ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.1, January 2006, pp.157−166
DOI: 10.1360/jos170157

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于安全多方计算的数字作品所有权证明*

朱 岩[1+], 杨永田[1], 孙中伟[2], 冯登国[2]

[1](哈尔滨工程大学 计算机科学与技术学院,黑龙江 哈尔滨 150001)

[2](中国科学院 信息安全国家重点实验室,北京 100049)

Ownership Proofs of Digital Works Based on Secure Multiparty Computation

ZHU Yan[1+], YANG Yong-Tian[1], SUN Zhong-Wei[2], FENG Deng-Guo[2]

[1](Computer Science and Technology College, Harbin Engineering University, Harbin 150001, China)

[2](The State Key Laboratory of Information Security, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: Phn: +86-10-88256433, Fax: +86-10-88256432, E-mail: martinzhu@msn.com

Zhu Y, Yang YT, Sun ZW, Feng DG. Ownership proofs of digital works based on secure multiparty computation. *Journal of Software*, 2006,17(1):157−166. http://www.jos.org.cn/1000-9825/17/157.htm

Abstract: Ownership proofs of digital works allow to justify the copyright claim to the buyers without revealing any secret information and prevent the owner from deceiving without the assumption of the trusted individual. This paper proposes an ownership proofs scheme for digital works based on proactive verifiable secret sharing and secure multiparty computation. In the proposed scheme, verifiable secret sharing ensures the correctness of ownership secrets and achieves security against cheating participants. Proactive security provides an automatic recovery feature to maintain the integrity and security of secret throughout the lifetime of the scheme. Furthermore, the ownership verification is implemented by using secure multiparty computation and zero-knowledge proofs with homomorphic commitments. Without the assumption of the existence of a trusted individual, the proposed scheme can provide effective computation and discover the dishonesty if not too many individuals collude.

Key words: ownership proof; secure multiparty computation; proactive secret sharing; commitment scheme; digital watermarking

摘 要: 数字作品的所有权证明允许在不泄漏任何秘密信息和防止所有者欺骗的前提下,对版权声明进行验证.提出一种基于 Proactive 可验证秘密共享和安全多方计算的数字作品所有权证明方案.在该方案中,可验证秘密共享,保证了所有权秘密的正确性,并防止对协议参与者的欺骗.通过 Proactive 安全提供自动恢复功能来保证协议生存周期内秘密的完整性和安全性.使用安全多方计算和同态承诺的零知识证明,实现了所有权验证.在不假设可信方存在的前提下,所提出方案能够在没有太多成员合谋的情况下,完成有效计算并发现不忠实成员.

关键词: 所有者证明;安全多方计算;前向秘密共享;承诺协议;数字水印

中图法分类号: TP309 文献标识码: A

Protection of intellectual property has become crucial in the widespread and rapidly growing use of digital media. Ownership proofs on digital works are the important issues of copyright protection. To solve such problems,

Received 2004-06-30; Accepted 2005-05-08

digital watermarking has been proposed as a strong tool. However, it is not enough for ownership dispute[1] to merely hide information within digital works. How to justify the copyright claim without revealing any secret information and how to prevent the owner from deceiving are the central issues in ownership dispute.

The feasible schemes of proving ownership include asymmetric watermarking scheme, zero-knowledge watermark detection and so on. Asymmetric watermarking is similar to public-key cryptography. It uses two different keys to embed and detect watermark. The detection key is public while the embedding key is kept secret. However, the public detection key leads to oracle/sensitivity attacks. Another approach is to use zero-knowledge watermark detection[2]. In such a scheme, the main parties involved in this scheme are prover and verifiers. A prover convinces a verifier that she knows watermark secret and proves the existence of the watermark in a given work. But the verifier learns nothing new from the scheme-run. Although these schemes are cryptographically secure, the main drawback is the large number of interaction and computation cost required. Furthermore, the prover must be trusty since the verifier has to reveal the checked work to the prover.

In order to avoid the assumption of a trusted third party, a possible approach keeps secret information collectively by a group of participants in such a way that only a subgroup is able to reconstruct and the secret does not depend on any single person. Hence, the secret sharing is an effective way to construct ownership proofs. At present, many scholars have already noticed this problem and have proposed some schemes[3], but there are many questions that have not yet been resolved. For example, Guo *et al.* proposed a watermark scheme for the problem of joint ownership by introducing secret sharing. This method distributes the shares of the watermark key to a group of participants so that only when enough members in the group present their keys can the ownership of the image be verified. However, the sharing scheme is one-time, and a trusted party is required to verify the image ownership though the watermark key is kept secret collectively by secret sharing scheme.

In this paper, we propose an ownership proofs scheme of digital works based on proactive secret sharing and secure multiparty computation. The scheme is a collection of three protocols: registration, renewal, and verification protocols. In the registration protocol, an owner assigns the shares of the ownership secrets to the participants by the Verifiable Shamir Secret Sharing[4]. During the verification protocol, the buyer and the participants calculate the watermark correlation by the multiparty computation[5,6] and send the results to the verifier and the buyer. Furthermore, both of them can identify the ownership by interactive zero-knowledge proofs with homomorphic commitments. In order to keep the secret integral and secure throughout the lifetime of the scheme, the secret renewal protocol is constructed by proactive secret sharing[7] such that the proposed scheme can discover the dishonesty and keep secure and efficiency if not too many individuals collude.

The paper is organized as follows: The overview of the proposed scheme and basic frame of digital watermarking is explained respectively in Sections 1 and 2. Section 3 describes the cryptographic techniques from three aspects: commitment schemes, verifiable secure sharing, and secure multiparty computation. The ownership proofs scheme based on secret sharing is proposed in Section 4. Section 5 then presents and discusses security and performance analysis. Finally, conclusions are drawn in Section 6.

1 Overview of the Proposed Scheme

Ownership proofs are the methods to resolve ownership dispute which may arise after many person claims respectively to be the rightful owner for a certain digital work. Ownership proofs of digital works involve two kinds of requirements: on the one hand it guarantees the buyers that they obtain the rights of usage from the real copyright holder and avoids the owner deceiving; on the other hand it assures the owner that the buyers can not modify copyright information by the ownership proofs scheme.

In our proposed scheme the main individuals are an owner, a buyer, n participants $P=\{P_1,\ldots,P_n\}$ and a verifier. The owner holds the copyright of a certain work that the buyer purchases. The participants preserve the shares of copyright watermark. The verifier wants to ensure the buyer that their works come from the real copyright holder. Here we do not assume that all parts are trusted in our scheme. An ownership proofs scheme is a collection of three protocols: *registration*, *renewal*, and *verification*. These protocols are described as follows:

- **Registration** protocol generates the shares of an ownership secret $wm\in WM$. The share $s_i\in S$ is communicated via a secure channel to the participant $P_i(i=1,\ldots,n)$.
- **Verification** protocol takes an arbitrary collection of shares s_i and attempts to compute the watermark correlation $Corr=\langle wm,W\rangle$ and identifies the copyright of a certain work W.
- **Renewal** protocol keeps the secret unchanged and uncompromised throughout the lifetime of the scheme.

In order to avoid the owner deceiving, during the registration, the proposed scheme assigns the ownership secrets of the digital work to many participants via secure channel. The verifier recovers the secret successfully only if the number n of different shares is greater or equal to t. Otherwise, the verifier fails. Furthermore, to guard the collusion between the dishonest owner and some participants, the shares of each participant must be regenerated in relatively short periods of time. According to foregoing analysis, the proposed scheme employs the Shamir scheme with Proactive Secret Sharing. In addition, to prevent the buyer from modifying copyright information with revealed secrets in verification process, the proposed scheme uses Secure Multiparty Computation based on secret sharing. During the ownership verification, the buyer generates the shares of his work and then sends to the participants. The participants compute the shares of the correlation between the watermark and the work by secure multiparty computing. Next, the participants send the shares and their share commitments back to the verifier and the buyer, respectively. Finally, the verifier confirms the ownership to the buyer by Zero-Knowledge Proofs. In conclusion, these employed methods ensure that the proposed scheme is efficient and provably secure.

2 Basic Framework of Digital Watermarking

Digital watermarking is a collection of the algorithms: embedding and detection. A general digital watermarking scheme is described as follows:

In the embedding process, a secret message M of the owner is first converted into a binary sequence and then is shuffled as WM by means of a secret key K known by the owner only. The sequence WM is mapped from $\{0,1\}$ to $\{-1,1\}$ such that WM is pseudorandom sequence with zero mean and unit variance. Finally, in a certain transform domain, WM will be magnified under the constraint of perceptual masking α and embedded into a cover works W to produce a watermarked works W' by

$$W'(k)=W(k)+\alpha(k)\cdot WM_s(k),\ k=1,\ldots,L \tag{1}$$

Where L denotes the length of W and α stands for the masking matrix derived from W. The finally embedded sequence $\alpha\cdot WM_s$ is called the watermark WM. WM is assumed to be a pseudorandom sequence with zero mean and variance σ. Noticed that the commitment schemes will be replaced by the bit commitment scheme if the perceptual marking $\alpha=1$. In the detection process, given a work W'', a watermark exists provided that the correlation $Corr$ between W'' and WM is larger than a threshold δ, where

$$Corr=\sum_{k=1}^{L}W''(k)\cdot WM(k)\geq\delta\,. \tag{2}$$

Usually, the watermark WM and the work W are regarded as integer vectors and the detection involves only multiplication and addition. In this paper, our proposed scheme complies with these assumptions.

3 Preliminaries

In order to explain the proposed scheme, we introduce some notations of cryptographic techniques used in our scheme. First we review commitment schemes and verifiable secure sharing techniques. Next we state briefly the secure multiparty computation exploited in our scheme.

3.1 Commitment schemes

Commitment schemes are basic ingredients in many cryptographic protocols. Loosely speaking, a commitment scheme is an efficient two-phase two-party protocol between the sender and receiver. The *commit phase* allows sender to commit to a value s by sending a special encryption $C=E(s,u)$ of s to the receiver. In the *reveal phase*, the sender can open commitment to convince the receiver that s is the encrypted value.

The security requirements of commitment scheme are the *Secrecy* or *Binding* properties. The former requires that the receiver does not gain any knowledge of the sender's value and the latter requires that there exists at most one value that the receiver can later accept as a legal 'opening' of the commitment. Let $n=pq$ be a product of two safe primes p and q, g be a randomly chosen generator of $GF(n)$, and h be a randomly selected integer such that the Discrete Logarithm $\log_g h$ is unknown. The commitment scheme[8] is based on the function

$$E(s,u)=g^s h^u (\mathrm{mod}\ n) \tag{3}$$

where s is a value that the sender commits to and u is a randomly selected secret key, which is later used to open the commitment. This scheme is statistically hiding and computationally binding under the factoring assumption. The commitment scheme has *homomorphic* property: Let $E(s_1,u)$ and $E(s_2,u)$ be commitments to arbitrary values s_1,s_2, the sender can open $E(s_1,u)*E(s_2,u)$ to s_1+s_2 without revealing additional information about the contents of $E(s_1,u)$ and $E(s_2,u)$.

3.2 Verifiable secure sharing

A (t,n) threshold secret sharing scheme distributes a secret among n participants in such a way that any t of them can recreate the secret, but any t–1 or fewer members gain no information about it. The piece held by a single participant is called a *share* of the secret. Secret sharing schemes are normally set up by a trusted authority *dealer* who computes all shares and distributes them to participants via secure channels. The participants hold their shares until some of them decide to pool their shares and recreate the secret. The recovery of the secret done by the so-called *combiner* is successful only if the cooperating group computes the secret. In many applications, a secret sharing scheme is also required to withstand active attacks. This is accomplished by verifiable secret sharing schemes (VSS), as first introduced in Ref.[9]. It is an explicit goal of this scheme that not just the participants can verify their own shares, but that anybody can verify that the participants received correct shares.

The shamir secret sharing scheme described previously is one-time. Once shares have been pooled, the secret is recovered and used. Also if a participant loses his share, the whole scheme needs to be regenerated and new shares redistributed. This can be avoided if the Shamir scheme is combined with *Commitment* function in $GF(q)$ in which discrete logarithm instances are intractable. This scheme is called *non-interactive VSS*[4] because the distribution protocol does not require any interaction between the dealer and participants, nor between participants among each other, except for the filing of complaints. On the other hand, we know that the shares may be either compromised, lose or corrupted throughout the lifetime of the scheme. If we assume that shares are being compromised gradually, then it is possible to divide the lifetime of the system into relatively short periods of time. At the beginning of each consecutive period, if the shares are regenerated, then we can keep the secret unchanged throughout the lifetime of the scheme. In terms of this idea, Herzberg *et al.* came up with a concept of Proactive Secret Sharing (PSS)[7]. In this paper, the presented renewal protocol is based on proactive security on the assumption of active attacks. That is,

the adversary may choose to corrupt different participants at different times, as long as at any given time the number of infected participants is limited.

3.3 Secure multiparty computation

Secure Multiparty computation is a cryptographic task that allows a group of participants to emulate any trusted party protocol[5]. The problem of secure multiparty computation is as follows: n players $(P_1,P_2,\ldots,P_n)$ wish to evaluate a function $F(x_1,x_2,\ldots,x_n)$, where x_i is a secret value provided by P_i. The result of this function can then be revealed publicly or privately to some particular player. The goal is to preserve the privacy of the other party's inputs/outputs and guarantee the correctness of the computation. Security is then defined by requiring that whatever the adversary achieves in a real-life execution of the protocol can efficiently simulate while corrupting at most t parties in an ideal model, in which a trusted party is being used to evaluate the function. Thus, the protocol prevents the adversary from gaining an extra advantage over what it could have gained in an ideal solution. In the following we shall present a simple method for computing the addition and multiplication of two secrets which are distributed among a set of parties. Given two secrets α and β shared by polynomials $f_\alpha(x)$ and $f_\beta(x)$ of degree $t-1$ respectively, the parties would like to compute $\alpha+\beta$ and $\alpha\beta$. In terms of the property of polynomial, the addition of $f_\alpha(x)$ and $f_\beta(x)$ is $f_\alpha(x)+f_\beta(x)=(\alpha+\beta)+\gamma_1x+\ldots+\gamma_{t-1}x^{t-1}=f_{\alpha+\beta}(x)$ and the product of both is $f_\alpha(x)f_\beta(x)=\alpha\beta+\lambda_1x+\ldots+\lambda_{2t-2}x^{2t-2}=f_{\alpha\beta}(x)$. The Lagrange interpolation formula allows to determine $f_{\alpha+\beta}(x)$ and $f_{\alpha\beta}(x)$ from t and $2t-1$ different shares, respectively. (For details see Ref.[6])

4 Ownership Proofs Scheme

In this section, we describe how to carry out secure multiparty computations to prove the ownership of digital works. In order to explicitly explain the protocols, the symbols and its signification in the proposed scheme are defined as follows:

WM: Watermarking vector	x_i: Participant ID
wm: Watermarking mark	P_i: Participant i
S_i,T_i: Share vector	s_i,t_i,c_i: Share
$f_i(\cdot),g_i(\cdot),h_i(\cdot),h_i'(\cdot),\delta_i(\cdot),\lambda_i(\cdot)$: Polynomial	$Corr$: Correlation coefficient
$h,r,u_i,a_i,b_i,d_i,e_i,\beta_i,g_i$: The random integer	$Corr_i$: The share of correlation coefficient
δ: Threshold	δ_i: The share of threshold
E_i: Commitment	g:The generator of order q in Z^*_q

The construction of the proposed scheme is novel and practicable in many aspects. In the aspect of organization, every individual are independent of each other in order to enforce the trustiness. The owner is not concerned with the verification but registers his secrets. The participants take the responsibility for the security of secrets and computation. The verifier achieves the result of the ownership proofs. The buyer attains merely the final result. In the aspect of structure, the security of the proposed scheme depends on the assumption of the intractability of the Discrete Logarithm problems, and many fundamental security tasks are achieved with proactive security and the commitment scheme. Specially, the homomorphic commitment scheme is used to combine Secure Multiparty Computation to calculate the watermark correlation with Zero-Knowledge Proof to verify the watermark existence. In the aspect of performance, contrasted with Zero-Knowledge Watermark Detection, the scheme employs the arithmetic operation of the secret shares to avoid the exponential operation between two commitments. The proposed ownership proofs scheme consists of three sub-protocols: registration, verification, and renewal protocols, which are described as follows.

4.1 Registration protocol

The registration protocol is a two-party protocol between an owner and n participants $P=\{P_1,\ldots,P_n\}$. The secrets of the owner are the ownership watermark information $WM=(wm_1,wm_2,\ldots,wm_m)$, which is embedded into his works and a predefined detection threshold δ. To avoid statistical analysis of the shares, each element of the watermark employs different polynomials to generate the shares. After registration protocol, the participants $P_i(i=1,\ldots,n)$ receive the shares (S_i,δ_i), where S_i be the share set of WM.

Registration protocol

R1. Let p be a large primes such that q divides $p-1$, g be a generator of order, and h be a randomly selected integer such that the Discrete Logarithm $\log_g h$ is unknown. Suppose that the owner embeds an ownership watermark $WM=(wm_1,wm_2,\ldots,wm_m)$ into the work W, the owner designs a collection of (t,n) Shamir schemes with the polynomial $f_i(x)=a_{i,0}+a_{i,1}x+\ldots+a_{i,t-1}x^{t-1}$ of degree at most $(t-1)$ for $i=1,\ldots,m$. The watermark wm is preserved as the secret $f_i(0)=wm_i$. The shares $S_{ij}=f_i(x_j) \bmod q$ are assigned to participants $P_i(i=1,\ldots,n)$ via a secure channel, where $n\geq 2t-1$ is the number of all participants. The values $x_i\in Z_q$ are public. The shares are communicated secretly to the corresponding participants. The owner generates the share δ_j of a predefined detection threshold δ and then sends it to participants $P_i(i=1,\ldots,n)$ via a secret channel.

R2. The owner calculates $E_{i,0}=E(wm_i,u_i)$ $(i=1,\ldots,m)$ for a random integer $u_i\in_R Z_q$. $E_{i,0}$ is a commitment to the secret wm_i. Next, he chooses at random a sequence of $(t-1)$ elements $b_1,b_2,\ldots,b_{t-1}\in Z_q$ and computes the commitments $E_{ij}=E(a_{i,j},b_j)$ about the coefficients of the polynomial $f_i(x)$ for $i=1,\ldots,m$ and $j=1,\ldots,t-1$. All commitments E_{ij} are broadcast.

R3. The owner employs $u_i,b_1,b_2,\ldots,b_{t-1}$ to create a polynomial $g_i(x)=u_i+b_1x+\ldots+b_{t-1}x^{t-1}$ and sends $u_i=g_i(x_j)$ to the participant P_j via a secure channel $(j=1,\ldots,n)$.

R4. Each participant P_j calculates the share commitment $E_j(wm_i)=E(s_{ij},u_{ij})$ of wm_i and verifies whether

$$E(s_{ij},u_{ij})=\prod_{k=0}^{t-1}E_{ik}^{x_j^k} \bmod p \tag{4}$$

If not, the registration fails. However, each participant P_j saves information sets $\Omega_j=\{S_j,\delta_j\}$ for $j=1,\ldots,t-1$, where $S_j=\{s_{1j},\ldots,s_{mj}\}$.

R5. In order to check the validity of the shares, each participant P_j computes the inner product $Corr_j=\langle S_j,S_j\rangle=\sum_{i=1}^{m}s_{ij}s_{ij} (\bmod q)$, where $S_j=(s_{1j},s_{2j},\ldots,s_{mj})$, and broadcasts it. After receiving enough data (larger than $2t-1$), each participant calculates the inner product $Corr$ and the threshold δ in terms of Shamir secret sharing scheme, and then confirms that $Corr\geq\delta$. If not, the registration fails.

One problem of registration protocol is that a cheating ownership could distribute false shares. Such a problem can be solved with a verifiable secret sharing scheme. The verification for the scheme consists of checking whether the secret share is the discrete logarithm of a publicly known element by the share commitment. Therefore Eq.(4) allows the participants $P_j(j=1,\ldots,n)$to verify the validity of their shares if only it is true for each index $i=1,2,\ldots,m$ as the left side of the equation can be derived from the right one:

$$\begin{aligned}\prod_{k=0}^{t-1}E_{ik}^{x_j^k}&=E(wm_i,u_i)\prod_{k=1}^{t-1}E(a_{i,k},b_k)^{x_j^k}=g^{wm_i}h^{u_i}\prod_{k=1}^{t-1}(g^{a_{i,k}}h^{b_k})^{x_j^k}=g^{wm_i}h^{u_i}g^{a_{i,1}x_j}h^{b_1x_j}\ldots g^{a_{i,t-1}x_j^{t-1}}h^{b_{t-1}x_j^{t-1}}\\&=g^{wm_i+a_{i,1}x_j+\ldots+a_{i,t-1}x_j^{t-1}}h^{u_i+b_1x_j+\ldots+b_{t-1}x_j^{t-1}}=g^{f_i(x_j)}h^{g_i(x_j)}=E(s_{ij},u_{ij}) \bmod p\end{aligned} \tag{5}$$

4.2 Renewal protocol

The renewal protocol is a protocol among n participants. The renewal protocol is presented on the assumption that all participants follow the protocol and the opponents are active. The protocol employs a random polynomial

$\delta(x)$ such as $\delta(0)=0$ to renew the shares $f^{(l)}(x)=f^{(l-1)}(x)+\delta(x)$ (l is renewal count), but the secrets stays the same, such as $f^{(l)}(0)=f^{(l-1)}(0)$. To ensure the security of the shares, the protocol ought to execute every a relatively short periods of time.

Renewal protocol

N1. The participant P_i chooses at random a polynomial $\delta_i(x)=d_{i,1}x+d_{i,2}x^2+\ldots+d_{i,t-1}x^{t-1}$ in $Z_q[x]$ ($d_{i,j}\in_R Z_q$ for $j=1,\ldots,t-1$. Note that$\delta_i(0)=0$. Next the participant generates a collection of parameters for verification of the corrections $c_{ij}=\delta_i(x_j)$. And P_i computes the commitment $E_{i,j}=E(d_{i,j},e_{i,j})$, where $\lambda_i(x)=e_{i,1}+\ldots+e_{i,t-1}x^{t-1}$ is a random polynomial selected by P_i and $j=1,\ldots,t-1$.

N2. P_i calculates the corrections $c_{ij}=\delta_i(x_j)$, $j=1,\ldots,n(j\neq i)$, and a proper share of the polynomial $\lambda_i(x)$, i.e., $u_{ij}=\lambda_i(x_j)$. The pair (c_{ij},u_{ij}) is encrypted using public-key cryptosystems of the corresponding participants P_i, i.e., $v_{ij}=E_{K_j}(c_{ij},u_{ij})$, where K_j is the authentic public key of P_j.

N3. P_i broadcasts the message $(P_i,l,\{E_{i,j},j=1,\ldots,t-1\},\{v_{ij},\ j=1,\ldots,n,j\neq i\})$ and appends the signature to eliminate tampering with the contents of the message.

N4. After all participants have finished broadcasting, P_i decrypts the cryptograms v_{ji}, where $j=1,\ldots,n(j\neq i)$, and verifies the correctness of the shares c_{ij} and u_{ij} (generated by P_j) by checking

$$E(c_{ji},u_{ji})\equiv\prod_{k=1}^{t-1}E_{j,k}^{x_i^k}\ \bmod p \tag{6}$$

Note that P_i has to verify $n-1$ shares (corrections) generated by other participants. If all checks are hold, P_i broadcasts a signed acceptance message. Otherwise, P_i sends a signed accusation in which he specifies misbehaving participants.

N5. If all participants have sent their acceptance messages, then each P_j updates his shares to $s_{ij}^{(l)}=s_{ij}^{(l-1)}+\sum_{k=1}^{n}c_{kj}$ for $i=1,2,\ldots,m$. The old share is discarded.

N6. If there are some accusations, then the protocol resolves them (for details see Ref.[7]). As all messages are broadcast, it is reasonable to assume that all honest participants will come up with the same list of misbehaving participants and they update their shares ignoring corrections from misbehaving participants.

Similarly, the following expression proves that Eq.(6) can be satisfied:

$$\begin{aligned}\prod_{k=1}^{t-1}E_{j,k}^{x_i^k}&=\prod_{k=1}^{t-1}E(d_{j,k},e_{j,k})^{x_i^k}=\prod_{k=1}^{t-1}(g^{d_{j,k}}h^{e_{j,k}})^{x_i^k}=g^{d_{j,1}x_i}h^{e_{j,1}x_i}\ldots g^{d_{j,t-1}x_i^{t-1}}h^{e_{j,t-1}x_i^{t-1}}\\&=g^{d_{j,1}x_i+\ldots+d_{j,t-1}x_i^{t-1}}h^{e_{j,1}x_j+\ldots+e_{j,t-1}x_i^{t-1}}=g^{\delta_j(x_i)}h^{\lambda_j(x_i)}=E(c_{ji},u_{ji})\ \bmod p\end{aligned} \tag{7}$$

4.3 Verification protocol

The verification protocol is three-party protocol between a buyer, a verifier and n participants. The protocol is initiated by the buyer who wants to identify whether a work W' is embedded with the watermark claimed by the owner. The protocol consists of the correlation detection computation and zero-knowledge proofs. Considering scheme performance, the multiparty computations are executed in each participant and just involve addition and multiplication operations.

Verification protocol

V1. A buyer wants to confirm whether a work W'' is embedded with the watermark WM claimed by the owner. With respect to the registration protocol, W'' is transformed and segmented into a vector $W''=(w_1'',w_2'',\ldots,w_m'')$. The buyer chooses randomly the polynomial $h_i(x)=r_{i,0}+r_{i,1}x+\ldots+r_{i,t-1}x^{t-1}$ of degree $t-1$ and computes the shares $t_{ij}=h_i(x_j)$ of each element $r_{i,0}=w''_i$ for the participant P_i and $i=1,2,\ldots,m$. And then the shares t_{ij} are assigned to the

participant sets $\{P_1,P_2,\ldots,P_k\}$ via a secret channel, where $j=1,\ldots,k$ and $k\geq 2t-1$ is necessary and sufficient for reconstruction and verification.

V2. For the vector $T_j=(t_{1j},t_{2j},\ldots,t_{mj})$ and $S_j=(s_{1j},s_{2j},\ldots,s_{mj})$, each participant P_j calculates the inner product $\langle T_j,S_j\rangle$ respectively as follows:

$$Corr_j=\sum_{i=1}^{m}s_{ij}t_{ij} \bmod q \tag{8}$$

In order to verify whether $Corr\geq\delta$. holds for a predefined detection threshold δ, we use the detection criteria $Corr-\delta\geq 0$. Each participant P_j calculates $Corr'_j=Corr_j-\delta_j(\mathrm{mod}q)$.

V3. The verifier chooses at random a natural number r and sends it to all participants via secret channels. The participant P_j computes the commitment $E(Corr'_j)=E(Corr'_j,r)$ of the share $Corr'_j$. Finally, the participant P_j sends the set $(Corr_j,E(Corr_j))$ back to the verifier via a secret channel. At the same time, P_j sends the share $E(Corr_j)$ to the buyer via a secret channel.

V4. The verifier and the buyer receive the correlation shares and collect $2t-1$ shares $(c_{i_1}=E(Corr'_{i_1}),\ \ldots,\ c_{i_{2t-1}}=E(Corr'_{i_{2t-1}}))$ from participants $(P_{i_1},P_{i_2},\ldots,P_{i_{2t-1}})$, and set up the following system of equations constituted by a random polynomial $h'(x)=\beta_0+\beta_1x+\ldots+\beta_{2t-2}x^{2t-2}$ of degree $(2t-2)$ in $Z_q[x]$:

$$\begin{cases} c_{i_1}=g_0g_1^{x_{i_1}}\ldots g_{2t-2}^{x_{i_1}^{2t-2}} \\ c_{i_2}=g_0g_1^{x_{i_2}}\ldots g_{2t-2}^{x_{i_2}^{2t-2}} \\ \quad\vdots \\ c_{i_{2t-1}}=g_0g_1^{x_{i_{2t-1}}}\ldots g_{2t-2}^{x_{i_{2t-1}}^{2t-2}} \end{cases} \tag{9}$$

where $g_i=g^{\beta_i}$ for $i=0,\ldots,2t-2$. The system of equations has a unique solution. The secret

$$E(Corr')=g^{h'(0)}=\prod_{j=1}^{2t-1}\left(c_{i_j}\right)^{b_j} \tag{10}$$

where

$$b_j=\prod_{1\leq l\leq(2t-1),l\neq j}\frac{x_{i_l}}{x_{i_l}-x_{i_j}} \bmod q \tag{11}$$

Furthermore, the verifier recalculates the correlation $Corr'$ by the Shamir secret sharing with $2t-1$ shares $(Corr'_{i_1},\ldots,Corr'_{i_{2t-1}})$. Note that the permanent secret $Corr$ is never revealed to the buyer by the participants only if the corresponding instances of discrete logarithm are intractable.

V5. The verifier and buyer check whether there exists any inconsistency among different groups of n shares. If so, they declare that some participants are cheating. Otherwise, the verifier convinces the buyer that $E(Corr')$ contains the secret $Corr'$ and he holds this secret using the interactive zero-knowledge proof protocol.

V6. Finally, the verifier proves $Corr'\geq 0$ in zero-knowledge proofs, that the value contained in $E(Corr')$ is larger than 0 using protocols from Ref.[10]. The buyer accepts this proof if detection protocols end with *true*. Otherwise ownership proof fails.

In step V4 of the verification protocol, the verifier and the buyer receive the commitments $c_{i_j}=E(Cor\,r'_{i_j})$ of the correlation share to compute the commitment $E(Corr')$ of the correlation. Suppose the Discrete Logarithm $log_g^h=k$ and r is secret key that is later used to open the commitment, the correlation commitment is equivalent to appending an integer kr to the random polynomial, as follows:

$$E(Cor\,r'_{i_j})=E(Cor\,r'_{i_j},r)=g^{Cor\,r'_{ij}}h^r=g^{Cor\,r'_{ij}+kr}=g^{(Corr'+kr)+\beta_1x_{ij}+\ldots+\beta_{2t-2}x_{ij}^{2t-2}} \tag{12}$$

In terms of Eq.(9), the secret can be denoted as $h'(0)=\beta_0=Corr'+kr$ in the random polynomial $h'(x)$. The verifier and the buyer generate the commitment of watermark correlation by computing Shamir secure sharing, as follows:

$$E(Corr') = E(Corr', r) = g^{Corr'} h^{r} = g^{Corr'+kr} = g^{h'(0)} \tag{13}$$

Hence Eq.(10) holds.

5 Security and Performance Analysis

In principle, the proposed scheme is based on secure multiparty computation with proactive verifiable secret sharing, and its security depends on the assumption of the intractability of the Discrete Logarithm problems.

In order to prevent the owner from cheating, registration protocol must verify the consistency and authenticity of the owner secrets *WM*. In our registration protocol, steps R2-4 employ non-interactive verification of shares to check whether the secret sharing scheme parameters are consistent based on the commitment $E(s,u)=g^s h^u$. Step R5 is used to check the authenticity of the secrets by $\langle WM,WM\rangle \geq \delta$. Notice that the owner only participates in the registration protocol.

In our scheme, the participants are the proxies of the owner as well as the executants of the watermark detection. In order to ensure the honesty of the participants, on one hand the secrets of the owner are to be shared among all participants by verifiable secret sharing instead of Shamir's threshold scheme. The renewal protocol is used to ensure the validity of shares throughout the lifetime of the system. On the other hand, considering the security of the digital work, the buyer's work is also shared among all participants in the watermark detection. For the secrets of the owner and the buyer, the scheme should tolerate less than t dishonest individuals, where t is the security threshold. It is required that the number n of shares must be not less than $n>4t-3$, considering the multiplication operation. If Step V4 adopts the 'truncation' of polynomial by multiplying a fixed matrix to implement degree reduction, it is required that the number n of shares must be not less than $3t-2$($n\geq 3t-2$) if the method should tolerate less than t dishonest individuals in an asynchronous setting[5].

It is a serious problem that the watermark detection reveals the secret information to the buyer. In our verification protocol, the commitment and zero-knowledge proofs scheme are employed to avoid this threat. Above all, in Step V3, the participant sends the commitment $E(Corr_j)$ of the result back to the verifier and the buyer. The commitment ensures the security of the result only if discrete logarithm problem is intractable. Next, the verifier and the buyer compute the commitment $E(Corr)$ of the correlation value, respectively. In Steps V5, the verifier confirms the consistency of the secret between the verifier and the buyer using zero-knowledge proof. Step V6 confirms that the commitment is not less than 0 using interactive zero-knowledge proofs. We can indicate that the soundness of the scheme holds, because the verifier can only deceive by cheating in the computation of $E(Corr)$ or by cheating the buyer in proving that $E(Corr)$ contains a value $Corr\geq 0$. However, for this the verifier has to either break the soundness of zero-knowledge proof or the binding property of commitment scheme, which is assumed to be computationally infeasible. This method is similar to zero-knowledge watermark detection, where the buyer is able to prove the existence of the watermark without revealing any secret information about the watermark. Furthermore, the proposed scheme ensures that the verifier is not able to gain the knowledge of the checked work.

The performance of the proposed scheme is analyzed by computation and communication complexity. Suppose that modular addition and multiplication operation is 1 unit and the round of verification is 1 time, the computation cost of verification is $O(tmn)$, where, t and n are small integers. Registration is only performed once at $O(tmn)$ and the renewal cost of each participant is $O(m+tn)$, and thus they can be neglected. In the respect of communication, their communication complexity is $O(mn)$ since registration and verification protocol need to transmit the whole watermark and watermarked work, respectively. The cost of renewal is $O(n(n+t))$. In conclusion, the proposed scheme is feasible to prove ownership for practical applications.

6 Conclusions

In this paper, we propose an ownership proofs scheme using proactive secret sharing and secure multiparty computation. The scheme security and performance are improved since the secrets and operations are dispersed into many participants. As long as not too many individuals collude, the secrets of the ownership can be maintained. In conclusion, the secure multiparty computation is an effective approach to implement the watermark detection and ownership proofs of digital works.

Acknowledgement The authors would like to thank the anonymous reviewers of this paper for their insightful comments and suggestions and also thank the researchers in the State Key Laboratory of Information Security in the Chinese Academy of Sciences for their valuable discussions and comments.

References:

[1] Adelsbach A, Pfitzmann B, Sadeghi AR. Proving ownership of digital content. In: Pfitzmann B, ed. Proc. of the Information Hiding: The 3rd Int'l Workshop. Berlin: Springer-Verlag, 2000. 126−141.

[2] Adelsbach A, Sadeghi AR. Zero-Knowledge watermark detection and proof of ownership. In: Moskowitz IS, ed. Proc. of the Information Hiding: The 4th Int'l Workshop. Berlin: Springer-Verlag, 2001. 273−288.

[3] Guo H, Georganas ND. A novel approach to digital image watermarking based on a generalized secret sharing scheme. In: Dittmann J, Katzenbeisser S, eds. Proc. of the ACM/Springer Multimedia Systems. New York: Springer-Verlag, 2003. 249−260.

[4] Pedersen TP. Non-Interactive and information theoretic secure verifiable secret sharing. In: Feigenbaum J, ed. Advances in Cryptology (CRYPTO'91). New York: Springer-Verlag, 1991. 129−140.

[5] Hirt M, Maurer U, Przydatek B. Efficient secure multi-party computation. In: Okamoto T, ed. Advances in Cryptology (ASIACRYPT 2000). New York: Springer-Verlag, 2000. 143−161.

[6] Gennaro R, Rabin MO, Rabin T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proc. of the ACM Symp. on Principles of Distributed Computing (PODC). 1998. 101−111.

[7] Herzberg A, Jarechi S, Krawczyk H, Yung M. Proactive secret or: How to cope with perpetual leakage. In: Coppersmith D, ed. Advances in Cryptology (CRYPTO'95). New York: Springer-Verlag, 1995. 339−352.

[8] Fujisaki E, Okamoto T. Statistical zero-knowledge protocols to prove modular polynomial relations. In: Burton S, Jr Kaliski, eds. Advances in Cryptology (Crypto'97). New York: Springer-Verlag, 1997. 16−30.

[9] Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Proc. of the 26th IEEE Symp. on Foundations of Computer Science (FOCS'85). New York: IEEE Press, 1985. 383−395.

[10] Boudot F. Efficient proofs that a committed number lies in an interval. In: Ellis R, ed. Advances in Cryptology (EUROCRYPT 2000). Berlin: Springer-Verlag, 2000. 431−444.

ZHU Yan was born in 1974. He is a Ph.D. candidate at the Harbin Engineering University. His current research areas are computer security, cryptography, information hiding, media security and pattern recognition.

SUN Zhong-Wei was born in 1969. He is a Ph.D. candidate and an associate professor at the Institute of Software, CAS. His research areas are multimedia information processing and information security.

YANG Yong-Tian was born in 1939. He is a professor and doctoral supervisor at the Harbin Engineering University. His research areas are computer network and application, distribution system and fault-tolerant computer system.

FENG Deng-Guo was born in 1965. He is a professor and doctoral supervisor at the Institute of Software, CAS. His research areas are information security, network security and cryptography.