International Journal of Innovative Computing, Information and Control
Volume **6**, Number **3(B)**, March **2010**

ICIC International ©2010 ISSN 1349-4198
pp. **1271–1278**

EXPIRATION DATED FINGERPRINTING

Maki Yoshida and Toru Fujiwara

Graduate School of Information Science and Technology
Osaka University
1-5 Yamadaoka, Suita, Osaka 565-0871, Japan
{ maki-yos; fujiwara }@ist.osaka-u.ac.jp

Received December 2008; revised May 2009

Abstract. *This paper introduces a new anonymous fingerprinting scheme that keeps a buyer's privacy to be protected even after the copyright has expired. The proposed scheme allows buyers to obtain non-fingerprinted versions of any legally purchased digital goods when the copyright has expired. This means that all buyers can anonymously use legally purchased goods after they are in the public domain. In this sense, the new scheme enhances security in terms of buyer privacy.*
Keywords: Copyright protection, Privacy protection, Expiration of copyright, Anonymous fingerprinting

1. **Introduction.** Fingerprinting schemes are cryptographic methods of deterring people from illegally redistributing digital goods they have legally purchased [1, 3, 5, 10, 11, 12, 13]. The common feature of these schemes is that they enable the original merchant to identify the original buyer of a redistributed copy by providing all buyers with a slightly different version, called a fingerprinted version. Its difference to the original is called a fingerprint and represents information embedded in the content, which must be imperceptible. There are different classes of fingerprinting schemes, symmetric [1, 3], asymmetric [12] and anonymous [5, 10, 11, 13]. The anonymous class provides the most enhanced security as the schemes prevent a merchant from framing a buyer by making the fingerprinted version known only to the buyer; the schemes further protect buyers' privacy by preserving the anonymity of each buyer as long as she/he does not redistribute the purchased good.

Previous anonymous fingerprinting schemes preserve legal buyers' privacy for purchased goods after the copyright has expired unless no buyer wants to redistribute the purchased goods even after the copyright has expired. In general, once the copyright has expired, a buyer is allowed to freely use a purchased good. However, since the fingerprint remains, the original merchant can identify the original buyer of the redistributed good, i.e., the legal buyers' privacy is no longer protected. This might be a serious problem not only for the legal buyer but also for the merchant especially if the copyright will soon expire. In this case, potential buyers can wait for the expiration day to purchase the product and thereby protect their privacy. This means decrease of sales. Since privacy protection is one of the most important issues in information services [5, 6, 8, 10, 11, 13, 16], the anonymous fingerprinting scheme needs to be improved so that it can protect buyers' privacy even after copyright expiration. This is our motivation.

To solve the problem of buyers' privacy after copyright expiration, the merchant should allow buyers to obtain a non-fingerprinted version. In this case, the most important point is that all buyers obtain the same version, because a difference can be used as a fingerprint. So, the next question is how to convince buyers to receive the same version. A simple