Int. J. Electron. Commun. (AEÜ) 70 (2016) 278–288

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

ROI based robust and secure image watermarking using DWT and Arnold map

Razieh Keshavarzian[a], Ali Aghagolzadeh[b,*]

[a] Department of Electrical Engineering, Heris Branch, Islamic Azad University, Heris, Iran
[b] Faculty of Electrical and Computer Engineering, Babol University of Technology, Babol, Iran

ARTICLE INFO

Article history:
Received 4 October 2014
Accepted 3 December 2015

Keywords:
Arnold transform
Image watermarking
ROI
Wavelet transform

ABSTRACT

Three main requirements of any watermarking scheme are imperceptibility, robustness and security. In this paper, a new robust blind image watermarking scheme based on Region of Interest (ROI) using Arnold scrambling is proposed. The proposed scheme satisfies the requirements via using a watermark generated from the host image, the used embedding strategy and Arnold scrambling. In this paper, the ROI of the host image is used as the watermark image. First-level DWT is applied to the watermark and approximation coefficients are chosen as information to be embedded. Each approximation coefficient is embedded into the low frequency sub band of a selected block of the host image in the wavelet domain. Before embedding, Arnold scrambling is performed on the approximation coefficients of the watermark as well as the blocks of the host image. This makes the scheme more robust and secure. Simulation results show that the proposed scheme achieves high degree of security, imperceptibility and robustness against the variety of attacks.

1. Introduction

The rapid development of the digital multimedia technology and the internet allow people to copy, transmit, distribute and store information more easily. This advantage leads to the need for copyright protection and copy protection of multimedia data. Digital watermarking is an effective method for copyright protection, copy protection, proof of ownership, etc. [1]. Digital watermarking is the technique that embeds copyright or other information called watermark into an image or audio or video [2]. The watermark can be extracted later from multimedia to prove ownership, or to get some copyright-related information [3]. In some applications, like copyright protection, watermark extraction algorithms can use the original image to find the watermark. This is called non-blind watermarking. In most other applications, like copy protection, the watermark extraction algorithms do not have access to the original image. Watermarking algorithms of this kind are referred to as blind watermarking [4]. In a watermarking technique, several requirements must be satisfied. One of the most important requirements is the perceptual transparency of the watermark [3], i.e., the watermark should not degrade the quality of the host image. In addition to imperceptibility, a watermark should be robust to common signal processing operations and attacks. The watermarking technique must be secure. This means if knowing the exact algorithms for embedding and extracting the watermark does not help an unauthorized party to detect the presence of the watermark or remove it [4]; this can be achieved by choosing a secret key. In order to resist the different attacks, the embedding strength must be as high as possible. However, the higher the embedding strength, the lower the quality of the watermarked image [1]. Therefore, we should establish the balance between the robustness and the imperceptibility of the watermark.

According to the domain in which the watermark will be embedded, the watermarking techniques are categorized into spatial and transform domain techniques. In the spatial domain methods, the watermark will be embedded by directly changing the pixel values of the image. In the transform domain techniques, the embedding process will take place by altering the transform coefficients [5]. The spatial domain techniques are simple but are less robust than the transform domain techniques against different attacks [6]. Three common transform domain methods are discrete cosine transform (DCT) [7–9], discrete Fourier transform (DFT) [10,11] and discrete wavelet transform (DWT) [12–19]. Among the transform domain methods, wavelet based methods are more popular due to their excellent frequency localization properties. Here, some image watermarking schemes which are based on wavelet transform are reviewed.

* Corresponding author.
E-mail addresses: keshavarzian@herisiau.ac.ir (R. Keshavarzian), aghagol@nit.ac.ir (A. Aghagolzadeh).

http://dx.doi.org/10.1016/j.aeue.2015.12.003
1434-8411/© 2015 Elsevier GmbH. All rights reserved.

Barni et al. [12] proposed a wavelet based watermarking scheme which exploits the characteristics of human visual system (HVS). By taking into account the texture and the luminance content of all the image sub bands, a mask is built pixel by pixel. The watermark consists of a binary pseudorandom sequence is adaptively added to the DWT coefficients of the three largest detail bands of the image. Hsieh et al. [13] presented a multi-energy watermarking scheme based on the qualified significant wavelet tree (QSWT) by adding visually recognizable patterns to the large coefficients at the high and middle frequency band of the DWT of an image. Kang et al. [14] proposed a blind DWT–DFT composite image watermarking scheme in which a key based sequence is embedded in the coefficients of the *LL* sub band in the DWT domain. To resist geometric attacks, they embedded a template into the middle frequency components in the DFT domain of the watermarked image. Kundur et al. [15] presented a multiresolution fusion based watermarking scheme in the wavelet domain. The l-level and first level DWT are applied to host image and gray scale logo, respectively. The subimages of the host image are divided into blocks of size equal to the size of sub bands of the logo. Each sub band of the logo is added to selected blocks of the host image sub bands with the same orientation. Wang and Lin [16] proposed a watermarking scheme based on wavelet tree quantization. The host image is transformed into wavelet coefficients using a discrete time wavelet transform (DTWT). The wavelet coefficients of the host image are grouped into so-called super trees. The watermark is embedded by quantizing super trees. Each watermark bit is embedded using two trees in perceptually important frequency bands. The trees are so quantized that they exhibit a large statistical difference, which will later be used for watermark extraction. In this scheme, the original watermark is needed at the extraction process. Also the scheme's visual quality and robustness against some attacks is not good enough. Reddy et al. [17] proposed a wavelet based gray scale logo watermarking technique. They applied DWT to host image and used HVS characteristics given in [12] for calculating the weight factor for each wavelet coefficient of the host image. The significant coefficients of the host image are selected based on the weight factors and the watermark bits are added to these coefficients. Ghouti et al. [18] proposed a spread spectrum based watermarking scheme using balanced multiwavelet transform (BMW). The watermark data is coded with a pseudorandom sequence and is added into sub band coefficients of the host image using a perceptual model. The use of spread spectrum approach increase robustness against noise due to spread the power spectrums of the information data. Lin et al. [19] proposed a blind watermarking algorithm based on maximum wavelet coefficient quantization in which a binary watermark is embedded into DWT coefficients of host image. The wavelet coefficients of the host image are grouped into different block size and blocks are randomly selected from different sub bands. They embedded a watermark bit into every block by quantizing the local maximum wavelet coefficient of the block. Although this scheme performs well against some attacks, it is not robust enough against geometric attacks such as cropping. Bhatnagar et al. [20] presented a semi-blind reference watermarking scheme based on DWT and singular value decomposition (SVD). The original image is transformed into wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. They used a gray scale logo as watermark and embedded it into reference image by modifying the singular values of reference image using the singular values of the watermark. In another hybrid DWT-SVD based watermarking scheme given by Lai et al. [21], the watermark is directly embedded into the singular values of the host image's DWT sub bands. Li et al. [22] presented a method to enhance the robustness of wavelet based image watermarking schemes against geometric distortions by constructing an invariant wavelet domain. This scheme is resistant to multiples of 90 rotations and image flipping. Huang et al. [23] proposed an adaptive watermarking scheme based on morphological Haar wavelet transform (MHWT). The gray watermark image is adaptively embedded into low frequency band of MHWT of host image, combining the characteristic of HVS. Bhatnagar et al. [24] presented a watermarking scheme similar to Kundur et al. [15]. In [24], all sub bands are segmented into blocks using ZIG-ZAG sequence. The watermark is embedded in the blocks selected based on their variances. Ghebleh et al. [25] proposed a robust blind wavelet domain watermarking scheme based on chaotic maps. They embedded a black and white watermark logo in the mid-band components of a host image using discrete wavelet transform. This scheme provides higher security and robustness at the cost of low embedding capacity. Liu et al. [26] proposed a blind image watermarking scheme based on chaotic mixtures in the discrete wavelet domain. The black and white watermark image is firstly scrambled by using logistic maps and then embedded into the second-level approximation coefficients of the host image in discrete wavelet transform domain.

In this paper, a blind wavelet domain watermarking algorithm based on ROI using Arnold transform is proposed to simultaneously meet imperceptibility, robustness and security in copy protection applications. Unlike the above mentioned watermarking techniques in which the watermark is taken from an external source, this technique uses the ROI of the host image as the watermark. The approximation coefficients of the watermark are embedded into the low frequency band of the image blocks, to provide better robustness against the most attacks. Before embedding, Arnold transform is performed on the approximation coefficients of the watermark as well as the blocks of the host image, to make the scheme more robust and secure. In the embedding process, each coefficient of the watermark is replaced with a coefficient in a block of the image. The considered coefficient has the least difference with the coefficient of the watermark. Although human eyes are more sensitive to the small changes in the low frequencies components, but since the watermark is a part of the image and has high correlation with the host image, replacing the coefficients does not degrade the visual quality of the host image. This algorithm is blind; so it requires neither the original image nor the watermark at the extraction process. Also it is based on block image processing; so it can be adopted by the most existing image compression standards. This technique has shown high performance of security, robustness and imperceptibility. In particular, our simulation results show that our proposed technique achieves the maximum robustness against JPEG compression, filtering, scaling, motion blur and some other attacks compared with the existing schemes. Furthermore, the results show that the proposed scheme exhibits more robustness over our previous work [27]. Unlike the proposed scheme, our previous work does not take the advantage of Arnold transform. Thus, the claim that Arnold transform makes the scheme more resistant to the various attacks is supported.

The rest of the paper is organized as follows: in Section 2, Arnold transform is described. In Section 3, the proposed algorithm is presented in details. The simulation results are described in Section 4. Finally, the conclusion is provided in Section 5.

2. Arnold transform

Arnold transform is a 2D chaotic map for scrambling a digital image. Let us consider the original image is of size $N \times N$. Arnold transform is defined as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \qquad (1)$$

where $x, y \in \{0, 1, 2, ..., N-1\}$. Each pixel (x,y) in the image is transformed to another pixel (x',y') by (1). When all of pixels in the