Information Sciences 269 (2014) 21–34

Contents lists available at ScienceDirect

Information Sciences

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

Image cryptographic algorithm based on the Haar wavelet transform

Sara Tedmori [a,*], Nijad Al-Najdawi [b,1]

[a] Computer Science Department, The King Hussein Faculty of Computing Sciences, Princess Sumaya University for Technology, Jordan
[b] Computer Science Department, Prince Abdullah Bin Ghazi Faculty of Information Technology, Al-Balqa Applied University, Jordan

ARTICLE INFO

Article history:
Received 8 September 2013
Received in revised form 21 January 2014
Accepted 1 February 2014
Available online 8 February 2014

Keywords:
Cryptography
Lossless image encryption
Symmetric key encryption

ABSTRACT

Lossless encryption methods are more applicable than lossy encryption methods when marginal distortion is not tolerable. In this research, the authors propose a novel lossless symmetric key encryption/decryption technique. In the proposed algorithm, the image is transformed into the frequency domain using the Haar wavelet transform, then the image sub-bands are encrypted in a such way that guarantees a secure, reliable, and an unbreakable form. The encryption involves scattering the distinguishable frequency data in the image using a reversible weighting factor amongst the rest of the frequencies. The algorithm is designed to shuffle and reverse the sign of each frequency in the transformed image before the image frequencies are transformed back to the pixel domain. The results show a total deviation in pixel values between the original and encrypted image. The decryption algorithm reverses the encryption process and restores the image to its original form. The proposed algorithm is evaluated using standard security and statistical methods; results show that the proposed work is resistant to most known attacks and more secure than other algorithms in the cryptography domain.

1. Introduction

Cryptography is a means of storing and transmitting data in a form that only targeted people can read or process. It is an effective way of protecting sensitive data stored on media or transmitted over unsecured network communication paths. On the receiving end, the encrypted information is then processed and decrypted by humans or machines to reveal the original message [8]. The goal of cryptography is to hide information from unauthorized individuals. The changes that cryptography has undergone closely follow advances in technology [42]. Image cryptography has many applications in various areas. Researchers may employ the traditional text cryptosystems to encrypt images directly; however, since image sizes are far greater than text, and differ in nature from normal text, traditional text encryption methods are not applicable to images. Image encryption methods can be classified into either lossy or lossless. In lossy encryption methods, were the image details are somewhat distorted, the resulting decrypted image is different from the original image. Due to the characteristics of human perception, and depending on the application, a decrypted image with little distortion is usually acceptable. However, lossless encryption methods are more applicable in applications where the distorted-free original image is required, such as in: medical images, aerospace images, satellite images, and in applications that involve highly classified images. As with any

[*] Corresponding author. Tel.: +962 (0)779969654.
E-mail addresses: s.tedmori@psut.edu.jo (S. Tedmori), n.al-najdawi@bau.edu.jo (N. Al-Najdawi).
[1] Tel.: +962 (0)775054992.

http://dx.doi.org/10.1016/j.ins.2014.02.004
0020-0255/© 2014 Elsevier Inc. All rights reserved.

technology, cryptography is not foolproof. With enough motivation, time and resources, even the most advanced digital cryptography techniques can be broken by some person or organization. A variety of image encryption schemes have been proposed [12] and can be classified into three major categories: position permutation, value transformation, and visual transformation. In this work, the authors propose a novel lossless encryption/decryption technique based on the three categories (position permutation, value transformation, and visual transformation). The proposed system reduces the risk of sensitive images being accessed or stolen by someone other than the intended recipient. This is important in situations that require the transmission of high quality confidential images. In the proposed algorithm, the image is transformed into the frequency domain using the Discrete Wavelet Haar Transform (DWT) with two levels of decomposition, where the image sub-bands are processed in such a way that ensures that the original image can never be recovered without using the proposed decryption algorithm. The image decryption is also applicable in the frequency domain where the image sub-bands are converted back to their original form by reversing the encryption process.

The rest of the paper is organized as follows: Section 2 presents a literature review of previous studies, and highlights the significance of this research. Section 3 discusses the transformation methods that can be used to transform the image information from one domain into another; Section 3 also discusses the use of the discrete wavelet transformation method. Section 4 presents the encryption and decryption methods proposed in this research. Section 5 discusses the experimental results of both a subjective and an objective quality assessment. Finally, Section 6 concludes this research.

2. Related works

There are two major characteristic differences between text and image data which make text encryption methods in most cases not applicable to images. One difference is the size. Image data is typically much larger than that of text data. The other difference relates to data loss when a compression technique is used. Unlike image data, text data when compressed rarely permit loss. Hence, researchers investigated several lossy/lossless image encryption methods.

Image encryption schemes can be classified into two broad categories: spatial domain methods and frequency domain methods. The term spatial domain refers to the image plane itself, and approaches in this category are based on direct manipulation of the pixels in an image. In these algorithms, the general encryption usually destroys the correlation amongst pixels and thus makes the encrypted images incompressible. Frequency domain methods are based on modifying the frequencies of an image. The image pixels can be reconstructed (recovered) completely via an inverse process with no loss of information. This allows working in the frequency domain (where image data is highly decorrelated) and then returning to the spatial domain without any loss in information. Encryption techniques based on a mixture of methods from these two categories are not unusual.

2.1. Pixel based cryptography (spatial domain)

A variety of encryption schemes in the spatial domain have been proposed in literature. Maniccam and Bourbakis [22] presented a lossless method which performs lossless compression and encryption of binary and gray-scale images. The schemes are based on patterns generated by the two-dimensional spatial-accessing method that can specify and generate a wide range of scanning paths or space filling curves. Bhatnagar and Jonathan Wu [3] presented a selective encryption technique based on space filling curve, pixels of interest, non-linear chaotic map and singular value decomposition. In their work, the scheme scrambles the pixel positions and then selects significant pixels using the pixels of interest method. Then the diffusion process is done on the significant pixels using a secret image key obtained from non-linear chaotic map and singular value decomposition. Yen and Guo [38] presented an image encryption algorithm, based on a binary sequence generated from a chaotic system; the image is scrambled according to the proposed algorithm. A related research can be found in the work proposed by Gao et al. [13] where the authors proposed a similar encryption scheme. Zhang and Karim [41] proposed a method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats. In the encoding stage, images are encoded with white noise filter using two masks; the first mask is in the input plane whilst the other one is in the Fourier plane. In the decryption stage, the color images are recovered by converting the decrypted indexed images back to their RGB formats. Sinha and Singh [30] proposed a technique that encrypts images for secure image transmission using digital signatures. In their approach, the digital signature of the original image is added to the encoded version of the original image. Image encoding is performed using Bose–Chaudhuri Hochquenghem error code. At the receiving end, after the image is decrypted, the digital signature is used to verify the authenticity of the image. Hou [15] used the characteristics of human vision to decrypt encrypted images. In his work, the author proposed three methods for visual cryptography of gray-level and color images based on the halftone technology and the color decomposition method. In [40], Zhang and Liu proposed an encryption method based on skew tent chaotic map and permutation–diffusion architecture, the proposed method shuffles the positions of pixels, and the generated key stream is then related to the plain-image. Yahya and Abdalla [37] proposed a shuffle encryption algorithm that performs non-linear byte substitution. The algorithm performs a shuffling operation partially dependent on the input data and uses the given key. The results of their work were implemented and tested on different data, mainly consisting of images. Chen et al. [7] proposed a method to encrypt a color image based on the Arnold transform and the interference method. In their