," *Signal Processing*, vol. 92, no. 2, pp. 587–600, 2012.
- [30] W. Wen, C. He, Y. Zhang, and Z. Fang, "A novel method for image segmentation using reaction-diffusion model," *Multi-dimensional Systems and Signal Processing*, vol. 28, no. 2, pp. 657–677, 2017.
- [31] J. D. Watson and F. H. C. Crick, "Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid," *Nature*, vol. 171, no. 4356, pp. 737–738, 1953.
- [32] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7111–7130, 2019.
- [33] 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.
- [34] 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.
- [35] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.
- [36] K. Abhimanyu Kumar Patro, B. Acharya, and V. Nath, "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation," *IETE Technical Review*, vol. 37, no. 3, pp. 223–245, 2019.
- [37] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Computing and Applications*, vol. 31, no. 1, pp. 219–237, 2019.
- [38] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.
- [39] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.
- [40] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Information Processing*, vol. 14, no. 4, pp. 1193–1213, 2015.
- [41] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, "Image encryption scheme by combining the hyper-chaotic system with quantum coding," *Optics and Lasers in Engineering*, vol. 124, Article ID 105836, 2020.
- [42] K. Abhimanyu Kumar Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools and Applications*, vol. 79, pp. 12959–12994, 2020.