Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 1640 – 1644

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Asymmetric Watermarking Scheme Based on Shuffling

Yong-Gang Fu*

College of Computer Engineering, Jimei University, Xiamen, China, 361021

Abstract

In this paper, a novel asymmetric watermarking scheme is proposed. Both the user side watermark and copyright owner's one are generated from the copyright owner's private keys, and the watermark detection can be finished either by public watermark or the copyright owner's private one. Given the public watermark, it is impossible to guess or remove the embedded watermark. Performance of the proposed scheme is studied and the experimental results against removal attack and Jpeg compression show good robustness of proposed scheme.

Key words: Asymmetric watermarking, Digital watermarking, Removal attacks

1. Introduction

It is commonly assumed that digital watermarking is only one of several measures that have to be combined to build a good copy protection mechanism [1]. One particular problem with state-of-the-art watermarking schemes is that they are symmetric. The keys necessary for watermark embedding and detection are identical. It implies that whoever allowed detecting the watermark gets to know the parameters that can also be used to remove it. Thus, the watermark detector knows all critical parameter of the watermarking scheme that also allows efficient removal of the embedded watermark.

However, cheap tamper-proof devices are hardly producible [1], and thus, pirates can obtain the private key from such devices and use them to outwit the copy protection mechanism. A solution to this problem is the asymmetric scheme that uses two different keys for encoding and decoding as in cryptography. Recently, a number of papers on asymmetric watermarking method have been proposed [2]–[6]. Asymmetric watermarking is based on a one way relationship between the embedding (secret) key and the detection (asymmetric) key. A central issue in asymmetric watermarking scheme is the design of a detector that will not reveal sufficient information that leads to the erasure of the embedded

*Corresponding author. Tel.: +86-018950182770
E-mail address: yonggangfu@jmu.edu.cn.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.01.187

watermark, even if the pirates knows the detection algorithm and the public detection keys. It is a big challenge for design a asymmetric watermarking scheme, because revealing too much information implies the risk that hacker is able to remove the mark, whereas not revealing too much information implies less reliable detection. For this reason, we would like to develop a watermarking scheme where the watermark detection is possible with a public key that does not give enough information to impair the embedded watermark.

The asymmetric watermarking schemes proposed up to now can be classified into two categories. One is watermark characteristics based method, using watermarks signals which have special characteristics such as periodicity [2,3]. The other is transform based method to make a detection key from a given embedding key by a proper transform [6-9,11]. Some nice reviews on asymmetric watermarking schemes can be found in[7,9]. Our proposed scheme in the following belongs to the second category. The public key is generated from the embedding key by a proper one transform.

The paper is organized as follows: section 2 describes the proposed embedding and detection scheme; some robustness analyses are exhibited in section 3; sections 4 gives experimental results and the conclusion is drawn in section 5.

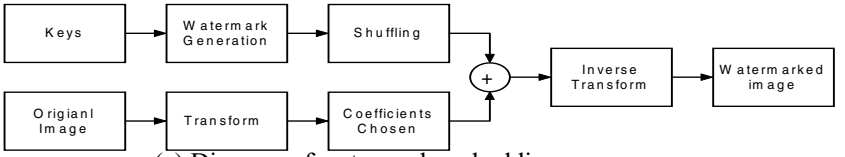
2. The Proposed Scheme.

In asymmetric watermarking scheme, for the embedded watermark to be detected by the usual correlation test, the reference watermark of the detector and the embedded watermarks should have some correlation. There exist numerous ways to generate signals that are different from each other, but have a fixed correlation with a given reference watermark. Hyuk et al[6] proposed a transformed key based method to generate the public key; J.Picard[7] introduced neural networks for the generation of the public detection. In this paper a simple and effective public key watermarking scheme is proposed, in which two shuffled versions of the same watermark are all generated from the copyright owner's private key, only the copyright owner's one is embedded into the host signal. The detection process can be finished by either public or private watermark.

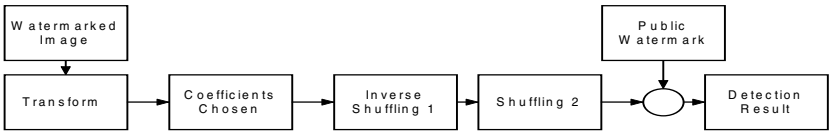
The block diagram of proposed embedding and detection are shown in Fig.1(a) and Fig.1(b) respectively. The embedding procedure can be depicted as following four steps:

1)The host data, such as image or video, is firstly transformed by conventional transforms, such as discrete cosine transform, then the DC coefficients are left unused since its modification may cause great artifacts. After the proper embedding positions are chosen, the transformed coefficients are reorganized into a line order. This leads to a vector has zero mean, which is denoted as: $\vec{C} = \{c(1), c(1), ..., c(M)\}$, where M is the watermark length.

2) Two key groups, $K_1 = \{k, k_1, k_2\}$ and $K_2 = \{k_3, k_4\}$ are chosen by the copyright owner, where k, k_1 and k_3 are arbitrary integers, k_2 and k_4 are integers within the interval $[M/3, 2M/3]$ and are



(a) Diagram of watermark embedding



(b) Diagram of watermark detection

Fig.1 System Block Diagram

prime to M at the same time.

Define $f_1(i) = ((k_1 + k_2 i) \bmod M) + 1$, *and* $f_2(i) = ((k_3 + k_4 i) \bmod M) + 1, \quad i = 1,2,.....,M$. *One can see it clearly that these two mappings* $i \mapsto f_1(i)$ *and* $i \mapsto f_2(i)$ *are one to one, the inverse transform corresponding to* f_1 *is denoted as* f_1^{-1}.

3) The original watermark signal $\vec{W} = \{w(1), w(2),..., w(M)\}$ is generated with zero mean and variance σ_w^2 by copyright owner's key k, which needs to be i.i.d and independent of the original host signal $\vec{C}$. Then two watermarks for the copyright owner and the user are respectively generated as follows:

$$\vec{W}_o = \{w_o(1), w_o(2),..., w_o(M)\} = \{w(f_1(1)), w(f_1(2)),..., w(f_1(M))\}$$

$$\vec{W}_u = \{w_u(1), w_u(2),..., w_u(M)\} = \{w(f_2(1)), w(f_2(2)),..., w(f_2(M))\}.$$

4) The watermark is embedded into the host signal according to the following manner:

$$c'(i) = c(i) + \alpha w_o(i), \ i = 1,2,....,M,$$

where α is a constant parameter to control the compromise between the watermark transparency and robustness. Then the watermarked coefficients together with the DC coefficients are reordered into the original two dimension form, and the watermarked signal is reached by the corresponding inverse transform.

In the detector side, both the original signal and the original watermark are not necessary for the watermark detection. Firstly, the host content is transformed into its transform domain, and the proper embedding positions are selected, then selected transformed coefficients are reorganized into a line order, which is denoted as: $\hat{C} = \{\hat{c}(1), \hat{c}(1),....,\hat{c}(M)\}$. Here we should note that these coefficients may undergo some attacks such as filtering, distortions and so on.

Using the given public watermark, W_u, the following correlation parameter is firstly computed:

$$corr = \frac{1}{M}\sum_{i=1}^{M} \hat{c}(f_1^{-1}(f_2(i)))w_u(i)$$

And then the mean value of *corr* can be obtained as follows:

$$E(corr) = E\{\frac{1}{M}\sum_{i=1}^{M} \hat{c}(f_1^{-1}(f_2(i)))w_u(i)\} = E\{\frac{1}{M}\sum_{i=1}^{M} [c(f_1^{-1}(f_2(i))) + \alpha w_o(f_1^{-1}(f_2(i)))]w_u(i)\}$$
$$= E\{\frac{1}{M}\sum_{i=1}^{M} [c(f_1^{-1}(f_2(i))) + \alpha w_u(i)]w_u(i)\}$$

Since $\vec{W}_u$ is independent of $\vec{C}$, $E\{\frac{1}{M}\sum_{i=1}^{M} c(f_1^{-1}(f_2(i)))w_u(i)\} = 0$. When the watermark is present, multiplicity between α and the watermark energy is equal to the expectation of corr, i.e. $E(corr) = \alpha\sigma_w^2$. When there is no watermark embedded, the expectation of the corr must be equal to zero.

After we set the threshold T between 0 and $\alpha\sigma_w^2$, the watermark detection is finished by the comparison between the absolute value of corr and the threshold. Commonly we use the threshold $T = \alpha\sigma_w^2 / 2$. When $corr$ is greater than T, a watermark decision is made, otherwise, the host is not watermarked.

3. Simulation results.

The proposed scheme can be applied to protect any properties including image, video, audio and so on against removal attacks. In our experiment, the watermark is embedded into the DCT domain of images to test the performance of our scheme.

The tested image is classical Lena gray image with 512×512 pixels. And the watermark embedding strength α is set to 1. The image is firstly segmented into 8×8 blocks with 64*64=4096 blocks, which is in accordance with the Jpeg compression standard. And then each block is undergone discrete cosine transforms to reach the transformed coefficients. Next the DC coefficients are left unmodified and select

the middle frequency coefficients at position (1,2) and (2,1) from each block as host signal. Finally the selected coefficients are reorganized into line order and the watermark is embedded. The watermarked image is reached after the inverse DCT.

The detector response vs the watermark energy and the result is shown in Table 1. The false-positive and false-negative errors can be effectively avoided with larger watermark energy. But too strong watermark may cause detectable artifacts. So we have to get a compromise between detection errors and the host quality. Here watermark energy is 80 for good robustness of the watermark and the visual quality.

It is difficult to remove the private watermark if he doesn't know the keys. As to the public watermark

Table 1 Detection responses $corr / \sigma_w^2$ against different watermark energy

Watermark energy	PSNR (dB)	Public detection with wrong reference		Public detection with right reference		Private detection	
		Variance	Mean	Variance	Mean	Variance	Mean
10	53.18	0.0657	0.0018	0.0634	1.0680	0.0634	1.0680
40	47.17	0.0165	0.0011	0.0158	1.0542	0.0158	1.0542
80	44.15	0.0083	8.51E-4	0.0079	1.0185	0.0079	1.0185
160	41.14	0.0042	6.99E-4	0.0041	1.0310	0.0041	1.0310
400	37.16	0.0017	5.50E-4	0.0016	0.9843	0.0016	0.9843
600	35.40	0.0012	5.16E-4	0.0011	1.0103	0.0011	1.0103

holder, the attacker may try to eliminate the watermark by successive subtraction of the user watermark or the pirates try to deceive the public detection into believing that another watermark is embedded in the work. Fig.2 (a)(b) exhibit the private and public detector responses without any attacks respectively. Fig.2 (c) shows the public watermark detector response when the watermarked image is attacked by removal

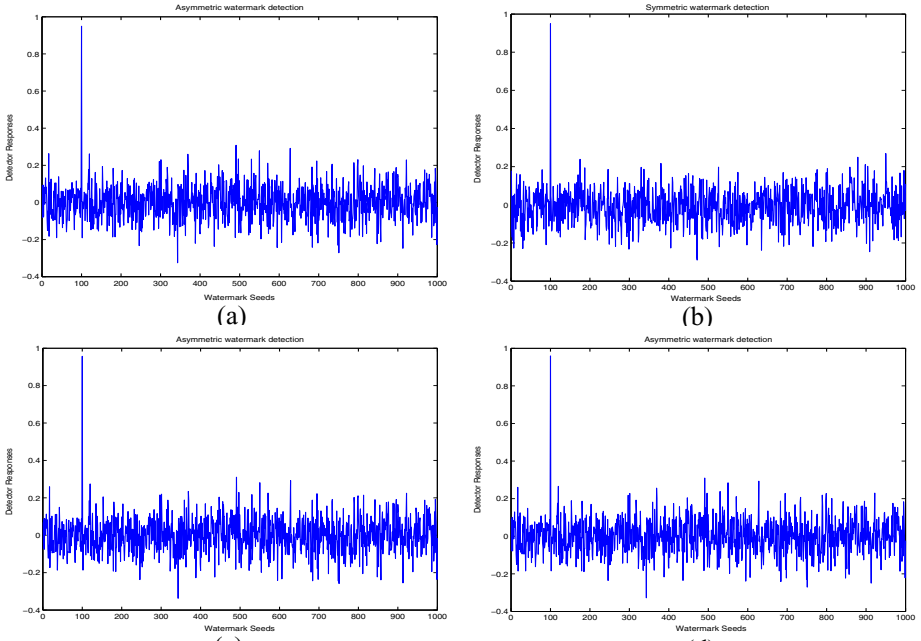


Fig.2 (a) Public detector responses; (b) Private detector response; (c) Public detector responses after removal attack; (d) Public detector responses after Jpeg compression

attack with subtraction the public watermark with the same watermark energy as embedded. The public watermark detector responses corresponding to the Jpeg compressed image with quality factor 50 is shown in Fig.2(d). From the two detector responses figure under these attacks, it can be found that the detector responses can not be weakened. We also tested the watermark under Jpeg compressions, the watermark can still be detected in the image compressed at the quality factor 8 with conventional threshold. It cannot confuse the dominance of the watermark even when the user knows the public watermark.

4. Conclusions

A novel asymmetric key watermarking scheme that has a private watermark and a public watermark is proposed. Since the private one is difficult to guess from the public one, the watermarking scheme is robust against the removal attack. The experimental results show good robustness of our proposed scheme.

Acknowledgement

This work is partially supported by the Foundation of Xiamen Science Project (No.3502Z20075054) and the Foundation for Young Professors of Jimei University

References

[1] T. Furon and P. Duhamel. Copy Protection of Distributed Contents: An Application of Watermarking Technique. In Workshop COST 254: Friendly Exchange through the net, Bordeaux, France, March 2000.

[2] J. J. Eggers, J. K. Su, and B. Girod, Asymmetric watermarking schemes, Tagungsband des GI Workshops Sicherheit in Mediendaten, Berlin, Germany, Sept. 2000.

[3] J. J. Eggers, J. K. Su, and B. Girod, Public key watermarking by eigenvectors of linear transforms, in Proc. Eur. Signal Processing Conf., Tampere, Finland, Sept. 2000.

[4] T. Furon and P. Duhamel, An asymmetric public detection watermarking technique, in Proc. 3rd Int. Information Hiding Workshop, Dresden, Germany, Oct. 1999, pp. 88–100.

[5] Tae Young Kim, Hyuk Choi, Kiryung Lee, and Taejeong Kim, An asymmetric watermarking system with many embedding watermarks corresponding to on detection watermark, IEEE signal processing letters, Vol.11(3), 2004, pp.375-377.

[6] Hyuk Choi, Kiryung Lee, and Taejeong Kim, transformed-key asymmetric watermarking system, IEEE signal processing letters, Vol.11(2), 2004, pp.251-254.

[7] Justin picard and Arnaud Robert,On the public key watermaking issue, Security and watermarking of multimedia contents, proceeding of SPIE Vol.4314, 2001, pp.290-299.

[8] Geunsil Song, Miae Kim and Wonhyung Lee, Asymmetric watermarking scheme using permutation braids, WISA 2003, LNCS 2908, pp.217-226.

[9]Furon, T., Duhamel, P.: Robustness of asymmetric watermarking technique. In Proc. of the Int. Conf. on Image Processing, Vancouver, Canada (2000)

[10] Xinpeng Zhang, Shuozhong Wang, Watermarking scheme capable of resisting attacks based on availability of inserter, Signal processing, Vol.82,2002, pp.1801-1804.

[11] F. Hartung and B. Girod, Fast public-key watermarking of compressed video, in *Proc. IEEE Intl. Conf. Image Processing*, vol. 1, Oct. 1997, pp. 528–531.