Journal of Information Security and Applications 42 (2018) 57–70

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Novel method for image security system based on improved SCAN method and pixel rotation technique

Ali Shakir Mahmood [a,b,*], Mohd Shafry Mohd Rahim [b,c]

[a] Department of Computer Science, College of Education, Al-Mustansiriyah University, Baghdad, Iraq
[b] School of Computing, Faculty of Engineering, University Technology Malaysia, Johor Bahru, Malaysia
[c] UTM-IRDA Digital Media Centre, Institute of Human Centered Engineering (iHumEn), University Technology Malaysia, Johor Bahru, Malaysia

ARTICLE INFO

Article history:

Keywords:
Image encryption
Knight tour
SCAN method
Confusion
Diffusion
Pixel rotation

ABSTRACT

Image scrambling is the conversion of images to unreadable format for security reasons. Encrypting an image with an acceptable level of security requires a cryptography system that follows the rules of confusion and diffusion. This paper introduces the SCAN method for scrambling and pixel rotation for diffusion. This image encryption method uses a knight tour to generate a scrambling key that is equal to the image size. The main advantage of this generator is that only a small initial value is needed to generate a full image size key. To realize confusion, a plain image is applied with an improved discrete diagonal SCAN (D-SCAN) method to generate a scrambled image for confusion. Then, to achieve diffusion, pixel values are changed by rotating all image pixels according to the generated keys. Results of statistical and security tests indicate that the proposed systems of D-SCAN and pixel rotation scheme can achieve excellent scrambling effect, high security, strong robustness against several attack types, and high sensitivity.

1. Introduction

The huge development of computer networks has changed the way by which people communicate with one another. Today, people can easily transfer multimedia information through computer networks. However, network environments can be accessed by unauthorized people, indicating the need for strong security strategies that can secure information, particularly images that are frequently used on the Internet [29].

Image protection is performed by using traditional encryption methods, such as AES, DES, and RSA. However, these algorithms are unsuitable for images because images are of bulk data size and pixels are relative with each other. Therefore, other encryption schemes, such as chaotic methods, should be developed, because these methods have high sensitivity to initial values and have unforeseeable properties [1,21]. Furthermore, cryptosystems are based on two main steps: diffusion and confusion.

The diffusion step changes the pixel position and diffuses the pixels all over the image. However, this step is not sufficient for image encryption, given that the security is threatened by statistical analysis because the histogram of the plain image is the same as the histogram of the cipher image. In the confusion step, pixel values are changed to match the gray level of the pixels. Compared with diffusion, confusion allows for more security; however, from a visual perspective, the encryption effect is not good. Therefore, a strong image encryption system that combines diffusion and confusion should be designed to improve the security of images [12,13].

Researchers have proposed several image encryption algorithms, such as the SCAN method, in which the movement and encryption of image pixels are dependent on certain patterns. [10] used a combination of SCAN methods to scramble the pixel location, and they achieved good results; however, no security analysis was provided in their paper. Where [25] conducted the scrambling of image pixels by using a chaotic algorithm of image encryption based on SCAN pattern. Their algorithm achieved good scrambling effect, but it had a small encryption key space, Moreover, the encryption method was applicable for gray images only. Network bandwidth limitation should be considered when images are sent and received on the Internet. Therefore, several researchers have proposed a method that can compress and encrypt simultaneously. These combinations are illustrated in [31], wherein SCAN method is used to compress and encrypt images. The major drawbacks of this method include long encryption time and low compression rate, there is another work that overcome the time consuming and introduced an excellent image encryption methods

* Corresponding author at: Department of Computer Science, College of Education, Al-Mustansiriyah University, Baghdad, Iraq.
E-mail addresses: asmjhm2006@yahoo.com, asmjhm2006@uomustansiriyah.edu.iq (A.S. Mahmood), shafry@utm.my (M.S.M. Rahim).

https://doi.org/10.1016/j.jisa.2018.08.001
2214-2126/

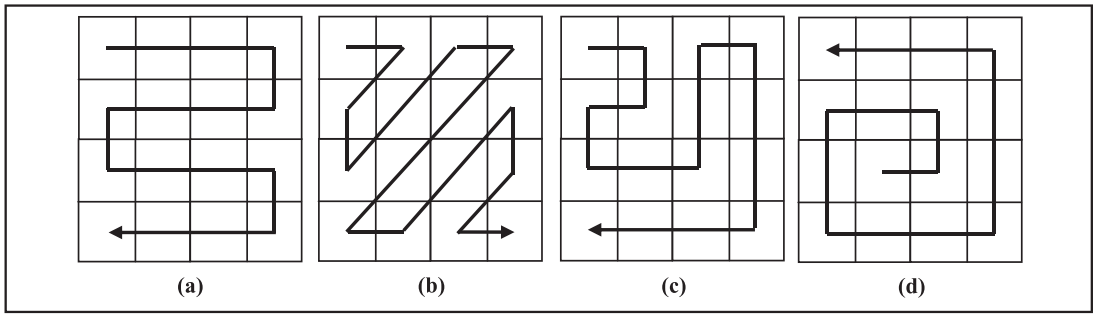

Fig. 1. SCAN patterns (a) C-SCAN (continuous raster), (b) D-SCAN (continuous diagonal), (c) O-SCAN (continuous orthogonal) and (d) S-SCAN (continuous spiral).

behinds the compression by using vector quantization technique [9]. A hybrid technique is proposed in [37] by combining the carrier image with the SCAN pattern. Hybridization achieves better results than the application of an individual encryption process. SCAN method uses few SCAN patterns and few carrier-keywords, which can be considered a drawback. SCAN patterns work as a chain wherein all image pixels move in same manner as the same number of pixels. One such patterns is zigzag scanning, in which, in most cases, the following pixel to be scanned is neighbouring to the present one with a various row and column. Subsequently, to some degree, this scanning mode can be suitable for more kinds of images [50].

The proposed system in this work is mainly based on the improvement of D-SCAN method for pixels scrambling; that is, converting it from a contiguous chain to discrete. Consequently, the movement becomes diagonal in two sides (up and down) on the basis of the generated key by using knight tour problem [30]. Each diagonal movement differs in the number of pixels and the direction. If the key is even, the pixels move diagonally upward; otherwise, the pixels move diagonally downward. In addition, pixel rotation scheme is proposed to improve image confusion. In this technique, each image pixel is rotated with a different value based on the generated key.

This paper is structured as follows. In Section 2, we introduce the general description of the SCAN method. The key generator is explained in Section 3. The design of the proposed image encryption scheme is discussed in Section 4. In Section 5, the performance and analysis of the proposed method, as well as comparisons with other works, are given. Section 6 presents the drawn conclusion.

2. SCAN method

Many image encryption algorithms have been proposed. Most of them are focused on both of confusion and diffusion property; while the rest of the encryption algorithms are apply one of property. One such algorithm is SCAN method, which is a category of formal languages that can be implemented for image compression, data encryption, and information hiding [8,39]. The SCAN family of formal languages includes distinctive versions, for example, simple SCAN, extended SCAN, and generalized SCAN; every type can describe and create a specific scanning paths [20,45].

A scanning of a 2D array is a request in which every element of the array is accessed precisely once. SCAN is a formal language based on two dimensional spatial for developing methodologies that can characterize and create countless combinations of scanning paths. SCAN language uses four fundamental scan patterns, as explained in Fig. 1, where the different scan types are illustrated.

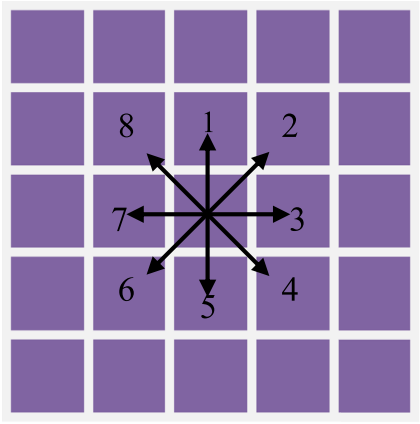

Fig. 2. Different movement possibilities for each SCAN patterns.

Each basic pattern can produce eight transformations patterns for image pixels, as illustrated in Fig. 2, [10,20,32]).

The scanning path of an image is a random code pattern in which essentially every pixel of the image is accessed exactly once. Therefore, encryption requires a method that can effectively generate a large number of scanning paths [14,34].

3. Key generator

The process of changing pixel positions in an image requires the use of a set of numbers that are random and unpredictable for subsequent occurrences. Moreover, these sequences cannot be reproduced unless the same generator functions with the exact initial values are used. This paper uses a knight tour as a tool for generating pseudo random numbers. The generated numbers can be used as keys for the scrambling process. Statistical properties and security analysis indicate that the knight tour application can successfully generate a pseudo random number with good statistical results, high linear complexity, and strong resistance against several attacks. For additional details, read paper [30]. The generated key size is equal to the input image dimensions, such that each pixel in the plain image corresponds to a unique number in the generated key.

3.1. Mathematical model of key generator and expander

The knight tour has been used as a random number generator to generate an encryption key. Where firstly the knight need to be initiated on $N \times N$ chess board with an initial position denoted by $x,\ y$), these two numbers $x,\ y\ \varepsilon\ Z^+$ and as known the chess board