COMMITMENT BASED WATERMARK DETECTION PROTOCOLS[1]

Liu Yongliang

Harbin Institute of Technology, China

ABSTRACT

In traditional watermark detection scheme, a prover exposed a watermark to be present in a digital data to the possible dishonest verifier. However, a potential attacker is able to destroy the watermark entirely once secret information like the watermark or the embedding location is known. Some of previous schemes proposed as solution haven't achieved desirable result really. In this paper, we propose the commitment based watermark detection protocols. They can be used to prove the copyright ownership of the digital multimedia content without revealing any secret information to remove the watermark. And we show the protocols are zero knowledge protocols.

1. INTRODUCTION

With the rapid spread of computer networks and the further development of multimedia technologies, digital contents can be accessed easily, and the protection of intellectual property becomes more and more important every day. Digital watermark is proposed as an approach to solve this problem. Copyright protection of digital contents, as one of the most important applications of digital watermark, works by watermark detection, works by watermark detection.

In traditional watermark detection scheme, a prover exposed secret information that can be used to remove the watermark in order to prove a watermark presents in a digital object to the verifier. This is a significant security risk because a potential attacker can destroy the watermark to defeat the intention of proving ownership. Zero knowledge watermark detection is a promising approach to overcome security issue during watermark detection. Its basic idea is to apply cryptography tools to hide classified information and implement the detection without disclosing any information. The idea of zero knowledge watermark detection was first proposed in [1]. Further zero knowledge interactive proposals (ZKIP) for watermark detection are presented in [2]~[9].

In [1] a graph generated from an image that must have a signature and an isomorphic graph is concealed in this image. The ZKIP for the graph isomorphism is applied to assert the copyright of this image. One problem is that adversary can modify the least significant bits easily, thus prevent copyright owner from showing his ownership of the image. More importantly, the adversary can embed forgery watermark into the image, then he can prove he is "real" copyright owner by ZKIP too.

A protocol for the watermarking decision problem is proposed in [2] and [3]. The basic idea is to secretly and verifiably compute the correlation between the watermark and the underlying stego-data: The seller use his public key of well-known RSA public key cryptosystem to encrypts the watermark and stego-data added by a random sequence and sends them to the verifier. In a challenge-response manner the seller convinces the verifier that the watermark correlates with stego-data. However, both ensuring the randomness of sequence and computing method to measure correlation are inherent problem of that protocol.

Craver presents two schemes for zero knowledge watermark detection in [4]. The first one relies on some permutation of images, where the permutation must be secret. As uncommon intensity values in the image are mapped to uncommon values in scrambled image, giving an attacker a great deal of information by narrowing down the set of original pixels mapping to a scrambled pixel. The same problem also exists in the second one. More recently, Craver et al give a refined protocol [5], but the protocol does not state how to verify the presence of scrambled watermark in the scrambled image without revealing secret information.

Adelsbach et al give a formal definition of zero knowledge watermark detection protocols based on definitions known from cryptography [6]~[9]. For both blind and non-blind versions of a well-known class of watermarking schemes introduced in [10], they propose zero knowledge detection protocols based on commitment

[1] This work was supported by National Natural Science Foundation of China under grant No. 60472043 and the National High Technology Development 863 Program under grant No. 2002AA119010

schemes. The authors understand this protocol a provable secure protocol. The detection process disclosed watermark embedding location so as to an attacker could easily remove watermark information.

These protocols mentioned above should be improved for actual application due to the lacking of the security or the validity. In this paper we propose the commitment based watermark detection protocols. It provides copyright proving without revealing any information to remove the watermark.

The rest of the paper is organized as follows. In Section 2, we present the proposed protocols. In Section 3, we show the proposed protocols are zero knowledge protocol. In Section 4, we give a conclusion and future research direction.

2. COMMITMENT BASED WATERMARK DETECTION PROTOCOL

2.1. Definitions and notations

Let $h=(h_1, h_2, \cdots, h_L)$ denote the host data, $h^{'}=(h_1^{'}, h_2^{'}, \cdots, h_N^{'})$ denote the sequence coefficients of host data into which the watermark will be embedded, $w=(w_1, w_2, .., w_N)$, $N<L$, denote the watermark, $\overline{h}=(\overline{h}_1, \overline{h}_2, \cdots, \overline{h}_L)$ be the watermarked host data, $\overline{h}^{'}=(\overline{h}_1^{'}, \overline{h}_2^{'}, \cdots, \overline{h}_N^{'})$ denote the subset of $\overline{h}$, i.e., the sequence of modified coefficients of host data into which the watermark was embedded.

In blind watermark detection, the correlation value between w and $\overline{h}^{'}$

$$cr=<w, \overline{h}'>/<w, w>$$

is computed, where $<a, b>$ denotes the scalar product of the vectors a and b . Given the threshold ε , if $cr>\varepsilon$, we can conclude the presence of the watermark w in $\overline{h}$. An equivalent version to $cr>\varepsilon$ is $<w, \overline{h}^{'}>-<w, w>*\varepsilon>0$. And its spreading version is $(w_1\overline{h}_1^{'}+w_2\overline{h}_2^{'}+\cdots+w_N\overline{h}_N^{'})-(w_1^2+w_2^2+\cdots+w_N^2)\varepsilon>0$.

In non-blind watermark detection, the correlation value between w and $\overline{h}^{'}-h^{'}$

$$cr=<w, \overline{h}'-h^{'}>/<w, w>$$

is computed. An equivalent version to $cr>\varepsilon$ is $<w, \overline{h}^{'}-h^{'}>-<w, w>*\varepsilon>0$. Its spreading version is $(w_1\overline{h}_1^{'}+w_2\overline{h}_2^{'}+\cdots+w_N\overline{h}_N^{'})-(w_1h_1^{'}+w_2h_2^{'}+\cdots+w_Nh_N^{'})-(w_1^2+w_2^2+\cdots+w_N^2)\varepsilon>0$.

2.2. The commitment scheme

We will use a commitment scheme of [11] to construct the watermark detection protocols. Let n is a safe prime product and its factorization is unknown by the prover P and the verifier V . Let g is an element of large order in Z_n^*, h is an element of large order generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by P . To commit to an integer $m\in Z_n$, P randomly chooses r in $[0, 2^L n)$, and sends $com(m)=g^m h^r \bmod n$ to V , where L is in the order of the bit length of n , r is in secret, n, g and h are public. To open a commitment, P must send m, r such that $com(m)=g^m h^r \bmod n$. P is unable to commit himself to two values m_1 , m_2 such that $m_1\neq m_2$ by the same commitment unless he can factor n or solve the discrete logarithm of g in base h or the discrete logarithm of h in base g . And this commitment scheme statistically reveals no information to V .

2.3. The proposed protocol for blind detection

(1) P sends the commitment to the watermark $com(w)$ and the judge's signature $S_J(com(w))$ to V . Here we assume that the judge is trusted by all. The process of the signature can reference [6].

(2) V verifies the signature.

(3) P generates a random number λ and a random permutation τ . Then, he computes $com(\lambda\tau(\overline{h}))$, $com(\lambda\tau(w))$ and $com(\varepsilon)$ and sends them to V .

(4) V chooses at random a bit b , and sends it to P .

(5) If $b=0$: P reveals λ and τ . He first opens the commitment $com(\lambda\tau(\overline{h}))$ to show the correctness of $com(\lambda\tau(\overline{h}))$ to V . Then P and V compute $com(\lambda)$ and $com(\tau(w))$ ($com(\tau(w))=\tau(com(w))$) and P proves V the correctness of $com(\lambda\tau(w))$ using zero knowledge protocol [12][13].

If $b=1$:

(a) P sends the $com(\lambda\tau(\overline{h}'))$ to V .

(b) V verifies $com(\lambda\tau(\overline{h}_i'))\in\{com(\lambda\tau(\overline{h}_j))\,|\,1\le j\le L\}$, $1\le i\le N$.

(c) P computes $com(\lambda\tau(\overline{h}_i')\lambda\tau(w_i))$, $com(\varepsilon\lambda^2\tau(w_i)^2)$ and sends them to V .

(d) P proves V that $com(\lambda\tau(\bar{h}_i')\lambda\tau(w_i))$ contains the product of the two numbers contained in $com(\lambda\tau(\bar{h}_i'))$ and $com(\lambda\tau(w_i))$ and $com(\varepsilon\lambda^2\tau(w_i)^2)$ contains the product of the number contained in $com(\varepsilon)$ and the square of number contained in $com(\lambda\tau(w_i))$ using zero knowledge protocol respectively, $1 \le i \le N$.

(e) P computes $com(<\lambda\tau(\bar{h}'), \lambda\tau(w)>)$ and $com(\varepsilon < \lambda\tau(w), \lambda\tau(w)>)$ and sends them to V.

(f) P proves V that $com(<\lambda\tau(\bar{h}'), \lambda\tau(w)>)$ contains the sum of the numbers contained in $com(\lambda\tau(\bar{h}_1')\lambda\tau(w_1))$, $com(\lambda\tau(\bar{h}_2')\lambda\tau(w_2))$, … , $com(\lambda\tau(\bar{h}_N')\lambda\tau(w_N))$ and $com(\varepsilon < \lambda\tau(w), \lambda\tau(w)>)$ contains the sum of the numbers contained in $com(\varepsilon\lambda^2\tau(w_1)^2)$, $com(\varepsilon\lambda^2\tau(w_2)^2)$,…, $com(\varepsilon\lambda^2\tau(w_N)^2)$ using zero knowledge protocol respectively.

(g) P and V compute

$$com(\lambda^2(<\bar{h}', w> - <w, w>\varepsilon)) = \frac{com(<\lambda\bar{h}', \lambda w>)}{com(\varepsilon < \lambda w, \lambda w>)}$$

$$= \frac{com(<\lambda\tau(\bar{h}'), \lambda\tau(w)>)}{com(\varepsilon < \lambda\tau(w), \lambda\tau(w)>)} \bmod n$$

(h). P proves V $com(\lambda^2(<\bar{h}', w> - <w, w>\varepsilon))$ contains a value ≥ 0 using zero knowledge protocol [14].

(6) The prover and the verifier perform these steps n times. The verifier accepts the fact that w is present in $\bar{h}$ if all tests passed.

2.4. The proposed protocol for non-blind detection

(1) P sends the commitments to $com(w)$ and $com(h)$ and their signatures $S_J(com(w))$ and $S_J(com(h))$ to V.

(2) V verifies the signature.

(3) P generates a random number λ and a random permutation τ. Then, he computes $com(\lambda\tau(\bar{h}))$, $com(\lambda\tau(h))$, $com(\lambda\tau(w))$ and $com(\varepsilon)$ and sends them to V.

(4) V chooses at random a bit b, and sends it to P.

(5) If $b = 0$: P reveals λ and τ. He first opens the commitment $com(\lambda\tau(\bar{h}))$ to show the correctness of $com(\lambda\tau(\bar{h}))$ to V. Then P and V compute $com(\lambda)$ and P proves V the correctness of $com(\lambda\tau(w))$ and $com(\lambda\tau(h))$ using zero knowledge protocol [5][6].

If $b = 1$:

(a) P sends V $com(\lambda\tau(\bar{h}'))$ and $com(\lambda\tau(h'))$.

(b) V verifies $com(\lambda\tau(\bar{h}_i')) \in \{com(\lambda\tau(\bar{h}_j)) \mid 1 \le j \le L\}$ and $com(\lambda\tau(h_i')) \in \{com(\lambda\tau(\bar{h}_j)) \mid 1 \le j \le L\}$, $1 \le i \le N$.

(c) P computes $com(\lambda\tau(\bar{h}_i')\lambda\tau(w_i))$, $com(\lambda\tau(h_i')\lambda\tau(w_i))$, $com(\varepsilon\lambda^2\tau(w_i)^2)$ and sends them to V.

(d) P proves V that $com(\lambda\tau(\bar{h}_i')\lambda\tau(w_i))$ contains the product of the two numbers contained in $com(\lambda\tau(\bar{h}_i'))$ and $com(\lambda\tau(w_i))$, $com(\lambda\tau(h_i')\lambda\tau(w_i))$ contains the product of the two numbers contained in $com(\lambda\tau(h_i'))$ and $com(\lambda\tau(w_i))$, and $com(\varepsilon\lambda^2\tau(w_i)^2)$ contains the product of the number contained in $com(\varepsilon)$ and the square of number contained in $com(\lambda\tau(w_i))$ using zero knowledge protocol respectively, $1 \le i \le N$.

(e) P computes $com(<\lambda\tau(\bar{h}'), \lambda\tau(w)>)$, $com(<\lambda\tau(h'), \lambda\tau(w)>)$, $com(\varepsilon < \lambda\tau(w), \lambda\tau(w)>)$ and sends them to V.

(f) P proves V that $com(<\lambda\tau(\bar{h}'), \lambda\tau(w)>)$ contains the sum of the numbers contained in $com(\lambda\tau(\bar{h}_1')\lambda\tau(w_1))$, $com(\lambda\tau(\bar{h}_2')\lambda\tau(w_2))$, … , $com(\lambda\tau(\bar{h}_N')\lambda\tau(w_N))$, $com(<\lambda\tau(h'), \lambda\tau(w)>)$ contains the sum of the numbers contained in $com(\lambda\tau(h_1')\lambda\tau(w_1))$, $com(\lambda\tau(h_2')\lambda\tau(w_2))$, … , $com(\lambda\tau(h_N')\lambda\tau(w_N))$, and $com(\varepsilon < \lambda\tau(w), \lambda\tau(w)>)$ contains the sum of the numbers contained in $com(\varepsilon\lambda^2\tau(w_1)^2)$, $com(\varepsilon\lambda^2\tau(w_2)^2)$,…, $com(\varepsilon\lambda^2\tau(w_N)^2)$ using zero knowledge protocol respectively.

(g) P and V compute

$$com(\lambda^2(<\bar{h}', w> - <h', w> - <w, w>\varepsilon))$$

$$= \frac{com(<\lambda(\bar{h}' - h'), \lambda w>)}{com(\varepsilon < \lambda w, \lambda w>)}$$

$$= \frac{com(<\lambda(\tau(\bar{h}') - \tau(h')), \lambda\tau(w)>)}{com(\varepsilon < \lambda\tau(w), \lambda\tau(w)>)} \bmod n$$

(h). P proves $com(\lambda^2(<\bar{h}' - h', w> - <w, w>\varepsilon))$ contains a value ≥ 0 using zero knowledge protocol .

(6) The prover and the verifier perform these steps n times. The verifier accepts the fact that w is present in $\bar{h}$ if all tests passed.

3. ANALYSES

Now, we show the proposed protocols are zero knowledge protocols.

(1) Completeness: the proof always succeeds if w is present in $\bar{h}$.

(2) Soundness: for cheating P has to break either the soundness of sub-protocols or the binding property of the commitment scheme. However, it is impossible because a cheating V can succeed with very small probability and binding is assumed to be computationally impossible.

(3) Zero knowledge: the proposed protocol is zero knowledge protocol because two sub-protocol used during the detection are zero knowledge protocol and all results correlated with the information about watermark and the location of embedding watermark (the coefficients of host data) are hidden in the commitments.

Note that the random number λ and the random permutation τ are necessary for hiding the location of embedding watermark.

4. CONCLUSIONS

In this paper, we propose the commitment based watermark detection protocols. And we show the protocols are zero knowledge protocols. It provides copyright proving without revealing any information to remove the watermark. This brings a significant improvement of watermark detection scheme in terms of security.

Future research may investigate how secret extracts watermark for more accurate computing correlation value. Another research direction may be to further develop asymmetric watermark technique for secure watermark detection.

11. REFERENCES

[1] H. Kinoshita, "An Image Digital Signature System with ZKIP for the Graph Isomorphism Problem" *Proc. IEEE Conf. Image Processing (ICIP96)*, IEEE Press, Piscataway, N.J., vol. 3, 1996, pp. 247-250.

[2] K. Gopalakrishnan, N. Memon, P. Vora, "Protocols for Watermark Verification" *Multimedia and Security, Workshop at ACM Multimedia*, 1999, pp. 91-94.

[3] K. Gopalakrishnan, N. Memon, P. Vora, "Protocols for Watermark Verification", IEEE Multmedia October-December 2001 66-70.

[4] S. Craver, "Zero Knowledge Watermark Detection" *Information Hiding: Third International Workshop*, LNCS 1768, Springer-Verlag, 2000, pp. 101-116.

[5] S. Craver, S. Katzenbeisser, "Copyright Protection Protocols Based on Asymmetric Watermarking: The Ticket Concept " *in Proceedings of Communications and Multimedia Security* 2001

[6] A. Adelsbach, and A. Sadeghi. Zero knowledge watermark detection and proof of ownership, 4th international workshop on information hiding, IHW 2001, Springer-Verlag, vol. 2137, 273-288.

[7] A. Adelsbach, S. Katzenbeisser, and A. Sadeghi, Cryptography meets watermarking: detecting watermarks with minimal or zero knowledge disclosure, 11th European signal processing conference, vol. 1 pp. 446-449 2002.

[8] A. Adelsbach, and A. Sadeghi. Advanced techniques for dispute resolving and authorship proofs on digital works. Proceedings of SPIE, vol. 5020, 2003

[9] A. Adelsbach, S. Katzenbeisser, and A. Sadeghi, "Watermark Detection with Zero-knowledge disclosure" *Multimedia Systems* 2003 Volume 9, Number 3 pp 266-278

[10] I. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, 1997, vol. 6, pp. 1673–1687.

[11] E. Fujisaki, T. Okamoto, "A practical and provably secure scheme for publicly verifiable secret sharing and its applications," Eurocrypt'98, LNCS 1403, Springer - Verlag, 1998, pp. 88-100.

[12] J. Camenisch, M. Michels, "Proving in Zero- Knowledge that a Number is the Product of Two Safe Primes," Eurocrypt'99, LNCS 1592, Springer-Verlag, 2000, pp. 101-116.

[13] I. Damgard, E. Fujisaki, "An Integer Commitment Scheme based on Groups with Hiding Order," Preliminary Version.

[14] F. Boudot, "Efficient Proofs that a Committed Number Lies in an Interval," Eurocrypt'00, LNCS 1807, Springer-Verlag, 2000, pp. 431-444.