J. Vis. Commun. Image R. 38 (2016) 858–871

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Secure multicasting of images via joint privacy-preserving fingerprinting, decryption, and authentication ☆

Chih-Yang Lin [a,b], Kahlil Muchtar [c], Chia-Hung Yeh [c,*], Chun-Shien Lu [d]

[a] Dept. of Bioinformatics and Medical Engineering, Asia University, Taichung, Taiwan
[b] Dept. of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan
[c] Dept. of Electrical Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan
[d] Institute of Information Science, Academia Sinica, Taipei, Taiwan

ARTICLE INFO

Article history:
Received 21 September 2015
Accepted 5 February 2016
Available online 11 February 2016

Keywords:
Authentication
Joint fingerprinting and decryption (JFD)
Privacy-preserving fingerprinting
Secret sharing
Multimedia distribution
Content integrity
Data encryption
Image authentication

ABSTRACT

Joint fingerprinting and decryption (JFD) is useful in securing media transmission and distribution in a multicasting environment. Common drawbacks of the existing JFD methods are the transmitted data may leak the content of data, and a subscriber cannot determine if a received image is modified such that tampering attack can be mounted successfully. Here we focus on security and privacy of image multicasting and introduce a new framework called JFDA (joint privacy-preserving fingerprinting, decryption, and authentication). It has several main characteristics, JFDA: (1) accomplishes fingerprinting in the encryption domain to preserve privacy and prevent encrypted data from being tampered without additional hash code/digest, (2) prevents tampering attack on the decrypted data to ensure the fidelity of the fingerprinted data, (3) makes user subscribing to a visual media be an examiner to authenticate the same visual media over the Internet. The effectiveness of the proposed method is confirmed by experimental results.

1. Introduction

In the scenario of a sender–receiver–user (w.r.t. source-proxy-destination) multimedia multicasting system, traditional encryption is a common way used to secure media transmission, but the protection capability is nullified after decryption. In order to solve this problem, fingerprint-based methods, in which all the fingerprinted copies of a medium are different but appear to have the same visual perception, have been extensively investigated [3,5,8,9,11,14,16–18,20]. If a fingerprinted copy is illegally distributed, the fingerprint extracted from it can be used to identify the corresponding user. Despite the fact that multicasting of multimedia data has been broadly studied [5,10,12,31], we focus in this paper on several aspects of security and privacy.

In general, there are two types of fingerprinting approaches: server-side fingerprinting and receiver-side fingerprinting. The latter is more practical since only one media stream is required to be disseminated to users in a multicast manner [16,30]. On the contrary, if server-side fingerprinting is used [5,11], the sender needs to consume a lot of bandwidth to send different copies to different users. Therefore, this paper focuses solely on receiver-side fingerprinting.

Here, a receiver can be the set top box or another device to perform the joint fingerprinting and decryption task on behalf of a specific user who subscribes to the content from the server and receives a fingerprinted copy decrypted by the receiver. In the threat model considered in this paper, a receiver is not ideally assumed to be reliable, an attacker may intrude to obtain decrypted data from a receiver or modify it, and data transmitted from the sender to a receiver may be intercepted or modified. We follow the general rules of the media fingerprinting framework under the application scenarios of media fingerprinting [12,28,31], where robustness (aiming to remove fingerprints via any possible attacks excluding the collusion) and blind detection of embedded fingerprints are not the major concerns. Moreover, the collusion attack pertaining to media fingerprinting at the receiver side has also been thoroughly investigated in [28,29,32]. Therefore, we focus on the threat model presented in this paper in order to distinguish our paper from the existing works.

1.1. Conventional receiver-side fingerprinting architectures

The main concerns with receiver-side fingerprinting are content leakage and tampering attacks. If the fingerprint is embedded after

☆ This paper has been recommended for acceptance by M.T. Sun.
* Corresponding author.
E-mail address: yeh@mail.ee.nsysu.edu.tw (C.-H. Yeh).

http://dx.doi.org/10.1016/j.jvcir.2016.02.003
1047-3203/

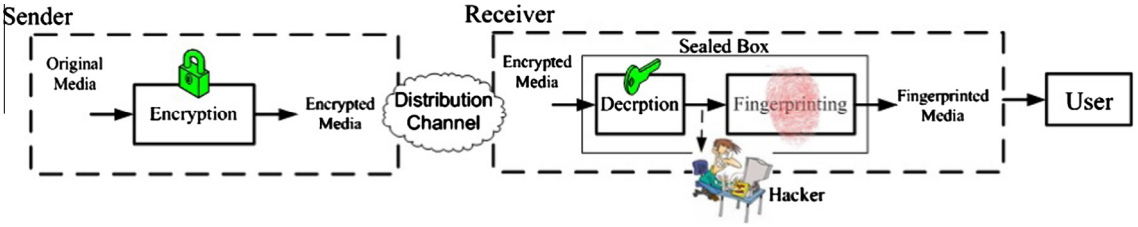

Fig. 1. Framework for receiver-side fingerprinting.

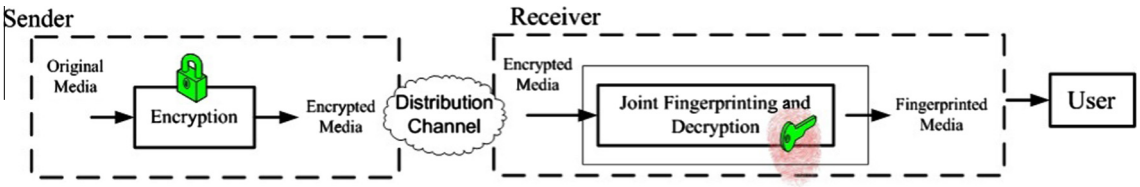

Fig. 2. The typical JFD framework.

the media stream is decrypted [20], as shown in Fig. 1, attackers gain the opportunity to obtain the decrypted data before being fingerprinted. Therefore, a conventional conception is that security entirely depends on the hardware design and the assumption that the sealed box cannot be cracked to avoid content leakage.

Recently, a new receiver-side fingerprinting framework, called joint fingerprint embedding and decryption (JFD) [1,2,6,13–15], as shown in Fig. 2, has received considerable attention as a possible solution to the secure transmission and traceable distribution problem. The JFD approach encrypts the media on the server side to secure media transmission, and decrypts and fingerprints the media simultaneously on the receiver side by way of using multiple decryption keys on behalf of users. Note that decrypting the same encrypted data with different decryption keys yields different fingerprinted data for traceable distribution. Anderson and Manifavas proposed the Chameleon method [2] following this concept by using a lookup table. The lookup table functions as the key generator from which the key can be used to encrypt the media data using XOR operations. The decryption process is identical to the encryption process except that the keys for the two processes involved are slightly different. More specifically, the corresponding least-significant bits of entries in lookup tables, which belong to encoding and decoding phases, respectively, are different. Therefore, the difference between the encryption and decryption keys draws the fingerprint of a user. Although Chameleon is easy to implement, it is vulnerable to image processing and collusion attack [6,16].

Later, Kundur and Karthik [14], inspired by the concept of Chameleon [2], proposed an alternative JFD method. In their method, the signs of significant DCT coefficients of an image are encrypted on the sender side, and are partially decrypted by the receiver to perform fingerprinting. The positions of the undeciphered coefficients in an image form the fingerprint of a user. Thus, different arrangements of these undeciphered coefficients determine different fingerprints for users. Kundur et al.'s method provides a good framework for JFD, but it is found to have difficulty in achieving the tradeoff between unintelligible encryption and transparent fingerprinted copies. An improved version of Kundur et al.'s method using perceptual models is proposed by Karthik and Hatzinakos [13] to achieve imperceptible fingerprinting by the receiver. However, in this sign bit plane encryption method, the choices of suitable AC coefficients without causing ringing artifacts are content dependent. That is, the selective bit positions in each block for partial decryption, which is related to the user's fingerprint, should be additionally transmitted to the receiver. These operations would increase computation and bandwidth consumption. Adelsbach et al. [1] extended Chameleon cipher to spread-spectrum watermarking. They also complemented the lack of security proof of Chameleon. Similarly, Lemma et al. [15] proposed a Chameleon-based JFD method using algebraic operations to achieve additive or multiplicative spread-spectrum watermarking. The processes of encryption and decryption are performed by means of different key streams, and each key stream has the same size as the media, leading to prohibitive transmission cost. A generalized version of Lemma et al.'s method has been proposed by Celik et al. [6] based on lookup table operations. In Celik et al.'s method, transmission cost is reduced, and an efficient fingerprint detection method and rigorous security proofs are provided. Lin et al. [17,18] proposed a JFD method based on vector quantization that performs two server-side encryption techniques. The aim of their method is to preserve image quality and resist to noise interference. Nevertheless, the drawback of this method is if the original image is lost or severely damaged, the fingerprint cannot be extracted and the tampered area cannot be identified. This led to the extension work as discussed in [19]. Recently, Czaplewski and Rykaczewski [9] presented a JFD method that utilizes a simple block cipher based on matrix multiplication to encrypt original images. In addition, an individual decryption keys approach is introduced to increase the robustness of proposed system. The above methods, however, still encounter some problems, which are discussed as follows.

1.2. Potential problems of conventional JFD methods and possible solutions

1.2.1. Problems

As shown in Fig. 3, there are two types of attackers over a JFD system: one can eavesdrop to obtain the transmitted encrypted data or tamper it, and the other is an intruder obtaining essential information from a receiver and can further modify not only the encrypted data but also the decrypted data. Since an attacker of the second type can obtain more information than the first type, we mainly focus on the unreliable receiver in the proposed method.

A successful *tampering attack on the encrypted data* means that malicious manipulation of the encrypted data would not cause significant damage to the decrypted data, as shown in Fig. 4. In Fig. 4, the sender sends the encrypted image to the receiver, but the