Computers and Electrical Engineering 37 (2011) 526–531

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An ID-based digital watermarking protocol for copyright protection ☆

Peng Zeng [a], Zhenfu Cao [b,*], Kim-Kwang Raymond Choo [c]

[a] Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, PR China
[b] Department of Computer Science and Engineering, Shanghai Jiaotong University, PR China
[c] School of Computer and Information Science, University of South Australia, Australia

ARTICLE INFO

Article history:
Received 26 July 2010
Received in revised form 25 April 2011
Accepted 25 April 2011
Available online 24 May 2011

ABSTRACT

Digital watermarking techniques are a means of protecting the copyrights of digital contents. In this paper, we propose an identity-based (ID-based) digital watermarking protocol and point out several previously unpublished flaws in Hwang et al. (2005)'s scheme. We hope that by identifying the design flaws, similar structural mistakes can be avoided in future designs. We also claim that our proposed digital watermarking scheme can effectively solve the problem of multiple claims of ownership, and is suitable for any practical and secure watermarking algorithm.

1. Introduction

Digital watermarking schemes are designed to embed an imperceptible and generally encoded message (i.e. watermark) into a host digital content. Since the concept was first introduced, digital watermarking has been used in a wide variety of schemes to protect the intellectual property and copyright of still images, sound clips, and video streams [1–4]. We can broadly categorise digital watermarking schemes into *public* watermarking schemes, in which the watermark detection (or extraction) algorithms do not require the presence of the original digital work, and *private* watermarking schemes, in which the watermark detection algorithms require the original digital work as an input. Because of the inherent robustness of the latter scheme, significant research efforts have been devoted to designing imperceptible and private watermarking schemes.

In general, a practical and secure digital watermarking scheme should satisfy the following requirements:

- **Effectiveness**: The probability that an embedder will successfully embed a watermark in a randomly selected work should be high.
- **Imperceptibility**: The difference between the original work and the watermarked work should be imperceptible.
- **Robustness**: The watermarking scheme should have the ability to detect the watermark after common signal processing operations such as spatial filtering, lossy compression, printing, scaling, and geometric distortions.
- **Kerckhoffs principle**: The watermarking scheme should be secure even if everything about the system, except the watermark-key, is public knowledge.

Several watermarking schemes have been published in recent years (e.g. [5–17]). Although these schemes have been shown to be rather robust against lossy image compression, filtering, and scanning, etc, there are many unsolved problems. An example is how can we solve the problem of multiple claims of ownership [18]? Craver et al. [19] pointed out that several published watermarking techniques are not secure by demonstrating that counterfeit watermarking schemes can be

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author.
E-mail address: zfcao@cs.sjtu.edu.cn (Z. Cao).

0045-7906/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2011.04.014

performed on the target watermarked work, which results in multiple claims of ownership. To solve this problem, Hwang et al. [18] proposed a time-stamping protocol for digital watermarking in which the notion of a trusted third party (TTP) was introduced into the signing processing. Unfortunately, Chou et al. [20] showed that Hwang et al.'s scheme is vulnerable to an off-line guessing attack and proposed a fix. In this paper, we reveal previously unpublished flaws in Hwang et al.'s scheme, and hence show that both Hwang et al.'s and its predecessor are unable to efficiently solve the problem of multiple claims of ownership as claimed.

We propose a new digital watermarking protocol for copyright protection, which allows the rightful owner to generate the watermarked work with his/her watermark-key. A TTP will then generate a signature associated with the identity of the owner, timestamp of the watermarked work, watermark and original work. If multiple copyright ownership claims arise at a later stage, an arbiter can first verify the validity of data provided by each claimer. By comparing the timestamps, the arbiter can easily determine the rightful owner.

Organization of the paper as follows: In Section 2, we revisit the scheme proposed by Hwang et al. [18] and demonstrate some previously unpublished flaws in their scheme. Section 3 describes our proposed digital watermarking protocol. Section 4 concludes our paper.

2. Revisiting the work of Hwang et al.

In 2005, Hwang et al. [18] proposed a time-stamping protocol for digital watermarking where a TTP serves as a time-stamping service (TSS). We now describe the cryptographic notations.

- $E_K(M)$: symmetric encryption of message M using key K
- $D_K(C)$: symmetric decryption of ciphertext C using key K
- (P_I, S_I): public–private key pair of entity I where P_I denotes the public key of I and S_I denotes the private key of I
- $AE_{P_I}(M)$: asymmetric encryption of message M using public-key P_I
- $AD_{S_I}(C)$: asymmetric decryption of ciphertext C using private-key S_I
- $\mathrm{Sig}_{S_I}(M)$: signature of message M using private-key S_I
- $\mathrm{Ver}_{P_I}(s) = M$: verification of signature s of message M using public-key P_I
- H: one-way hash function

The signing phase of Huang et al.'s protocol is described in Fig. 1.

In the verifying phase, a notary verifies the validity of the two signatures s_1 and s_2:

$$\mathrm{Ver}_{P_{TSS}}(s_1) = (t, H(CX)) \quad \text{and} \quad \mathrm{Ver}_{P_{TSS}}(s_2) = (s_1, H(X_w)).$$

Hwang et al. claimed that their proposed protocol provides a solution to the problem of multiple claims of ownership. We pointed out that the protocol is unable to solve the problem of rightful ownership when implemented as it does not consider any distortion of X_w. It is a well-known fact that, in the world of watermarks, distortion is generally inevitable [7]. When a pirate obtains the watermarked work X_w, he/she can introduce his/her own watermark into X_w by running the protocol with TSS and obtain a perceptually similar version of X_w, say X'_w. Hence the pirate has the corresponding signatures s'_1 and s'_2 and claims ownership of X'_w (since s'_1 and s'_2 will verify true). Contrarily, the rightful owner will be deprived of his/her ownership of X'_w because

$$\mathrm{Ver}_{P_{TSS}}(s_2) \neq (s_1, H(X'_w)).$$

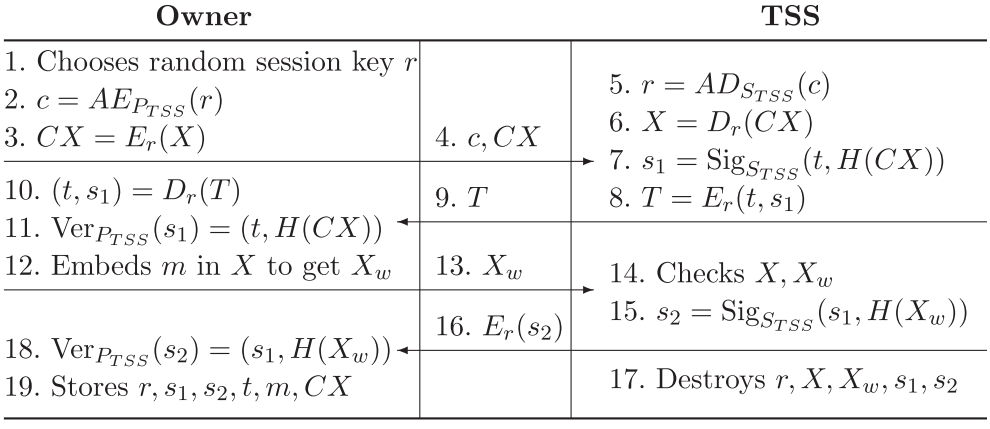

Fig. 1. The signing phase of Hwang et al.'s time-stamping protocol [18].