Information Sciences 349–350 (2016) 137–153

Contents lists available at ScienceDirect

Information Sciences

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

A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system

Xiangjun Wu[a,b,c,*], Dawei Wang[a], Jürgen Kurths[b,c], Haibin Kan[d,**]

[a] College of Software, Henan University, Kaifeng 475004, China
[b] Potsdam Institute for Climate Impact Research (PIK), 14473 Potsdam, Germany
[c] Department of Physics, Humboldt University, 12489 Berlin, Germany
[d] Shanghai Key Lab of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China

ARTICLE INFO

Article history:
Received 21 December 2014
Revised 17 February 2016
Accepted 21 February 2016
Available online 27 February 2016

Keywords:
Color image encryption
Lossless encryption
Six-dimensional (6D) hyperchaotic system
Discrete wavelet transform (DWT)
Haar wavelet
Frequency domain

ABSTRACT

This paper proposes a new lossless encryption algorithm for color images based on a six-dimensional (6D) hyperchaotic system and the two-dimensional (2D) discrete wavelet transform (DWT). Different from the current image encryption methods, our image encryption scheme is constructed using the 2D DWT and 6D hyperchaotic system in both the frequency domain and the spatial domain, where the key streams depend on not only the hyperchaotic system but the plain-image. In the presented algorithm, the plain-image is firstly divided into four image sub-bands by means of the 2D DWT. Secondly, the sub-bands are permutated by a key stream, and then the size of them is decreased by a constant factor. Thirdly, the 2D inverse DWT is employed to reconstruct an intermediate image by the four encrypted image sub-bands. Finally, to further enhance the security, the pixel values of the intermediate image are modified by using another key stream. Experimental results and security analysis demonstrate that the proposed algorithm has a high security, fast speed and can resist various attacks.

1. Introduction

With the rapid development of modern communication techniques, a great amount of digital images are transmitted over the networks. How to protect the image information against illegal usage, unauthorized access, disruption or destruction has attracted increasing attention. The traditional cryptographic algorithms such as DES, AES, IDEA, RSA etc., are not suitable for practical image encryption due to some inherent features of images such as bulk data capacity, strong correlation among pixels and high redundancy. In recent years, chaos has been shown to be a powerful tool in image encryption [4,12]. Comparing with the conventional cryptosystems, chaos-based image encryption algorithms have some attractive advantages such as high security, fast speed, reasonable computational overheads and computational power.

In the past decades, many chaotic image encryption schemes were proposed. For example, in [48,58], the Logistic map is employed to construct the image encryption algorithms, while the image cryptosystems in [11-13,25,27,32,33,42,63,72] are designed using the 2D chaotic maps or systems. The aforementioned encryption schemes based on the one-dimensional (1D) chaotic maps or the low-dimensional chaotic systems have some fundamental drawbacks such as

* Corresponding author at: College of Software, Henan University, Kaifeng 475004, China. Tel.: +863783883010.
** Corresponding author.
E-mail addresses: wuhsiang@yeah.net (X. Wu), hbkan@fudan.edu.cn (H. Kan).

http://dx.doi.org/10.1016/j.ins.2016.02.041
0020-0255/

insufficient key space, poor efficiency and weak security. To solve these defects, the high-dimensional chaotic systems and spatiotemporal chaos have been frequently used to devise the image encryption algorithms in recent years [14,17-19,21,24,26,31,35,41,45,50,53,57,59,64,66,67,69-71,73]. In [21,41,57], the 2D chaotic maps have been extended to corresponding three-dimensional (3D) maps for developing fast symmetric encryption schemes. Gao and Chen [14] introduced a novel image encryption scheme using a hyperchaotic system. But this encryption approach is very weak against the chosen-plaintext and chosen-ciphertext attacks [50]. Huang and Nien [26] presented a color image cryptosystem using four 3D chaotic systems. Solak et al. [53] pointed out that this method cannot resist the known-plaintext and chosen-plaintext attacks. Zhu [73] proposed an image encryption scheme, where the hyperchaotic sequences are modified to generate the chaotic key stream, and then both the chaotic key stream and the plaintext are used to generate the final encryption key stream. Unfortunately, this scheme is not secure enough and the secret parameters of the cryptosystem can be obtained by the chosen-plaintext attack [45]. Zhang et al. [66] put forward a new image fusion encryption algorithm based on DNA sequence operation and a hyperchaotic system. However, two chaotic key streams in this encryption method can be revealed by choosing $4mn/3+1$ plain-images [70]. In [18,35,59,69,71], spatiotemporal chaos was applied to design the image encryption algorithms to strengthen the security of the cryptosystems. Note that all the above mentioned image algorithms are constructed in the spatial domain, where one directly manipulates the image pixels. Such image encryption methods are prone to destruct the correlation amongst pixels, which makes the cipher-images incompressible [56]. In addition, the encryption schemes that scramble the images in the spatial domain are not secure because the features of the permutated images can be used to recover the plain-images [36]. In contrast to the spatial domain methods, the frequency domain (transform domain) image encryption techniques have a higher efficiency, are more robust against many image processing operations, and can recover the original images without losing any information [36,56]. The lossless encryption schemes are more applicable in some special applications such as satellite images, military images, medical images, biological images etc., where a decrypted image is required to be identical to the original plain-image completely. Therefore, it becomes important from the viewpoints of theory and practice to investigate frequency based image encryption.

Recently, many researchers have attempted to design the image encryption methods in the frequency domain, where the plain-images are encrypted by modifying the image frequencies, and the image pixels can be reconstructed without loss of information through a reverse process [29,30,37,38,49,54-56]. For instance, Liu et al. [37] presented a triple image encryption scheme using the fractional Fourier transform (FrFT), where the plain-image is encoded in the amplitude part and other two images are encoded into the phase information. In [38], a color image encryption algorithm was developed by using the Arnold transform and color-blend operation in discrete cosine transform (DCT) domain. Tedmori and Al-Najdawi [55] designed a lossless image encryption scheme in the transform domain. In this method, DCT is employed to convert the target image into the frequency domain, and then the encryption involves scattering the distinguishable lowest frequency value using a reversible weighting factor amongst the rest of the frequencies. Sui et al. [54] proposed a single-channel color image encryption method using a phase retrieve algorithm, which is based on the iterative FrFT and a two-coupled logistic map. However, these image encryption approaches using DCT or Fourier transform have the deficiency that it is impossible to completely decorrelate the blocks at their boundaries, which usually results in undesirable blocking artifacts, and influences the recovered images. In addition, DCT is inflexible. For example, it cannot be adapted to source data, does not implement efficiently for binary images with large periods of constant amplitude (low spatial frequencies), and is followed by brief periods of sharp transitions [55,56].

The DWT has at least four advantages compared with DCT and Fourier transform [9,40,43,44,56]: (1) DWT provides higher compression ratios and avoids blocking artifacts because it needs not to decompose the input coding into non-overlapping 2D blocks; (2) DWT introduces inherent scaling and better identification of which data is relevant to human perception; (3) DWT allows good localization both in spatial and frequency domain; (4) DWT has higher flexibility than DCT. Hence, the DWT is naturally considered to construct the frequency-based image encryption methods [3,46,47,56,68]. However, the encryption algorithm in [56] has a very small key space and requires high computation cost due to using the two-level DWT. The encryption methods in [3,46,47] are very weak against the differential attacks. In addition, the DWT-based encryption algorithms in [3,46,47,56,68] mainly focus on gray-scale images, and cannot be simply applied to color images. It is known that using the high-dimensional chaotic systems to design encryption algorithms can enhance the security of the cryptosystems [14,39,66,73]. To the best of our knowledge, there are few reports on the secure and fast encryption methods based on DWT for color images, which motivates us to devise the lossless color image encryption scheme with high security and fast speed based on the DWT and high-dimensional chaotic systems.

Motivated by the above discussions, this paper proposes a new lossless encryption scheme for color images by using the 2D DWT and a 6D hyperchaotic system. First, the original color image is converted into the frequency domain by the 2D DWT and four image sub-bands are obtained. Then the sub-bands are shuffled by a key stream and the size of them is reduced by a constant factor. Next, the 2D inverse DWT is performed to get the intermediate image. To further enhance the security, another key stream is utilized to change the value of each pixel of the intermediate image followed by obtaining the final cipher-image. In our method, a 6D hyperchaotic system and the plain-image are together utilized to generate two different key streams. Corresponding simulation results and performance analysis verify the feasibility and superiority of the proposed encryption scheme. The main contributions of this paper can be highlighted as follows: (1) the 1-level 2D DWT and a 6D hyperchaotic system are employed to design the color image encryption algorithm. This algorithm makes full use of the advantages of image encryption in both spatial domain and transform domain, and has a high security and