Digital Image Encryption and Detection Based on Plaintext-Related Chaotic Map and SHA-256 Algorithm: Postprint

Authors: Liu Xilin, Yan Guangle

Date: 2018-10-11T00:00:00+00:00

Abstract

To address the security issues in digital image dissemination, as well as the problems of digital image encryption being decoupled from plaintext and excessive reliance on chaotic systems, a digital image encryption and monitoring algorithm based on plaintext-related chaotic mapping and the SHA-256 algorithm is proposed. The algorithm utilizes the SHA-256 algorithm to compute the hash value of the plaintext image as a digest for monitoring digital image dissemination; it employs forward diffusion, plaintext-associated scrambling, and backward diffusion methods to encrypt digital images, with the Lorenz chaotic map generating the corresponding cipher. Experimental results demonstrate that the algorithm possesses strong resistance against various attacks, achieving the objectives of security and confidentiality in image dissemination.

Full Text

Preamble

Encryption and Monitoring of Digital Images Based on Plaintext-Related Chaotic Maps and SHA-256 Algorithm

Liu Xilin, Yan Guangle
(Business School, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: To address the security issues in digital image transmission and the problem that digital image encryption schemes often operate independently of plaintext and rely excessively on chaotic systems—thereby weakening algorithm reliability—this paper proposes a digital image encryption and monitoring algorithm based on plaintext-related chaotic mapping and SHA-256. The algorithm employs SHA-256 to compute a hash value of the plaintext image as a digest

for monitoring image dissemination. It encrypts digital images using forward diffusion, plaintext-related scrambling, and backward diffusion, with the Lorenz chaotic map generating corresponding cipher sequences. Experimental results demonstrate that the algorithm exhibits strong resistance to various attacks and achieves secure and covert image transmission.

Keywords: chaotic systems; image encryption; SHA-256; hash value; Lorenz chaotic map

0 Introduction

With the rapid development of network information technology, digital image information is highly vulnerable to interception by malicious actors during transmission through communication systems, posing risks of privacy leakage and data security. In applications such as telemedicine, military communications, personal imaging, video conferencing, and biometric systems, image transmission requires guaranteed security, yet leakage incidents occur frequently. Consequently, digital image encryption serves as a critical safeguard for secure image transmission.

As security concerns in digital image transmission have grown increasingly prominent, scholars have proposed numerous image encryption algorithms in recent years. Some schemes based on pixel position permutation and pixel value diffusion, as referenced in [2-4], accomplish digital image encryption but suffer from small key spaces. References [5,7,8] combine frequency domain transformations with chaotic systems to achieve better encryption effects, yet they exhibit the problem of low information entropy in ciphertext images. Reference [4] integrates multiple methods with chaotic systems for image encryption, offering a large key space but involving cumbersome encryption and decryption processes with low efficiency. Furthermore, some of these algorithms suffer from excessive reliance on chaotic systems and operate independently of plaintext, thereby weakening their reliability. In many classical digital image cryptosystems, the key is the sole basis for generating the cipher for encrypting plaintext images—that is, the cipher is controlled only by the key and is related to the key but independent of the plaintext. Such image cryptosystems are vulnerable to chosen-plaintext attacks or known-plaintext attacks Error! Reference source not found.

To address these issues, this paper proposes an encryption and monitoring scheme based on plaintext-related chaotic mapping and SHA-256. First, a 256-bit hash value is generated from the grayscale version of the digital image using the SHA-256 algorithm as a digest to monitor whether the ciphertext image has been tampered with during transmission. Second, the digital image is encrypted using a combination of forward and backward diffusion methods for pixel value scattering, along with a plaintext-related scrambling algorithm for pixel position permutation to form the ciphertext. This means that cipher generation depends

not only on the key but also on plaintext information. The three-dimensional Lorenz chaotic map generates corresponding cipher sequences. This approach enables covert transmission of encrypted images. Experimental results show that the algorithm not only improves key sensitivity and monitors transmission security but also effectively resists plaintext attacks, brute-force attacks, and other threats.

---

1 SHA-256 Algorithm and Chaotic Systems

1.1 SHA-256 Algorithm

SHA (Secure Hash Algorithm) is one of the most widely used secure compression algorithms internationally, jointly developed by NIST and NSA in the United States. This algorithm was established as an encryption standard by NIST and NSA on May 11, 1993. SHA-256 is one of its variants, addressing the security vulnerabilities of SHA-1. It can convert digital image information into a 256-bit hash value. Any minute change in the digital image content will cause a dramatic change in the hash value. A digital image processed with SHA-256 thus possesses a unique "fingerprint."

1.2 Lorenz Chaotic System

This paper employs the Lorenz system mapping, whose specific dynamic equations are as follows Error! Reference source not found.:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ \dot{z} = xy - cz \\ \dot{w} = r(z - xy) + w \end{cases}$$

where a, b, c, and r are parameters of the hyperchaotic system, and x, y, z are three state variables generated by the Lorenz chaotic system. When $a = 10$, $b = 8/3$, $c = 28$, and $1.52 \leq r \leq 0.06$, Equation (1) is in a chaotic state Error! Reference source not found.

---

2 Encryption Scheme Design

The proposed encryption algorithm first performs forward diffusion on the original image' s pixel values, then applies plaintext-related scrambling to permute pixel positions, and finally conducts backward diffusion to form the ciphertext. The parameters and initial values of the chaotic Lorenz system serve as the key. The decryption process is the inverse of the encryption process.

Assume the plaintext image is P with size $M \times N$, grayscale level L, key $K = \{x_0, y_0, z_0, w_0, r_0, r_1, r_2\}$ as the initial state values, and r_1, r_2 as two 8-bit random numbers. The specific encryption steps are as follows:

a) Using the key initial state values, iterate the chaotic Lorenz system to generate four pseudo-random sequences $\{x_i\}$, $\{y_i\}$, $\{z_i\}$, $\{w_i\}$, where $i = 1, 2, \ldots, MN$. Using these four pseudo-random sequences, generate matrices X, Y, Z, W, U, and V according to the following formulas Error! Reference source not found.:

$$\begin{cases} X(k,l) = (500 \times x_{13(k-1)N+13(l-1)+1} \mod 1) \times 10^{14} \mod M \\ Y(k,l) = (500 \times y_{13(k-1)N+13(l-1)+1} \mod 1) \times 10^{14} \mod N \\ Z(k,l) = ((z_{13(k-1)N+13(l-1)+1} \times 10^{14}) \mod M) + 1 \\ W(k,l) = (((500 \times w_{13(k-1)N+13(l-1)+1} \mod 1) \times 10^{14}) \mod N) + 1 \\ U(k,l) = (((500 \times x_{13(k-1)N+13(l-1)+2} \mod 1) \times 10^{14}) \mod M) + 1 \\ V(k,l) = (((500 \times w_{13(k-1)N+13(l-1)+2} \mod 1) \times 10^{14}) \mod N) + 1 \end{cases}$$

where $k = 1, 2, \ldots, M$; $l = 1, 2, \ldots, N$; and floor(t) returns the greatest integer less than or equal to t.

b) Convert plaintext image P to matrix A through forward diffusion using the following formula:

$$A(i,j) = \begin{cases} (P(i,j) + X(i,j)) \mod 2^L, & i = 1, j = 1 \\ (P(i,j) + A(i,j-1) + X(i,j)) \mod 2^L, & i = 1, 1 < j \le N \\ (P(i,j) + A(i-1,j) + X(i,j)) \mod 2^L, & i > 1, j = 1 \\ (P(i,j) + \text{sum}(A(1:i-1, 1:j-1)) + X(i,j)) \mod 2^L, & i > 1, j > 1 \end{cases}$$

where sum(t) returns the sum of all elements in vector t.

c) Convert image matrix A to matrix B through plaintext-related scrambling using the following formula:

$$\begin{cases} m = (U(i,j) + \text{sum}(A(1:Z(i,j), 1:W(i,j))) \mod M) + 1 \\ n = (V(i,j) + \text{sum}(A(1:M, 1:W(i,j))) \mod N) + 1 \end{cases}$$

where m and n are the coordinates of matrix B. In cases where $m = i$ or $Z(i,j)$, or $n = j$ or $W(i,j)$, or $Z(i,j) = i$ or $W(i,j) = j$, the position of $A(i,j)$ remains unchanged; otherwise, $A(i,j)$ and $A(m,n)$ swap positions.

d) Perform backward diffusion on matrix B to obtain matrix C using the following formula:

$$C(i,j) = \begin{cases} (B(i,j) + Y(i,j) + r_1) \mod 2^L, & i = M, j = N \\ (B(i,j) + C(i,j+1) + Y(i,j)) \mod 2^L, & i = M, 1 \le j < N \\ (B(i,j) + C(i+1,j) + Y(i,j)) \mod 2^L, & i < M, j = N \\ (B(i,j) + \text{sum}(C(i+1:M, j+1:N)) + Y(i,j)) \mod 2^L, & i < M, j < N \end{cases}$$

The scheme design flowchart is shown in Figure 1 [Figure 1: see original paper].

2.1 Generating Image Digest

Convert the digital image to a grayscale image (i.e., transform the three-dimensional matrix into a two-dimensional matrix, which is irreversible). The 256-bit hash value generated from the grayscale image using the SHA-256 algorithm serves as a digest, forming the digital image' s "fingerprint." The 256-bit digest (hash value) produced by applying SHA-256 encoding to the classic Lena grayscale image is: 9a9b4963ddaa149de2d7d66b5c952e2fe0036f4a819046998f766be605eb3f18. The sender saves this digest value for matching after the receiver decrypts the ciphertext.

---

3 Simulation Experiments

The proposed algorithm was simulated in MATLAB 7.1. The original Lena image is shown in Figure 2 [Figure 2: see original paper], the encrypted Lena image in Figure 3 [Figure 3: see original paper], the correctly decrypted Lena grayscale image in Figure 4 [Figure 4: see original paper], and the image decrypted with an incorrect key in Figure 5 [Figure 5: see original paper]. The original Cameraman image is shown in Figure 6 [Figure 6: see original paper], the encrypted Cameraman image in Figure 7 [Figure 7: see original paper], the correctly decrypted Cameraman image in Figure 8 [Figure 8: see original paper], and the image decrypted with an incorrect key in Figure 9 [Figure 9: see original paper].

The digest (hash value) generated from the Lena image decrypted by the receiver after SHA-256 encoding is: 9a9b4963ddaa149de2d7d66b5c952e2fe0036f4a819046998f766be605eb3f18. If the image information is slightly altered during transmission, the SHA-256 algorithm will produce a different digest. The receiver' s digest value is compared with the sender' s digest value; any discrepancy indicates that the image has been tampered with during transmission, while identical values confirm secure transmission.

Similarly, the digest (hash value) generated from the Cameraman image decrypted by the receiver after SHA-256 encoding is: 29c69af72fd1e6f6b1e7603573a2b750e11a30480516af6ea34f17e

If the image information is slightly modified during propagation, using SHA-256 will yield a different hash value.

---

4 Security Analysis

4.1 Histogram Analysis

Digital image encryption can convert plaintext into noise to hide information. Histograms can represent the distribution frequency of image pixels and describe the statistical correlation of images. Generally, the more uniformly distributed the grayscale histogram of an image, the more effectively it can resist statistical analysis attacks. Taking the classic Lena image as an example: the grayscale histogram of the original image is shown in Figure 10 [Figure 10: see original paper], and the grayscale histogram of the encrypted image is shown in Figure 11 [Figure 11: see original paper]. The figures demonstrate that the encrypted image' s grayscale histogram is closer to a uniform distribution, indicating that the encryption can effectively resist statistical analysis attacks.

4.2 Correlation Analysis

Adjacent pixels in plaintext images exhibit strong correlations, and these correlations contain partial plaintext information that, if exploited by malicious actors, could lead to image leakage Error! Reference source not found.. An excellent encryption algorithm should weaken the correlation between image pixels. This paper randomly selected 2000 pairs of adjacent pixels from both the original Lena image and the encrypted ciphertext image, plotted their correlation in various directions as shown in Figure 12 [Figure 12: see original paper], and calculated the correlation coefficients in each direction as presented in Table 1 . The figures and table clearly show that the correlation between adjacent pixels in the encrypted image is significantly reduced, making the image more secure.

The correlation coefficient is calculated using the following formula:

$$r_{xy} = \frac{\operatorname{cov}(u, v)}{\sqrt{D(u)}\sqrt{D(v)}}$$

where

$$\operatorname{cov}(u, v) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))(v_i - E(v))$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i, \quad D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2$$

Here, N is the number of randomly selected adjacent pixel pairs, their grayscale values are (u_i, v_i) for $i = 1, 2, \ldots, N$, and the vectors are $\{u_i\}$ and $\{v_i\}$.

4.3 Information Entropy Calculation

Information entropy reflects the uncertainty of an image. Generally, the better the encryption effect of an algorithm, the greater the image' s information entropy, and the larger the image' s information content and randomness. Table 2 shows the information entropy results for the classic Lena image encrypted by several algorithms. The information entropy formula is as follows:

$$H = -\sum_{i=0}^{L-1} P(i) \log_{2P}(i)$$

where L is the number of image grayscale levels, and $P(i)$ represents the probability of grayscale value i occurring. For grayscale images with $L = 256$, the theoretical value of information entropy H is 8. The data in the table reveals that although the information entropy values of references [1], [3], and this algorithm are all close to the theoretical value, the information entropy of the Lena image encrypted by this algorithm is closer to 8, indicating that this algorithm can more effectively resist data attacks Error! Reference source not found..

4.4 Key Space Analysis

The key space refers to the set of all legitimate keys; the better the encryption algorithm, the larger the corresponding key space Error! Reference source not found.. In this paper, the key is $K = \{x_0, y_0, z_0, w_0, r_1, r_2\}$, where $x_0 \in (-40, 40)$, $y_0 \in (-40, 40)$, $z_0 \in (1, 81)$, and $w_0 \in (-250, 250)$. The step sizes for x_0, y_0, and z_0 are 10^{-13}, while the step size for w_0 is 10^{-12}. Both r_1 and r_2 are integers ranging from 0 to 255. The resulting key space is approximately $6.4 \times 10^{16} \times 2^{16}$, equivalent to about 213 bits. In comparison, reference [2] has a key space of only 2^{128}. Although this algorithm' s key space is large, its average encryption speed ranges between 14-20 seconds, while reference [2] averages around 10 seconds and reference [4] exceeds 30 seconds. Comprehensive analysis shows that this algorithm offers a larger key space and better resistance to brute-force attacks while maintaining a moderately fast encryption speed.

4.5 Differential Attack Analysis

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are important metrics for measuring an image encryption algorithm's ability to resist differential attacks Error! Reference source not found.. Differential attack involves making slight changes to the plaintext, encrypting it again, and comparing the differences between the resulting ciphertexts. If the ciphertexts differ significantly, the algorithm demonstrates strong resistance to plaintext and differential attacks. Table 3 shows the average NPCR and UACI

values from 100 repeated experiments. The specific formulas for NPCR and UACI are as follows:

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

where

$$D(i,j) = \begin{cases} 1, & \text{if } P_1(i,j) \neq P_2(i,j) \\ 0, & \text{if } P_1(i,j) = P_2(i,j) \end{cases}$$

$$\text{UACI} = \frac{1}{255 \times M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |P_1(i,j) - P_2(i,j)| \times 100\%$$

where M and N are the image dimensions, and $P_1(i,j)$ and $P_2(i,j)$ represent the ciphertext pixel values before and after plaintext modification, respectively.

Table 3 shows that when encrypting plaintext with slightly altered pixels, the resulting ciphertext differs significantly, with NPCR and UACI values very close to their theoretical expectations. This indicates that the algorithm possesses excellent resistance to plaintext and differential attacks.

---

5 Conclusion

This paper proposes a digital image encryption and monitoring scheme based on plaintext-related chaotic mapping and SHA-256. First, the hash value generated from the grayscale version of the image to be encrypted using the SHA-256 algorithm serves as a digest to monitor whether the ciphertext image has been tampered with during transmission. Second, the digital image is encrypted using two different diffusion methods combined with a plaintext-related scrambling algorithm, with the Lorenz chaotic map generating corresponding cipher sequences. Experimental results demonstrate that the algorithm not only provides a large key space but also effectively resists brute-force attacks, plaintext attacks, statistical attacks, and differential attacks, thereby better ensuring the secure transmission of digital images.

References

[1] Han Dong, Wang Chunhua, Xiao Min. Color image encryption method based on chaotic map and quadratic residue cryptosystems [J]. Application Research of Computers, 2018, 35(9): 2757-2761.

[2] Li Chunhu, Luo Guangchun, Li Chunbao. Image encryption scheme based on skew tent chaotic map and Arnold transformation [J/OL]. Application Research of Computers, 2018, 35(11). (2017-11-10) [2017-11-10]. http://www.arocmag.com/article/02-2018-11-028.html.

[3] Jiang Junli, Zhang Xuefeng. Color image encryption method based on chaotic system [J]. Application Research of Computers, 2014, 31(10): 3131-3136.

[4] Sun Li, Huang Zhengqian, Liang Li. Image encryption algorithm based on composite chaotic maps and continuous diffusion [J]. Computer Engineering and Design, 2017, 38(12): 3374-3379.

[5] Yan Bing, Bai Sen, Liu Bowen, et al. Algorithm of image encryption in wavelet domain based on cross chaotic map [J]. Application Research of Computers, 2018, 35(6): 1797-1799, 1811.

[6] Zhang Xuncai, Liu Yishan, Cui Guangzhao. Image encryption algorithm based on DNA encoding and hyper-chaotic system [J/OL]. Application Research of Computers, 2019, 36(4). (2018-02-07) [2018-02-07]. http://www.arocmag.com/article/02-2019-04-034.html.

[7] Chai Xiuli, Gan Zhihua. A novel bit level adaptive color image encryption algorithm based on hyper chaotic system [J]. Computer Science, 2016, 43(4): 133-139.

[8] Zhao Jiaxing, Zhang Xuefeng. Spatiotemporal color image encryption method based on combined chaotic system [J]. Computer Engineering and Design, 2016, 37(9): 2354-2360.

[9] Zhang Yong. Chaotic digital image cryptosystem [M]. Beijing: Tsinghua University Press, 2016: 105.

[10] He Runmin, Ma Jun. Analysis safety of SHA-256 algorithm [J]. Electronic Design Engineering, 2014, 22(3): 31-33.

[11] Wang Hongda. A novel image encryption algorithm based on chaotic system [J]. Optical Technique, 2017, 43(3): 260-266.

[12] Zhu Hegui, Zhao Cheng, Zhang Xiangde. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem [J]. Signal Processing: Image Communication, 2013, 28(6): 670-680.

[13] Zhu Shuqin, Li Junqing, Ge Guangying. Fast image encryption algorithm based on novel five dimensional discrete chaos [J]. Computer Science, 2016, s2(43): 411-416.

[14] Zhang Miao, Tong Xiaojun. A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system [J]. Multimedia Tools and Applications, 2014, 71: 1-25.

Note: Figure translations are in progress. See original paper for figures.