Optics and Laser Technology 106 (2018) 506–516

Contents lists available at ScienceDirect

Optics and Laser Technology

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

Full length article

Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets

Han-wen Xue, Juan Du [*], Shou-liang Li, Wei-jiao Ma

School of Information Science and Engineering, Lanzhou University, Lanzhou 730000, China

ARTICLE INFO

Article history:
Received 6 October 2017
Received in revised form 18 April 2018
Accepted 25 April 2018

Keywords:
Hyperchaos
Three positive Lyapunov exponents
Wide parameter range
Color image encryption
ROI

ABSTRACT

We propose a hyperchaotic encryption algorithm for the region of interest (ROI) in a color image. The ROI for the human face is first identified based on the Open Source Computer Vision library by using a Gaussian mixture model. It is then encrypted using a novel hyperchaotic system, which has three positive Lyapunov exponents. The system can be in a hyperchaotic state with the parameter changing over a wide region, which is proved by Lyapunov exponent spectrum calculations. Furthermore, hierarchical keys are adopted to ensure the security of the encrypted sequences generated. In the encryption process, crossed image row–column scrambling and pixel value diffusion are experienced. The hyperchaotic sequences required for the encryption relate not only to the keys but also to the plaintext images. Consequently, the algorithm is effective against plaintext and ciphertext attacks. The security performance is also verified in detail with respect to histograms, correlations, information entropy, key space, key sensitivity analysis, number of pixel change rate, unified average changing intensity, and known and chosen attacks. The results indicate that the proposed algorithm has a large key space and a low correlation between adjacent pixels, hence, it can also be usefully employed to resist brute-force and statistical attacks.

1. Introduction

With the rapid development of information and network technology, vast amounts of information are transmitted over networks, especially in the form of images; therefore, information security has received widespread attention [1–3]. Because of multidimensional data and large correlations between adjacent pixels, traditional Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest, Shamir, and Adelman (RSA) technologies are no longer applicable to image encryption. Since Matthews [4] first introduced chaos into cryptography in 1989, it has been widely applied in image encryption for its high sensitivity to initial values and strong pseudo-randomness [5,6]. Various schemes have been employed based on one-time keys [7], bit-level scrambling [8], the DNA complementary rule [9], high-dimension chaotic maps [10], etc. In [8], images were decomposed into an eight-binary-bit plane, and then they were scrambled separately. At the same time, the value and the position of pixels were changed. However, this comes at the expense of a large number of data operations and low encryption efficiency. Use of the DNA complementary rule entails encoding and decoding images by using the double helix structure of DNA molecules and complementary base binding. Although the performance is excellent, the principle is complex, the equipment requirements are high, and the key space is small, making it difficult to apply the technique widely at present.

Chaotic-based scrambling and diffusing of the pixel level have been the basic framework of related algorithms [11–16], such as two layer structure [11], pixel-level and bit-level permutation [12], and variable chaotic control parameters [13]. In fact, in such systems, the keystream generators have short cycle length, owing to the limited computer accuracy. To prolong the periodic length of a chaotic system, a dual chaotic system has been used to produce a pseudo-random sequence [14]. However, in some of those algorithms, the cipher always keeps the selected parameter values and initial values unchanged for any encrypted plaintext, so the algorithms are not robust enough to resist chosen-plaintext attacks. If an image encryption algorithm relates to a plaintext image, the size of the key space can be greatly increased, and different plaintext images have different keys, that is, one-time keys. Therefore, the algorithm can effectively resist attacks. Unlike the keystreams used in other schemes that are solely determined by the keys, a plaintext-related strategy has been proposed in [15]. Along this line, in [16], the pixel values of a plaintext image were taken as initial values of a chaotic system, then the chaotic sequences used in encryption are produced by those values and equations.

[*] Corresponding author.
E-mail addresses: Hanwen_Xue@163.com (H.-w. Xue), duj@lzu.edu.cn (J. Du), lishoul@lzu.edu.cn (S.-l. Li), mawj2015@lzu.edu.cn (W.-j. Ma).

https://doi.org/10.1016/j.optlastec.2018.04.030
0030-3992/© 2018 Elsevier Ltd. All rights reserved.

Sometimes multimedia data contain a lot of redundant information. To improve the encryption efficiency, we can encrypt the key information extracted to avoid wasting computing memory and bandwidth resources. Hamza and Muhammad [17–19] proposed an image color coding method aimed at increasing the encryption efficiency and security of keyframes extracted from video summarizations. The above encryption schemes apply to the entire image, while encryption in a particular area is often more practical than encrypting the whole image. Because different regions have different importance, only the important region in which the users are really interested, namely, the region of interest (ROI), needs to be encrypted and protected [20,21]. A chaotic image encryption algorithm for the ROI was proposed by Xiao [20]; this algorithm can encrypt an irregular region; however, it cannot automatically recognize the ROI.

Owing to its uniqueness, stability, and convenience, biometric recognition technology has been more and more widely used. Because biological characteristics are not easily lost and only depend on the characteristics of the human body, biometric recognition technology provides a reliable individual identification process [22], so it has been broadly applied in many fields, such as personal identification and identification of criminal suspects. As is well known, the human face, fingerprint, palm print, retina, iris, and voice pattern can all be used as biological characteristics. The human face is more informative than the other characteristics, and its extraction is not significantly hampered by noise, so recognition accuracy is high and recognition speed is fast. Consequently, the study of the face region as the ROI has become an important research topic.

Although both accuracy and speed of face recognition are very important, the storage security of face images cannot be ignored. At present, numerous such images collected by the public security and corporate sectors are stored in databases directly, without security protection measures. Therefore, unexpected security risks to protecting the privacy of such images exist. Because these images contain important privacy information, once hackers and other criminals get them, the consequences can be dire. Faced with this threat, we need to study privacy-preserving techniques for user face images [23,24]. At present, some face encryption schemes based on chaotic systems are in use. Ntalianis [25] has proposed a human video objects encryption system, in which autodetection is used to extract the face and body, then a chaotic system encrypts the arranged pixels of the above objects. This scheme has attached an importance to the security of the information for the ROI, but the operations of the *XOR* function and time-variant S-box still need to be improved and perfected. After that, a hybrid encryption algorithm was proposed by Liu [26]. In this algorithm, chaotic encryption is combined with RSA encryption to meet the security needs and the matching rate of the protection of the facial feature template. Cheng [27] presented a template protection algorithm for face recognition, in which chaotic cryptographic technology was adopted. Although those algorithms can realize encryption and protection of the face image, during the permutation process some information regarding the original template is lost, and important security performance metrics, such as analyses of adjacent pixel correlation, information entropy, and key sensitivity, are still to be investigated.

In this paper, based on facial feature extraction methods and chaos theory, a hyperchaotic encryption algorithm is introduced into a face detection system. A hyperchaotic system with three positive Lyapunov exponents is investigated that can present hyperchaotic characteristics over a very wide parameter range. Hierarchical keys are also introduced to ensure the security of the encrypted sequences generated. The chaotic sequences produced by it have excellent performance and are suitable for image encryption. For a color face image, only the face feature vector extracted from the image is encrypted. Unlike in other encryption methods, the proposed chaotic sequences for encryption are related to the keys as well as to the plaintext images, which can realize one-time keys. Therefore, the method not only improves the security of the encryption but also effectively offers resistance to plaintext and ciphertext attacks. The experimental results demonstrate that the algorithm has good performance and offers high security.

The rest of this paper is organized as follows: In Section 2, a novel hyperchaotic system is introduced. The proposed encryption algorithm is then discussed in Section 3. In Section 4, the experimental results are presented, and the security of the algorithm is evaluated as well. Conclusions are finally drawn in Section 5.

2. A novel hyperchaotic system

At present, hyperchaotic systems with more than two positive Lyapunov exponents are rarely reported [28]. Compared with a system that can only be chaotic over a narrow range, our novel five-dimensional chaotic system constructed with three positive Lyapunov exponents can be in a hyperchaotic state with parameter changes over a wide region.

The mathematical expression is described as

$$\begin{cases} \dot{x} = a(x+y) + z - w, \\ \dot{y} = b(a(x+y) + z - 0.5\,\mathrm{sign}(y-0.5)), \\ \dot{z} = -c(x+y), \\ \dot{w} = d(x + \sin(u) - 0.5\sinh(w+1)), \\ \dot{u} = kw. \end{cases} \tag{1}$$

Among these terms, a, b, c, d, and k are the real parameters of the system and x, y, z, w, and u are the state variables. Fig. 1 presents the Lyapunov exponent spectrum changes with the parameter k varying over a wide range, when $a = 0.03, b = 10, c = 0.1$, and $d = 0.8$.

It is interesting to see that the hyperchaotic system always has two or more positive Lyapunov exponents with k varying. In particular, when $k \in [-14.5, 13.4]$, the system even has three positive Lyapunov exponents, and thus, over a wide parameter range, the system stays in a hyperchaotic state, which means it has complex dynamic characteristics and a large key space for secure communication. When $k = 8.5$, the Lyapunov exponents of System (1) are

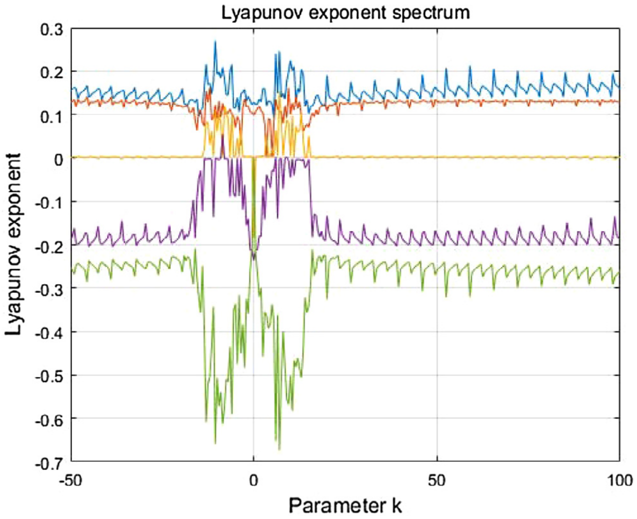

Fig. 1. Lyapunov exponent spectrum of System (1).