Robust Hybrid Plaintext-Related Image Encryption using Hyper Chaos Signal Processing

Wenting Yuan[1], Amber Sultan[1,2], Syed Baqar Hussain[1,2*]

[1]Shanghai Jiao Tong University, PRC, [2]The University of Lahore, Pakistan,

Summary
This paper proposes a novel encryption scheme for digital images, which utilizes chaotic diffusion in spatial-domain and plaintext-related shuffling in frequency-domain based on a hyper chaos, where the initial values of the hyper chaos are served as keys to the encryption. In spatial-domain, the original digital image is diffused using chaotic XOR operation. After that, both phase and magnitude spectra of the cipher image are further encrypted using chaotic shuffling. The highest entropy and lowest correlation are achieved for the sample image in the proposed hybrid plaintext-related encryption, in which a huge key space of 6.5×1064 is created due to the multi-fold encryption algorithm. The high-level security of the proposed hybrid encryption is also verified with the capability against various attacks. In addition, the hybrid encryption scheme is optimized via the performance comparisons among the encryption procedures.

Key words:
Transport security, digital image encryption, digital chaos, double-domain, plaintext-related algorithm.

1. Introduction

Digital images and videos are becoming the mainstream of information carrier within the networks, since the image/video information is easier to be captured and understood. However, security issues become a big challenge for image transmission, which draws public attention from researchers to network users. Meanwhile, traditional encryption techniques cannot satisfy the needs for image encryption, because of the data size and high redundancy among the raw pixels of a digital image [1]. It is also mentioned in [2] that certain properties of images make classical ciphers impractical. Image encryption schemes based on digital chaos have been proposed recently [3-6], since digital chaotic systems possess the properties of ergodicity and high sensitivity to the initial values, which is essential for the data encryption. The important characteristics of digital chaos are given in Ref. [7]. In addition, it has been proved that, the hyper chaos provides much bigger key space and stronger ergodicity, if compared with low-dimensional chaos [8].

Encryption schemes based on hyper chaos have been proposed using chaotic scrambling and diffusion in spatial-domain [9-12]. However, the chaotic scrambling and diffusion operations reported so far have not the capability to resist the chosen and known-plaintext attacks. To deal with this issue, encryption based on the plaintext-related algorithm is proposed, where hyper-chaos-based shuffling in spatial-domain was utilized to enhance the security level by resisting the chosen and known-plaintext attacks [13]. Moreover, it is verified statistically that the frequency-domain encryption can effectively enhance the encryption quality by improving the entropy of the cipher image [14-15]. In general, the chaotic encryptions published are aimed at solving only one of the security problems for image transmission.

In this paper, we will incorporate for the first time the plaintext-related algorithm into the recently-proposed frequency-domain encryption, to enhance the security level and improve the encryption performance. We propose a novel hybrid plaintext-related image encryption based on chaotic diffusion in spatial-domain and chaotic shuffling in frequency-domain respectively. It is verified with the statistical analysis that, chaotic shuffling in frequency-domain is a key part of the encryption, as it provides the robustness against various attacks including the chosen and known-plaintext. The encryption scheme will be analyzed in detail, in terms of the histogram, entropy and correlation. It will be optimized by comparing among various encryption schemes within both single (spatial) and double (spatial and frequency) domains. The statistical results will verify the robustness and effectiveness of the proposed hybrid plaintext-related image encryption. Moreover, the highest entropy and lowest correlation are achieved for three different image samples, which indicates that the proposed scheme is independent of image selection.

2. Block Diagram

The schematic setup of the proposed encryption scheme is presented in Fig. 1, which consists of two key parts: spatial-domain chaotic diffusion and chaotic shuffling in frequency-domain. In the spatial-domain encryption, a digital image with $M \times N$ pixels is regarded as a 2-dimensional (2-D) matrix with M rows and N columns. The gray-level value of a pixel varies from 0 to 255, which is the value of the corresponding element in the matrix. The shuffling operation in frequency-domain not only randomizes the distribution of the cipher image to improve the performance in statistical characteristics, but also

Manuscript received September 5, 2019
Manuscript revised September 20, 2019

spreads each plain-pixel and cipher-pixel to the whole cipher image to enhance the security against the chosen and known-plaintext attacks.

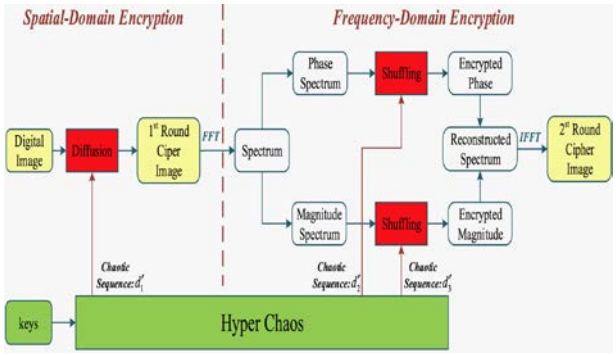

Fig. 1 Schematic of the proposed hybrid encryption scheme.

3. Hyper Chaos

The complicated dynamics of chaos is essential to ensure the security level of the chaotic encryption. To generate the chaotic sequences for double-domain encryption, a four-dimensional (4-D) hyper digital chaos is utilized, which can be expressed as

$$\begin{cases} \dot{h}_1 = a(-h_1 + h_2) + h_2 h_3 h_4 \\ \dot{h}_2 = b(h_1 + h_2) - h_1 h_3 h_4 \\ \dot{h}_3 = c h_2 - h_4 + d h_1 h_2 h_4 \\ \dot{h}_4 = -e h_4 + h_1 h_2 h_3 \end{cases} \quad (1)$$

where the initial parameters a, b, c, d, and e are all real constants, which are shared between the transmitter and receiver. It can be verified from the Lyapunov exponent that, the system enters a chaotic zone, when the constants are set with certain value ranges as in Ref. [16]. These initial values are applied as the secure keys between the transmitter and receiver in the proposed encryption scheme. Eq. (1) can be solved by Runge-Kutta approach with an iteration time of t=20,000. To prevent repetition as much as possible in the following sorting algorithm, the generated 4-D chaotic sequences $\{h_1\}$, $\{h_2\}$, $\{h_3\}$ and $\{h_4\}$ are then digitalized using

$$h_i' = mod(decimal(h_i) \times 10^{14}, L), \quad i = 1,2,3,4 \quad (2)$$

where $L = m \times n / 4$ (i.e., the length of sequences which will be operated a sorting algorithm on), mod is the residue-generating function, and decimal is the picking function of the decimal part of a real number.

The chaotic sequences used in encryption are generated with a sorting algorithm by the following steps:

1) Pick the first 3L elements of each h_i', and divide each result into three parts with the same length, named as: x_i, y_i and z_i.
2) Sort x_1 in ascending-order to get x_1', find out the new position of x_1' in x_1, and record the transform-position vector in I_1, then use the vector I_1 to permute x_2 into x_2'. Similarly, I_2 is recorded and then used to permute x_3, and so on. In this way, four permuted sequences (x_1', x_2', x_3', x_4') are obtained.
3) Merge the four sequences into one, with a total length of $m \times n$ (the same as the pixel dimension of the original images) using $d_1 = \{x_1', x_2', x_3', x_4'\}$. Similarly, $d_2 = \{y_1', y_2', y_3', y_4'\}$ and $d_3 = \{z_1', z_2', z_3', z_4'\}$ can be generated.
4) The three chaotic sequences $d_i (i = 1,2,3)$ can be further digitalized into $d_i' (i = 1,2,3)$ using

$$d_i' = \mathrm{mod}(d_i, 256), \quad i = \{1,2,3\} \quad (3)$$

since the gray-level of a pixel varies from 0 to 255.

The digitalized chaotic sequences will be used in later chaotic diffusion and shuffling algorithms.

4. Chaotic Diffusion in Spatial-Domain

In spatial-domain, the original image is encrypted with chaotic XOR diffusion. It is well known that XOR operation can enhance the security of the cipher image due to its destructiveness on statistical characteristics of images (e.g., histogram). Thus, the security level will be much enhanced after the chaotic XOR diffusion, if compared with the encryption with only pixel-position scrambling.

In the proposed scheme, the chaotic sequence d_1' is applied for diffusion in spatial-domain, as shown in Fig. 1. It will be proved in Section 4, that the histogram of the cipher image is equalized with uniformity after the chaotic XOR diffusion.

5. Chaotic Shuffling in Frequency-Domain

The chaotic shuffling algorithm is performed in frequency-domain where the plaintext-related mechanism is introduced, therefore every cipher-pixel is generated associated with the following elements: the former plain pixel, cipher pixel and one chaotic sequence, to ensure the capability of resisting the chosen and known-plaintext

attacks. The schematic encryption procedure of chaotic shuffling is illustrated in Fig. 2, where P and M are the phase and magnitude-spectra respectively of the 1st round cipher image, P' and M' are the corresponding 1-D sequences which are obtained by converting the 2-D matrixes P and M into 1 D sequences, $d_j''(i)=d_j'(i+P'_{i-1})$, j=2,3; i=1,2,…,mn. Besides, d_2' and d_2'' are used to encrypt P', while d_3' and d_3'' are used to encrypt M'.

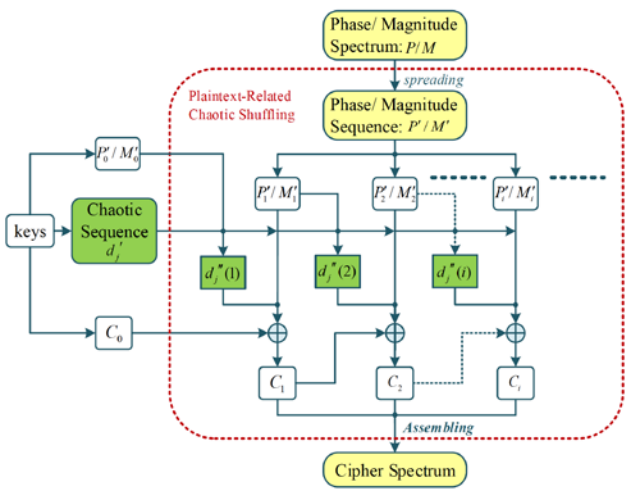

Fig. 2 Procedure of the plaintext-related chaotic shuffling algorithm.

The encryption procedure of chaotic shuffling is described in the following steps:

1) Transform the 1st round cipher image obtained after diffusion in spatial-domain with Fast Fourier Transform (FFT), to get its phase (P) and the magnitude spectra (M).
2) Reconstruct P and M by spreading these two matrixes into 1-D sequences, to obtain the sequences P' and M', each with pixels.
3) Generate the cipher pixel using the following four elements: P'_i, C_{i-1}, $d_2'(i-1)$ and $d_2''(i)$, i.e., the ith plain pixel, the $(i-1)^{th}$ cipher pixel, the ith and $(i+P'_{i-1})^{th}$ elements of the chaotic sequence d_2', to obtain the new cipher image element C_i:

$$\begin{cases} u = \mathrm{mod}(d_2'(i+P'_{i-1})+P'_i, 256) \\ v = \mathrm{mod}(C_{i-1}+d_2'(i), 256) \\ C_i = bitxor(u,v) \end{cases} \quad (4)$$

where the function bitxor returns the bit-wise XOR of the two input arguments. The initial values can be randomly assigned, such as, C_0 =277, and P'_0 =100, which can also be regarded as additional secure keys.

The chaotic sequence d_3' is used to operate chaotic shuffling on the magnitude sequence M', the similar way as P' is encrypted with d_2' in step 3. The parameter M'_0 can also be served as an additional key.

6. Decryption Algorithm

As all the necessary secure keys were shared between the transmitter and the receiver, the cipher image can be decrypted into the original digital image with the reverse operations. The procedure of decryption is described as follows:

1) Obtain the chaotic sequences using Eq. (1).
2) Obtain the phase and magnitude spectra of the cipher image using FFT, and spread them into 1-D sequences for latter operation.
3) Remove the shuffling in the phase spectrum obtained in step 2, using:

$$\begin{cases} u' = \mathrm{mod}(C_{i-1}+d_2'(i), 256) \\ v' = bitxor(C_i, u') \\ P'_i = \mathrm{mod}(v'-d_2'(i+S_{i-1}), 256) \end{cases} \quad (5)$$

4) Remove the shuffling in the magnitude spectrum using Eq. (5) as well, to get the magnitude sequence without shuffling (M'), then convert P' and M' into phase and magnitude-spectra in matrix-forms (P and M).
5) Reconstruct P and M into spectrum, using:

$$S = M\cos P + jM\sin P \quad (6)$$

then perform IFFT on S, to obtain the original image in spatial-domain.

After all these operations, the original image can be correctly recovered.

7. Comparison and Analysis

For the deep understanding of key elements in the encryption algorithm, as well as for summarizing the procedure of the proposed encryption, more algorithms are analysed as comparisons to the proposed one.

The encryption effects are compared and analysed among different algorithms, such as: performing shuffling operation in spatial or frequency-domain alone, using shuffling operations to replace XOR operations in spatial-domain, or exchanging the encryption orders, i.e., to perform the shuffling operation in frequency first, then

perform XOR operation in spatial-domain. Several definitions should be given for simplification, where

- "S(X)" stands for "performing XOR in spatial-domain";
- "S(S)" stands for "performing shuffling operation in spatial-domain";
- "F(S)" stands for "performing shuffling operation in frequency-domain";
- "A & B" stands for "operate A first, then B".

Taking the sample image Lena as an example, the simulation results are shown in Table 1.

Table 1: Entropy and correlation coefficients of the original encrypted image.

	S(X) & F(S) (proposed)	S(S)	F(S)	S(S) & F(S)	F(S) & S(X)
Entropy	7.9969	7.9925	7.9946	7.9961	7.9937
Correlation	0.002212	0.025386	0.002312	0.006455	0.003891

7.1 F(S) Compared with S(S)

Comparing with S(S) (the scheme proposed in [10], F(S) performs better in both entropy and correlation, which means that performing shuffling algorithm in frequency-domain is better than in spatial-domain. The reason behind is that, shuffling algorithm in frequency-domain has been applied twice, for both phase and magnitude-spectra. It has also been verified in another paper [15] from the author of this paper that, the cipher image obtained after specified encryption operations performed in frequency-domain appeared more confused than the cipher image obtained after the same operations performed in spatial-domain.

7.2 S(X) & F(S) Compared with S(S) & F(S)

To obtain a uniform histogram for the cipher image, the chaotic diffusion is operated in spatial-domain before the frequency-domain encryption. XOR or shuffling can be performed upon digital images alone, followed with shuffling in frequency-domain algorithm. It can be seen from the comparison between the schemes (S(X) & F(S)) and (S(S) & F(S)) that, if the original image is diffused with chaotic XOR, the encryption effects become better, since XOR is a more straight-forward and effective method in diffusion to achieve a uniform histogram in spatial-domain. While plaintext-related algorithm mainly contributes to resist various attacks.

7.3 S(X) & F(S) Compared with F(S) & S(X)

Results in Table 1 prove that, if the image is first encrypted with shuffling algorithm in frequency-domain and then with diffusion in spatial-domain, the performance is worse than that of the proposed encryption scheme. This helps to optimize the encryption procedure.

In summary, the proposed hybrid plaintext-related image encryption algorithm achieves the best results. Shuffling algorithm in frequency-domain mainly brings resistance to known and chosen-plaintext attacks. In addition, the proposed algorithm outputs the highest value in entropy and lowest in correlation, when compared with any other schemes proposed in Section 4. Thus, the robustness of the proposed scheme is fully verified, which suggests that the scheme could be applied as a successful candidate in digital image encryption. Besides, it is the first time that the chaotic shuffling is successfully applied in frequency-domain, with significant security improvements.

8. Security analysis

The proposed algorithm is performed on hundreds of images for testing, where three representative sample pictures (Lena, Gelada and Boat) each with a size of 512×512 pixels are used to verify the security performance of the proposed image encryption algorithm. The encryption and security analysis of the sample pictures will be given in detail thereafter.

8.1 Key Space Analysis

To evaluate the robustness of an encryption scheme quantitatively, key-space is always the most important parameter to be analysed. In the proposed algorithm, four chaotic sequences are generated by hyper digital chaos. Elements of $\{key\}=\{h_1(0),h_2(0),h_3(0),h_4(0)\}$ are chosen as keys to the encryption and decryption methods in this paper, where $h_i(0)$ is the initial value of the ith chaotic sequence. If the parameters L, C_0, P_0' , M_0' and t are considered as additional keys, the key space would be much bigger. For example, the iteration time t is a 16-bit integer, so its key space would be 216 [17]. Thus, the key-space grows to ~6.5536×10^{64}. It will take 2.2902×10^{55} years to obtain the correct keys of the proposed scheme, when calculating with the fastest computer with a computing speed of ~9.3×10^{16} s^{-1} [18], which statistically verifies that such a giant key space created in the proposed encryption scheme provides enough secure capability against any brute-force attacks.

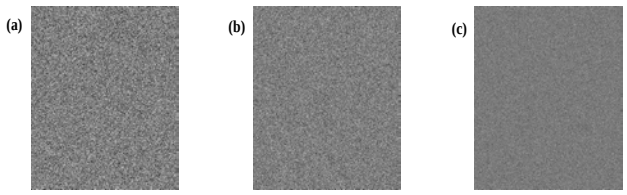

Fig. 3 Decrypted images with wrong keys.

(a) Single incorrect key, (b) Single incorrect key, and (c) Single incorrect key.

8.2 Key Sensitivity Analysis

The cipher image of Lena is decrypted with right keys except for a single wrong key to demonstrate how sensitive the encryption scheme is to the encryption keys. It can be seen from Fig. 3, that the decrypted image is unrecognizable. As it has also been proved in [16], a tiny change (1×10^{-15}) of the initial values will lead to a totally different result. Therefore, the key space of the chaotic system alone is 10^{60} ($10^{15}\times10^{15}\times10^{15}\times10^{15}$), much bigger than that of the 128-bit advanced encryption standard (AES) algorithm, who owns a key space of the ~3×10^{38}(~2^{128}).

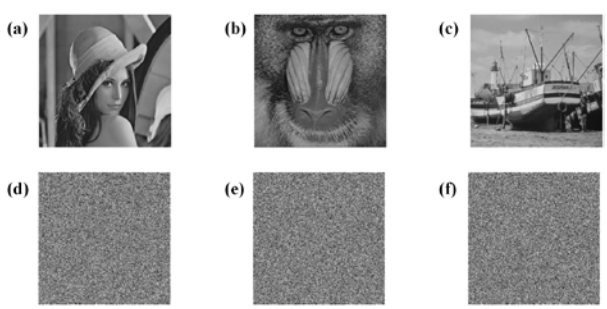

Fig. 4 Plain images and the corresponding ciphers (a)-(c). Plain images, (d)-(f). Pixel distributions of the cipher images.

8.3 Against Statistical Attacks

Statistical analysis only works when the plain image and cipher image change correspondingly, which means their statistical characteristics change correspondingly. It is said that attacks based on statistical analysis exploits the predictable relationship between data segments of the plain-image and cipher-image [19]. To demonstrate the resistance to statistical analysis, both histogram and correlation are presented in this section.

From Fig.4, we can see that histogram of either one of the three test images performs uniform, which is totally different with that of the original image.

Correlation coefficient between two adjacent pixels could be calculated with [20]:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{7}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{9}$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{10}$$

The simulation results are presented later in Section 8.3.3, which has also been explained and analysed. It would be well seen that the neighbour pixels of an image show no correlation at all.

8.3.1 Histogram

Uniformity in histogram shows that there is no chance for attackers to capture vital characters of the original image. The uniform effect in histogram of the cipher image is one of the key parameters in image encryption, which suggests that gray-level values of pixels will be distributed equally among all values from 0 to 255.

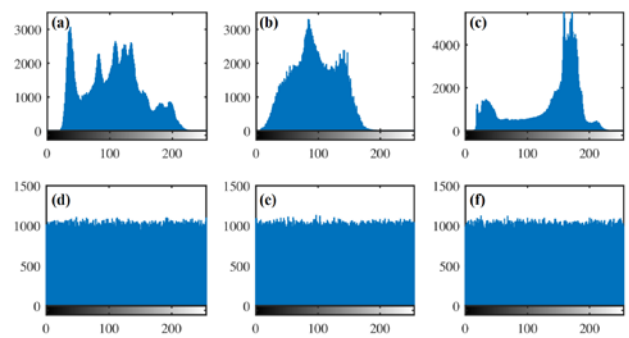

Fig. 5 Histograms of plain images and corresponding ciphers after using the proposed encryption. (a)-(c) Histogram of plain images, (d)-(f) Histogram of the cipher images.

8.3.2 Entropy

Entropy is another important key parameter for the evaluation of the randomness in an image. Theoretically, the maximum value of entropy is 8, and an image is more confused if the entropy value was much closer to 8 [21]. It suggests that, the statistical characteristics in an image will be totally lost if the entropy value is very close to 8. After the operations of the proposed encryption, the entropy values of the original and encrypted images are listed in Table 2.

Table 2: Entropy values of original and cipher images

	Lena	Gelada	Boat
Original	7.3871	7.1658	7.1268
Cipher	7.9969	7.9954	7.9969

When compared with the shuffling algorithm in spatial-domain in [13], the corresponding entropy values using chaotic diffusion is much higher. The highest entropy of 7.9969 is achieved for the original image of Lena and Boat, while all the entropy values are improved significantly, which proves the robustness of the proposed chaotic diffusion and shuffling scheme.

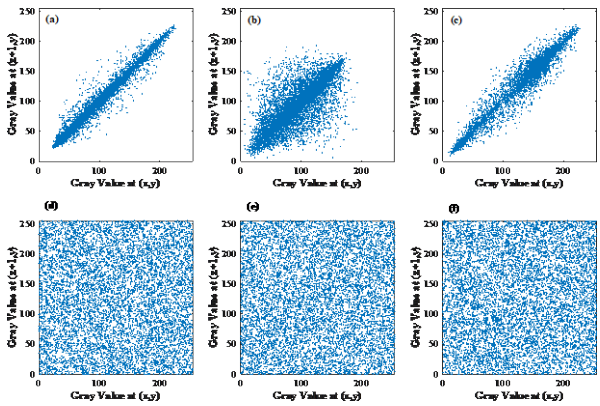

Fig. 6 Correlation maps of Lena, Gelada, Boat and corresponding cipher image by using proposed algorithm. (a)-(c) Correlation maps of original images, (d)-(f) Correlation maps of the cipher images.

Table 3:Correlation coefficients of original and cipher images

		Lena	Gelada	Boat
Original	Horizontal	0.9841	0.7491	0.9798
	Vertical	0.9760	0.7488	0.9671
	Diagonal	0.9627	0.8853	0.9463
Cipher	Horizontal	0.002212	0.001481	0.001815
	Vertical	0.002341	0.001617	0.001783
	Diagonal	0.002204	0.001502	0.001775

8.3.3 Correlation

The horizontal correlation coefficients of the original and corresponding cipher images after using the proposed encryption are shown in Fig. 6. It can be noted that, the horizontal correlation maps of the three cipher images appear totally uncorrelated, which implies that the security is enhanced as the statistical clues are all destroyed. Correlation maps in other two directions appear uncorrelated as well.

The corresponding correlation coefficients between adjacent pixels in horizontal, vertical and diagonal directions are listed in Table 3.

Theoretically, the lower the correlation coefficient is, the more secure the corresponding cipher image will be. A correlation coefficient entering a zone of [0, 0.09] means the neighbour pixels of an image have no correlation at all, which was mentioned and verified in [22].

8.4 Against Chosen and Known Plaintext Attacks

In the proposed encryption method, a plaintext-related algorithm is implemented in frequency-domain, where each cipher-pixel is decided by the chaotic keys, previous plaintext and cipher-text. As a result, the plain-pixels are spread into all the subsequent cipher-pixels, which implies that the predetermined relationship between a certain cipher-pixel and its corresponding plain-pixel changes every time when it comes to a different plain-image. In other words, the chaotic keys used in the encryption scheme change dynamically with the change of the input plaintext. Therefore, chosen and known-plaintext attacks are useless on this scheme.

8.5 Against Differential Cryptanalysis

Differential cryptanalysis is a kind of chosen plaintext attacks, from which as many keys as possible can be obtained through analysis of the relationship between specified plaintext differential-pairs and corresponding cipher-text differential-pairs. Since there is no fixed relationship between the cipher-text and plaintext, the attackers are not able to obtain the keys to the encryption system by differential cryptanalysis. As explained in Section 8.3, chaotic shuffling algorithm is implemented, which is based on the plaintext-related mechanism. Accordingly, the encryption scheme possesses the capability against attacks with differential cryptanalysis.

The encryption effects can also be expressed by NPCR (number of changing pixel rate) and UACI (unified averaged changed intensity). NPCR addresses how many pixels are different between two encrypted images, whose original images are almost the same but differ at only one pixel. UACI addresses how much the mentioned two encrypted images differ from each other, by calculating each difference between corresponding pixels from the two encrypted images. The expressions of NPCR and UACI are listed as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\% \quad (11)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{c_1(i, j) - c_2(i, j)}{255} \times 100\% \quad (12)$$

where (M, N) is the size of the encrypted images, $c_k(i, j),\ k = 1, 2$ is a certain pixel in the two encrypted images, and

$$D(i, j) = \begin{cases} 0, \ if \ \ c_1(i, j) = c_2(i, j) \\ 1, \ if \ \ c_1(i, j) \neq c_2(i, j) \end{cases} \quad (13)$$

For any two random images, the expected NPCR and UACI can be calculated by equations below:

$$NPCR_{Expected} = (1 - 2^{-L}) \times 100\% \quad (14)$$

$$UACI_{Expected} = \frac{1}{2^{2L}} \frac{\sum_{i=1}^{2^L - 1} i(i+1)}{2^L - 1} \times 100\% \quad (15)$$

where L is the pixel depth of the tested images. Images with pixel depth of 9 are used in this paper, thus the expected NPCR and UACI would be NPCRExpected =99.8047%, UACI Expected =33.3984%.

Several testing images (all with a size of 512*512, which means the pixel depth is 9) are chosen as tested images to perform differential-attack-resistance test, by calculating the average value of NPCR and UACI with Eq. (11) - (13). Each tested image would be changed for 512*512 times to replace one of the pixel in it.

From the Table 4 shown below, the mean value of NPCR and UACI for each tested image reach the expected values. It is proved that the proposed algorithm performs well in resisting against differential attacks.

Table 4: NPCR/UACI of Tested Images and the Expected Values

	Lena	Gelada	Boat	Expected
NPCR	0.997511	0.997321	0.997096	**99.8047%**
UACI	0.332547	0.333604	0.332816	**33.3984%**

Table 5: Computational Load

Operator	Computational Load
Addition	11t+2K+1+Klog2N
Multiplication	13t+K+4+2Klog2N
Modulus (Mod)	2K+7
bitwise (XOR)	K
decimal	4

8.6 Computational Load and Encryption Speed

The basic operations used in the proposed scheme are addition, multiplication, modulus, decimal, and XOR. The total operation numbers are shown in Table 5, where K=M N (size of an image, M=N), and t=20,000 is the iteration time of the chaotic system used in the scheme.

The proposed algorithm is run on MATLAB R2014b in a personal computer with a 2GB memory and a Windows 7 system. While the encryption scheme for every testing image with a size of 512*512 (including generating simulation figures such as correlation maps), takes several seconds, to calculate the operations listed in Table 5. The mean encryption speed would be 0.44MB/s, which is much higher than that in [2] (0.1MB/s, with MATLAB running on a PC with the same size of memory and the same operating system) and [23] (0.188MB/s, with C++ running on a PC with 2GH processor and 256 MB RAM). Since the decryption method is a reversed version of the encryption method and share the same time complexity, the decryption speed would be at the same level as the encryption speed. It is believed that if it was computed with a more excellent computer, the encryption would go on faster.

9. Conclusion

In this paper, a robust plaintext-related image encryption is proposed based on hyper-chaos, where chaotic diffusion and shuffling in spatial- and frequency-domain are implemented. Uniform histograms of the cipher images are achieved for the sample images, mainly attributed to chaotic XOR diffusion. Moreover, the chaotic shuffling algorithm is firstly introduced to resist the chosen and known-plaintext attacks. Statistically, the proposed encryption scheme is verified via uniformity in histograms, high entropy (7.9969) and low correlation coefficient (0.002212). Meanwhile, the proposed scheme possesses a large key space, which can resist brute-force attacks. The proposed algorithm performs well in resisting well-known attacks, and the encryption speed (0.44MB/s) can be elevated with more excellent computer. In the future, compression would be introduced in this scheme to achieve better transmission effect.

Acknowledgements

This work was supported in part by International S&T Cooperation Program of China, 2016YFE0104500, National Natural Science Foundation of China under Grants 61571291, 61431009 and 61221001.

References

[1] L. Xu, Z. Li, J. Li, et al., “A novel bit-level image encryption algorithm based on chaotic maps,” Optics & Lasers in Engineering, 78(21), 17-25(2016).
[2] B. Murugan, A.G.N. Gounder, “Image encryption scheme based on block-based confusion and multiple levels of diffusion,” IET Computer Vision, 10(6), 593-602(2016).
[3] Y. Mao, G. Chen, “Chaos-Based Image Encryption,” in Handbook of Geometric Computing, 231-265, Springer, Berlin Heidelberg (2005).
[4] J. Fridrich, “Image Encryption Based on Chaotic Maps,” IEEE Int. Conf. on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, Orlando, FL, 1105-1110(1997)
[5] Y. Wang, K. Wong, X. Liao, et al., “A New Chaos-Based Fast Image Encryption Algorithm,” Applied Soft Computing, 11(1), 514-522(2011).
[6] X. Wang, S. Gu, Y. Zhang, “Novel image encryption algorithm based on cycle shift and chaotic system,” Opt. Lasers Eng., 68, 126–134(2015).
[7] D. Solev, P. Jantic, and L. Kocarev, “Chapter-1: Introduction to Chaos,” in Chaos Based Cryptography: Theory, Algorithms, and Applications, 1-25, Springer, Berlin Heidelberg (2011).
[8] K. Kaneko, “Chaos as a Source of Complexity and Diversity in Evolution,” Artificial Life, 1(1_2), 163-177(Oct. 2010).
[9] T. Gao, Z. Chen, “A New Image Encryption Algorithm Based on Hyper-Chaos,” Physics Letters A, 372(4), 394-400(2008).
[10] L. Lei, F. Bai, and X. Han, “New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos,” Int. Conf. on Computational and Information Sciences, China, 713-716(2013).
[11] S. Rohith, and B.K. Sujatha, “Image Encryption and Decryption Using Combined Key Sequence of Logistic map and Lozi map,” IEEE Int. Conf. on Communications and Signals (ICCSP), Melmaruvathur, 1053-1058(2015).

[12] Y. Abanda, and A. Tiedeu, “Image Encryption by Chaos Mixing,” IET Image Processing, 10(10), 742-750(2016).
[13] X. Deng, C. Liao, C. Zhu, et al., “A Novel Image Encryption Algorithm Based on Hyperchaotic System and Shuffling Scheme,” IEEE Int. Conf. on High Performance Computing and Communications & International Conference on Embedded and Ubiquitous Computing, China, 109-116(2013).
[14] R. Munir, “A Block-Based Image Encryption Algorithm in Frequency-Domain using Chaotic Permutation,” 8th Int. Conf. on Telecommunication Systems Services and Applications, Kuta, 1-5(2014).
[15] W. Yuan, X. Yang, and W. Guo, “A Double-Domain Image Encryption Using Hyper Chaos,” 19th Int. Conf. on Transparent Optical Networks, Girona, Spain, paper We.P.1(2017).
[16] X. Hu, X. Yang, “Chaos-Based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON,” IEEE Photonics Technology Letters, 27(23), 2429-2432(2015).
[17] H. Huang, and S. Yang, “Colour Image Encryption based on Logistic Mapping and Double Random-Phase Encoding,” IET Image Processing, 11(4), 211-216(2017).
[18] H. Fu, J. Liao, J. Yang, et al., “The Sunway Taihu Light supercomputer: system and applications,” Science China Information Sciences, 59(7), 1-16(2016).
[19] Marion, An introduction into image processing, 193-230, Springer, US (1991).
[20] S. Mazloom, A.M. Eftekhari-Moghadam, “Color image encryption based on coupled nonlinear chaotic map,” Chaos Solitons Fractals, 42, 1745-1754(2009).
[21] P. Baldi, S. Brunak, Information Theory, Entropy, and Relative Entropy, 2nd ed., 357-363, MIT Press (2011).
[22] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, 2nd ed., ISBN: 978-0-12-179060-8, Elsevier Inc. (1988).
[23] T. Xiang, X. Liao, G. Tang, et al., “A novel block cryptosystem based on iterating a chaotic map,” Phys. Lett. A, 349, 109-115(2006).