Egyptian Informatics Journal (2016) 17, 139–146

Cairo University

Egyptian Informatics Journal

www.elsevier.com/locate/eij
www.sciencedirect.com

FULL-LENGTH ARTICLE

Image encryption based on Independent Component Analysis and Arnold's Cat Map

Nidaa AbdulMohsin Abbas

University of Babylon, College of IT, Iraq

Received 27 May 2015; revised 3 October 2015; accepted 16 October 2015
Available online 23 November 2015

KEYWORDS

Arnold's Cat Map;
Image encryption;
Independent Component Analysis;
JADE

Abstract Security of the multimedia data including image and video is one of the basic requirements for the telecommunications and computer networks. In this paper, a new efficient image encryption technique is presented. It is based on modifying the mixing matrix in Independent Component Analysis (ICA) using the chaotic Arnold's Cat Map (ACM) for encryption. First, the mixing matrix is generated from the ACM by insert square image of any dimension. Second, the mixing process is implemented using the mixing matrix and the image sources the result is the encryption images that depend on the number of sources. Third, images decrypted using ICA algorithms. We use the Joint Approximate Diagonalization of Eigen-matrices (JADE) algorithm as a case study. The results of several experiments, PSNR, SDR and SSIM index tests compared with standard mixing matrix showed that the proposed image encryption system provided effective and safe way for image encryption.

1. Introduction

Over the years, there has been an important development in the field of information security. Yun-Peng et al. [1] presented the encryption scheme that realizes the digital image encryption through the chaos and improving DES. First, encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, makes double time encryptions with improvement DES, and displays the respective merit. Lin et al. [2] proposed a way to encrypt the image using a linear mixed model of blind source separation (BSS). The encrypted simultaneously multiple images with the same size by mixing it with the same number of key images are statistically independent, the size of which is equal to that of images to be encrypted. Since these multiple images cover mutually through mixing among them while the key images cover them, there are no restrictions on the main space. The proposed method has a high level of security, and the computer simulation results showed its validity.

Ravishankar and Venkateshmurthy [3] proposed several schemes for image encryption. These schemes are produced

E-mail address: drnidaa_muhsin@ieee.org

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.eij.2015.10.001

in the form of random so that the content not appears. Encryption and decryption consume large amount of time. Therefore, there is a need for effective algorithm. They proposed a region based selective image encryption technique which provides facilities of selective encryption and selective images of reconstruction. Gao et al. [4] proposed a nonlinear chaotic algorithm (NCA), which uses the power function and the tangent function instead of the linear function.

Yu et al. [5] suggested that the efficiency of image encryption algorithm depends on the reconstruction of the image using some neighboring pixel characteristics. In accordance with the characteristics of different images of various bilateral level slightly, encryption system proposed reconstructs of the bit-level. Since the permutation of sub-images composing high 4-bits of the original image has a relatively high computational complexity, in this scheme the permutation of sub-images is performed with low 4-bits instead, which therefore has a lower computational complexity.

Kamali et al. [6] proposed encryption system that modifies the AES algorithm on the basis of each Shift Row Transformations. If the value in the first row and first column is even, the first and fourth rows are unchanged, and each byte in second and third rows is shifted periodically over different numbers. Last rows' first and third values are unchanged and are periodically turned to leave each byte in the rows. The second and fourth quarters of the state to a different number of bytes. Experimental result showed that MAES gave better results in terms of encryption for security against attacks and increased the statistical performance. Paul et al. [7] proposed encoder to convert bitmaps tricks encryption. Replacement and dissemination processes, based on the matrix, to facilitate fast convert plain text into cipher text, and images encryption. The results of the simulation compared with the results obtained from the Advanced Encryption Standard (AES), showed that the proposed image encryption algorithm was eight times faster than AES. Gautam et al. [8] discussed the use of a block based transformation algorithm, in which image is divided into number of blocks. These blocks are transformed before going through an encryption process. At the receiver side these blocks were retransformed into their original position and decryption process is performed. The advantage of such approach is used mainly on reproducing the original image without loss of information for the encryption and decryption process (based on a blowfish algorithm). Fei and Xiao-cong [9] presented an image encryption algorithm based on two-dimensional (2D) map and complex logistics system Chua's system. It used two successive chaos generated by the MAP logistics 2D (to change the features of color image). Then it used the chaos resulting from the successive models to maximize the benefits of the Chua system on the production of new pixel values. Simulation results showed that the algorithm has good properties of confusion and diffusion, and the big key space.

Ye and Zhao [10] proposed chaos-based image encryption scheme using affine modular maps, which are extensions of linear congruential generators, acting on the unit interval. A permutation process utilized two affine modular maps to get two index order sequences for the shuffling of image pixel positions, while a diffusion process employed another two affine modular maps to produce two pseudo-random gray value sequences for a two-way diffusion of gray values. Liu and Tian [11] proposed algorithm to encrypt images using color map and spatial chaos at the bit level flipping (SBLP). First, the algorithm used the logistic chaos sequence to shuffle the positions of image pixels and then to convert them into a binary matrix component including red, green and blue at one time, rather than the order of the matrix as well as at the level prior to appointment of scrambling bit that has been created by SBLP. Second, the logistics rearranged the chaotic sequence for the position of the current image pixel else. Results of the experiment and security analysis algorithm achieved good results and the complexity of encryption is low, and in addition to that, the key space is large enough to resist against a common attack.

In this paper, a new efficient image encryption technique is presented. It is based on modifying the mixing matrix in Independent Component Analysis (ICA) using the chaotic Arnold's Cat Map (ACM) for encryption. First, the mixing matrix is generated from the ACM by inserting square image of any dimension. Second, the mixing process is implemented using the mixing matrix and the image sources. The result is the encrypted images that depend on the number of sources. Third, images are decrypted using ICA algorithms. The Joint Approximate Diagonalization of Eigen-matrices (JADE) algorithm was tested as a case study. The results of several experiments, PSNR, SDR and SSIM index tests compared with standard mixing matrix showed that the resulted encrypted images from the proposed system provided effective and safe way for image encryption.

2. Arnold's Cat Map (ACM)

According to Arnold's transformation, an image is hit with the transformation that apparently randomizes the original organization of its pixels. However, if iterated enough times, eventually the original image reappears. The number of considered iterations is known as the Arnold's period. The period depends on the image size; i.e., for different size images, Arnold's period will be different [12].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\text{mod } N) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\text{mod } N) \tag{1}$$

where N is the size of the image, p and q are positive integer and $det(A) = 1$. (x_n, y_n) is the position of samples in the $N \times N$ data such as image, so that

$$(x_n, y_n) \in \{0, 1, 2, \ldots, N-1\}$$

And (x_{n+1}, y_{n+1}) is the transformed position after cat map, Cat map has two typical factors, which bring chaotic movement: tension (multiply matrix in order to enlarge x, y) and fold (taking mod in order to bring x, y in unit matrix).

Eq. (1) is used to transform each and every pixel coordinates of the image. When all the coordinates are transformed, the image resulted is a scrambled image. At a certain step of iterations, if the resulted image reaches our anticipated target (i.e. up to secret key), we have achieved the requested scrambled image. The decryption of image relies on the transformation periods (i.e. the number of iterations to be followed = Arnold's period – secret key) [13].