Available online at www.sciencedirect.com
SCIENCE DIRECT®
APPLIED MATHEMATICS AND COMPUTATION
ELSEVIER Applied Mathematics and Computation xxx (2004) xxx–xxx
www.elsevier.com/locate/amc

A time-stamping protocol for digital watermarking☆

Min-Shiang Hwang [a,*], Kuo-Feng Hwang [b], Chin-Chen Chang [c]

[a] *Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, ROC*
[b] *Department of Information Management, National Taichung Institute of Technology, 129 Section 3, San-min Road, Taichung 404, Taiwan, ROC*
[c] *Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, ROC*

Abstract

Digital watermarking techniques have recently been proposed for the copyright protection of digital media. Time-stamping is one technique used to ascertain at what time a certain digital medium was created or signed. In this paper, a new time-stamping protocol for digital watermarking is proposed that adds a time-stamp to digital watermarking algorithms through a trusted third party. The goals of the proposed protocol are (1) the trusted third party is not required to store any messages relating to the signed time-stamp, (2) it is suitable for all digital watermarking algorithms, and (3) it contains a time stamp that is impervious to forgery.

Keywords: Digital watermarks; Intellectual property; Copyright protection; Time-stamping.

☆ This research was partially supported by the National Science Council, Taiwan, ROC, under contract no.: NSC90-2213-E-324-004.
* Corresponding author.
E-mail address: mshwang@nchu.edu.tw (M.-S. Hwang).

0096-3003/$ - see front matter © 2004 Published by Elsevier Inc.
doi:10.1016/j.amc.2004.10.094

1. Introduction

Digital media has several advantages over analog media: (1) the quality of digital audio, images, and video is higher, (2) editing is easier, (3) copying is simpler, and (4) the media is easily transmitted over networked information systems. Since computer networks provide rapid and convenient communication, they have become the principal media for the distribution of information. Therefore, the problems associated with multimedia security and copyright protection have become important issues.

Time-stamping [2,7,14,15] is one technique used to ascertain whether a certain digital medium was created or signed at a certain time. Since digital media are reproduced easily, the rightful owner can use this technique to protect his copyright through verification of the earliest time stamp. Digital media, images, video, and audio all possess one characteristic that is distortion allowable. A pirate can utilize this characteristic by slightly modifying a rightful owner's digital medium. The modified medium can be totally different in digital data style while still possessing the original characteristics that makes it look/sound as if it has not been tampered. It is very difficult for anyone to recognize the difference using just the human eye/ear. Afterward the pirate can argue that he is the rightful copyright owner of that medium. A time-stamped message on a different data stream that produced a similar looking image could not be used as evidence in court.

Digital watermarking techniques have been proposed in recent years as another technique for digital media copyright protection [3,4,11,13,16,18,21]. A digital watermarking technique is a technique that embeds invisible/visible watermarks into a host digital media stream. Of the proposed schemes, the majority address invisible watermarking techniques. The watermarks must be designed to be unrecognizable by unauthorized individuals and easily identified by the legal copyright owner of the medium. In order to create a practical digital security scheme, the digital watermarking technique must satisfy the following requirements:

1. The quality of the watermarked image must be very high. In another words, if the original image is modified by the embedded watermark, the modification should be perceptually invisible.
2. As for cryptography, the security of the algorithm cannot be based upon the assumption that possible attackers do not know how the watermark was embedded into the host media.
3. Only the copyright owner be able to detect or remove the watermark from the image, so that even if the attacker knows how the watermark was embedded, he still cannot remove it.
4. It must be possible to retrieve the watermark after multiple and varied image processes, such as low-pass filtering, high-pass filtering, lossy compression,

scaling, format change, color quantization, etc. The premise behind this is that the quality of the altered watermarked image must be immutable.

However, there are still many unsolved problems. One, as pointed out by Craver et al. from IBM [6], is how to resolve the rightful ownership of the invisible watermarking schemes. Craver et al. attacked existing watermarking techniques by proving that counterfeit watermarking schemes can be performed on a watermarked medium to allow multiple claims of ownership. Furthermore, in order to resolve this problem, Craver et al. proposed a watermarking scheme based on the concept of non-invertibility. Unfortunately, their scheme cannot be proven to be non-invertible. Until now, most proposed digital watermarking schemes involved only the owner's information, i.e., the company's logo, uniform commercial code, or personal ID. Furthermore, the owner had complete control over the watermark embedding process and its verification, which is why Craver et. al. could create the problem of counterfeit digital water-marking.

In order to provide proper copyright protection, a trusted third party should be introduced into the watermark embedding process. In this paper, a new time-stamping protocol for digital watermarking is proposed. This protocol adds a time-stamp to digital watermarking algorithms through a trusted third party. The problem, as mentioned above, could be solved by comparing whose time-stamp in the watermark occurred earlier. The goals of the proposed protocol are described as follows:

1. The trusted third party is not required to store any messages relating to the signed time-stamp.
2. This protocol must be suitable for all digital watermarking techniques. In another words, it must be independent of all watermarking algorithms.
3. The time-stamp must be impervious to forgery.
4. The original medium X must be kept secret during the verification phase.

The rest of this paper is organized as follows. Section 2 reviews some digital watermarking and digital time-stamping schemes. We propose a new time-stamping process for a digital watermarking protocol in Section 3. The security analysis of the proposed time-stamping protocol is described in Section 4. Section 5 presents discussions and Section 6 presents the conclusions of our research.

2. Related work

In this section, the related work in the areas of digital watermarking and time-stamping are introduced. More information about digital watermarking can be found in [5,9,10,21,23].

Swanson et. al. [22] proposed a watermarking process for audio. Its robustness to noise addition, compression and re-sampling is analyzed. Langelaar et al. [17] proposed two digital watermarking schemes for digital images. Kutter et al. [16] proposed a watermarking scheme for color images, which embedded a watermark into the Blue-channel. These three watermarking techniques only focus on digital images.

Hartung and Girod [8] proposed a watermarking scheme using a direct sequence spread spectrum technique which can embed watermarks into both uncompressed and compressed video sequences. Linnartz and Talstra [19] presented a watermarking system for MPEG video based on the asymmetry and complexity between encoding a frame as a particular picture type versus detecting that picture type.

As mentioned above, there is not one watermarking technique suitable for all types of digital media. If a time-stamping protocol existed that was applicable to all watermarking schemes, the watermarking algorithm design process could focus upon improving the robustness and reducing the complexity of the watermarking algorithm.

Digital media does not seal its moment of creation in time. In another words, the actual time that a digital media was created cannot be obtained by examining the data in the digital media. Time-stamping is one technique that can be used to ascertain whether a certain digital medium was created or signed at a certain time. Haber and Stornetta [7] proposed linking a time-stamping protocol with a trusted third party such as a Time-stamping service (TSS), who signs the current time t_n to the nth submitted document X_n as

$$s = \mathrm{sig}_{\mathrm{TSS}}(n, t_n, \mathrm{ID}_n, X_n, L_n),$$

where t_n is the current time, ID_n is the identity of the submitter, and L_n is the linking information. L_n is defined as

$$L_n = (t_{n-1}, \mathrm{ID}_{n-1}, X_{n-1}, H(L_{n-1})),$$

where $H()$ is a one-way hash function. This scheme has some complications with regards to practical implementation. First, the TSS must store each value for L_n. However, it's time consuming to verify the signed time-stamp s. For more information and improved schemes, please refer to [1,2].

3. Time-stamping protocol for watermarking

In this section, a new time-stamping protocol for digital watermarking is proposed. This scheme is based upon mixed asymmetric and symmetric cryptosystems. The main goal of our method is to design a time-stamping protocol that is applicable to all watermarking algorithms.

The new watermarking time-stamping scheme consists of the following two basic stages: signing the time-stamp in the watermark and verifying the time-stamp. In the signing phase, a digest of the host media is calculated using one-way hash functions. Next, the owner sends the digest to TSS, and TSS appends a signed time-stamp for the submitter using the private key of TSS. Finally, the owner initiates the watermarking algorithm to embed the time-stamped watermark. The key point of the proposed protocol is the watermarking algorithm secret key involved in the time-stamp signed by TSS. Afterward, in the time-stamping verification phase, someone else can use the TSS public key to validate that the watermark was embedded at a certain time.

The system is initialized by each participant having a pair of keys—a public key P_u and a private key S_u for user u. All participants must be authenticated by a trusted certification authority (CA). A public one-way hash function $H()$ is known by all participants. The owner of the original host media X has a random session key r that is used in symmetrical cryptosystems during each service request made to TSS. Furthermore, it is assumed that TSS is also a trusted third party. Consequently, CA and TSS might be the same party. The detailed procedures for our watermarking time-stamping protocol in the signing phase are presented as follows (refer Fig. 1):

1. Two secret values c and CX are obtained using the following process:

$$c = rP_{\mathrm{TSS}},$$
$$CX = \{X\}r.$$

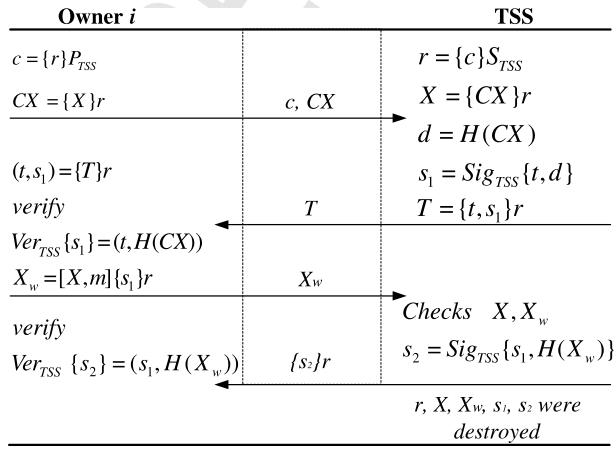

Fig. 1. Time-stamping protocol for watermarking.

The owner i randomly chooses a random number r and computes the ciphered session key c. Here c is encrypted r by the public key of TSS and CX is encrypted by the session key r using a symmetrical cryptosystems.

2. (c, CX) is sent to TSS. Because the session key r was encrypted using TSS's public key, TSS can obtain r from c by using the private key S_{TSS}. TSS decrypts c and CX as follows:

$$r = \{c\}S_{\mathrm{TSS}},$$
$$X = \{CX\}r.$$

3. Before the time-stamp s_1 is signed the following process is used:

$$s_1 = \mathrm{sig}_{\mathrm{TSS}}\{t, H(CX)\},$$
$$T = \{t, s_1\}r,$$

where t is the current time, s_1 is the signed time-stamp using the private key of TSS, and T is the encrypted time-stamp using session key r. After that, TSS sends the signed time-stamp T to the owner.

4. After the owner i receives T, the current time t and the signed time-stamp s_1 can be obtained using the session key r. Before embedding the watermark, the time-stamp s_1 must be verified by first checking to see if the current time t is correct. Then, the time-stamp s_1 is validated if the following equation is established

$$\mathrm{Ver}_{\mathrm{TSS}}\{s_1\} = (t, H(CX)). \tag{1}$$

5. The owner's watermark m is embedded to get a watermarked medium X_{w} using the correct watermarking algorithm. The secret key used in the watermarking algorithm is $\{s_1\}r$. X_{w} is obtained by

$$X_{\mathrm{w}} = [X, m]\{s_1\}r.$$

6. The owner i sends $\{X_{\mathrm{w}}\}$r to TSS, TSS checks to verify that the X_{w} has been constructed from X. First, TSS checks to see if the value of PSNR is reasonable between X_{w} and X. Second, TSS can use $\{s_1\}r$ to retrieve the watermark m from X_{w}. If X_{w} is validated, the time-stamp s_2 is obtained by computing

$$s_2 = \mathrm{sig}_{\mathrm{TSS}}\{(s_1, H(X_{\mathrm{w}}))\}.$$

TSS sends $\{s_2\}r$ to the owner i and destroys X, r, s_1, s_2 and X_{w}.

7. Then the owner i receives S_2 using session key r. The time-stamp s_2 is validated if the following equation is established:

$$\mathrm{Ver}_{\mathrm{TSS}}\{s_2\} = (s_1, H(X_{\mathrm{w}})). \tag{2}$$

After that, the time-stamp watermark signing phase is complete.

Note that, the time-stamps s_1, s_2, and the session key r must be kept by the owner. The time-stamping verification procedures are described as follows:

1. A notary Ψ requests that the owner i verify the time-stamp of a medium X_w.
2. The owner i sends (t, s_1, s_2, CX) to notary Ψ.
3. Ψ checks the time-stamps s_1 and s_2 using Eqs. (1) and (2).

The time-stamp verification phase is completed after Eqs. (1) and (2) are established.

4. Security analysis

In the proposed watermarking time-stamping protocol, a session key r is randomly selected by the owner i. The session key r is encrypted as c using the public key of TSS, P_{TSS}. TSS is the only one who can decrypt c to get r. All messages transmitted between the owner i and TSS are encrypted using session key r. Therefore, the original host medium X, watermarked medium W_w, and time-stamps s_1, s_2 are protected against forgery.

According to the assumptions of one-way hash functions [12,20], the signed time-stamps s_1 and s_2 cannot be forged even though the signing time t, original host medium X, and watermarked medium X_w are known by the owner i. Since the original host medium X is encrypted during the verification phase, X is always kept secret by the owner. The owner i may use s_1 to embed the watermark into another host medium X' and attempt to get a forged time-stamp s_2 for X'. However, this is impossible because the relationship between X and X_w will be checked by TSS. Furthermore, the signed time-stamp s_2 is embedded into the time-stamp s_1. Hence, the time-stamp s_2 cannot be forged from s_1. To verify the time-stamps s_1 and s_2, the signing time t, encrypted original medium CX, and watermarked medium X_w are needed. The watermark m was certified as embedded at a certain time t, if the time-stamps s_1 and s_2 is authenticated after Eqs. (1) and (2) were examined by the verifier. Not only the secret key $\{s_1\}r$ of the watermarking algorithm kept secret, but also the original host medium X is still kept secret by its owner.

TSS checks to see if the X_w is really constructed from X to decide if the time-stamp will be signed s_2. PSNR (Peak Signal-to-Noise Ratio) is the first rule for checking this relationship. As mentioned in Section 1, the quality of the watermarked medium must be immutable. The reasonable value of PSNR must be greater than or equal to 27 for high quality. Watermarking algorithms must be subject to opening, which is one of the requirements of digital watermarking techniques. The secondary rule for checking X_w is using $\{s_1\}r$ to retrieve the watermark m' using the correct watermarking algorithm. The watermarked medium X_w is checked to confirm that m' definitely belongs to the owner i. Therefore, the watermarked medium X_w cannot be forged by the owner. Consequently, the watermark was embedded at a certain time t which can be certified by verifying the time-stamps s_1 and s_2.

5. Discussions

TSS does not store any information about the submitting medium after the time-stamp signing phase. This is valuable in reducing the space requirement for TSS and does not affect the verification of the signed time-stamp. TSS has no responsibility to insure that the signed medium actually belongs to the submitter. TSS is only responsible for the signed time-stamp in the proposed watermarking time-stamping protocol. In order to confirm the rightful owner of the watermarked medium, digital watermarking algorithms require a secret key which is selected by the rightful owner. The watermarking algorithm secret key uses the signed time-stamp, however, the watermarking algorithms are not affected by other processes in the proposed protocol. Consequently, the proposed watermarking time-stamping protocol is independent of the watermarking algorithms.

The secondary rule is to check the watermarked medium whether or not involves the correct watermark done by TSS. There is another approach for examining a watermarked medium. TSS can use the original medium X, secret key $\{s_1\}r$, and watermark m of the submitter to construct the watermarked medium X_w using the correct watermarking algorithm. Nevertheless, TSS can choose the better performer among these two approaches.

6. Conclusions

In this paper, a new time-stamping protocol for digital watermarking has been proposed. This protocol adds a time-stamp to digital watermarking algorithms through a trusted-third party. The proposed time-stamping protocol achieves the following goals: (1) the trusted-third party is not required to store any information about the signed time-stamp, (2) this protocol is suitable for all digital watermarking algorithms, (3) the time-stamp cannot be forged, and (4) the original medium X is kept secret even during the verification phase.

References

[1] A. Buldas, P. Laud, New linking schemes for digital time-stamping, in: International Conference on Information Security and Cryptology—ICISC'98, 1998.
[2] A. Buldas, P. Laud, H. Lipmaa, J. Villemson, Time-stamping with binary linking schemes, in: Advances in Cryptology—CRYPTO'98, 1998, pp. 486–501.
[3] C.-C. Chang, K.-F. Hwang, M.-S. Hwang, A digital watermarking scheme using human visual effects, Informatica: An International Journal of Computing and Informatics 24 (4) (2000) 505–511.
[4] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) (1997) 1673–1687.

[5] Ingemar J. Cox, M.L. Miller, A.L. McKellips, Watermarking as communications with side information, Proceedings of the IEEE 87 (7) (1999) 1127–1141.
[6] S. Craver, N. Memon, B.-L. Yeo, M.M. Yeung, Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications, IEEE Journal on Selected Areas in Communications 16 (4) (1998) 573–586.
[7] S. Haber, W.S. Stornetta, How to time-stamping, Journal of Cryptology 3 (2) (1991) 99–111.
[8] F. Hartung, B. Girod, Watermarking of MPEG-2 encoded video without decoding and re-encoding, Signal Processing 66 (3) (1998) 283–301.
[9] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proceedings of The IEEE 87 (7) (1999) 1079–1107.
[10] J.R. Hernandez, F. Perez-Gonzalez, Statistical analysis of watermarking schemes for copyright protection of images, Proceedings of the IEEE 87 (7) (1999) 1142–1166.
[11] H.C. Huang, F.H. Wang, J.S. Pan, A VQ-based robust multi-watermarking algorithm, IEICE Transactions on Fundamental E85-A (7) (2002) 1719–1726.
[12] M.-S. Hwang, C.-C. Chang, K.-F. Hwang, A watermarking technique based on one-way hash functions, IEEE Transactions on Consumer Electronics 45 (2) (1999) 286–294.
[13] M.-S. Hwang, C.-C. Chang, K.-F. Hwang, Digital watermarking of images using neural networks, Journal of Electronic Imaging 9 (4) (2000) 548–555.
[14] M.-S. Hwang, E.J.-L. Lu, I.-C. Lin, Adding timestamps to the secure electronic auction protocol, Data and Knowledge Engineering 40 (2) (2002) 155–162.
[15] M.-S. Hwang, W.-G. Tzeng, W.-P. Yang, An access control scheme based on Chinese remainder theorem and time stamp concept, Computers and Security 15 (1) (1996) 73–81.
[16] M. Kutter, F. Jordan, F. Bossen, Digital watermarking of color images using amplitude modulation, Journal of Electronic Imaging 7 (2) (1998) 326–332.
[17] G.C. Langelaar, J.C.A. Lubbe, R.L. Lagendijk, Robust labeling methods for copy protection of images, in: Proceedings of SPIE Electronic Images, '97, pp. 298–309, San Jose, CA, February 1997.
[18] W.B. Lee, T.H. Chen, A public verifiable copy protection technique for still images, Journal of Systems and Software 87 (3) (2002) 195–204.
[19] J.P.M.G. Linnartz, J.C. Talstra, MPEG PTY-marks: cheap detection of embedded copyright data in DVD-video, in: Fifth European Symposium on Research in Computer Security, ESORICS'98, September 1998, pp. 221–240.
[20] R.C. Merkle, One-way hash functions and DES, in: Advances in Cryptology, CRYPTO'89, Lecture Notes in Computer Science, vol. 435, 1989, pp. 428–446.
[21] M.D. Swanson, M. Kobayashi, A.H. Tewfik, Multimedia data-embedding and watermarking technologies, Proceedings of IEEE 86 (6) (1998) 1064–1087.
[22] M.D. Swanson, B. Zhu, A.H. Tewfik, L. Boney, Robust audio watermarking using perceptual masking, Signal Processing 66 (3) (1998) 337–355.
[23] R.B. Wolfgang, C.I. Podilchuk, E.J. Delp, Perceptual watermarks for digital images and video, Proceedings of the IEEE 87 (7) (1999) 1108–1126.