

基于水印的数字作品所有权证明协议研究

数字水印技术是近年来出现的用于数字作品版权保护的一种解决方案。数字水印技术通过将相关信息嵌入到数字作品中以证明所有者对数字作品的所有权。为了实现基于水印的数字作品所有权证明，不仅要求能够抵抗各种针对水印算法鲁棒性攻击的水印方案，而且要求能够抵抗各种协议攻击的所有权证明协议。这是因为攻击者可以采取各种手段直至攻击成功为止。由此可见，所有权证明技术是非常有挑战性的。尽管研究者们进行了很多相关的研究努力，但是已有的方法并不总是能够成功用于所有权证明。本文致力于基于水印的数字作品所有权证明协议的研究。本文的主要研究内容总结如下：

(1) 研究了作为所有权证明协议基础的零知识水印检测协议。分别提出了用于盲水印检测方案和非盲水印检测方案的零知识水印检测协议。在协议中，通过使用随机置换、盲因子和承诺方案隐藏了水印信息和水印嵌入位置信息，弥补了Adelsbach等的协议中由于泄漏水印嵌入位置信息使得水印容易遭受攻击的缺陷。

(2) 研究了零知识水印检测协议的延展性问题。提出了不可延展的零知识水印检测协议。通过引入证明者和验证者双方的身份信息以及时间戳信息到协议中以获得不可延展性。协议使得验证者无法使用从验证过程中获得的信息向其它人证明水印信息的存在。这可以看作是对Adelsbach等的协议在不可延展性方面的进一步改进。

(3) 研究了零知识水印检测协议的非交互性问题。提出了非交互的零知识水印检测协议。协议使用单向散列值作为随机抛币的结果以实现协议的非交互性。与已有的非交互零知识水印检测协议相比，本文提出的协议是不可延展和不可复制的，同时具有更为广泛的应用范围。

(4) 研究了数字作品交易过程中的所有权证明问题。提出了一个用于数字作品交易的简单所有权证明协议。在协议中，出售者通过出示所有权证书以及使用零知识水印检测子协议证明水印的存在性完成对作品的所有权证明。该协议使得数字作品交易时出售者向购买者正确而不泄露任何秘密信息地证明其是作品的合法所有者。因此，恶意的购买者无法利用验证过程中所获得的信息冒充合法的出售者出售复制的作品。

(5) 研究了作品所有权出现纠纷情况下的所有权证明问题。提出了一个无需注册机构参与的数字作品纠纷所有权证明协议。协议以简单所有权证明协议为基础，并添加使用图像检索技术衡量作品之间的相似性，以确定纠纷作品的所有权。协议使得纠纷发生时在没有作品真正所有者参与的情况下，仲裁者能够正确解决所有权纠纷，避免了已有纠纷所有权协议中可能发生的所有权误判问题。

(6) 研究了多个所有者共同拥有作品版权情况下的联合所有权证明问题。提出了一个基于可验证的秘密共享方案和安全多方计算协议的数字作品联合所有权证明协议。联合所有权证明协议使得数量不小于预先确定的阈值的共同所有者一起能够正确地完成对作品的所有权证明，单个或数量小于阈值的共同所有者不能完成对作品的所有权证明。协议既可以防止欺骗的联合所有权证明，又可以防止秘密敏感信息的泄漏。

关键词 数字水印；所有权证明；零知识证明

Digital watermarking is an emerging technique used for copyright protection to digital works in recent years. Digital watermarking is used for proving ownership to digital works by detecting the message embedded into digital works. In order to achieve the ownership proof for digital works, not only the watermarking schemes that can resist all kinds of attacks to the robustness are required, but also the ownership proof protocols that can resist all kinds of attacks to the protocol are required, because the attackers may exploit all kinds of attacks until one of the attacks succeeds. Thus, it is very challenging to prove the ownership of digital works. Although many related research efforts have been carried out by researchers, the existing approaches do not always make a success in the ownership proof. This dissertation addresses the research on the watermarking-based ownership proof protocol to digital works. The main research contents of this dissertation are summarized as follows:

(1) Study the zero-knowledge watermarking detection protocol which is the building block of the ownership proof protocol. Zero-knowledge watermarking detection protocols for both blind watermarking detection scheme and non-blind watermarking detection scheme are proposed respectively. In the proposed protocols, random permutation, blind factor, and commitment scheme are used together to hide both watermarking information and watermarking embedding location information to supply a gap that watermarking information suffers from the attack due to the revealing watermarking embedding location information in Adelsbach et al's protocol.

(2) Study the malleability problem in zero-knowledge watermarking detection protocol. The non-malleable zero-knowledge watermarking detection protocols are proposed. Both prover and verifier's identification information and time-stamp are added into the protocols to achieve the non-malleability. Under the proposed protocol the verifier can not to prove the presence of the watermarking information by using the information learned during the verification. This protocol may be seen as a further improvement to Adelsbach et al's protocol.

(3) Study the non-interactivity problem in zero-knowledge watermarking detection protocol. Non-interactive zero-knowledge watermarking detection protocols are proposed. One-way hash function value is used as the simulation of the random coin flipping to achieve the non-interactivity goal in the protocols. Compared with the previous non-interactive zero-knowledge watermarking detection protocol, the protocols proposed in this dissertation are non-malleable and non-duplicated. Meanwhile, the proposed protocols have a broader application range.

(4) Study the ownership proof problem during digital works trade. A simple ownership proof protocol for digital works trade is proposed. Under this protocol, the seller executes the ownership proof by showing the ownership certificate and proving the presence of watermarking in the digital works with zero-knowledge watermarking detection sub-protocol. This protocol enables the seller to correctly prove the buyer

that he/she is the legal owner of digital works without disclosing any secret information in digital works trade. Thus, the malicious buyer could not use the information learned during the verification to imitate the rightful seller to sell the duplicated works.

(5) Study the ownership proof problem in the ownership dispute of digital works. An ownership proof protocol in the dispute is proposed without requiring the participation of the registration authority. The protocol is based on simple ownership proof protocol and additionally uses the image retrieval technique to measure the similarity between the works to determine the ownership of the disputing works. It enables the dispute arbitrator to correctly resolve the ownership dispute without the attendance of rightful owner and avoids the possible false decision existing in previous dispute resolving protocol

(6) Study the joint ownership proof problem in which multiple owners jointly hold the ownership to digital works. A joint ownership proof protocol, which is based on verifiable secret sharing scheme and secure multiparty computation protocol, is proposed. The protocol enables the co-owners whose number is not less than the predefined threshold together to correctly prove the joint ownership to digital works whereas single or part of owners whose number is less than the predefined threshold could not prove the ownership to digital works. This protocol prevents not only the cheating joint ownership proof but also revealing secret sensitive information.

Keywords Digital watermark; ownership proof; zero-knowledge proof