Signal Processing 181 (2021) 107911

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Content-adaptive image encryption with partial unwinding decomposition

Yongfei Wu[a,b], Liming Zhang[b,*], Tao Qian[c], Xilin Liu[a], Qiwei Xie[d,e]

[a] College of Data Science, Taiyuan University of Technology, Taiyuan, Shanxi, 030024, China
[b] Faculty of Science and Technology, University of Macau, Taipa, Macau, China
[c] Macao Center of Mathematical Sciences, Macau University of Science and Technology, Avenida Wai Long, Taipa, Macau, China
[d] Data Mining Lab, Beijing University of Technology, Beijing, 100190, China
[e] Institute of Automation, Chinese Academy of Sciences, Beijing, 100190, China

ARTICLE INFO

Article history:
Received 17 August 2020
Revised 27 October 2020
Accepted 23 November 2020
Available online 26 November 2020

Keywords:
Information security
Image encryption
Image-content-adaptive encryption
Partial unwinding decomposition

ABSTRACT

This study designs a novel image encryption cryptosystem through the two-dimensional partial unwinding decomposition (2D-PUD). It consists of three stages. Firstly, a stream sequence (first part of the security key) is generated by pseudo-random number. Secondly, the plain image is decomposed into three parts by 2D-PUD: one 2D decomposition component, two 1D decomposition components, and the average intensity value of the image. Finally, the 2D decomposition component is shuffled by a generalized Arnold transform where the average intensity value is selected as second part of the security key. The diffusion scheme is subsequently applied to the scrambled image via exclusive OR operations with the randomized 1D decomposition components (third part of the security key) along rows and columns to obtain the cipher image. Due to the adaptive attribute of 2D-PUD, the generated 1D decomposition components are completely distinct for different images. In addition, we can also make them significantly different by tuning the decomposition times for the same image. Thus, the proposed algorithm is an image-content-adaptive encryption scenario that can effectively resist cryptographic attacks. Simulation results demonstrate that our proposed method has excellent encryption performance and can resist against various typical attacks, including brute force, statistical, entropy, and differential attacks.

1. Introduction

The utilization and exchange of multimedia content, such as digital images, video sequences, and audio signals, have shown an explosive growth owing to the dramatic development of computer network and communication technology. Digital images as visual multimedia content are widely used in many fields, including medical, commercial and military. In these cases, the transmission and storage of images across a public channel and cloud service must be private and accessible only by authorized agencies. Thus, the security problem of digital images has become increasingly imperative and drawn extensive attention. To maintain the confidentiality of important digital images, researchers have developed different types of technology, such as image hiding [1,2], image watermarking [3,4] and image encryption [5,6]. Among these security measures, image encryption that typically converts meaningful images into unrecognized and unintelligible noise-like image is the most straightforward strategy [7,8].

So far, tremendously different schemes and algorithms [9–20] for encrypting image have been developed in the literature, and from the perspective of the encryption domain, they are generally classified into the spatial-domain and frequency-domain image encryption algorithms. The spatial domain-based encryption techniques directly manipulate the pixels or blocks of the image plane itself, whereas the frequency domain-based methods modify the frequency coefficients of the transformed image. In the early stage, image encryption is achieved by permutation-only algorithms, which simply scrambles image matrices/blocks in the spatial domain [11,16,19] or coefficient matrices/blocks in the transform domain [21,22] based on different technologies. Nevertheless, these approaches have a low security level because they incompletely dislocate the essential characteristics (frequency distribution) and use a permutation mapping matrix based on a pseudo-random number generator that can generate only limited keys. Furthermore, the permutation-only based encryption schemes are known to be fragile to ciphertext-only attack and known-plaintext attack [23–25]. To achieve a higher level of security, another

* Corresponding author.
E-mail addresses: lmzhang@um.edu.mo, lmzhang@umac.mo (L. Zhang).

https://doi.org/10.1016/j.sigpro.2020.107911
0165-1684/

method termed permutation-diffusion is used to shuffle the image matrices/blocks and modify image pixel values via different techniques. Thereafter, image encryption technologies based on permutation-diffusion theory in the spatial or transform domain have been proposed [26,27] and have become the main architecture in the field of current image encryption.

However, encryption algorithms based on permutation-diffusion in the spatial domain still cannot satisfy the security requirements, because they often have limited key space and are insecure against classical statistical attack and chosen-chipertext attack [28]. To overcome these limitations, permutation-diffusion based image encryption technology in the transform domain, such as Fourier transform (FT) [27], discrete cosine transform (DCT) [29,30], and discrete wavelet transform (DWT) [31], achieve better security. For instance, double random phase encoding (DRPE) [9] is a well-known optical image encryption technique in the Fourier domain. Many improved variants that generalize the DRPE method by changing the masks and Fourier transform into other transforms such as the fractional Fourier transform [10], the Fresnel transform [32], the jigsaw transform [33], the Gyrator transform [34] and the Hartley transform [35], have been proposed and reported. Unfortunately, these transform domain-based encryption algorithms still have limitations and are easy to be cracked because they usually use fixed basis functions (trigonometric functions, wavelet functions) in the process of representing all images.

In this paper, we propose a novel image cipher algorithm based on the two-dimensional partial unwinding decomposition (2D-PUD) [36] method. Firstly, By using a pseudo-random number generator, we generate a stream sequence that is set as the first part of the security key. Secondly, The original image is decomposed into three main parts by the 2D-PUD method: the 2D decomposition component, 1D decomposition components and the average intensity value of the image. In the permutation phase, the average intensity value of the image is chosen as the second part of the security key for the generalized Arnold transform, which shuffles the pixels position of the 2D decomposition component. In the diffusion process, the randomized 1D decomposition components are selected as the third part of the security key to modify the value of the shuffled image via exclusive-OR (XOR) operations along the rows and columns of the scrambled image, respectively. Since the third part of the security key (randomized 1D decomposition components) we use for encryption is dependent on the plainimage, the whole cryptosystem is plain-image-content-adaptive. The proposed cryptosystem achieves an upgraded level of security when measured by the number of pixel change rate (NPCR) and unified average changing intensity (UACI) [37]. In contrast to the existing transform methods, such as DFT and DWT, which use the same fixed basis functions to represent all images, the 2D-PUD method adaptively selects different basis functions in a given search dictionary space to represent different images. The contributions and novelties of this article are summarized as follows:

- The study introduces and applies the 2D-PUD method to image encryption first time in the literature, and the proposed encryption scheme can well protect plain images.
- The 2D-PUD technology introduced as the core of image cryptosystem can produce encryption key from the plain image which greatly improves the diffusion property of cryptosystem. Hence, the designed encryption scheme enhances the protection performance against the differential attack.
- The generated two 1D decomposition components are distinct for two different images; even for the same image, a significant difference in 1D decomposition components can be generated by setting different decomposition times. Therefore, the designed cryptosystem is an image-content-adaptive encryption scenario that is robust against cryptographic attacks, such as chosen-plaintext attack and chosen-ciphertext attack.

The rest of the paper is organized as follows. A brief mathematical foundation of unwinding decomposition (UD) and 2D-PUD are provided in Section 2. Section 3 introduces the proposed encryption scheme in detail. To assess the encryption performance of the proposed scheme, simulation results and security analysis performed on various images are presented in Section 4. Finally, conclusions are drawn in Section 5.

2. Mathematical foundation

Adaptive Fourier decomposition (AFD) proposed by Qian et al. [38] offers fast decomposition of any 1D input signal in energy sense via adaptively selecting basis functions based on a given basis search dictionary, which is a type of positive frequency expansion algorithm and has been successfully applied to different signal processing fields [39–41]. AFD is different from traditional Fourier decomposition, which uses the fixed Fourier bases (trigonometric functions). One-dimensional unwinding decomposition (1D-UD) based on the factorization operation is another type of AFD, which is first proposed by Coifman et al. in [42–45] and achieves faster positive frequency decomposition than AFD. In [46,47], the author proposes a novel algorithm that combines the maximal selection and factorization process together to decompose the 1D signals, which further improves the convergence speed. To decompose any 2D signal, such as an image, 2D partial unwinding decomposition (2D-PUD) [36] that generalizes the 1D-UD case to the 2D case has recently been proposed. The effectiveness of the UD approaches has been verified through theoretical analysis and practical applications [43].

2.1. Mathematical foundation of 1D-UD

Let $\mathbb{C}$ denote the complex plane, $\mathbb{D} \subset \mathbb{C}$ be the open unit disc and $\mathbb{T}$ be its boundary. Based on classical Fourier series theory, any complex-valued function of finite energy defined on the unit circle $f(e^{it}) \in L^2(\mathbb{T})$ can be expressed as

$$f(e^{it}) = \sum_{k=-\infty}^{\infty} c_k e^{ikt} = \sum_{k=0}^{\infty} c_k e^{ikt} + \sum_{k=-\infty}^{-1} c_k e^{ikt} = f^+(e^{it}) + f^-(e^{it}). \quad (1)$$

If f is real-valued, due to the relation $c_{-k} = \bar{c}_k$ ($\bar{c}_k$ is the conjugate complex of c_{-k}), we can obtain

$$f = 2\mathrm{Re} f^+ - c_0, \quad (2)$$

where *Re* denotes the real part of the complex-valued function f^+, and f^+ is called the analytic signal associated with f. Thus, the formulation (2) indicates that the study of f can be transformed into the study of f^+.

Based on the Nevanlinna factorization theorem [48], the analytic function $f^+(z)(z = e^{it})$ can be decomposed into a product of an inner function $I(z)$ and an outer function $O(z)$ as follows:

$$f^+(z) = I(z)O(z), \quad (3)$$

where the outer function has the following formulation:

$$O(z) = \exp\{\frac{1}{2\pi}\int_{-\pi}^{\pi} \frac{e^{it}+z}{e^{it}-z} \log|f^+(e^{it})| dt\}. \quad (4)$$

The inner function part $I(z)$ can be further decomposed into a product of a Blaschke product part $B(z)$ and a singular inner function part $S(z)$. Thus, we have

$$f^+(z) = I(z)O(z) = B(z)S(z)O(z), \quad (5)$$

where

$$B(z) = z^m \prod_{z_k \neq 0} \frac{|z_k|}{z_k} \frac{z_k - z}{1 - \bar{z}_k z}, \tag{6}$$

and

$$S(z) = \exp\{-\int_{-\pi}^{\pi} \frac{e^{it} + z}{e^{it} - z} d\mu(t)\}, \tag{7}$$

where $d\mu(t)$ is a positive regular Borel measure singular to the Lebesgue measure.

Note that the outer function $O(z)$ and singular inner function $S(z)$ are non-vanishing in the unit disc, so the Blaschke product collects all the zero roots of f^+. Accordingly, we can rewrite the formulation (5) as $f^+(z) = B(z)T(z)$ with $T(z) = S(z)O(z)$. The 1D-UD is given by the following iterative process:

$$\begin{aligned} f^+ &= B_1 T_1 = B_1(T_1(0) + (T_1(z) - T_1(0))) \\ &= B_1(T_1(0) + B_2 T_2) \\ &= c_1 B_1 + B_1 B_2 (T_2(0) + (T_2(z) - T_2(0))) \\ &\cdots \\ &= c_1 B_1 + c_2 B_1 B_2 + \cdots + B_1 B_2 \cdots B_N T_N, \end{aligned} \tag{8}$$

where $c_k = T_k(0), k \geq 1$, and each $B_k, k \geq 2$ is the Blaschke product generated by the zeros of the function $T_k(z) - T_k(0)$ in Hilbert space. It is noted that each of the Blaschke products B_k contains a factor z. It has also been showed that $\lim_{N\to\infty} \|B_1 B_2 \cdots B_N T_N\| = 0$. Hence, we obtain in the L^2-norm sense:

$$f^+(z) = \sum_{k=1}^{\infty} c_k B_1 B_2 \cdots B_k. \tag{9}$$

Due to the positive instantaneous frequency property of Blaschke products, 1D-UD gives rise to a fast positive instantaneous frequency decomposition of an analytic signal.

2.2. Mathematical foundation of 2D-PUD

Like the 1D signal, an image can be viewed as a real-valued function of finite energy defined on the square region $[0, 2\pi] \times [0, 2\pi]$ that is the characteristic boundary of 2-torus $\mathbb{D}^2 := \mathbb{D} \times \mathbb{D} = \{(z, w) : |z| < 1, |w| < 1\}$. For two functions f and g in the space, the square integral function on the boundary is a Hilbert space equipped with the inner product

$$\langle f, g \rangle = \frac{1}{4\pi^2} \int_{-\pi}^{\pi} \int_{-\pi}^{\pi} f(e^{it}, e^{is}) \bar{g}(e^{it}, e^{is}) dt ds. \tag{10}$$

Denote $\mathbb{T} = \partial\mathbb{D}$. For $f \in L^2(\mathbb{T}^2)$, based on multiple Fourier series one defines

$$f^{+,+}(e^{it}, e^{is}) = \sum_{k,l \geq 0} c_{kl} e^{i(kt+ls)}, \tag{11}$$

$$f^{+,-}(e^{it}, e^{is}) = \sum_{k,-l \geq 0} c_{kl} e^{i(kt+ls)}, \tag{12}$$

$$f^{-,-}(e^{it}, e^{is}) = \sum_{-k,-l \geq 0} c_{kl} e^{i(kt+ls)}, \tag{13}$$

and

$$F(e^{it}) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(e^{it}, e^{is}) ds, \tag{14}$$

$$G(e^{is}) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(e^{it}, e^{is}) dt. \tag{15}$$

Since $f \in L^2(\mathbb{T}^2)$, the following relation can be deduced

$$\begin{aligned} f(e^{it}, e^{is}) =& 2\mathrm{Re}\{f^{+,+}(e^{it}, e^{is})\} + 2\mathrm{Re}\{f^{+,-}(e^{it}, e^{is})\} \\ &- 2\mathrm{Re}(F^+)(e^{it}) - 2\mathrm{Re}(G^+)(e^{is}) + c_{00}, \end{aligned} \tag{16}$$

where Re means taking the real part of the complex-valued function.

The analysis of 2D-PUD for a real-valued image is converted into that of 2D Hardy space functions and related 1D-UD of some 1D functions.

In the following, we present the decomposition process of $f^{+,+}(z, w)$, and the other components in Eq. (16) can be decomposed by a similar procedure. We first assume

$$f^{+,+}(z, w) = f(z, w) = f_1(z, w) = \sum_{k,l \geq 0} c_{kl} z^k w^l, \tag{17}$$

and we obtain the splitting

$$f_1(z, w) = g(z, w) + f_1(z, 0) + f_1(0, w) - f_1(0, 0), \tag{18}$$

where

$$g(z, w) = f_1(z, w) - f_1(z, 0) - f_1(0, w) + f_1(0, 0). \tag{19}$$

It can be easily verified that there exists a function $f_2 \in H^2(\mathbb{D}^2)$ such that

$$g(z, w) = zw f_2(z, w). \tag{20}$$

Therefore, we have the relation

$$f_1(z, w) = zw f_2(z, w) + f_1(z, 0) + f_1(0, w) - f(0, 0). \tag{21}$$

Repeating the same procedure for $f_2(z, w)$, we obtain

$$\begin{aligned} f_1(z, w) =& zw[f_2(z, 0) + f_2(0, w) - f_2(0, 0)] \\ &+ f_1(z, 0) + f_1(0, w) - f_1(0, 0) \\ &+ (zw)^2 f_3(z, w). \end{aligned} \tag{22}$$

Repeating this process up to N- times, we obtain

$$\begin{aligned} f_1(z, w) =& \sum_{n=1}^{N} (zw)^{n-1}[f_n(z, 0) + f_n(0, w) - f_n(0, 0)] \\ &+ (zw)^N f_{N+1}(z, w). \end{aligned} \tag{23}$$

This decomposition series quickly converges to the initial Hardy space function $f^{+,+}(z, w)$.

The decomposition process of $f^{+,-}(z, w)$ is similar to the process of $f^{+,+}(z, w)$, and the 1D signals F^+ and G^+ can be decomposed by the 1D-UD algorithm depicted in Eq. (8). We take the real parts of all obtained decomposing terms and add the two 2D decomposition terms $f^{+,+}(z, w)$ and $f^{+,-}(z, w)$ together. Finally, we obtain three components including a 2D decomposition component, two 1D decomposition components and average intensity value of the image as follows:

$$\begin{aligned} &f(e^{it}, e^{is}) \approx \\ &2\mathrm{Re}\left\{\left(f^{+,+}\right)^N(e^{it}, e^{is})\right\} + 2\mathrm{Re}\left\{\left(f^{+,-}\right)^N(e^{it}, e^{is})\right\} \\ &- 2\mathrm{Re}(F^+)^N(e^{it}) - 2\mathrm{Re}(G^+)^N(e^{is}) + c_{00}. \end{aligned} \tag{24}$$

To simplify the notation, we denote the Eq. (24) as

$$f \approx 2U^N + 2V^N - 2F^N - 2G^N + c_{00}. \tag{25}$$

In summary, 2D-PUD method generates an adaptive basis by pursuing the maximal energy gain of the outer function in each decomposition iteration. Although theoretically it is an open and difficult problem, numerically it consistently converges quickly and robustly in both the energy and pointwise measurements.

3. Proposed encryption cryptosystem

In this section, a new image encryption method based on the 2D-PUD technology is proposed. The proposed encryption scheme is composed of three stages. In the first stage, we generate a

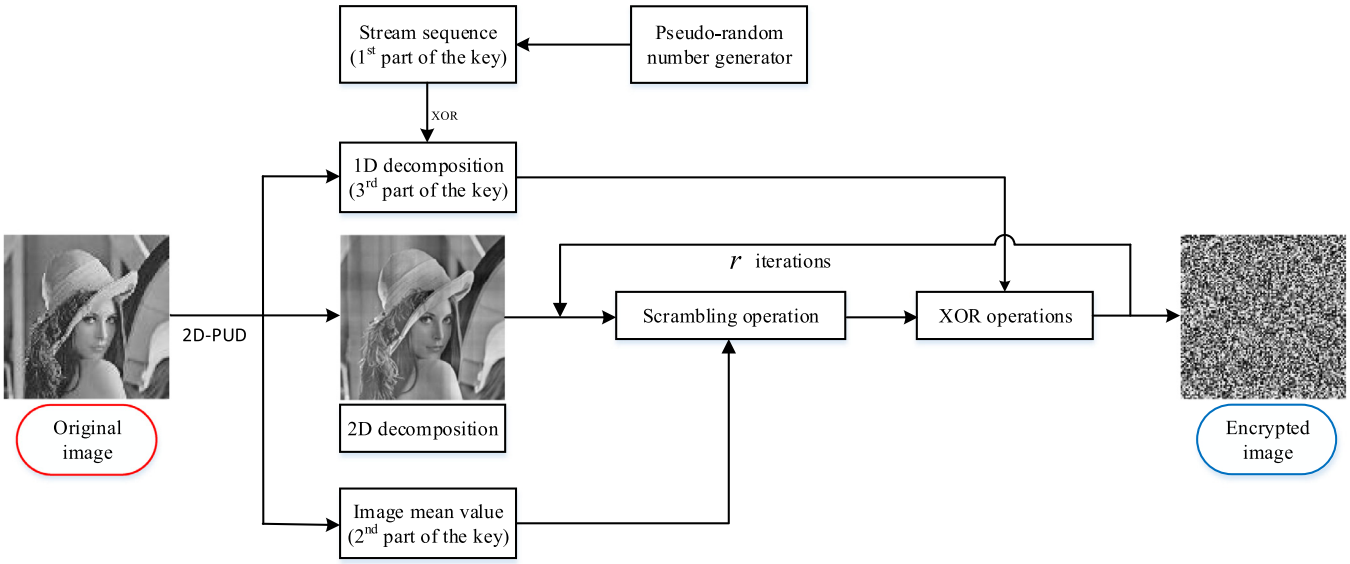

Fig. 1. Flowchart of the proposed encryption scheme.

stream sequence through certain pseudo-random number generator, such as chaotic systems. In the second stage, the plain image is decomposed into three parts which includes a 2D decomposing component, two 1D decomposing components and the intensity mean value of the image. Then, at the last stage, the 2D decomposing component is scrambled and diffused by the related algorithms using the intensity mean and randomized 1D decomposing components as the secure key, and a secure cipher image is obtained. The flowchart of the proposed encryption scheme is displayed in Fig. 1.

As depicted in Section 2, it can be found that the 2D-PUD transforms different images into different expanding systems (basic functions). It is completely different from classical transforms, such as DFT and DCT, which always use the same fixed bases (trigonometric functions) to represent all images. Based on the adaptive decomposition nature of 2D-PUD, we propose an image encryption scheme that can perform content-adaptive encryption for different images and even the same image.

3.1. Encryption and decryption process

In the encryption process, decompose the original image f up to N times by 2D-PUD first, and obtain Eq. (25). Denote $P = 2U^N + 2V^N$, and preprocess the 2D decomposition component and two 1D decomposition components by taking

$$P_1 = floor(P + 128), \tag{26}$$

$$F_1 = mod(2F^N \times 10^{15}, 255), \tag{27}$$

$$G_1 = mod(2G^N \times 10^{15}, 255). \tag{28}$$

Secondly, generate the scramble parameters p and q of the Arnold transform via mean image intensity value c_{00} as follows:

$$p = mod(c_{00} \times 10^{15}, 255), \tag{29}$$

$$q = mod(c_{00} \times 10^{17}, 255). \tag{30}$$

Thirdly, generate a stream sequence K by using a pseudo-random generator. The 1D decomposition components F_1 and G_1 are randomized via performing XOR operation with the generated stream sequence and obtain F_2 and G_2.

Fourthly, the 2D decomposition component is confused by a scrambling algorithm and c_{00} serves as the second part of the security key. In the confusion phase, any existing scrambling method can be exploited in the proposed scheme. Taking a simple example, this work employs the generalized Arnold transform to change the position of 2D decomposition components. Scramble the P_1 by the Arnold transform with parameters p, q and obtain P_2.

Fifthly, the scrambled image is diffused via conducting the XOR operations with the randomized 1D decomposition components. The randomized 1D decomposition components F_2 and G_2 are spliced together as the third part of the security key, denoted as $[F_2G_2]$. Perform the XOR operations on P_2 with F_2 and G_2 along the rows and columns, respectively.

Finally, repeat the scrambling and XOR procedures up to r rounds, and the cipher image C is obtained.

The detailed encryption process for the proposed algorithm is described in Algorithm 1.

Algorithm 1 Encryption Process.

Input: Original image f, decomposition times N, and the stream sequence K.
Output: Cipher image C.

1: Calculate F^N and G^N based on Eq. (8);
2: Calculate U^N and V^N based on Eq. (23);
3: Calculate P_1, F_1 and G_1 via Eqs. (26)-(28), respectively;
4: perform the XOR operations on F_1 and G_1 with K, respectively, and obtain F_2 and G_2
5: Calculate p and q via Eq. (29) and Eq. (30), respectively;
6: Scramble the P_1 by the Arnold transform with parameters p, q and obtain P_2;
7: Perform the XOR operations on P_2 with F_2 and G_2 along the rows and columns, respectively;
8: Repeat Step 6 to Step 7 up to r rounds, and the cipher image C is obtained. The encryption process is finished.

The procedure for image decryption is just a reverse of encryption scheme. Before the decryption, a secret key formed by three parts, i.e. splicing the stream sequence K, the average intensity value and two 1D decomposing components together, is transmit-

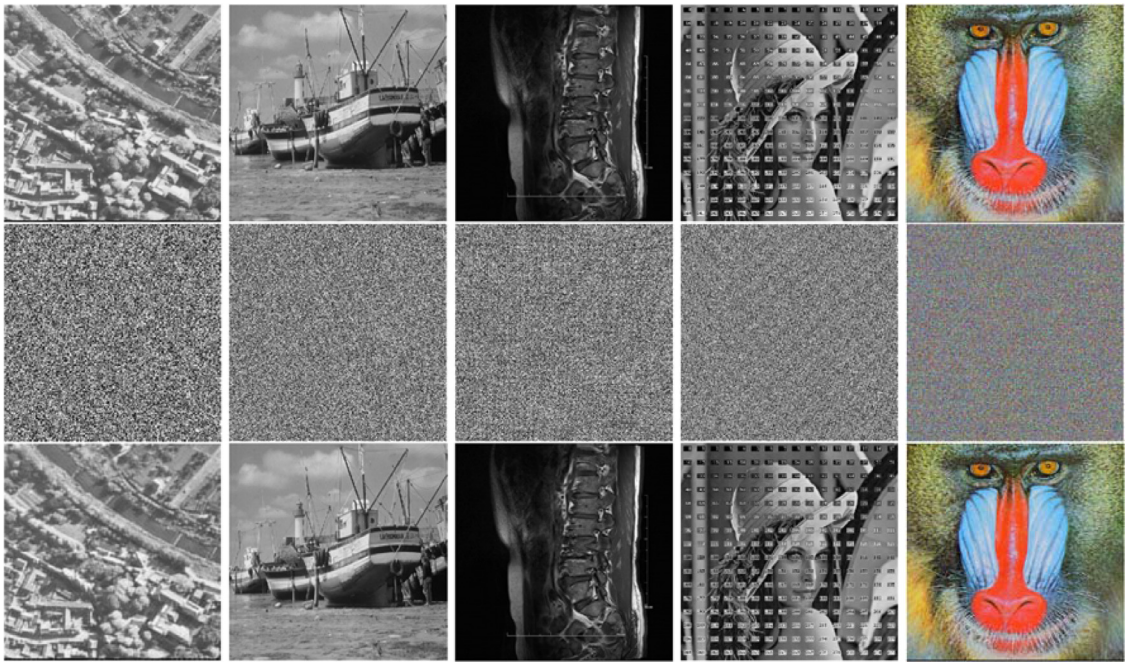

Fig. 2. Encrypted and decrypted results of different types of images. Top row: original images; Middle row: corresponding cipher images; Bottom row: restored images. Column one to five represents remote, grayscale, medical, synthetic and color images, respectively.

ted to the receiver. The authorized user applies the XOR operation to the encrypted image with the third part of the security key, and the unscrambling process is performed by using the corresponding scrambling algorithm and the second part of the security key. Finally, the original image could be restored by combining the restored 2D decomposition component and the other two parts.

The proposed encryption scheme can encode images from different modalities, such as grayscale, remote, medical and color images. Fig. 2 illustrates the encryption and corresponding decryption results of some sample images, including remote, grayscale, medical, synthetic and color images. To encrypt color image, each R, G, B component is encrypted individually and combined to produce the final encrypted color image. As observed in Fig. 2, all encrypted images shown in the middle row are noise-like and unrecognizable. Therefore, the proposed method can well protect different types of plain images. The restored images displayed in the bottom row are visually indistinguishable from their original counterparts.

3.2. Content-adaptive cryptosystem

Due to the adaptive decomposition nature of the 2D-PUD method, the generated 1D sequence $[F_1 G_1]$ for two different images are completely distinct; while for the same image, it will be significantly different by choosing different decomposition numbers N. Fig. 3 shows the generation process of the second part of the security key $[F_1 G_1]$ by exploiting two different images with the same decomposition times and the same image with different decomposition times. Due to space constraints, we show only the preceding 16 numbers of F_1 and G_1, respectively. As shown in the figure, the generated $[F_1 G_1]$ is completely distinct for different images; in addition, $[F_1 G_1]$ is significantly different for the same image due to the different decomposition times. Therefore, the proposed encryption algorithm is a content-adaptive encryption scenario.

4. Experimental results

In this section, we implement the proposed encryption algorithm by using MATLAB 2018b on a personal computer with an Intel Core i7-7700 CPU at 3.60 GHz and 16 GB of memory and perform the security analysis. Our experiments are conducted on the USC-SIPI Miscellaneous Image Database[1] in which total 44 images are included. To quantitatively evaluate the quality of the proposed approach, we test all the images in the database. Meanwhile, we conduct five sets of experiments to evaluate our proposed method, i.e., encryption and decryption evaluation, security analysis (including histogram analysis, correlation analysis, and information entropy analysis), noise attack, data loss attack, and differential attack. Our method is compared to some state-of-the-art methods, the comparison results are also presented in this section. Without loss of generality, the simulation set a fixed random secret key K='9F7ED402FBF47A4F91F44824E7288A684849B3E8C5F495 38496A3A83131373A5A510F5FF5DEDC6CD838DB139FB31E11D982C 5148C7A53B838 0CB49AD6ADAC4D7' (in hexadecimal format), and the parameters are set as follows: the decomposition times $N = 12$ and the round of scrambling and XOR procedure $r = 1$.

4.1. Encryption and decryption

Since with the decomposition number N, there is an error involved in AFD reconstruction (see Eqs. (24) and (25)), the proposed method falls into the category of lossy encryption. Thus, we need peak signal-to-noise ratios (PSNR) metric to measure the recover effect. The PSNR values between the 44 original and the corresponding restored images are illustrated in Fig. 4. In Fig. 4, we can observe that the obtained PSNR values remain consistently high, and under such PSNR values, the restored images are visually indistinguishable from their original counterparts.

4.2. Security analysis

In this subsection, we analyze the security of the proposed cryptosystem from five aspects, i.e., key space, key sensitivity, histogram, correlation, and information entropy.

[1] http://sipi.usc.edu/database/database.php?volume=misc.

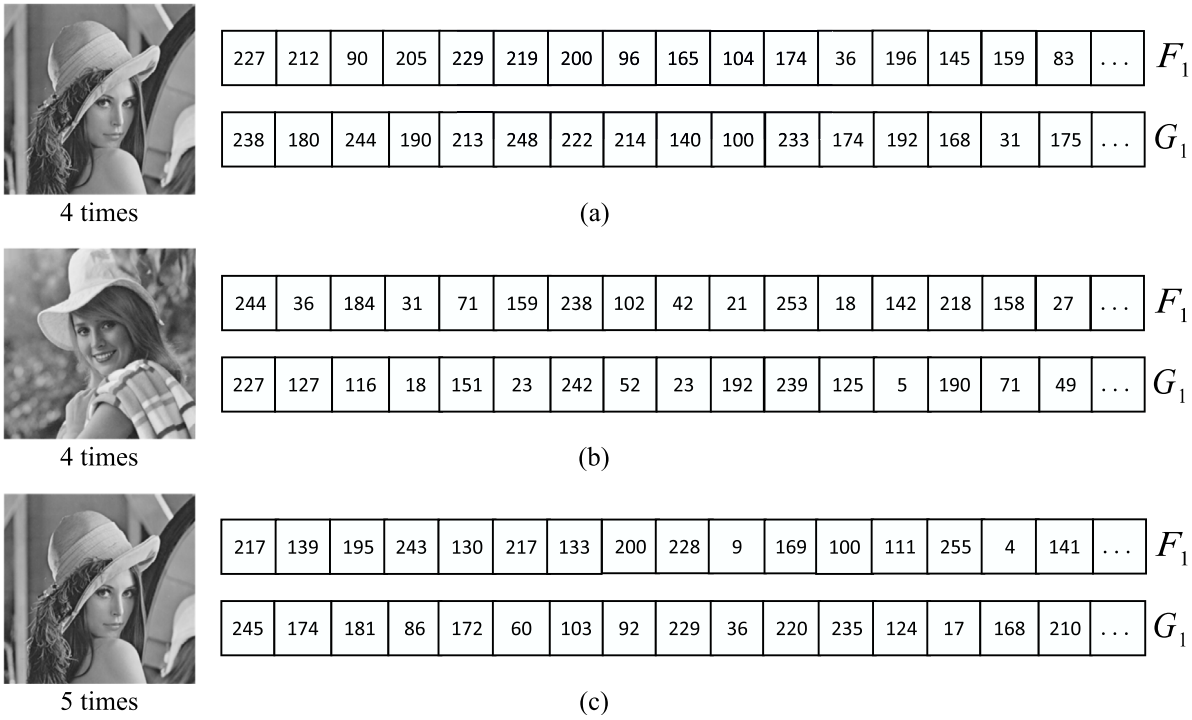

Fig. 3. Third part of the security key $[F_1G_1]$ generated from different images by setting identical decomposition times and the same image by setting different decomposition times. (a) The values of F_1 and G_1 generated from the Lena image using 4 decomposition times; (b) The values of F_1 and G_1 generated from the Elaine image using 4 decomposition times; (c) The values of F_1 and G_1 generated from the Lena image using 5 decomposition times.

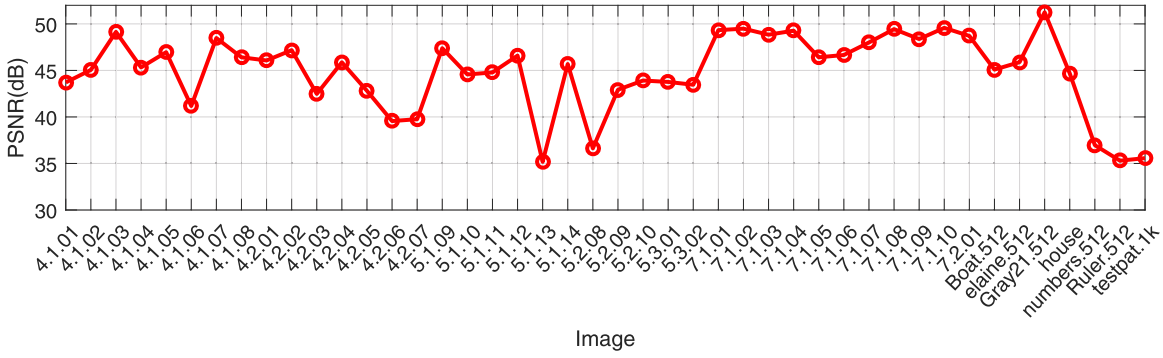

Fig. 4. PSNR values between the restored images and the original images from the USC-SIPI Miscellaneous Image Database.

4.2.1. Key space

Generally, the secret key should have appropriate size to resist the brute-force attack. For the proposed cryptosystem, the used secret key is composed of pseudo-random stream sequence K, 1D decomposition components $[F_1G_1]$ and the average intensity value c_{00}. The stream sequence has the size of 512 bits, the size of the 1D decomposition components is m when the original image has a size of $m \times m$, and the width of each number is 8 bits, and the average intensity value is a scalar. Therefore, the key space is of size $2^{512} \times 2^{(2m+1)\times 8}$. As suggested by Alvarez and Li [49], the cryptosystem can resist brute force attack when the key space is greater than 2^{100}. Therefore, the key space of the proposed encryption scheme is generally large enough to withstand against brute-force attack such as ciphertext-only attack.

4.2.2. Key sensitivity analysis

A robust image cryptosystem should be extremely sensitive to changes in the security key. Even a one bit deviation from the legal key, a completely different encrypted image can be generated from the same plain image. Additionally, the original image cannot be reconstructed by using any illegal key, even if the key is only modified by one bit.As mentioned above, the secret key consists of K, $[F_1G_1]$ and c_{00}. Without loss of generality, we choose the parameter K to test the key sensitivity of the proposed encryption scenario. We utilize the Lena image to show the experimental results of encryption and decryption with K and K'. K' is modified one bit from K as:

$$K =' 9F7ED402FBF47A4F91\ldots\ldots A53B8380CB49AD6ADAC4D7',$$

$$K' =' 9F7ED402FBF47A4F91\ldots\ldots A53B8380CB49AD6ADAC4D6'.$$

Fig. 5 illustrates encrypted and decrypted results with K and K'. Fig. 5(a) and (b) show the encrypted images with security K and K', respectively. The difference between the two encrypted images by K and K' is displayed in Fig. 5(c). Fig. 5(d) and (e) demonstrate the decrypted results of (a) using K and K'. It can be obviously

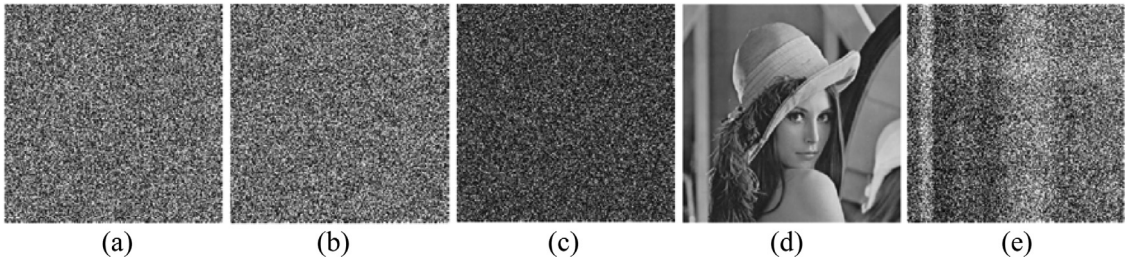

Fig. 5. Key sensitivity analysis. (a) Encryption result with K, (b) Encryption result with K', (c) Encryption difference between (a) and (b), (d) Decryption result of (a) with K, (e) Decryption result of (a) with K'.

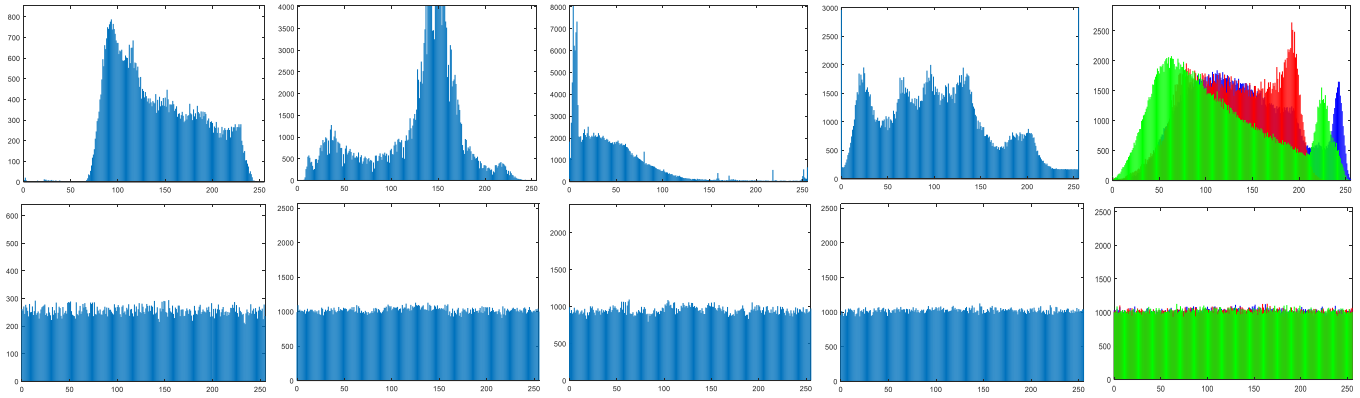

Fig. 6. Histogram analysis. Top row: histogram of original images in Fig. 2. Bottom row: histogram of corresponding cipher images.

Table 1
The variances of the plain and cipher images of the 5 images in Fig. 2 obtained by our method.

Images	Image 1	Image 2	Image 3	Image 4	Image 5		
					Red	Green	Blue
Plain	4.85×10^4	1.54×10^6	9.52×10^6	4.02×10^5	3.31×10^6	5.20×10^5	3.20×10^5
Cipher	288.55	1190.37	921.86	939.71	915.80	1169.96	1038.44

seen that our encryption scheme is extremely sensitive to the secret key during both encryption and decryption processes.

4.2.3. Histogram analysis

As a significant characteristic in statistical analysis, the image histogram describes the pixel distribution of an image by calculating the number of pixels at each intensity level and is an easily implemented cryptanalysis method. An effective cryptosystem should produce a cipher image with a uniform distribution of pixel values and should be significantly different from that of the original image. Fig. 6 shows the histogram plots of the original images and the corresponding cipher images in Fig. 2. As illustrated in Fig. 6, we can observe that the histograms of all cipher images are fairly uniform and significantly different from those of the original images. Besides, the uniformity of the histogram is further verified by the variances [20,50] described as

$$Var(X) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(x_i - x_j\right)^2, \tag{31}$$

where $X = \{x_0, x_2, \cdots, x_{255}\}$ represents the vector of the histogram values, and x_i and x_j are the numbers of pixels in which gray values are equal to i and j, respectively. The lower variance implies the higher uniformity of the image. Table 1 lists the variances of five images used in Fig. 2. Table 2 shows the variance comparison results of this algorithm and other algorithms [19,20] on color Lena image. As shown in Table 1 and Table 2, one can observe that the histograms of all cipher images are fairly uniform and significantly different from those of the original images. The variance of the plain image is very large, whereas that of the cipher image is significantly reduced. Compared with other algorithms, our proposed method achieves satisfactory performance. Therefore, the proposed encryption algorithm does not provide any useful information for statistical attack.

Table 2
The variance comparison results of color Lena image.

Algorithms	Variances of the cipher images		
	Red component	Green component	Blue component
Ref. [19]	1070	955.320	955.828
Ref. [20]	904.758	1013	923.656
Ours	819.117	1012	921.781

4.2.4. Correlation analysis

As a meaningful visual medium, an image has a high correlation between adjacent pixels in horizontal, vertical or diagonal directions. It is important for an image encryption algorithm to break the strong pixel correlation in the process of encryption. In order to visually display the correlation, we use the Lena image as the test image. Then randomly select 3000 pairs of pixels in three directions from the original image and its cipher image as the test samples, and plot their distributions in Fig. 7. As displayed in the first row of Fig. 7, the adjacent pixels in different directions have

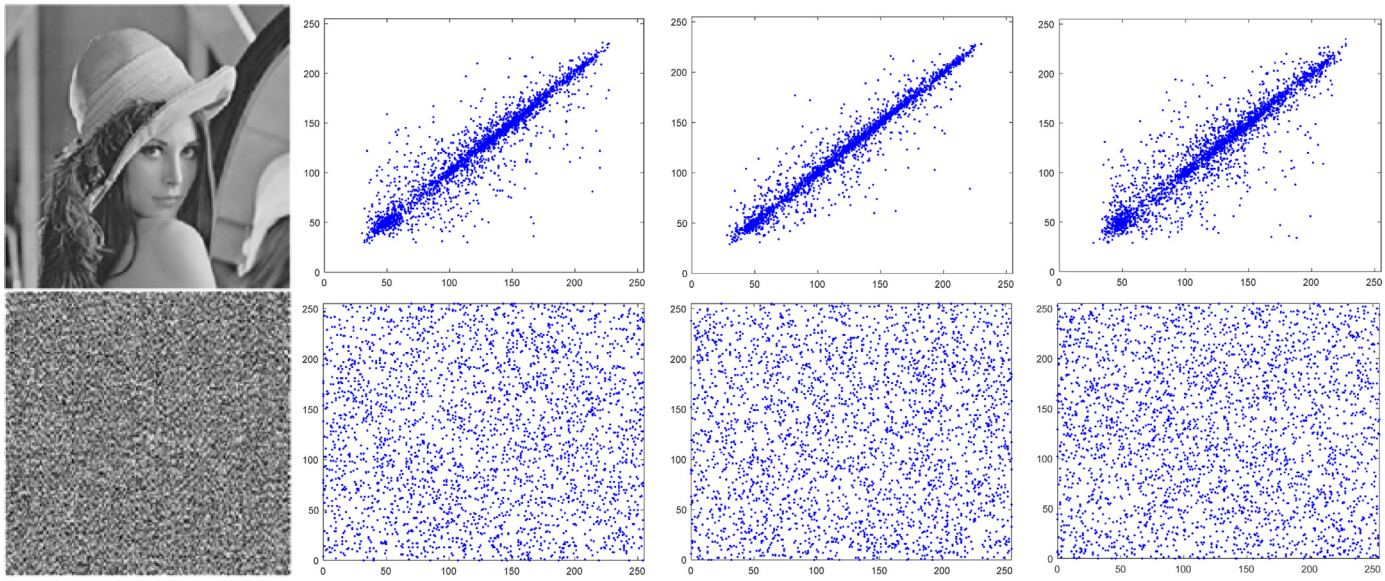

Fig. 7. Correlation plots of two adjacent pixels. The first and second rows are corresponding to the original and cipher images, respectively. The second to fourth columns illustrate the correlation plots of two adjacent pixels in horizontal, vertical, and diagonal, respectively.

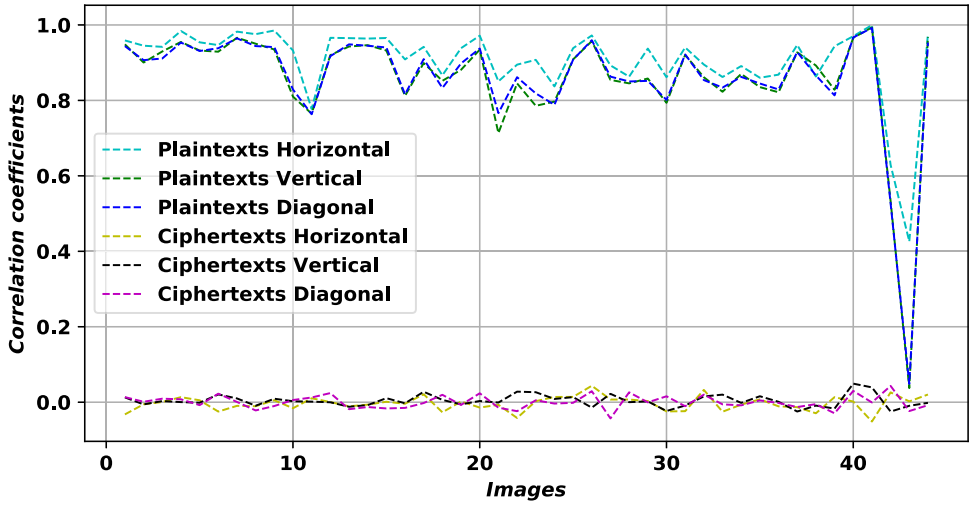

Fig. 8. Correlation coefficients of adjacent pixels.

strong correlations to the original image, whereas the adjacent pixels of the encrypted image are distributed uniformly.

The expression of the correlation coefficient [51] can be mathematically formulated as follows:

$$\gamma_{xy} = \frac{E(x - E(x)(y - E(y)))}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{32}$$

$$E(x) = \frac{1}{M}\sum_{i=1}^{M} x_i, \tag{33}$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M} (x_i - E(x)), \tag{34}$$

where x and y are two given sample sequences, $E(\cdot)$ and $D(\cdot)$ present the expectancy function and the variance function, respectively. A correlation coefficient close to 1 or -1 indicates that two sample sequences have a very strong correlation. Conversely, a value close to 0 means that they have very low correlation. Fig. 8 shows the correlation coefficients of the 44 images from the USC-SIPI Miscellaneous Image Database and corresponding cipher images. In Fig. 8, we observe that the proposed cryptosystem can reduce the correlation of pixels and thus advance the security level in the encryption process.

4.2.5. Information entropy analysis

Information entropy, first proposed by Shannon [52], is an efficient criterion to measure the randomness of an information source. The definition of information entropy $H(s)$ for a message source s can be given as follows:

$$H(s) = -\sum_{i=0}^{2^{M-1}} p(s_i)\log_2 p(s_i), \tag{35}$$

where M is the number of bits representing the symbol s_i, and $p(s_i)$ denotes its probability. For a genuine random source including 2^M symbols, the entropy value should be M. Therefore, the entropy value should theoretically be equal to 8 for an effectively encrypted image with 256 gray levels. We calculate the information entropy values of all images from the USC-SIPI Miscellaneous and

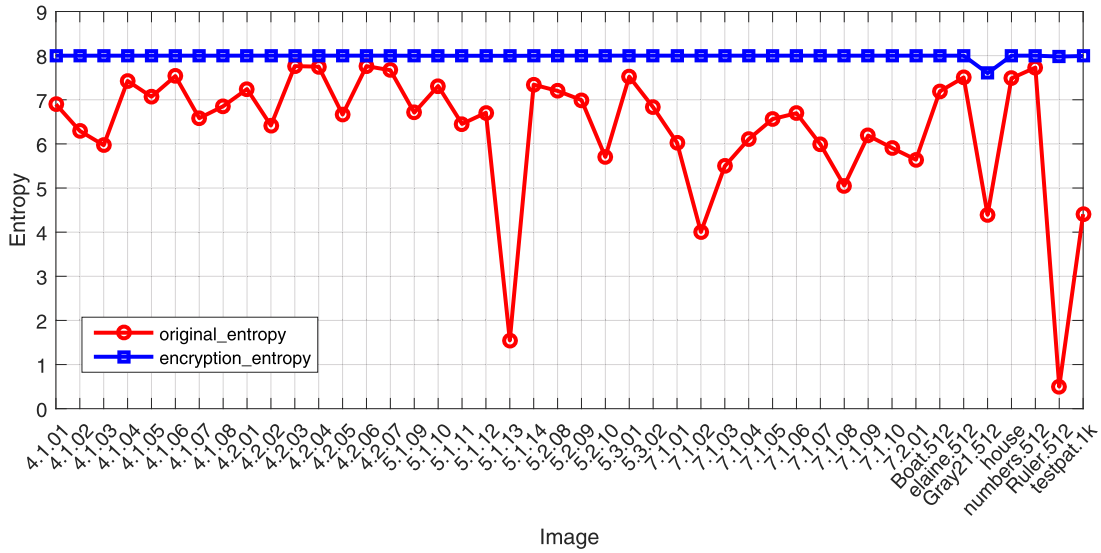

Fig. 9. Information entropy values of the original images and the encrypted images from the USC-SIPI Miscellaneous Database.

Fig. 10. Noise attacks of Lena image by different types of noise. Top row: restored images by adding Gaussian noise with variance 0.001, 0.005 and 0.01 on the cipher image, respectively; Bottom row: restored images by adding 1%, 2% and 5% salt-and-pepper noise on the cipher image, respectively.

their corresponding encrypted images. The calculation results are shown in Fig. 9. As seen in Fig. 9, the information entropy values of the cipher images are very close to the theoretical value 8, which confirms the encrypted images have good randomness. Therefore, the proposed encryption algorithm is secure against entropy attack.

4.3. Noise attack

It is unavoidable that an image may be degraded by noise or data loss in the process of transmission. An ideal encryption system should reduce the impact caused by changes in pixels on the decrypted images. We take the Lena image to assess the ability of our proposed scheme in the aspect of withstanding noise and data-loss attacks. Fig. 10 demonstrates the restored images under different noise attacks. The top row displays the Lena image restored by adding Gaussian noise (GN) with variance 0.001, 0.005 and 0.01 on the cipher image, respectively, and the bottom row shows the Lena image restored by adding 1%, 2% and 5% salt-and-pepper noise (SPN) on the cipher image, respectively. Although some visible noise-like points are distributed in the restored images, we can still identify most of the original images. To quantitatively show the performance of noise resistance in the proposed algorithm, the PSNR value between the decrypted image and the original image is calculated and shown in Fig. 11. We can observe in Fig. 11 that GN has the largest effect on the decryption process; the PSNR values vary from 39.47 dB to 12.74 dB. When the noise intensity increases from 0.0001% to 5%, the quality of the decrypted images decreases, however, they all can be recognized visually. Our encryption scheme has stronger resistance to SPN than GN; the PSNR values change from 44.84 dB to 22.52 dB.

4.4. Data loss attack

Fig. 12 illustrates the restored results of the Lena image under data-loss attack. The first and third rows show the cipher images

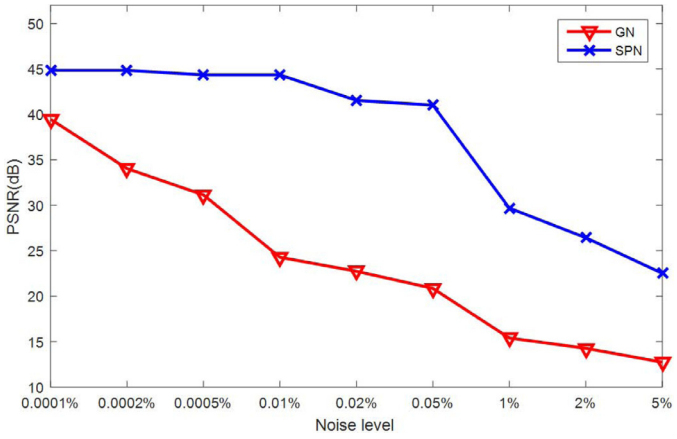

Fig. 11. PSNR values between the restored images and the original images with different noise.

with 1%, 2% and 5% data block losses, and the pixel values of the lost patches are set to 0 and 255, respectively. The corresponding restored images are given in the second and last rows, respectively. Despite noise-like points in the restored images, they still preserve most of the visual information and are recognizable. In addition, we calculate the PSNR values between decrypted images and the original images, shown in Fig. 13. From Fig. 13, we can see that the quality of the decrypted images decreases with increasing data losses, but they all are recognizable visually. Hence, the proposed encryption algorithm has the ability of resisting cropping attack.

4.5. Differential attack

The differential attack, as a chosen-plaintext attack, is a classic type of attack. To obtain information on the coding key, an eavesdropper usually makes a slight change to the original image and then compares the corresponding cipher image. Thus, an

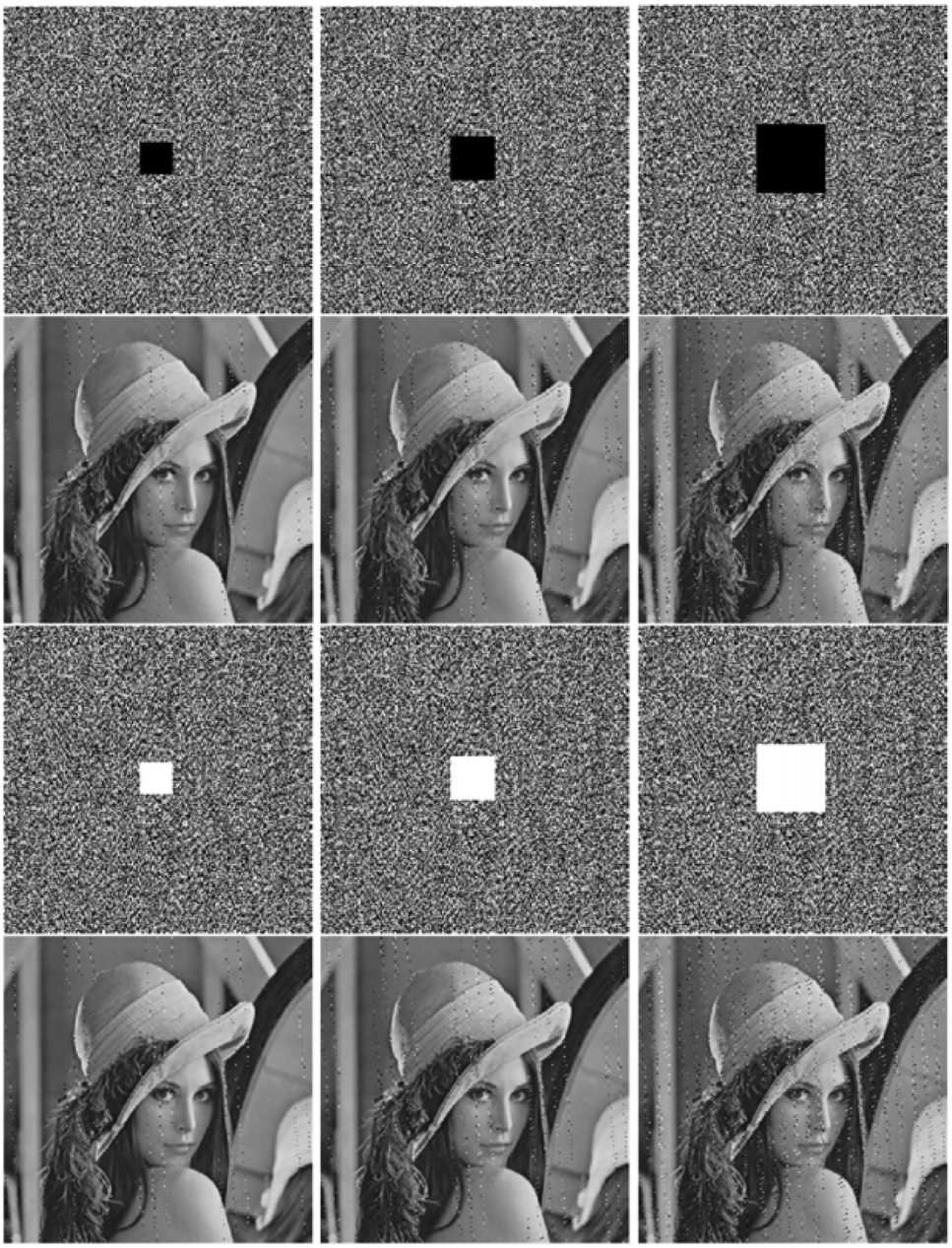

Fig. 12. Data-loss attacks on Lena image with different block sizes. First and third rows: cipher images with 1%, 2% and 5% data loss by setting the pixel values of the lost patches to 0 and 255, respectively; Second and fourth rows: corresponding reconstructed images.

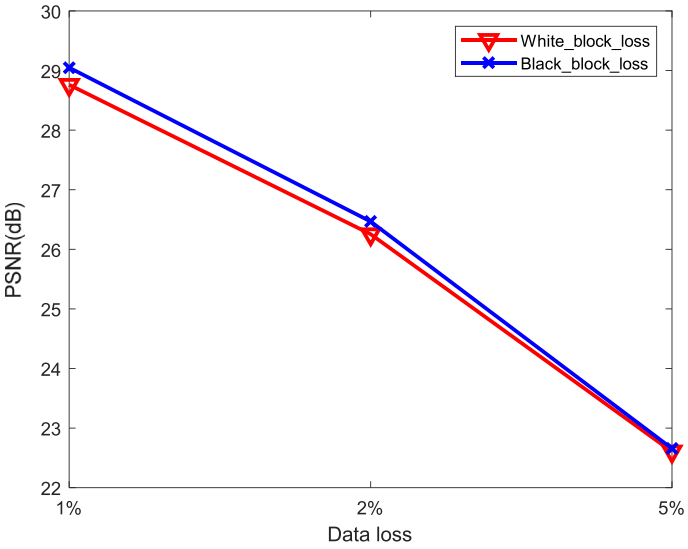

Fig. 13. PSNR values between the restored images and the original image with different data block losses.

encryption algorithm with strong ability to withstand differential attack should generate significant turbulence in the encrypted image even for a minor modification to the original image. The diffusion property describes a cipher's capacity to spread a change in a plaintext image over its ciphertext version. If a cipher has poor diffusion ability, it might be fragile to the chosen plaintext attack. To assess the performance of our cipher against differential attack, the Lena image is selected as the test image. One random bit pixel value is modified, generating a new image. These two images are then encrypted by the proposed scheme into two cipher images, and the results are illustrated in Fig. 14. Fig. 14 (e) shows the absolute difference of two cipher images. We can clearly see that the difference between two cipher images is huge.

The NPCR and UACI are two common tools to evaluate differential attack performance of an encryption algorithm. The formulation of the two indexes are defined as follows:

$$UACI = \sum_{i=1}^{m}\sum_{j=1}^{n}\left(\frac{|C_1(i,j) - C_2(i,j)|}{L \times G}\right) \times 100, \tag{36}$$

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{mn} \times 100, \tag{37}$$

with

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j), \end{cases} \tag{38}$$

where C_1 and C_2 are the cipher images before and after modifying one bit pixel value of the original image, and m and n represent the width and height of the image, respectively. L denotes the maximum intensity value of the image, and G is the total number of pixels in the image.

UACI and NPCR are two effective indictors to measure the pixel changes between two cipher images C_1 and C_2. The former depicts the average value of changed pixels, while the latter describes the number of changed pixels. Wu et al. in [37] provide critical NPCR and UACI values for a given significance level α. An image encryption scheme passes the diffusion property test if its UACI score falls within the critical UACI interval $(U_\alpha^{*-}, U_\alpha^{*+})$ and its NPCR value is higher than the critical NPCR N_α^*. The critical NPCR score N_α^* and UACI score $(U_\alpha^{*-}, U_\alpha^{*+})$ with given α can be calculated as follows:

$$N_\alpha^* = \frac{L - \Phi^{-1}(\alpha)\sqrt{L/G}}{L+1}, \tag{39}$$

and

$$\begin{cases} U_\alpha^{*-} = \mu_U - \Phi^{-1}(\alpha/2)\sigma_U \\ U_\alpha^{*-} = \mu_U + \Phi^{-1}(\alpha/2)\sigma_U \end{cases}, \tag{40}$$

where

$$\mu_U = \frac{L+2}{3L+3}, \tag{41}$$

and

$$\sigma_U = \frac{(L+2)\left(L^2+2L+3\right)}{18(L+1)^2 LG}. \tag{42}$$

$\Phi(\cdot)$ is the inverse cumulative distribution function of the standard normal distribution $N(1,0)$.

To quantitatively test the proposed cipher against differential attack, we follow other studies in the literature [53] and employ 25 sample images with 6 images having a size of 256×256, 16

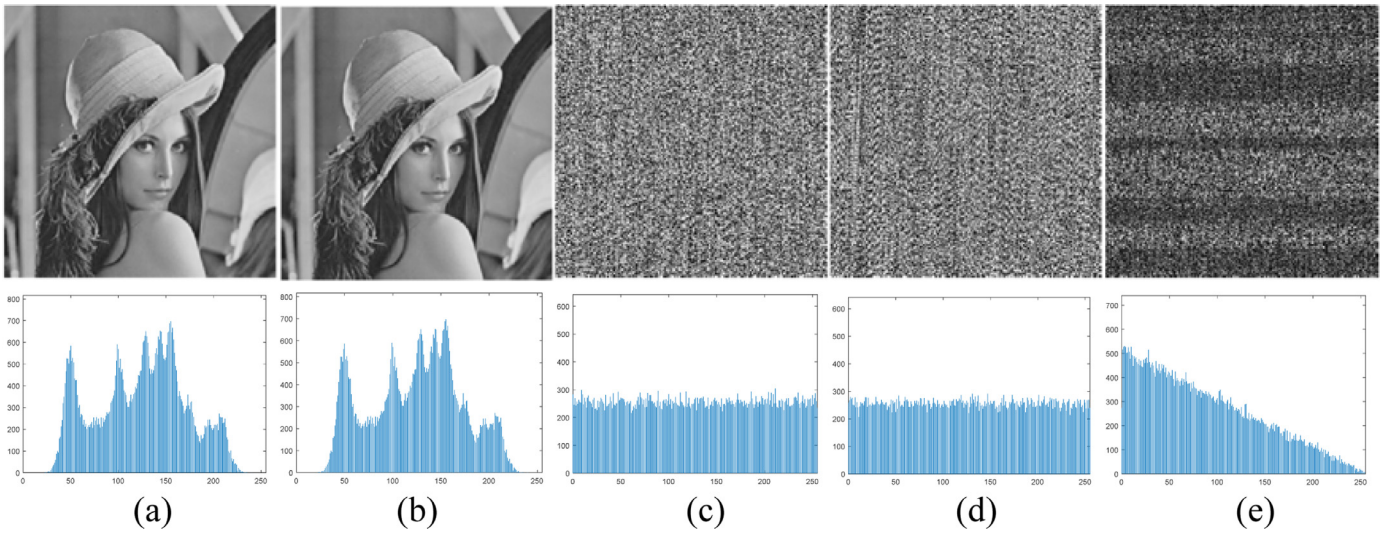

Fig. 14. Results of Lena image under differential attack. (a) Original image; (b) Original image with one bit randomly changed; (c) Cipher image C1 of (a); (d) Cipher image C2 of (b); (e) $|C1 - C2|$. The second row shows the histograms of the corresponding images in the first row.

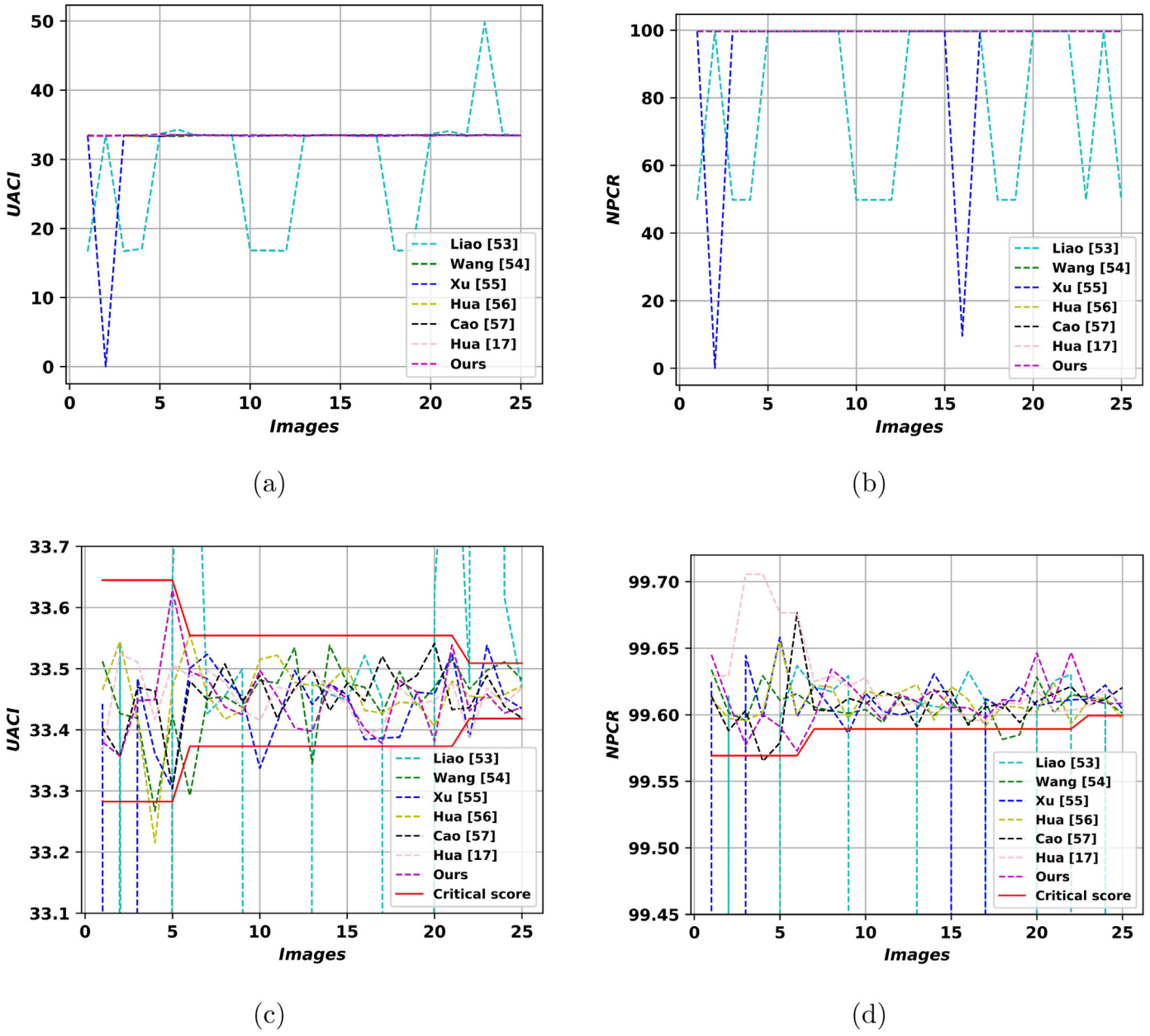

Fig. 15. UACI and NPCR performance comparisons of several encryption algorithms. (a) UACI performance comparisons; (b) NPCR performance comparisons; (c) UACI performance of special range; (d) NPCR performance of special range.

images having a size of 512×512, and the other 3 images having a size of 1024×1024 from the USC-SIPI Miscellaneous Image Database. We set the significance level $\alpha = 0.05$ as suggested in [37]. Then, for the images of size 256×265, $N^*_\alpha = 99.5693\%$ and $[U^{*-}_\alpha, U^{*+}_\alpha] = [33.2824\%, 33.6447\%]$; for the images of size 512×512, $N^*_\alpha = 99.5893\%$ and $[U^{*-}_\alpha, U^{*+}_\alpha] = [33.3730\%, 33.5541\%]$; and for the images of size 1024×1024, $N^*_\alpha = 99.5994\%$ and $[U^{*-}_\alpha, U^{*+}_\alpha] = [33.4183\%, 33.5088\%]$. The values of UACI and NPCR acquired by several different encryption schemes [17,53–57] are illustrated in Fig. 15(a) and Fig. 15(b). To clearly demonstrate the pass rate of several competing encryption algorithms, we display the values of UACI and NPCR locally and their corresponding critical score in Fig. 15(c) and Fig. 15(d), respectively. As seen, our proposed algorithm can pass the UACI and NPCR tests for all of images, while other encryption schemes failed to pass the tests for some images. Thus, these results confirm that the proposed algorithm has an excellent capacity to withstand the differential attack.

4.6. Resistance to some typical attacks

In the cryptanalysis, ciphetext-only attack, known-plaintext attack, chosen-plaintext attack and chosen-ciphertext attack are four typical security analysis methods. Among them, chosen-plaintext attack and chosen-chipertext attack are more powerful than other two attacks [20]. That is, if the encryption could withstand chosen-plaintext attack and chosen-chipertext attack, it has enough security level to resist other two attacks. For the chosen-plaintext and chosen-ciphertext attacks, adversary would choose some arbitrary plaintext and obtain its decrypted results, and the latter suggests that adversary could use any ciphertext to obtain the corresponding plaintext. In both attacks, the objective is to determine the secret key or a mapping from the differentials of the ciphertexts to those of the plaintexts [28,58]. For the proposed encryption scheme, the security key and the mapping are generated compositely. The 2D-PUD method is utilized to decompose the plain image

Table 3
Complexity analysis of different encryption schemes.

Algorithms	Scrambling	Diffusion	Sequence generation
Ref. [14].	$2mn + 2mn\log(mn)$	$2mn$	$56mn$
Ref. [20].	mn	$12mn$	$4mn$
Ref. [57].	$m\log(8n) + 8n\log(m) + 16mn$	$16mn$	$17(m+n)$
Ours	$8mn$	$16mn$	$2mn\log(mn) + T(m+n) + 2mn$

and generate two 1D decomposition components which is completely distinct for different images. Then, two 1D decomposition components are randomized by a given pseudo number sequence to determine the key stream for diffusion process. Thus, the attackers may not get useful information for key restore or mapping relation between plaintext and ciphertext via analyzing the plain images and corresponding cipher images. Consequently, the proposed algorithm can withstand chosen-plaintext and chosen-cipertext attacks.

4.7. Computation complexity analysis

In practice, the efficiency is important for image encryption system, which is usually determined by the encryption scheme and sequence generation method. We analyze and compare the computation complexity of different encryption schemes in [14,20,57] and ours. Assume a gray image with size of $m \times n$. In the processes of permutation and diffusion, the permutation operation is pixel level, and the time complexity is $8mn$. For the diffusion process, the manipulation object is bit-wise, then the time complexity is $16mn$. Moreover, for the decomposition of plain image, the 2D-PUD technology is iterated for many times, and the time complexity of floating point operation is $2mn\log(mn) + T(m+n) + 2mn$ [36], where T denotes the number of discrete points in the unit disc $\mathbb{D}$. The compared results are given in Table 3. It can be seen that the complexity of [20] is the lowest one in these schemes, and ours is only slightly higher than it. According to the above analysis, the 2D-PUD technique mainly takes most of the time. Actually, the 2D-PUD method is a novel designed decomposition method and the code is not yet optimized. In the future, the 2D-PUD algorithm would be executed in parallel, and it may shorten the encryption time and improve the encryption speed.

5. Conclusion

In this work, we proposed a novel image encryption scheme based on the 2D-PUD algorithm that can achieve a high security level. The proposed scheme associates the plaintext information with secret key based on the inherent decomposition attribute of the 2D-PUD method. Therefore, the proposed cryptosystem is an image-content-adaptive encryption scenario which can resist against chosen-plaintext attack and chosen-ciphertext attack. The experiment results and performance analysis show that the proposed scheme has good randomness and a large key space to resist brute force attack, and is secure against noise, data-loss and differential attacks in compared to some state-of-the-art algorithms. The limitation of this study is that we employ the Arnold transform in the permutation process, so our proposed algorithm can only encrypt square images. In the future work, some other permutation schemes can be used or improved such that the proposed algorithm can process rectangle images. In addition, it is worth more studies in the future to design method for hiding the plaintext-related information into chipertext.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Yongfei Wu: Conceptualization, Methodology, Visualization, Writing - original draft. **Liming Zhang:** Methodology, Writing - review & editing, Funding acquisition. **Tao Qian:** Methodology, Writing - review & editing, Funding acquisition. **Xilin Liu:** Software, Validation, Writing - review & editing. **Qiwei Xie:** Methodology, Writing - review & editing.

Acknowlgedgments

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61901292, the Natural Science Foundation of Shanxi Province, China under Grant No. 201801D221186 and Grant No. 201901D211080, the Science and Technology Development Fund of Macao SAR FDCT 079/2016/A2, 0123/2018/A3, and University of Macau Fund MYRG2018-00111-FST.

References

[1] W. Liu, X. Yin, W. Lu, J. Zhang, et al., Secure halftone image steganography with minimizing the distortion on pair swapping, Signal Process. 167 (2020) 1–10.
[2] X. Yin, W. Lu, J. Zhang, W. Liu, Reversible data hiding in halftone images based on minimizing the visual distortion of pixels flipping, Signal Process. 173 (2020) 107605.
[3] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, Reversible image watermarking using interpolation technique, IEEE Trans. Inf. Forensic Security 5 (1) (2010) 187–193.
[4] X. Liu, G. Han, J. Wu, Z. Shao, G. Coatrieux, H. Shu, Fractional krawtchouk transform with an application to image watermarking, IEEE Trans. Signal Process. 65 (7) (2017) 1894–1908.
[5] H. Liu, X. Wang, Color image encryption based on one-time keys and robust chaotic maps, Computers and Mathematics with Applications 59 (10) (2010) 3320–3327.
[6] R. Tao, X. Meng, Y. Wang, Image encryption with multiorders of fractional fourier transforms, IEEE Trans. Inf. Forensic Security 5 (4) (2010) 734–738.
[7] L. Gong, X. Liu, F. Zheng, N. Zhou, Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique, J. Mod. Opt. 60 (13) (2013) 1074–1082.
[8] C. Li, D. Lin, J. Lu, F. Hao, Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography, IEEE MultiMed. 25 (4) (2018) 46–56.
[9] P. Refregier, B. Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Let. 20 (7) (1995) 767–769.
[10] B. Hennelly, J.T. Sheridan, Optical image encryption by random shifting in fractional fourier domains, Opt. Let. 28 (4) (2003) 269–271.
[11] Z. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, Phys. Lett. A 346 (1–3) (2005) 153–157.
[12] S.J. Shyul, Image encryption by random grids, Pattern Recogni. 40 (3) (2007) 1014–1031.
[13] L. Krikor, S. Baba, T. Arif, Z. Shaaban, Image encryption using DCT and stream cipher, Eur. J. Sci. Res. 32 (2009) 47–57.
[14] Z. Hua, Y. Zhou, Image encryption using 2d logistic-adjusted-sine map, Inf. Sci. 339 (2016) 237–253.
[15] Y. Zhang, D. Xiao, An image encryption scheme based on rotation matrix bit-level permutation and block diffusion, Commun. Nonlinear Sci. Numer. Simul. 19 (1) (2014) 74–82.
[16] W. Zhang, H. Yu, Y. Zhao, Z. Zhu, Image encryption based on three-dimensional bit matrix permutation, Signal Process. 118 (2016) 36–50.
[17] Z. Hua, Y. Zhou, H. Huang, Cosine-transform-based chaotic system for image encryption, Inf. Sci. 480 (2019) 419–430.

[18] W. Wen, K. Wei, Y. Zhang, Y. Fang, M. Li, Colour light field image encryption based on DNA sequences and chaotic systems, Nonlinear Dynam. 99 (2) (2020) 1587–1600.
[19] X. Chai, Z. Gan, Y. Lu, M. Zhang, Y. Chen, A novel color image encryption algorithm based on genetic recombination and the four-dimensional memris-tive-hyperchaotic system, Chin. Phys. B 25 (10) (2016) 76–88.
[20] X. Chai, X. Fu, Z. Gan, Y. Lu, Y. Chen, A color image cryptosystem based on dynamic DNA encryption and chaos, Signal Process. 155 (2019) 44–62.
[21] W. Zeng, S. Lei, Efficient frequency domain selective scrambling of digital video, IEEE Trans. Multimedia 5 (1) (2003) 118–129.
[22] S. Liu, J.T. Sheridan, Optical encryption by combining image scrambling techniques in fractional fourier domains, Opt. Comm. 287 (2013) 73–80.
[23] S. Li, C. Li, G. Chen, N.G. Bourbakis, K.T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process. Image Commun. 23 (3) (2008) 212–223.
[24] A. Jolfaei, X.W. Wu, V. Muthukkumarasamy, On the security of permutation-only image encryption schemes, IEEE Trans. Inf. Forensic Security 11 (2) (2016) 235–245.
[25] L. Zhang, Y. Liu, C. Wang, J. Zhou, Y. Zhang, G. Chen, Improved known-plaintext attack to permutation-only multimedia ciphers, Inf. Sci. 430 (2018) 228–239.
[26] S.M. Seyedzadeh, B. Norouzi, M.R. Mosavi, S. Mirzakuchaki, A novel color image encryption algorithm based on spatial permutation and quantum chaotic map, Nonlinear Dyn 81 (1–2) (2015) 511–529.
[27] A.A.A. Latif, X. Niu, M. Amin, A new image cipher in time and frequency domains, Opt. Comm. 285 (21–22) (2012) 4241–4251.
[28] J. Chen, L. Chen, Y. Zhou, Universal chosen-ciphertext attack for a family of image encryption schemes, IEEE Trans. Multimedia (2020), doi:10.1109/TMM.2020.3011315.
[29] A. Nikolaids, Asymptotically optimal detection for additive watermarking in the DCT and DWT domians, IEEE Trans. Image Process. 12 (5) (2003) 563–571.
[30] Y. Liang, G. Liu, N. Zhou, J. Wu, Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion, J Mod Opt 62 (4) (2015) 251–264.
[31] K. Chan, F. Faramarz, A block cipher cryptosystem using wavelet transforms over finite fields, IEEE Trans. Signal Process. 52 (10) (2004) 2975–2991.
[32] G. Situ, J. Zhang, Double random-phase encoding in the fresnel domain, Opt. Let. 29 (14) (2004) 1584–1586.
[33] A. Sinha, K. Singh, Image encryption by using fractional fourier transform and jigsaw transform in image bit planes, Opt. Eng. 44 (5) (2005) 057001.
[34] Z. Liu, Q. Guo, L. Xu, M.A. Ahmad, S. Liu, Double image encryption by using iterative random binary encoding in gyrator domains, Opt. Express 18 (11) (2010) 12033–12043.
[35] N. Singh, A. Sinha, Optical image encryption using hartley transform and logistic map, Opt. Comm. 282 (6) (2009) 1104–1109.
[36] Y. Li, L. Zhang, T. Qian, 2D partial unwinding—a novel non-linear phase decomposition of images, IEEE Trans. Image Process. 28 (10) (2019) 4762–4773.
[37] Y. Wu, J.P. Noonan, S. Agaian, NPCR And UACI randomness tests for image encryption, J. Sel. Areas Telecommun. 1 (4) (2011) 31–38.
[38] T. Qian, L. Zhang, Z. Li, Algorithm of adaptive fourier decomposition, IEEE Trans. Signal Process. 59 (12) (2011) 5899–5906.
[39] Z. Wang, F. Wan, C.M. Wong, L. Zhang, Adaptive fourier decomposition based ECG denoising, Comput. Biol. Med. 77 (2016) 195–205.
[40] C. Tan, L. Zhang, H.T. Wu, A novel blaschke unwinding adaptive-fourier-decomposition-based signal compression algorithm with application on ECG signals, IEEE J Biomed Health Inform 23 (2) (2018) 672–682.
[41] Z. Wang, J.N.d. Cruz, F. Wan, Adaptive Fourier decomposition approach for lung-heart sound separation, in: Proceeding of IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015, pp. 1–5.
[42] M. Nahon, Phase Evaluation and Segmentation, Yale University, 2000.
[43] R. Coifman, S. Steinerberger, Nonlinear phase unwinding of functions, J. Fourier Anal. Appl. 23 (4) (2017) 778–809.
[44] R. Coifman, J. Peyrière, Phase unwinding, or invariant subspace decompositions of hardy spaces, arXiv:1707.04844 (2017).
[45] R. Coifman, S. Steinerberger, H. Wu, Carrier frequencies, holomorphy, and unwinding, SIAM J. Math. Anal. 49 (6) (2017) 4838–4864.
[46] T. Qian, Boundary derivatives of the phases of inner and outer functions and applications, Math. Methods Appl. Sci. 32 (3) (2009) 253–263.
[47] T. Qian, Intrinsic mono-component decomposition of functions: an advance of fourier theory, Math. Meth. Appl. Sci. 33 (7) (2011) 880–891.
[48] J. Garnett, Bounded analytic functions, Springer Science & Business Media 236 (2007).
[49] G. Alvarez, S.J. Li, Some basic cryptographic requirements for chaos-based cryptosystem, Int. J. Bifurcat. Chaos 16 (8) (2006) 2129–2151.
[50] X. Chai, X. Zheng, Z. Gan, et al., Exploiting plaintext-related mechanism for secure color image encryption, Neural Comput. Applic. 32 (2020) 8065–8088.
[51] Z. Gan, X. Chai, D. Han, Y. Chen, A chaotic image encryption algorithm based on 3-d bit-plane permutation, Neural Comput. Applic. 31 (2019) 7111–7130.
[52] C.E. Shannon, Communication theory of secrecy systems, Bell. Syst. Tech. J. 28 (1949) 656–715.
[53] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (9) (2010) 2714–2722.
[54] X. Wang, Q. Wang, Y. Zhang, A fast image algorithm based on rows and columns switch, Nonlinear Dyn. 79 (2) (2015) 1141–1149.
[55] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Opt. Lasers Eng. 78 (2016) 17–25.
[56] Z. Hua, Y. Zhou, Design of image cipher using block-based scrambling and image filtering, Inf. Sci. 396 (2017) 97–113.
[57] C. Cao, K. Sun, W. Liu, A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map, Signal Process. 143 (2018) 122–133.
[58] J. Chen, L. Chen, Y. Zhou, Cryptanalysis of image ciphers with permutation-substitution network and chaos, IEEE Trans. Circuits Syst. Video Technol. (2020), doi:10.1109/TCSVT.2020.3021908.