Journal of Information Security and Applications 41 (2018) 52–61

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Fingerprinting for multimedia content broadcasting system

Minoru Kuribayashi*, Nobuo Funabiki

Graduate School of Natural Science and Technology, 3-1-1, Tsushima-naka, Kita-ku, Okayama 700-8530, Japan

ARTICLE INFO

Article history:

Keywords:
Fingerprinting
Asymmetric property
Broadcasting
Time-bound key management

ABSTRACT

We investigated the traceability of illegal users to prevent illegal redistribution of pirated copies by adopting cryptographic and watermarking approaches. The former approach involves controlling the decryption key sequence issued to users, and the latter involves embedding fingerprint information into multimedia content. Since the cryptographic approach identifies illegal users from the decryption key sequence, a decrypted copy is not protected from illegal redistribution. The watermarking approach can trace illegal users if the fingerprint information is correctly extracted from a pirated copy. However, the transaction of legal distribution is one-to-one in conventional systems. In this paper, we propose a broadcast-type fingerprinting system by introducing a time-bound key management scheme based on the assumption that illegal users must financially compensate to the broadcaster for all content distributed during a certain period. In the proposed system, illegal users can be identified from the decryption key sequence issued to users as well as from pirated copies.

1. Introduction

Due to the development of services on the Internet, many users enjoy multimedia content by using streaming websites such as Youtube and Ustream. Different from video-on-demand services, broadcasting multimedia content has a large possibility for market due to its scalability for a large number of users on the system. On the other hand, violation of copyright and illegal redistribution must be strictly controlled.

1.1. Background

Cryptographic and watermarking approaches have been investigated to prevent illegal redistribution or reception. With the cryptographic approach, the idea is to control decryption keys issued to users to exclude non-authorized users from obtaining broadcasted content. It provides a convenient way to distribute content to users over an insecure broadcast channel, which allows a broadcaster to deliver to dynamically changing sets of users. The idea of broadcast encryption was introduced by Fiat and Naor [1], and an approach enabling tracing from the distinct key issued to each user was developed by Chor et al. [2]. The exclusion of a subset of users from receiving information may be required due to lack of payment, subscription expiration date, or leaking of the key. In broadcast encryption, a broadcaster can enforce conditional access by selectively encrypting content so that only the authorized users can decrypt it. The disadvantage is the impossibility of protection against illegal redistribution of decrypted content.

A simple solution to trace the rebroadcasting source is to embed fingerprint information indicating each user's identity by examining the fingerprint in a pirated copy. The dynamic traitor tracing scheme [3,4] allows a broadcaster to trace illegal users (hereafter, traitors) with a little sacrifice in bandwidth. The basic idea is to break time into consecutive intervals and modify the watermarking strategy of the broadcast system in each interval using the rebroadcasted content. After observing the rebroadcast for a long enough time, one or more traitors can be traced. However, this scheme is completely ineffective against delayed rebroadcast attack in which traitors rebroadcast the content with some delay. The sequential traitor tracing scheme [5] improves upon the dynamic scheme so that the channel feedback is only used for tracing, not for allocating watermarks to users. Although the sequential scheme can trace traitors from broadcasted content, a broadcaster cannot prove this fact to an arbiter. Because the broadcaster knows the content finally distributed to a user, he may attempt to frame an innocent user by distributing it himself. Therefore, an asymmetric property is required so that only the user can know the fingerprinted content being decrypted from broadcasted ciphertext.

The fingerprinting technique enables a seller to identify buyer(s) who redistribute unauthorized multimedia content by providing each buyer with slightly different content. The asymmetric property is achieved by using several cryptographic tech-

* Corresponding author.
E-mail addresses: kminoru@okayama-u.ac.jp (M. Kuribayashi), funabiki@okayama-u.ac.jp (N. Funabiki).

https://doi.org/10.1016/j.jisa.2018.06.002
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

niques. Most schemes [6–11] exploit homomorphic encryption schemes, such as the Paillier cryptosystem [12], and some schemes [13,14] use the commutative cryptosystem [15]. Because homomorphic encryption and commutative encryption are based on a public-key cryptosystem, the computational costs are too high. If the multimedia content is compressed before encryption, the watermark must be embedded into the compressed file to preserve the file format in the encrypted domain. In such a case, once the compressed file is transcoded, the extraction of the watermark becomes very difficult. Other schemes [10,16] introduce key management techniques to simply and efficiently satisfy the asymmetric property. With the scheme by Chu et al., the disadvantage is the difficulty in the renewal of keys issued to buyers [16], and the fingerprinting protocol is suitable for only one-to-one transaction with the scheme by Kuribayashi and Tanaka [10]. In [17,18], a peer-to-peer(P2P) network is considered to distribute multimedia content. An asymmetric fingerprinting protocol is performed between a merchant, a buyer and a set of P2P proxies in a presence of a trusted third party. Without the complexity of the management of trusted proxies, its distribution model is attractive in a sense of the efficient distribution over Internet.

1.2. Our contributions

The proposed broadcasting system is based on the following assumptions.

1. Once a traitor redistributes a pirated copy, he must financially compensate to a broadcaster for all content that will be broadcasted in a certain period.
2. A center is totally trusted.
3. The number of traitors is less than a certain threshold.

Under such assumptions, we developed a broadcasting system with the asymmetric property and traitor tracing capability from both decryption keys and redistributed content. The preliminary version of this paper was presented at IWDW2015 [19]. In this paper, we employ the authenticated encryption in the broadcasting phase so that uses can convince the success of decryption. The security, traceability, and computational costs are also considered in this version.

The proposed scheme is based on Kuribayashi and Tanaka [10] which introduces the idea of key management in a fingerprinting protocol. Its advantage is that it can use a symmetric cryptosystem and can compress watermarked content before encryption. Based upon the scheme in [10], we extend the scheme to one-to-many transaction, namely broadcasting. The proposed method introduces the concept of time-bound key management to reduce the cost of key management at the broadcaster. In addition, the concept of compensation in a certain period, the management costs are further reduced in the proposed method.

The basic idea of our system is to introduce a time-bound key management scheme into a fingerprinting technique so that a buyer key issued at a trusted center will be available before a certain expiration date. The expiration date is hierarchically designed based on the secret information issued to each buyer. As a result, each buyer receives multimedia content containing his fingerprint without increasing both the computational costs and amount of transmission data required for broadcasting.

The asymmetric property is satisfied by managing the decryption keys issued to buyers. In case of key leakage, it is possible to identify the buyers from the keys even if a coalition of buyers produces a new decryption key by combining the buyers' keys. With our system, once a pirated copy is detected, a traitor must pay compensation to the broadcaster for all content in a certain period even if he bought a license to receive the content for a shorter time period. Such a risk is expected to reduce the motivation of traitors to redistribute illegal copies.

1.3. Notations

$PRNG()$: pseudo-random number generator function
$\sigma_j(a,\ b)$: jth random permutation function which changes the order of bit-strings a and b
$OW()$: one-way function
$Enc()$: symmetric encryption function like AES (Advanced Encryption Standard)
$Dec()$: decryption function of $Enc()$
$Comp()$: compression function
$Decomp()$: decompression function
$Mac()$: message authentication code function
"$||$": concatenation
k_u: seller's secret key
k_s: broadcaster's secret key, called master key
$K_{[T_{start},T_{end}]}$: time-bound key with the expiration date $[T_{start}, T_{end}]$.
K_T: time-bound key at a time T
$\boldsymbol{key_u} = (key_{u,0}, key_{u,1}, \ldots, key_{u,L-1})$: buyer's secret key sequence
$\boldsymbol{w_u} = (w_{u,0}, w_{u,1}, \ldots, w_{u,L-1})$: jth buyer's fingerprint generated by a trusted center
$\boldsymbol{X} = (X_0, X_1, \ldots, X_{L-1})$: multimedia content
$X_j^{(b)}$: jth packet of $\boldsymbol{X}$ involving a watermark bit b
$\boldsymbol{k_s^\star} = \left(k^\star_{s,\bar{j}} = OW(PRNG(k_s), K_T) | 0 \le \bar{j} \le 2L-1\right)$: updated master key sequence
$\boldsymbol{key_u^\star} = \left(key^\star_{u,j} = OW(key_{u,j}, K_T) | 0 \le j \le L-1\right)$: updated buyer's secret key sequence
$c_j^{(b)}$: jth ciphertext of the packet $X_j^{(b)}$
$\tilde{c}_j^{(b)}$: jth ciphertext of the packet $X_j^{(b)}$ produced by authenticated encryption
TW: valid period of k_s and $\boldsymbol{key_u}$
$head$: header information file containing synchronization time

As enumerated above, parameters denoted by bold fonts represent a sequence. In the proposed broadcasting system, the valid period of k_s and $\boldsymbol{key_u}$ is TW.

1.4. Organization

The rest of this paper is organized as follows. In Section 2, we review related work and explain their drawbacks. In Section 3, we give details of the proposed system, and in Section 4, we discuss the security and traceability of our system and compare it with conventional systems. Finally, we conclude this paper in Section 5.

2. Related work

2.1. Broadcast encryption

In a broadcast encryption scheme, a broadcaster encrypts a message for a subset of buyers who have authorization to receive the message. Each buyer in a system has a unique decryption key; hence, it is possible to uniquely identify the buyer from the key. Considering collusion among some buyers, decryption keys should be designed in such a manner that a coalition of buyers outside of the subset cannot obtain any information about the content from the broadcasted ciphertext. If a broadcast encryption scheme satisfies such a requirement, it is said to be collusion resistant.

Broadcast encryption schemes were first formalized by Fiat and Naor [1], and traceability was introduced by Chor et al. [2], which enables a broadcaster to identify a traitor from illegally redistributed keys. Roughly speaking, a broadcaster first determines the