Efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors†

Chanjoo Chung*, Seungbok Choi*, Youngchul Choi**, Dongho Won*

* School of Electrical and Computer Engineering Sungkyunkwan University, Korea
  {cjchung, sbchoi, dhwon}@dosan.skku.ac.kr
** BCQRE Co., Ltd, Korea
  ycchoi@bcqre.com

Abstract. The proposed scheme by Domingo in Electronic Letters presented the first anonymous fingerprinting scheme in which help of a registration center is not required in order to identify redistributors. However, registration protocol of this scheme is 4-pass and identification process also required many exponential operations. In this paper, we propose more efficient protocol than the scheme by Domingo, which require 2-pass in registration protocol and need only 3+1 times exponential operation in identification process. In the electronic commerce of digital contents, registration protocol is more efficient than the previous scheme introduced. Moreover, computational complexity is diminished since identification process requires only 3+1 times exponential operations as the previous one requires 3+N/2 exponential operations. We now show efficient anonymous fingerprinting of electronic information with improved automatic identification of redistributors.

1. Introduction

Fingerprinting schemes do not prevent illegal copies; however, they do not deter people from illegally redistributing digital contents by enabling the original merchant of the contents to identify the original buyer of a redistributed copy. General methods of copyright protection previously proposed are to use the encryption and access control techniques. But those techniques are capable of illegal copying after acquisition of permission to the digital contents. The newly proposed method of copyright protection is copyright marking techniques. Copyright marking is the technique that an ownership information is embedded into digital contents to prevent illegal copies. Methods of copyright marking techniques are generally to use digital watermarking and digital fingerprinting techniques. Digital watermarking is the method which same authentication codes are embedded into same contents; whereas digital fingerprinting is different form it, in that different authentication codes are

† This paper is supported by Korea Science and Engineering Foundation(KOSEF) grant 97-01-00-13-01-5.

Springer-Verlag Berlin Heidelberg 2001
embedded into same contents. Since different authentication codes should identify redistributor of illegal copy.

The subordinate classification of digital fingerprinting is traitor tracing that provides identification with used keys. Traitor tracing techniques are to detect redistributor of used keys at an image decryption in broadcasting system such as pay-TV.

Before the emergence of computers, only physical fingerprinting had been studied and developed. With the increasing importance of digital contents, there is strong desire to use digital fingerprinting to protect intellectual properties, because it requires light-weight cryptographic capability but satisfies the purpose. Examples of digital contents to be fingerprinted include documents, images, movies, sounds and so on. Fingerprinting has a problem about collusions. Suppose digital contents are distributed with different fingerprints. If a collusion group that got those contents compare their copies, they can easily discover all the fingerprints. Therefore collusion group can remove these fingerprints, interpolate gaps, and resell the digital contents without worrying about being traced.

This problem of collusions was first discussed by Blakley et al. [2] and solution against larger collusions was presented by Boneh and Shaw [3]. Low and Maxemchuk [4] presented a collusion analysis in their model for general multiparty cryptographic protocols. Explicit collusion-tolerant constructions were given in [5, 6].

Traitor tracing is the equivalent of fingerprinting for cryptologic keys. It was introduced by Chor et al. [7] for broadcast encryption. For example, when digital movies are broadcasted in encrypted form, and only the decryption keys are sold, a different key is sold to each pay-TV subscriber. Furthermore, the encryption scheme is adapted so that all keys can be used to decrypt the same cipher-contents. Since decryption key is different for each subscriber, the pay-TV company can trace the redistributor who made illegal copies of his key. Naor et al. [8] introduced threshold traitor tracing a scheme. Boneh et al. [9] and Fiat et al. [10] introduced efficient public key and dynamic traitor tracing scheme.

Recently, several studies enhance the functionality of fingerprinting scheme in various ways. Asymmetric fingerprinting was introduced by Pfitzmann and Schunter [11]. Unlike conventional fingerprinting schemes, only the buyer of a fingerprinted object knows the contents with the fingerprints. When a merchant finds the illegal copy, he can nevertheless identify the buyer and prove to third parties that this buyer bought the copy from him. Pfitzmann [12] also proposed a traitor tracing scheme using asymmetric fingerprinting. Anonymous fingerprinting was introduced by Pfitzmann and Waidner [13] as an analogy of the blind signature for fingerprinting. It uses a trusted third party, called the registration center, to identify buyers suspected of behaving illegally. Thus the merchant is not able to identify him without help of the registration center. Coin-based anonymous fingerprinting was introduced by Pfitzmann and Sadeghi [14]. Automatic identifying redistributor when fingerprinted contents are illegally redistributed without help of the registration center was introduced by Domingo [1]. Figure 1 is presented by classification of copyright marking system [19].

The remainder of the paper is organized into the following sections: Section 2 describes the classification of fingerprinting techniques. Section 3 illustrates the requirement of digital fingerprinting system by contrary to digital watermarking