JOURNAL OF INFORMATION SECURITY AND APPLICATIONS 30 (2016) 105–117

Available online at www.sciencedirect.com

ScienceDirect

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

A novel and efficient method based on knight moves for securing the information contents of images — A parallel approach

Jalesh Kumar *, *S. Nirmala*

Department of CSE, JNNCE, Shimoga, Karnataka, India

ARTICLE INFO

Article history:
Available online 31 August 2016

Keywords:
Knight piece
Parallel approach
Crossover operation
Encryption
Linear Feedback Shift Register
Digital image

ABSTRACT

Protection of multimedia information from unauthorized access demands a mechanism that provides security. In addition, securing the information contents in less time is a challenging issue. In this work, a novel and efficient parallel approach is proposed based on moves of knight pieces to secure the contents of an image in short span of time. The novelty of the approach lies in simulating the moves of knight pieces in parallel and generation of key sequence based on crossover operation. Further, in this approach, initialization of positions of knight pieces results in generation of key sequence. The proposed approach comprises three stages. In the first stage, a number of knight pieces which process in parallel are selected automatically. In second stage, random keys are generated based on the linear feedback shift register to select one of one point, two point and arithmetic crossover operation. Using crossover operation key sequence is generated. In third stage, exclusive OR operation is performed on the selected position of knight piece and generated key to produce the encrypted image. Experiments are carried out exhaustively on various types of images and performance of the proposed approach is measured in terms of parameters structural similarity index, feature similarity index, entropy and correlation coefficient. The proposed approach is compared with an existing parallel approach and the comparative analysis reveals that the proposed method outperforms in securing contents of images.

1. Introduction

Most of the multimedia information in modern technical world is communicated through internet. Applications like satellite image transmission, medical image sharing and document image preservation need protection of information from hackers. Even though many security techniques exist based on conventional methods, chaos and SCAN patterns, most of these approaches compromise between processing time and security provided, to fortify multimedia information. All multimedia information possesses special features such as high redundancy, high correlation among pixels and voluminous in size. To protect contents of images of large size the algorithm should impart computational security. Securing information contents and in less time the information should be shared without loss of information. There is always tolerance in between security and speed among cryptographic

* Corresponding author. Department of CSE, JNNCE, Shimoga, Karnataka, India.
E-mail address: jalesh_k@yahoo.com (J. Kumar).
http://dx.doi.org/10.1016/j.jisa.2016.08.004

techniques. Most of the existing efforts use serial approach and designed for single core architecture. The speed of computation could be increased by designing security techniques that adopt a parallel approach without compromising protection of information.

In recent past many cryptographic techniques were developed to secure information contents of an image (El-Wahed et al., 2008). Conventional encryption approaches were designed on the basis of permutation and substitution techniques. Advanced Encryption Standard and blowfish are discussed for image encryption. In Zeghid et al. (2007), Advanced Encryption Standard (AES) is described for securing the information contents of images. A key stream generator A5/1 and W7 are added to AES to ensure improved performance of encryption scheme. A block based transformation algorithm based on the combination of image transformation and blowfish algorithm is discussed in Younes and Jantan (2008). The original image is divided into uniform blocks which were rearranged into a transformed image using any transformation algorithm. Blowfish algorithm is used for encryption. Transformation process adds additional processing overhead in this technique. The conventional algorithms are designed for textual information rather than an image. Also the procedures are time consuming and complex to process large volume of data in an image. The chaotic maps are used in image encryption. The permutation of information takes place according to the sequences generated from the maps. The Arnold Cat Map rearranges the order of the pixel values so that each one is shuffled around, and the Chen's chaotic map changes the grayscale values of the pixels (Struss, 2009). In Peterson (1997), image encryption based on Arnold's Cat map is described. The properties of the map with different iterations are used on pixels of an image. The construction of the cipher and random behavior of two dimensional baker map is explained in Salleh et al. (2012). Chaos based encryption has disadvantages like computationally inefficient and low cycle length. But it provides the potential for developing different numbers of algorithms. The SCAN is a formal language based on two dimensional spatial accessing methodology which can represent and generate a large number of varieties of scanning paths. Different patterns are considered for encryption (Rad et al., 2013). Generating the different patterns along with exclusive OR operation is additional overhead in this process.

Most of the encryption methods adopt serial approaches and mainly focus on the security. Few existing methods adopt parallel approach to secure the information. Parallel diffusion approach for images is discussed in Zhou et al. (2014). Permutation and substitution models are used for encryption. Chaotic technique is designed based on cat map and logistic map. Chaotic key streams are generated in parallel to secure images. Applying two different maps together consumes time for encryption of information. Huang et al. (2014) propose an encryption scheme based on compressive sensing. Block cipher structure with chaotic lattice is designed to enhance the security in this method. Piecewise linear chaotic map based encryption algorithm is proposed in Wang and Chen (2013). Piecewise linear chaotic map is used to generate chaotic cryptosystem. Parallel encryption of the image was carried out. Computing speed of the algorithms is increased by parallel mode of operation. Complexity of such chaos based methods lies in initial conditions of chaotic map. Wang et al. (2006) discuss encryption of three primary colors of the image with parallel operation. Lorenz chaotic sequences are used to encrypt the information. Separating the color channels and processing that separately enhance the operation time. Encryption of image by parallel algorithm based on discrete chaotic map is proposed in Zhou et al. (2008). Original image is divided into sub images and advanced encryption standards algorithm is used to encrypt each sub image. But standard algorithms are time consuming and computationally more complex. Mirzaei et al. (2012) describes a parallel sub image encryption approach with hyper chaos. The original image is decomposed into four sub images. Each sub image is scrambled by logistic sequences and permutation process. The encryption process adopts more time for securing the information. In Mohamed (2014), image is split into different blocks and each block is encrypted using reversible cellular automata. One dimensional cellular automata are used for the key sequence and parallel operation. Further, decryption process is carried out independently for different blocks. Behavior of cellular automata sequences is utilized for encryption in parallel. Strength of the approach lies in type of cellular sequence and initial conditions. Das and Ray (2010) propose a method based on block technique for encryption process. In this method, 2^{256} possible keys are generated based on cellular rules. Different rules of cellular automata are used to generate the key sequence. Security of the information depends on type of rule selected. Many innovative techniques are found in the literature to generate the unpredictable key sequence based on games (Diaconu, 2015; Zhang et al., 2011). Movement of knight piece on chess board is considered for generating unpredictable key sequence in cryptography. Delei et al. (2008) proposed a slip encryption-filter template matrix based on moves of knight for encryption of image. The technique adopted for encryption is computationally expensive. To encrypt the image, pixels are transposed between red, green and blue channels based on rules of knight piece movements and chaos based pseudorandom bit generator (Diaconu et al., 2014). Limitation of method is computationally expensive. Crossover operation of genetic algorithm based on number of knight pieces and moves of each knight piece to encrypt the document images are described in Kumar and Nirmala (2014). The encryption method is based on serial approach and time of processing depends on amount of security provided.

From the literature survey, it is evident that most of the parallel approaches for image encryption are block based and computationally more expensive, even though serial approaches provide more security but fails in fast processing. In this work, a novel parallel approach is proposed to protect the information contents in an image. Novelty of the approach lies in design of random moves of multiple knight pieces in parallel. Moves of knight pieces in chess board with different cross over operations of the genetic algorithm are selected automatically. The rest of the paper is organized as follows. Moves of knight piece are explained in Section 2. Proposed approach is described in Section 3. Results and discussions are carried out in Section 4. Analyses are presented in Section 5. In Section 6, histogram analysis is discussed. The key space and key sensitivity are analyzed in Section 7. Different types