Engineering Science and Technology, an International Journal xxx (2016) xxx–xxx

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

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

Full Length Article

A novel binary image encryption algorithm based on diffuse representation

Amrane Houas *, Zouhir Mokhtari, Kamal Eddine Melkemi, Abdelmalik Boussaad

Laboratory of Applied Mathematics, PB 145 University of Biskra, Algeria

ARTICLE INFO

Article history:
Received 15 February 2016
Revised 9 June 2016
Accepted 26 June 2016
Available online xxxx

Keywords:
Cryptography
Image encryption
Decryption
Security

ABSTRACT

In this paper, we propose a new algorithm to encrypt binary images. The proposed scheme is described in several steps. In the first step, we present a new basis to reduce the amount of data required to present the image. In the second step, the image is split into *d* blocks, which is used in new images of the same size as the original one, and represent them in the new basis to obtain a key-image and encrypted images. The parameters obtained by this transformation are considered as key-image for the encryption and decryption algorithm. The decryption algorithm is performed by the subtraction between each encrypted image and key-image, then summing them in an image to obtain the original one. In the same way, we can apply our proposed algorithm to encrypt a database of binary images. Experimental results demonstrate the efficiency of the proposed approach.

1. Introduction

Due to the huge expansion of images and multimedia use in current nowadays applications, the need for fast and secure representation, transmission and storage schemes become more and more crucial, especially because digital images can contain private and confidential information that may be associated with financial, medical or personal interest [1].

Encrypting images is a crucial tool for protecting information during communication in network, through the rapid development of computer network large sized images can be easily transmitted therefore, the encryption operation has become an important issue. The most classical encrypting techniques are well developed for the security of textual data, but these are not suitable with digital media such as images. The main constraint is that, the structure of image is complex compared to the text file, which implies that the size of image is much greater than the size of textual file. In this case the necessity of designing encryption and decryption algorithms with low complexity is very important. Many researches from different disciplines like mathematics, computer science and electrical engineering have focused for developing robust algorithms for encrypting images in order to offer a higher level of security in telecommunication networks.

Nowadays, different techniques of image encryption have been proposed. This is due to the proliferation of sophisticated sensors. By nature, the Internet by its TCP/IP protocol is a subject to any control, hence its vulnerability to hacker attacks. For this reason, the large number of researches in the field of visual cryptography have been developed. Exchange of secret digital images are frequently used worldwide in a second split on the Internet [2]. Therefore, it becomes very important to protect these information [3].

Cryptographic techniques can be divided into symmetric and asymmetric encryption [4]. As one of the important research topics, image encryption has been more developed. Due to its high processing speed and more degrees of freedom, the added value of image encryption is showed through the recent optical information processing technologies. Different optical techniques have been proposed for image encryption [5,6].

As known, digital images have important proprieties like, redundancy of data, less sensitive, correlation between pixels and massive capacity of data. Hence, many of image encryption algorithms have been proposed [7,8] taking profit from these characteristics. Recently, Guomin Zhou et al. [8] proposeed a fast symmetrical image encryption algorithm based on skew tent map. Based on a new chaos based Line map, their proposed algorithm encrypts images with different size. In order to perturb the correlations between the R, G and B components of the true color image, these three components are encrypted at bit level and operated at the same time [8]. In fact, several classical encryption schemes like data encryption standard (DES) [9], triple data encryption algorithm (TDEA) [10], advanced encryption standard (AES) [11] and Rivest, Shamir and Adleman (RSA) [11,12] have

* Corresponding author.
E-mail address: haouesamrane@hotmail.com (A. Houas).

http://dx.doi.org/10.1016/j.jestch.2016.06.013
2215-0986/

been developed. However, these algorithms are limited when they are applied in the encryption of digital images, especially for huge images [13].

Similar to DES algorithm but faster than DES, Nithin et al. [14] have proposed the fast image encryption algorithm (FEAL).

Using structurally random matrices and Arnold transform, Rawat et al. [15] have introduced a digital image encryption method based on a fast compressed sensing idea. Zhao et al [8] have recently presented a symmetric digital image encryption algorithm by a new improper fractional-order chaotic subsystem.

A binary image (bi-valued image) is the type of simple image that is widely used in various electronic applications such as fingerprint analysis, robot vision, motion detection and character recognition. It often appears as cartoons in newspapers and magazines. Moreover, binary images frequently emerge as the result of many automatic tasks, such as binarisation, halftoning, edge detection, segmentation, and thresholding. Certain input/output devices and sensors, like for examples laser printers, fax machines, biometric devices, and bi-tone machine screens, can only handle bi-level images.

Due to their simplicity compared with gray level images; it is better to process binary images in real time. In the context of binary image encryption, many schemes have been proposed. Among the most published works, we can find in [16] a scan language is proposed by Bourbaki in 1986 as a language for efficient accessing of a two dimensional array. In [17] a parallel implementation version for the scan language is presented, which shows that the parallel expansion scheme is faster and requires less storage space. Bourbaki and Alexopoulos in [18] proposed a new encryption scheme for binary images using scan pattern. This algorithm is based on a family of 2D transposition which is produced by the scan language. In [19] Chung and Chang developed an encryption scheme for binary images with higher security, this approach sets the different scan patterns at the same level in the scan tree structure and uses the two dimensional run-encoding technique in order to ensure a higher security and a good compression ratio. In [20] a very simple method for binary image encryption is reported based on inference of two phase-only masks, the main idea of this algorithm is that: the binary image is first modulated by a random phase mask and then separated into two phase-only masks. This approach offers a very low complexity and without any time consuming iterative computations. Most of the aforementioned algorithms, they have proved their effectiveness in the area of cryptography.

In this optic, our paper proposes an efficient encryption algorithm for binary images which is based on dividing the original image into d blocks, then constructing new images of the same size as the original one and representing them in a new proposed basis.

We call key-image the matrix of parameters obtained using this transformation, and we call the encrypted images the represented images in this new basis.

In the proposed decryption algorithm, a subtraction between each encrypted image and the key-image is applied, then we sum them in an image to get the original one.

Moreover, in the same way, we use this new basis to encrypt a database of binary images. In fact, the idea of this new basis construction is inspired from the paper of Mokhtari and Melkemi [21]. The authors [21] have proposed a semi-blind watermarking scheme in gray scale images. The new algorithm changes the coefficients of discrete cosine transform in homogeneous manner. This algorithm is based on the modification of the base using the concept of the norm or the distance.

The rest of the paper is organized as follows. Section 2 describes the details of our proposed image encryption/decryption algorithms. Section 3 expresse the details of encryption evaluations metrics. Experimental results and discussion are reported in Section 4. The conclusion is presented in Section 5.

2. The proposed scheme

2.1. The mathematical background of the proposed method

In the proposed idea, the transformation of an original binary image to another encrypted image is inspired from the work proposed by Mokhatri and Melkemi in [21]. This new transformation diffuses the images of a given data-set in a new basis, in order to share information quantity almost equal in different images of our data-set.

In [21], the authors have shown that if we have a database $\{I_k\}_{k=1,d}$ of d images, which are represented in the orthonormal basis $\{e_j\}_{j=1,n}$, such that for any value of k,

$$I_k = \sum_{j=1,n} a_{kj} e_j \tag{1}$$

There exists a new base $\{f_j\}_{j=1,n}$ where for all k:

$$I_k = \sum_{j=1,n} b_{kj} f_j \tag{2}$$

With

$$b_{kj} = \beta_j - a_{kj} \tag{3}$$

and

$$b_{kj} \sim \frac{\|I_k\|_1}{\sqrt{n}} \tag{4}$$

By choosing a suitable function and applying the method of least squares, they will get the optimal settings $j = 1, n$:

$$\beta_j^* = \frac{1}{d} \sum_{k=1,d} \left(a_{kj} + \frac{\|I_k\|_1}{\sqrt{n}} \right) \tag{5}$$

2.1.1. Example

The basis $\{e_j\}_{j=1,n}$ is the canonical basis of the vector space $\mathbb{R}^n$ with dimension n, in the following example we work with matrices with dimension 8×8 the dimension of our vector space is $n = 8 \times 8$, and the elements of this basis are matrices defined by :

$$e_{i,j}(s,l) = \begin{cases} 1 & \text{for } (s,l) = (i,j) \\ 0 & \text{otherwise} \end{cases}, \; s, \; l = 1, \ldots, 8$$

Let be I a matrix $n = 8 \times 8$ such that $I(i,j) \in \{0,1\}$.

$$I = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

If, we split matrix I vertically into $d = 2$ blocks, and construct 2 new matrices $I1$ and $I2$ with the same size as I such that each matrix contains one of the blocks and the remaining value is zero ($I = I1 + I2$), we get

$$I1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$