Signal Processing 99 (2014) 17–28

Contents lists available at ScienceDirect

Signal Processing

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

Attack and improvement of the joint fingerprinting and decryption method for vector quantization images

Ming Li [a], Di Xiao [a,*], Yushu Zhang [a], Hong Liu [a,b]

[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

ARTICLE INFO

Article history:
Received 10 September 2013
Received in revised form
1 December 2013
Accepted 11 December 2013
Available online 21 December 2013

Keywords:
Joint fingerprinting and decryption (JFD)
Vector quantization (VQ)
Traitor tracing
Attack
Codebook partition

ABSTRACT

The first joint fingerprinting and decryption (JFD) scheme proposed by Lin et al. in 2012 aims to protect the distribution of vector quantization (VQ) images. If the decrypted image is illegally redistributed, the fingerprint embedded in the image can be used to trace the traitor. However, this scheme is not secure enough, and it can be broken by a novel attack method proposed in this paper. The embedded fingerprint can be replaced arbitrarily, and therefore the traitor tracing would fail. Besides, the intercepted encrypted image using the static key-trees based approach of the original scheme is also cracked. To make improvements, a new JFD method using codebook partition is proposed. Experiments and analyses show that the proposed method outperforms the original one: the security is enhanced; both the robustness and fragileness are equipped; the fingerprint extraction is simplified; the distortion is limited; and at the same time, the computation and communication overheads are not increased.

1. Introduction

Fingerprint, which was first proposed by N.R. Wagner [1], is the characteristic of an object that tends to distinguish it from other similar ones. Fingerprinting refers to the process of adding fingerprints to an object and recording them, or of identifying and recording fingerprints that are already intrinsic to the object. In the application of multimedia distribution and traitor tracing, digital fingerprinting is a widely used technology to protect the copyright of the multimedia products [2–5]. Here, digital fingerprint represents the unique identity message of each user. When a multimedia product is distributed, the digital fingerprint of the legal user is embedded into the product; therefore, if the user illegally redistributes the product to unauthorized users, the traitor, i.e., the illegal user, could be traced through the fingerprint extracted from the copies.

Encryption aims to protect the confidentiality of the multimedia product. In some applications, the content owner may not want the multimedia content to be open before distributed, therefore, encryption is used. Then, both decryption and fingerprinting are needed at the receiver side. In [6], the decryption and fingerprinting are performed independently. However, the decrypted media content could be intercepted in the gap between the decryption and fingerprinting operations, so the security is low. Thus, a series of joint fingerprinting and decryption schemes (JFD) [7–11] have been proposed to solve the content leakage problem.

Vector quantization (VQ) [12] is an attractive block-based image encoding method due to its high compression ratio. Many kinds of watermarking and data hiding technologies have been researched in the VQ domain in recent years [13–16]. Nevertheless, few papers pay attention to fingerprinting in VQ domain. And no JFD method for VQ

* Corresponding author. Tel.: +86 23 8633 3521; fax: +86 23 6510 4570.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

0165-1684/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2013.12.011

images was presented until 2012 [11]. In the JFD phase of [11], the codeword is substituted by its most similar one to embed one specific binary bit of the user's fingerprint. However, if the fingerprint embedded in the image is replaced, traitor tracing would be impossible. The attack of fingerprint replacement is proposed in this paper, and the static key-trees based encryption approach is also cracked. In addition, an improvement measure is presented to enhance the security and usability of the original scheme.

The rest of the paper is organized as follows. The original scheme is reviewed in Section 2. The attack on the original method is provided in Section 3. Section 4 presents the improvement measure in detail. Section 5 shows the performance of our proposed method compared with the original scheme. Section 6 concludes this paper.

2. Review of the original scheme

A general illustration of the original scheme is shown in Fig. 1. The VQ image should be first encrypted on the sender side. On the receiver side, the fingerprinted and decrypted image can be obtained after the JFD, which is performed directly on the encrypted image. The encryption is based on the key-trees which represent the relationships between the codewords in the codebook. The construction of the key-trees is as follows. First, the codewords in the codebook are sorted by the principal components analysis (PCA) algorithm. The sorted codebook is denoted by $Y=\{Y_0, Y_1, ..., Y_{(L-1)}\}$, where L denotes the size of the codebook. Thus, the neighboring codewords in Y are similar, and the difference between two codewords becomes more significant as the difference between their corresponding indices becomes larger. Then, the sorted codebook is divided into two sets: $\{Y_0, Y_1, ..., Y_{L/2-1}\}$, and $\{Y_{L/2}, Y_{L/2+1}, ..., Y_{(L-1)}\}$. Therefore, $(Y_0, Y_{L/2})$, $(Y_1, Y_{L/2+1})$, …, $(Y_{L/2-1}, Y_{L-1})$ constitute the $L/2$ dissimilar pairs. At last, each codeword Y_i has one dissimilar codeword $Y_{[i+(L/2)]\bmod L}$, and one similar codeword Y_i' which can be found through an exhaustive search of the codebook according to the Euclidean distance determined by the following equation:

$$d(Y_i, Y_i') = ||Y_i - Y_i'|| = \sqrt{\sum_{j=1}^{k} (y_{i,j} - y_{i,j}')^2} \quad (1)$$

where $y_{i,j}$ and $y_{i,j}'$ represent the jth elements of vectors Y_i and Y_i', respectively. And k represents the dimension of the vector. In this way, the relationships between the codewords are built up and the key-trees are constructed.

The original scheme is equipped with two encryption techniques. One is based on the static key-trees and the other is based on the dynamic key-trees. Fig. 2 shows the

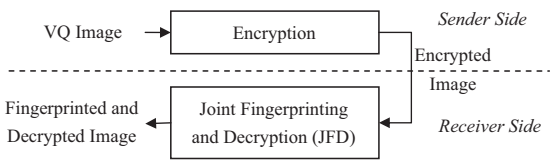

Fig. 1. A general illustration of the original scheme.

Fig. 2. The static key-trees based encryption.

static key-trees based encryption process in which the VQ blocks of the image is first permuted by Cat map, as shown in (2).

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p\times q+1 \end{bmatrix}^k \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \quad (2)$$

where (x_i, y_i) is the block position in the image, p, q and k are control parameters for permutation, which are regarded as secrets, and N is the number of blocks in a line or a row of the squared image. After permutation, the codeword Y_i of each block is replaced by $Y_{[i+(L/2)] \bmod L}$ to produce the encrypted image. With respect to the dynamic key-trees based encryption method, the permutation step is eliminated and the codeword Y_i of each block is replaced by $Y_{[i+(L/2)+k] \bmod L}$, where $k=H_{sk}(i) \bmod (L/4)$ is a random index generated by the session key sk, ranging from 0 to $\lfloor L/4 \rfloor - 1$.

To decrypt the image, the reversed codeword substitution is performed. To add fingerprint simultaneously, either Y_i or its similar codeword Y_i' is restored, which is determined by the embedding bit of the fingerprint. With respect to the static key-trees based approach, one needs an additional inverse permutation, as shown in Fig. 2. Clearly, the final fingerprinted and decrypted images of various users are different from each other, and they are all similar to the original image. By comparing with the original VQ image, the fingerprint embedded in the image can be extracted; therefore the traitor can be traced.

3. Attack on the original scheme

3.1. Replace the fingerprint arbitrarily of the fingerprinted and decrypted image

The fingerprint embedded in the image is crucial for traitor tracing. If the fingerprint of the illegally distributed image is removed, modified, or replaced by an innocent user's fingerprint, the traitor tracing would fail. In the original scheme, the bit of the fingerprint embedded in each block of the fingerprinted and decrypted image is indicated by the codeword. The pair of similar codewords Y_i and Y_i' are used to represent 0 and 1 embedded, respectively. Once one of the two codewords is known, the other one can be easily found through an exhaustive search of the codebook according to the Euclidean distance. The method to replace the fingerprint arbitrarily is described in detail below. It is noted that, according to Kerchoff's principle [17], the attacker knows everything about the cryptosystem except the secret keys.

Step 1: Collect the codewords to obtain the full codebook. Because the codebook is always invariant, all the codewords in the codebook can be collected from different VQ images. If the size of the codebook is known, one can easily obtain the full codebook.