

Digital Fingerprinting Scheme with a Robust Anonymity and Asymmetry

Jae-Gwi Choi¹, Kouichi Sakurai², Ji-Hwan Park¹

1. Department of Information Security, Graduate School, Pukyong Nat'l Univ.

08-737. Dept. of Information Security, Pukyong Nat'l Univ., 599-1 Daeyeon-dong Nam-ku, Busan, Korea.

jae@{tcslab.csce.kyushu-u.ac.jp, mail1.pknu.ac.kr}

2. Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, Kyushu Univ.

812-8581. Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1. Hakozaki, Higashi-ku, Fukuoka-city, Japan.

Digital fingerprinting schemes are techniques applied to protect the copyright on digital contents. This is similar to digital watermarking, except that different information such as the user ID is embedded in each distributed digital contents. Thus every sold copy is slightly different from the original data item and unique to its buyer. In short, digital fingerprinting schemes are cryptographic methods applied to deter people from redistributing a data item by enabling the original merchant to trace a copy back to its original buyer.

Motivations:

However, the known digital fingerprinting schemes have the serious problems: the weak anonymity and the weak asymmetry. The first problem is that; when the second illegal distribution occurred, the merchant cannot get means that the buyer is a traitor. The second problem is that; if the registration center and the merchant collude, even if the buyer is honest, his/her real identity can be revoked. In previous works, a collusion of the merchant and the registration center can simply know the buyer's real identity by using the buyer's anonymous public key and certificate on it. It is undesirable matters in E-commerce.

Methodology:

Thus, what we need is "a robust anonymous asymmetric fingerprinting scheme". First, to achieve a robust asymmetry, we use multiple watermarking. We increase in embedding information by two. One is information for tracing a traitor, the other is thing for reliable evidence about redistribution. Thus upon finding a redistributed copy, the merchant can obtain means to prove to a third party that the buyer redistributed the copy. Next, we introduce secret sharing scheme in registration protocol in order to take a robust anonymity. So, in our proposal, the cooperation of more than a certain numbers of the registration centers (servers) is necessary for revelation of the buyer's real identity. Thus if the merchant want to know the buyer's real identity, he/she has to collude many registration centers (servers). As a result, our scheme diminishes the chances the merchant knows the buyer's identity.

Our Constructions:

In this paper, we addressed two shortcomings of the previous works. Added to this, we suggested an anonymous fingerprinting scheme with a robust anonymity and asymmetry. The two main objectives of this paper were: (1) to point out the serious problems of the previous schemes, (2) to propose solution ("digital fingerprinting scheme with a robust anonymity and a robust asymmetry) of the problems by using secret share schemes and multiple watermarking.