Journal of Information Security and Applications 40 (2018) 111–133

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Secure multi–level permutation operation based multiple colour image encryption

K Abhimanyu Kumar Patro*, Bibhudendra Acharya

Department of Electronics and Telecommunication Engineering, National Institute of Technology Raipur, Raipur, Chhattisgarh–492010, India

ARTICLE INFO

Article history:

Keywords:
Multiple colour image encryption
Multi-level permutation
PWLCM system
Key space
Randomness

ABSTRACT

In recent days, there is a high demand of encryption of multiple digital images for secure transmission of multiple images. This paper proposes a multi-level permutation operation based secure multiple colour image encryption technique which is totally different than the currently used multiple image encryption techniques. The proposed encryption technique uses three levels of permutation operation: the first level of permutation operation performs pixel-shuffling operations in R, G, and B components, itself; the second level of permutation operation performs row-shuffling operations in between the pixel-shuffled R, G, and B components; the third level of permutation operation performs column-shuffling operations in between the row-shuffled components. At last, the proposed encryption algorithm performs block-diffusion operations to get the final encrypted images. Multi-level permutation operations and diffusion operation only use PWLCM systems multiple times to make the algorithm more secure and stronger. Multiple PWLCM systems in multi-level permutation operations not only produces larger key space and higher key sensitivity but also generates greater randomness of pixels and weaker correlation of adjacent pixels in images as compared to the currently used multiple image encryption techniques. In addition the secret keys which are used in this proposed algorithm not only depends on the original key values but also depends on the original colour images. This protects the algorithm against known-plaintext attack and chosen-plaintext attack. The simulation results and the security analysis indicate that the proposed algorithm has good encryption results, large secret-key space, higher sensitivity towards secret keys and the plaintext, weaker correlation of adjacent pixels, greater randomness of pixels, and enough resistance against various common attacks.

1. Introduction

Nowadays, internet is the medium through which large number of digital images is transmitted. However, the securities in transmission of large number of digital images become an issue. In last several years, many single image encryption techniques [1-18] based on transform domain [1, 3, 4, 8], vector quantization [2], DNA computing [14, 17], chaotic systems [5-7, 10-12, 15, 16, 18], hyper-chaotic systems [9, 13], etc. are proposed by different cryptographers for securing digital images. Single image encryption techniques are suitable for the encryption of single images; however, for the case of encryption of multiple images, the use of single image encryption techniques are not so efficient and hence they lack the desired encryption efficiency [19].

So, to overcome the problem of encryption of multiple digital images all together, there is an increasing attention of using multiple image encryption techniques. During the past few years, researchers have proposed different multiple image encryption techniques in transform domain and also in the domain of chaos. Kong *et al.* [20] proposed a cascaded fractional Fourier transform based multiple image encryption technique, Wei *et al.* [21] proposed a wavelet transform based multiple image encryption technique, Yanbin *et al.* [22] proposed a cascaded fractional Fourier transform based asymmetric multiple image encryption technique. In the above transform domain based multiple image encryption techniques [20-22], there is a need of converting spatial domain into transform domain and then converting transform domain into spatial domain in the final stage of output. These extra steps of domain conversion decrease the encryption efficiency [19]. Tang *et al.* [23] proposed a bit-plane operation and chaotic map based multiple gray scale image encryption technique. Here also, the complex computation of bit-plane operation reduced the encryption efficiency [19]. Hence, to improve the encryption efficiency, Zhang *et al.* [24] proposed a mixed image element and chaos based multiple gray scale image encryption technique. This technique no doubt increases the encryption efficiency, but the securities may be lit-

* Corresponding author.
E-mail addresses: abhimanyu.patro@gmail.com (K.A.K. Patro), bacharya.etc@nitrr.ac.in (B. Acharya).

https://doi.org/10.1016/j.jisa.2018.03.006
2214-2126/

tle weaker than the securities in [23]. This is because in [23], the order of the blocks and the contents in the blocks both are processed, while in [24], only the order of the blocks are processed; this lacks the desired amount of security in theory. Moreover, by observing the histograms of encrypted images in [24], we found that the gray scale values are not uniformly distributed; this may not resist the statistical attack efficiently in theory. Apart from that the algorithm in [24] does not produce a satisfactory result of key-space ($10^{56} = 1.0196 \times 2^{186}$) and the secret keys used in this algorithm are not related to the plain image, hence may not resist the known-plaintext attack and chosen-plaintext attack efficiently. To overcome these problems, the same author in [19] has proposed a mixed image element and permutation based new multiple image encryption technique. This technique solves all the lacunae demanded in [24] except the key space, which is $10^{60} = 1.2446 \times 2^{199}$ in [19]. Apart from that the algorithms in [19, 20-24] used only gray scale images and did not use any colour image which is in demand nowadays.

So, by aiming all the above problems in [19, 20-24], in this paper, a multi-level permutation operation based multiple colour image encryption by using multiple PWLCM systems is proposed. The main contributions in this proposed algorithm are as follows:

- PWLCM systems are utilized to get better encryption efficiency as compared to deficiencies present in high-dimensional chaotic and hyper-chaotic systems.
- To make the algorithm hardware efficient, only PWLCM systems are utilized to permute and diffuse the pixels in colour images.
- Multiple PWLCM systems are utilized to increase the key space as required and also to increase the information entropy.
- Multi-level permutation operations are performed to generate weaker correlation in adjacent pixels of encrypted images.
- SHA-256 hash algorithm is utilized to generate the secret keys of the proposed cryptosystem.

The securities which exist in this proposed algorithm are as follows:

- Multiple PWLCM systems not only increase the key space and key sensitivity but also increase randomness of pixels in images. The higher key space improves the amount of resistance against brute-force attack and the higher randomness reduces the amount of leakage of information.
- The multi-level permutation operation reduces the correlation in between the adjacent pixels of encrypted images.
- The relation of secret keys with the original images increases the resistivity against known-plaintext attack and chosen-plaintext attack.
- Since, all the initial values and system parameter are in relation with all the colour images, each colour image is equally important. This will strongly resist known-plaintext attack and chosen-plaintext attack.
- Since, bit-lane operation (as in [23]) is not performed in this algorithm; it results in increased encryption efficiency.
- The proposed algorithm resists all kinds of statistical attacks, differential attacks, occlusion attack, etc.

The simulation results and security analysis show that the proposed algorithm is secure and stronger as compared to other existing multiple image encryption techniques [19, 23, 24].

The rest of the paper is organized in the following way. Section 2 comprises the background knowledge of the proposed encryption algorithm. The proposed key generation algorithm, image encryption and decryption algorithms are described in Section 3. Section 4 presents the simulation results and the security analysis of the proposed cryptosystem. Finally, Section 5 concludes the paper.

2. Background study

2.1. Secure Hash Algorithm SHA – 256

SHA-256 is one of the family members of SHA-2 whose aim is to provide privacy, authenticity, and integrity in data transmission. Quoting from [25],

> "*Secure one-way hash functions are recurring tools in cryptosystems just like the symmetric block ciphers. They are highly flexible primitives that can be used to obtain privacy, integrity and authenticity*."

SHA-256 is an iterative and one-way hash function which to produce 256-bits of fixed length message digest for any given size of input data. There are two stages of processing performed on the input data such as pre-processing and digest computing. In pre-processing stage, an initial hash value is generated and in digest computing stage, a series of hash values are generated to produce a message digest [17]. One of the important properties of SHA-256 hash function is its high sensitivity towards input data that means small changes in input data will lead to large change in output hash values. Hence, due to this sensitive property, SHA-256 hash values of original image are used in this proposed cryptosystem to generate the secret keys. This protects the proposed algorithm against known-plaintext attack and chosen-plaintext attack efficiently.

2.2. PWLCM system

Due to good dynamical behaviour, excellent ergodicity, efficient implementation, simpler representation, and uniform invariant distribution [19, 26], the PWLCM system is repeatedly popular in chaos for generating a pseudo-random chaotic sequence. It is defined by the equation [19]:

$$x_{i+1} = F_a(x_i) = \begin{cases} x_i/a & 0 \le x_i < a \\ (x_i - a)/(0.5 - a) & a \le x_i < 0.5 \\ F_a(1 - x_i) & 0.5 \le x_i < 1 \end{cases} \quad (1)$$

where $a \in (0,\ 0.5)$ is the control parameter and $x_i \in (0,\ 1)$ is the initial value. By observing the bifurcation diagram in [26], we realize that, in Logistic map, when the system parameter r approaches to 4, the Logistic map is ergodic in the range of $(0,\ 1)$ while in PWLCM system, a wider range of parameter choices is presented for ergodicity in the range of $(0,\ 1)$.

3. Proposed methodology

3.1. Generation of secret keys

The step-by-step descriptions of generating the secret keys are as follows:

Step-1: Take k numbers of original colour images of same size $M \times N \times 3$ and then separate the R, G, and B components of each of the original colour images.

Step-2: Horizontally concatenate the R components of each of the k original colour images. Similarly, horizontally concatenate the G and B components of each of the k original colour images.

Step-3: Now, combine the horizontally concatenated R, G, and B components.

Step-4: Apply SHA-256 hash algorithm on this combined image to generate 256-bits of hash value. Now, express the 256-bits of hash value into 64-hex values (4-bits of each). The expression of 64-hex values is as follows: