Applied Soft Computing 12 (2012) 2879–2895

Contents lists available at SciVerse ScienceDirect

Applied Soft Computing

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

Stream cipher for binary image encryption using Ant Colony Optimization based key generation

N.K. Sreelaja [a,*], G.A. Vijayalakshmi Pai [b]

[a] Sri Krishna College of Engineering and Technology, Coimbatore, India
[b] PSG College of Technology, Coimbatore, India

ARTICLE INFO

Article history:
Received 30 December 2010
Received in revised form
19 December 2011
Accepted 8 April 2012
Available online 24 April 2012

Keywords:
Binary image encryption
Ant Colony Optimization
Stream cipher

ABSTRACT

Encryption of binary images is essential since it is vulnerable to eavesdropping in wired and wireless networks. The security of data becomes important since the communications over open network occur frequently. This paper focuses on encryption of binary image using a stream cipher method. In this paper we propose an Ant Colony Optimization (ACO) based approach of generating keys for encryption. The binary image is represented in a text form and encrypted using a stream cipher method. A novel technique termed Ant Colony Optimization Key Generation Binary Image Encryption (AKGBE) algorithm employs a character code table for encoding the keys and the plain text representing the binary image. The main advantage of this approach is that it reduces the number of keys to be stored and distributed. Experimental results demonstrating AKGBE's encrypting binary images of different sizes and the comparison of its performance with other stream cipher methods are presented.

1. Introduction

Binary images are the simplest type of image which is used widely in a variety of industrial and medical applications. Binary images will be a black-and-white or silhouette image. Binary images are images that have been quantized to two values, usually denoted 0 and 1, representing black and white. Binary images can be classified as either halftone or non-halftone. Halftone images are binary representations of grayscale images. Non-halftone binary images may be composed of characters, drawings, schematics, diagrams, cartoons, equations etc. [11]. The value of the pixels in these images will be '0' or '1'. The advantage of binary image is that it is easy to acquire, simple digital cameras can be used together with very simple frame stores or low-cost scanners. Binary images have a low storage since it has no more than 1 bit per pixel.

As digital devices such as scanners and digital cameras become more and more available and mass storage media for digital data become more affordable, the use of digital images in practical applications are becoming more widespread [18]. The wired and wireless IP networks are vulnerable to eavesdropping making essential the data traffic to be encrypted. Consequently, confidentiality is especially important for secure media distributions over IP networks. Though image compression reduces the bandwidth, transferring compressed images alone is not secure [4]. Thus, it is essential that the images must be encrypted before being transmitted in a network.

Stream cipher is a symmetric key encryption where the crypto key used to encrypt the binary image is randomly changed so that the cipher image produced is mathematically impossible to break. Also each bit of data is encrypted with each bit of key. The random keys are changed so that it will not allow any pattern to be repeated which would give a clue to the cracker to break the cipher image. The advantage of using stream cipher is that the execution speed is higher when compared to block ciphers and have lower hardware complexity. Unlike block ciphers, stream cipher will not produce the same cipher text even for repetitive blocks of plain text, since the keys are changed constantly for every bit of plain text.

Martin del Rey [17] had proposed a novel stream cipher method for binary image encryption. Lee et al. [13] had proposed a scan pattern method for binary image encryption. Krikor et al. [14] had proposed image encryption using DCT and stream cipher. El-Khamy et al. [21] had proposed a partial encryption system based on chaotic stream cipher (ELKNZ) and the Discrete Wavelet Transform (DWT). Liu et al. [23] had proposed a chaos-based image encryption system, in the framework of stream cipher architecture. However these methods suffer from the drawback in terms of the number of keys to be stored and distributed. Some of the traditional stream cipher methods such as RC4 and Vernam cipher considered to be a perfect cipher also suffer from drawbacks. The drawback in

* Corresponding author. Tel.: +91 422 2572177/477; fax: +91 422 2573833.
E-mail addresses: sreelajank@gmail.com (N.K. Sreelaja), paigav@mca.psgtech.ac.in (G.A. Vijayalakshmi Pai).

1568-4946/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.asoc.2012.04.002

Vernam cipher is that a large number of keys have to be stored and distributed. Also it is shown that the keys can be cracked in RC4 method.

Swarm Intelligence [26], is an algorithm that models the collective behavior of social insects. Here, an autonomous agent is a subsystem that interacts with its environment, which probably consists of other agents, but acts relatively independently from all other agents. The autonomous agent does not follow commands from a leader, or some global plan [20]. Ant System is a Swarm Intelligence algorithm to solve optimization problems. Artificial Ants [20] have some characteristics which do not find counterparts with real ants. They live in a discrete world and the moves consist of transitions from discrete state to discrete states. They have an internal state. This private state contains the memory of the ant agent's past action. They deposit a particular amount of pheromone, which is a function of the quality of the solution found. An Artificial Ant's timing in pheromone deposition is problem dependent and often does not reflect real ant's behavior.

In this paper, a stream cipher method similar to Vernam cipher employing an Ant Colony Optimization [25] based approach to generate keys for encrypting binary images is proposed. A novel approach called Ant colony Optimization Key Generation Binary Image Encryption (AKGBE) algorithm is proposed to generate the keystream. The novelty in the approach is that an Ant Colony Optimization approach is used to generate the keystream used for encryption based on the distribution of characters in the plain text denoting the binary image so that the keys in the keystream are encoded using a mutated character code table which would enable to increase the security of the system.

According to this approach, the binary image is encoded in the form of a plain text. An ACO based technique is used to generate the keystream based on the distribution of the characters in the plain text representing the encoded binary image. The length of the keystream should be less than or equal to the length of the plain text representing the encoded binary image. The keystream is a group of characters denoting the keys for encryption. Depending on the distribution of characters in the plain text representing the encoded binary image, a character code tree is formed to generate the code for each character. To increase the security of the system, mutation is done randomly at any level of the tree and a character code table is generated from the mutated tree. The characters in the plain text representing the encoded binary image are encoded using the values from the mutated character code table. Each key in the keystream is given a value. The keys in the keystream occurring in the plain text representing the encoded binary image are encoded using the values in the mutated character code table. The keys in the keystream which are not occurring in the plain text are replaced with their ASCII values. The values of the keys in the keystream are added to a predetermined value to generate the keys for the portion of the plain text representing the encoded binary image exceeding the length of the keystream. An XOR operation is performed with the key values and the plain text values to obtain the cipher image.

The advantage of the proposed stream cipher method is that it would increase the security of the system by encoding the keys in the keystream and the characters in the plain text representing the encoded binary image using the mutated character code table. It reduces the number of keys to be stored and distributed when compared to that of Vernam cipher considered to be the perfect cipher. It overcomes the drawback of boolean cellular automaton method for binary image encryption and scan pattern method of binary image encryption in terms of the number of keys to be stored and distributed. The length of the key in AKGBE algorithm is less when compared to ELKNZ and DWT and chaos based image encryption method. Unlike other methods, the keystream generator cannot be cracked since the keys used for encryption depends on the binary image to be encrypted. Also the keys cannot be found as in the case of RC4 algorithm. Also it overcomes the drawback of fast and secure stream cipher method and key pooled RC4 method in terms of the number of keys stored and distributed.

The rest of the paper is organized as follows. Section 2 describes the related work. Section 3 describes the system architecture for encryption and decryption. Section 4 explains the Ant Colony Optimization. Section 5 explains Ant Colony Optimization Binary image encryption. Section 6 describes the character code table generation. Section 7 describes the case study. Section 8 describes the computational complexity of the system. Section 9 describes the experimental results. Section 10 explains the comparison of stream cipher using AKGBE algorithm with existing stream cipher methods. Section 11 discusses the security analysis of stream cipher method using AKGBE algorithm. Section 12 discusses the conclusion.

2. Related work

Martin del Rey [17] had proposed a novel cryptosystem for binary images. According to this approach, a stream cipher cryptosystem is used whose cryptographic secure pseudorandom bit generator is a hybrid boolean cellular automaton. The drawback is that the secret key of the cryptosystem and the characteristic vector distributed to the receiver is formed by 256 cells. Thus a total of 512 keys have to be distributed to the receiver.

Lee et al. [13] have proposed a method for encrypting binary images. According to this approach, the binary image is treated as a bit string and the bits are grouped to form a block for encryption. A scan pattern is generated using a pseudorandom generator to generate a sequence of selected random patterns and the position of the bits in each block is changed according to the scanned pattern. This is followed by a flipping process in which for each x bit group, a value of x bits is randomly selected and an XOR operation is performed. The drawback is that the values used for performing XOR operation and the selected scan pattern has to be distributed to the receiver which will be as long as the number of bits in the binary image. A large number of keys are to be distributed to the receiver for larger images.

Biham and Seberry [2] proposed a fast and secure stream cipher for encryption. This method is based on a new kind of primitive, called Rolling Arrays. It also includes variable rotations and permutations. The security claims of the cipher are that no key recovery attacks can be performed with complexity smaller than that of exhaustive search, and distinguishing attacks are also impractical with a similar complexity. It is also shown that the speed of the cipher is impressively fast when compared to RC4. The drawback in the fast and secure stream cipher method is that a total of 256 keys have to be stored for initial permutation. Also the keystream generated does not depend on the plain text to be encrypted and the plain text is not encoded.

Kim et al. [12] proposed a method to implement and evaluate an efficient RC4 stream cipher, called key-pooled RC4, to transfer securely multimedia files in the wireless mobile network. In this method, a 1 MB-sized keystream pool, which consists of 2048 or 8192, or 32,768 keystream frames, is created uniquely for each client device in the registration step. When a client requests a multimedia file, the server delivers the file after encrypting it using the sequence of keystream frames which are randomly selected from the corresponding keystream pool. It is also shown that the proposed scheme is more time efficient than the normal RC4 and more secure than normal RC4. The drawback in this method is that the number of keystream frames to be stored and distributed is large.

Wu and Jay Kuo [4] proposed a method of encrypting images using a stream cipher method. In this method a pseudorandom number generator is used to generate the keys for encrypting the