Signal Processing: Image Communication 45 (2016) 41–51

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

Robust and hierarchical watermarking of encrypted images based on Compressive Sensing

Hong Liu [a,b], Di Xiao [a,*], Rui Zhang [a], Yushu Zhang [c], Sen Bai [d]

[a] *Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, College of Computer Science, Chongqing University, Chongqing 400044, China*
[b] *College of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[c] *School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China*
[d] *Department of Information Engineering, Chongqing Communication Institute, Chongqing 400035, China*

ARTICLE INFO

Article history:
Received 3 September 2015
Received in revised form
30 December 2015
Accepted 13 April 2016
Available online 14 April 2016

Keywords:
Image encryption
Watermarking
Commutative
Compressive Sensing
Hierarchical security

ABSTRACT

We propose a method that allows watermarking encrypted image and detecting the watermark in encrypted domain or decrypted domain. First, image is divided into blocks and transformed to wavelet coefficients, and then scrambled with Arnold map and encrypted with Compressive Sensing. Next, watermark is embedded into the encrypted image using the Scalar Costa Scheme. The operations of watermark extraction and image decryption are commutative. The watermark can be extracted in the compressed encrypted domain and then the original image can be decrypted and reconstructed. In the other case, the image can be decrypted and the watermark can be extracted in the decrypted domain. The proposed method is compared with the-state-of-art methods, where its superiority in terms of robustness, high correct bit extraction rate, flexible data embedding capacity and hierarchical security are highlighted.

1. Introduction

Multimedia content is often distributed in compressed and encrypted format. Watermarking of multimedia for copyright violation detection, proof of ownership, media authentication, etc, needs to be carried out in compressed–encrypted domain. Watermarking in compressed–encrypted content saves the computational complexity as it does not require decompression or decryption, and also preserves the confidentiality of the content. In secure multimedia distribution scenario based on multimedia proxies [1–3], the multimedia proxy needs to embed the watermark into the encrypted media data directly without decryption, which avoids the leakage of media content. The watermark can be extracted from the encrypted or decrypted media data. Additionally, the media content receiver can have full access to both the watermark and encrypted image using data hiding key and decryption key. In this paper, we propose a method that allows watermarking encrypted image and detecting the watermark in encrypted domain or decrypted domain.

There have been several joint image encryption and watermarking techniques proposed to date [4–9]. Commutative watermarking and encryption methods are proposed in [4,5,8], however they apply partial encryption to image, which are not secure enough against replacement attacks. A commutative watermarking and encryption method is proposed in the tree structured Haar transform domain in [6]. In [9], a robust watermarking technique for JPEG2000 images is proposed, in which the watermark can be embedded in compressed–encrypted byte stream by exploiting the homomorphism property of the RC4 stream cipher. The computational complexity of [9] is high.

Reversible data hiding in encrypted images has attracted considerable attention from the communities of privacy security and protection. A reversible data hiding method in encrypted image is proposed in [10]. [11] modifies the algorithm of [10] with side math method, which improves the correct bit extraction rate of embedding bits. However, in order to correctly extract the embedding bits, both [10] and [11] have to take advantage of the original image. [10] and [11] embed additional bits in the spatial domain. They are limited by their embedding capacities and are not robust against attacks. A novel scheme of commutative reversible data hiding and encryption is proposed in [12]. In encryption part, the gray values of two neighboring pixels are masked by the same pseudo-random bits. In data-hiding part, the additional data are embedded into various bit planes with a reversible manner. However, since the encryption method is simple

[*] Corresponding author.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

http://dx.doi.org/10.1016/j.image.2016.04.002
0923-5965/© 2016 Elsevier B.V. All rights reserved.

exclusive-or calculation, there exists some correlation between two bits in a same plane and a same block. The method of [13] aims at encrypting a JPEG bit stream into a properly organized structure, and embedding a secret message into the encrypted bit stream by slightly modifying the JPEG stream. A scheme for separable reversible data hiding in encrypted images is proposed in [14]. A novel scheme of reversible data hiding in encrypted images using distributed source coding is proposed in [15]. In [16], the authors take advantage of the patch-level sparse representation when hiding the secret data. Thanks to the powerful representation of sparse coding, a large vacated room can be achieved, and thus the data hider can embed more secret messages in the encrypted image. A novel reversible image data hiding scheme over encrypted domain is proposed in [17]. The data embedding is achieved through a public key modulation mechanism, in which access to the secret encryption key is not needed. In [18], the authors proposed to consider every two adjacent prediction-errors jointly to generate a sequence consisting of prediction-error pairs. Then, based on the sequence and the resulting 2D prediction-error histogram, a more efficient embedding strategy can be designed to achieve an improved performance. A blind image watermarking resynchronization scheme against local transform attacks is proposed in [19].

In most multimedia applications, compression is necessary for limited network resources. In recent years, a new theory Compressive Sensing (CS) has been proposed as a more efficient sampling scheme. The theoretical framework of CS was developed by Candes et al. [20] and Donoho [21]. The CS principle claims that a sparse signal can be recovered from a small number of random linear measurements [22,23]. CS has been used to design secure digital image encryption schemes [24–28]. Zhang et al. proposed a CS-based encryption algorithm, where the original image is encrypted as a set of coefficients by a secret orthogonal transform [24]. Liu et al. proposed an image encryption scheme with enhanced security and robustness against packet loss [25]. Zhou et al. proposed a new hybrid image compression–encryption algorithm based on Compressive Sensing [26]. The proposed algorithm with sensitive keys and nice image compression ability can resist various attacks. Liu et al. proposed a novel real-time and progressive secret image sharing with flexible shadows based on Compressive Sensing [27]. Liu et al. proposed an optical image encryption based on Compressive Sensing and chaos in the fractional Fourier domain [28].

In addition, some CS-based watermarking methods have been proposed. In [30], a CS-based watermark method embeds additional bits by utilizing the relationships between measurements. It can be applied to lossy channels for data delivery, but the watermark extraction accuracy is not ideal. The traditional joint encryption and watermark process is to embed watermark in the spatial domain and then to encrypt the watermarked image. In [31], the watermark is embedded into bit planes of the image and then encrypted with Compressive Sensing. The output from Compressive Sensing is scrambled with Arnold map transformation. If the image proxy wants to embed watermark, he must decrypt the encrypted image which leaks the content of image and has additional cost. In decryption stage, [31] applies inverse Arnold map transformation and then takes Compressive Sensing reconstruction to obtain the watermarked image. Different from [31], our proposed method firstly encrypts image with Arnold map transformation and Compressive Sensing. And then it allows the image proxy to embed watermark directly in the encrypted image. In decryption stage, our proposed method applies Compressive Sensing reconstruction and then inverse Arnold map transformation to obtain the watermarked image. At last, the watermark can be extracted.

In this paper, we propose an encryption method with the data embedding feature based on CS. Firstly, we propose an image encryption algorithm based on Arnold map and CS. Then we use the Scalar Costa Scheme (SCS) to embed watermark in the compressed and encrypted domain. The operations of watermark extraction and image decryption are commutative. The watermark can be extracted in the compressed encrypted domain and then the original image can be decrypted and reconstructed. In the other case, the image can be decrypted and the watermark can be extracted in the decrypted domain. Experimental results have proved the superiority of the proposed method.

The proposed method has the following properties:

(1) It allows directly embed the watermark into the encrypted image without decryption, which avoids the leakage of image content.
(2) It is possible to detect the watermark correctly in encrypted or decrypted domain.
(3) It does not result in cipher text expansion and high compression gain is obtained.
(4) It is robust against noise during transmission which is essential for limited network resources.

The paper is organized as follows. In Section 2, Compressive Sensing, Arnold map and chaotic sensing matrix are introduced. In Section 3, the method of image encryption and watermarking based on CS is proposed. In Section 4, the simulation results and analyses of the proposed method are given. Finally, some conclusions are drawn in Section 5.

2. Related works

2.1. Compressive Sensing

Compressive Sensing theory asserts that it is possible to perfectly recover a signal from a limited number of incoherent linear measurements, provided that the signal can be represented by a small number of nonzero coefficients in some basis expansion.

Let $x \in R^n$ denote the signal of interest and $y \in R^m$, $m < n$, be a number of linear random projections (measurements) obtained as $y = \Phi x$. Let $\Psi \in R^{n\times n}$ denote an orthonormal matrix whose columns are the basis vectors. We can have $x = \Psi\theta$, where θ is k sparse. Given the measurements $y = \Phi x$, the signal can be reconstructed by solving the following problem:

$$\min \|\theta\|_1 \text{s.t.} y = \Phi\Psi\theta \tag{1}$$

For the case of noisy measurements, the signal model can be expressed as $y = \Phi x + z$, where the noise amplitude is assumed to be bounded, i.e., $\|z\|_2 \le \varepsilon$. This situation occurs when the measurements are quantized. An approximation of the signal can be obtained by solving the following problem:

$$\min \|\theta\|_1 \text{s.t. } \|y - \Phi\Psi\theta\|_2 \le \varepsilon \tag{2}$$

In this work, we adopt the GPSR algorithm [23] to find a solution to (2).

2.2. Arnold map

Arnold map has wide applications in the field of image encryption. Two-dimensional (2D) Arnold map is given as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A\begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) = \begin{bmatrix} 1 & u \\ v & uv+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) \tag{3}$$

where (x, y) are the coordinates of the original image pixel, $(x^{'}, y^{'})$are the coordinates of the scrambled image, N is the pixel