# Improvement of the Digital Watermarking Protocol based on the Zero-Watermark Method

Quan Wen* and Yufei Wang†
*Jilin University, Changchun
E-mail: wenquan@jlu.edu.cn
†Jilin Normal University, Siping
E-mail: yufei-522@hotmail.com
†Corresponding Author

***Abstract*—This paper focuses on improvement to the digital watermarking protocol by adopting a zero-watermarking method. Theoretical analysis shows that the improved protocol can solve the customer's rights problem, the client's problem of anonymity and the unbinding problem. At the same time, the transaction steps and operations are simplified, and the transmission times of digital work are reduced. Practicality and security are greatly improved in the zero-watermark protocol, thereby benefiting the application of digital watermarking.**

## I. INTRODUCTION

The concept of digital watermarking was first proposed in the 1990s [1]. Through the efforts of scholars in the past two decades, fruitful results have been achieved in this domain. From an academic point of view, these findings can be divided into two classes: watermarking algorithms and watermarking protocols.

Because of the practicality of *invisible watermarking*, most studies on watermarking algorithms deal with how to embed watermarks that people cannot detect, so the biggest difficulty is how to solve the contradiction between robustness and imperceptibility. In addition, the endless means of attack are a problem. The zero-watermark method proposed by the authors fundamentally solves these difficulties in theory [2], and is introduced in the next section.

More fruitful results have been achieved with watermarking algorithms than with the watermarking protocols. As the immaturity of key technologies has caused a bottleneck in the application of digital watermarking, this paper focuses on the watermarking protocol. Study of watermarking protocol focuses on the implementation steps and rules for watermarking in a network environment. Because that environment is complex, both buyers and sellers cannot be trusted. This leads to the problem of designing a safe and effective watermarking protocol to solve difficult issues such as the customer's rights problem [3], the client's problem of anonymity [4] and the unbinding problem [5]. In addition to these problems, we have to take into account that the buyer and seller do not usually have an IT background.

Although the focus of research into watermarking algorithms and watermarking protocols differs, the two fields affect each other. The security of a protocol depends on the robustness of the algorithm it uses. Different algorithms correspond to different protocols. The zero-watermark protocol is attributable to the results of watermarking algorithm research. As there is an essential difference between zero-watermarking and most watermarking algorithms, there is also a difference in how the protocol is designed. Lei et al. [6] designed a watermarking protocol based on the private watermarking algorithm, with original digital work required. The Lei protocol solved the client's problem of anonymity and the unbinding problem, and the buyer only has to communicate with the seller when completing the transaction. There is no need to communicate with a *trusted third party* (TTP). The Lei protocol was a great improvement on existing protocols, but it still has many shortcomings, as will be discussed in a later section. To overcome those shortcomings, the study reported here redesigned the Lei watermarking protocol by replacing the private watermarking algorithm with the zero-watermark algorithm. A detailed theoretical analysis shows that a watermarking protocol using the zero-watermark algorithm will offer enormous advantages.

The rest of this paper is organized as follows. In section II we briefly introduce the *zero-watermark* method. In section III we describe the efficient anonymous buyer-seller watermarking protocol proposed by Lei. We improve the Lei protocol using the *zero-watermark* method in section IV and discuss the properties of the new watermarking protocol in Section V. We present our conclusions in section VI.

## II. INTRODUCTION TO ZERO-WATERMARK

From the perspective of embedding space, a watermarking algorithm can be divided into spatial and transform domains [7]. Many watermarking algorithms have been put forward in both domains, but most have been broken. Of course, designing watermarking algorithms with absolute security is impossible, and only experts in digital watermarking have the ability to do this successfully. The key issue here is conflict between robustness and imperceptibility. As long as the watermark information is embedded in the original digital media, this conflict can only be overcome to some extent; a fundamental solution is almost impossible. However, if the information cannot be embedded in the original image, that is, the original image cannot be modified to completely protect

The authors of this paper received a grant from the Youth Science Foundation of Jilin Province (20100183), the Scientific Frontier and interdisciplinary Project of 2009 Jilin University grant (200903298).

the digital watermark, then a perfect solution to this conflict is only theoretical.

The watermarking scheme described above is essentially the idea of zero-watermark. Is this possible? The answer is yes. If the digital media itself is watermarked, there is no need to further embed the watermark in the original image. It can simply use the unique characteristics of the digital work to achieve the concept of a zero-watermark.

Each digital work should have unique characteristics that can be used as a watermark and registered in the database of a trusted third party. Then the function of watermark copyright protection can be completed without modifying the original digital work. In fact, in the traditional digital watermarking scheme, the watermark embedded in the original digital work also has to be on file in a reliable place, to compare with the watermark extracted from the suspected pirated one when a copyright dispute occurs. An important feature is extracted from the controversial digital work when the zero-watermark method deals with copyright issues: the watermark information that will be compared with the registered watermark. Hence, we also complete copyright protection. The registered watermark is for published original digital work.

In fact, the general watermarking algorithm can be abstracted as the following formula.

$$X_w = X_O \oplus \alpha \cdot W \tag{1}$$

In the above formula, $X_O$ is the original work, $X_w$ is the watermarked work after embedding a watermark in $X_O$, W is the watermark, $\alpha$ is the strength of the embedded watermark. Obtaining the appropriate value of $\alpha$ is important for the watermarking algorithm. According to the *zero-watermark* method, $\alpha$ is 0.

The zero-watermark concept as first proposed by the authors had a great impact on digital watermarking research, and many scholars have followed up on the study over the past decade. It is recognized by most watermarking experts [8][9][10][11].

## III. THE LEI PROTOCOL

The symbols used in the watermark protocol are explained below.

**S:** The seller, who wants to make a profit on the sale of certain digital content. The seller may be the rightful owner of the original digital content or an authorized reselling agent.

**B:** The buyer, who wants to purchase a copy of the digital content from **S**.

**CA:** A trusted certification authority, which is responsible for issuing anonymous certificates. The existence of a **CA** provides the possibility of **B** purchasing his or her favorite digital work anonymously on the Internet. The **CA** provides the true identity of **B** to the **ARB** when piracy occurs.

**WCA:** A trusted watermark certification authority, responsible for the generation of random and valid watermarks. The existence of a **WCA** asserts the validity of watermarks over the course of the protocol.

**ARB:** An arbiter, who adjudicates lawsuits against the infringement of copyright and intellectual property.

$(pk_I, sk_I)$ : A public-private key pair, where I is the identity of the owner. $pk_I$ is I's public key, and $sk_I$ is I's private key.

$Sign_I(M)$ : The signature of message M signed by subject I with his or her private key.

$E_{pk_I}(M)$ : The ciphertext of message M encrypted with subject I's public key.

$D_{sk_I}(C)$ : The original message of ciphertext C decrypted by subject I with private key $sk_I$ to obtain plaintext.

$Cert_J(I)$ : The digital certificate issued to subject I by certification authority J.

The Lei protocol comprises three sub-protocols: a registration protocol, a watermarking protocol and an arbitration protocol. The major role of the registration protocol is **B** and **CA**, mainly to obtain a digital certificate $Cert_{CA}(pk_{\mathrm{B}})$ of **B** from the **CA**, which can be understood as the online ID for **B**. Participants in the arbitration protocol are **ARB**, **S**, and **WCA.** This will achieve the copyright judgment for a digital work without the cooperation of **B**. The watermarking protocol is the core part; the roles in the protocol are **S**, **B**, and **WCA**, including the following four steps.

(1)
$$B \to S : Cert_{CA}(pk_B), Cert_{pk_B}(pk^*), ARG, Sign_{pk^*}(ARG)$$

(2)
$$S \to WCA : Cert_{pk_B}(pk^*), ARG, Sign_{pk^*}(ARG), X'$$

(3)
$$WCA \to S : E_{pk^*}(W), E_{pk_{WCA}}(W), Sign_{WCA}(E_{pk^*}(w), pk^*, Sign_{pk^*}(ARG))$$

(4) $S \to B : E_{pk^*}(X'')$

Figure 1 shows the details of watermarking protocol. As shown in Figure 1, **ARG** represents the order of digital works that will be purchased, and $X'$ is first embedded with **S**'s watermark. $X''$ is the encrypted watermarked work, with watermark generated and secondly embedded by **WCA**, and the final digital work **B** wants to obtain.

## IV. WATERMARKING PROTOCOL IMPROVEMENT

Although the Lei protocol described above solves the client's problem of anonymity and the unbinding problem in theory, there are still some shortcomings in the protocol design, as follows.

(1) Original digital work has to complete two embedded watermark operations, which not only delays the real-time transaction but also makes it very difficult to guarantee the quality of the original work is not affected. In addition, such a professional operation is a burden for **S**.

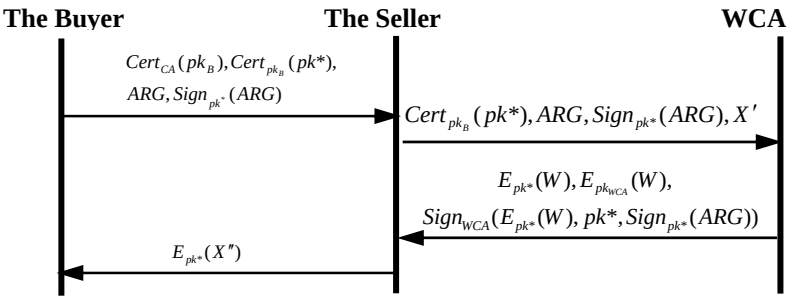


Fig. 1 Details of watermarking protocol in the Lei protocol

(2) There are still too many steps in the protocol, although **B** is only trading with **S**. In fact, most of the time is wasted in communication between **S** and **WCA**.

(3) $X'$ with **S**'s watermark information has to be sent to **WCA.** If $X'$ is a large file containing audio and video multimedia formats, it will place a heavy burden on the already crowded network.

(4) The security of the protocol is heavily dependent on the security of the watermarking algorithm. If any one of two watermarks in $X''$ is removed, the arbitration watermarking will fail. In fact, almost no one is secure in the watermarking algorithms that have been published.

On the basis of the Lei protocol and improvements by using the zero-watermark method, these four problems can be solved in theory. The modified protocol is also divided into a registration protocol, a watermarking protocol and an arbitration protocol, introduced as follows.

### *A. Registration Protocol*

Similar to the Lei protocol, the registration protocol is the preparation before the trade. In this protocol, **B** applies an anonymous digital certificate $Cert_{CA}(pk_B)$ to **CA**. The true identity of **B** is known only by **CA**, who is responsible for binding **B** and the anonymous certificate.

Because it uses the zero-watermarking algorithm, zero-watermark construction for digital work can be completed in the registration protocol. **S** has to issue the online sale work X to **CA** for a marketing authorization application. After receiving X, **CA** will use the following formula to complete the *zero-watermark* construct.

$$W = F_{extract}(X) \tag{2}$$

where $F_{extract}$ means feature extraction algorithm, which extracts the characteristic information of **X** to be sold online and construct zero-watermark **W** corresponding to **X**. Later, **CA** will sign **W** and send $Sign_{CA}(W)$ back to **S**, so registration watermarking is complete.

The requirement for $F_{extract}$ is as follows.

(1) The characteristics information extracted from **X** are unique, so different digital work will have different characteristic information.

(2) The capacity of constructed zero-watermark information should be much smaller than the original digital work, in order to facilitate preservation and transmission.

(3) When **X** is subjected to certain modifications, as long as the important characteristics of the digital work are not damaged, the characteristic information can be extracted after **X** is modified.

### *B. Watermarking Protocol*

After using the zero-watermarking algorithm, the watermarking protocol can only participate with **B** and **S**. This is more in line with real transactions. In reality, during a transaction, only the buyer and the seller can be reached. The steps in the protocol can be simplified to the following.

(1) When **B** browses the summary information of digital work **X** belonging to **S** on the Internet and has the intention to purchase, **B** can download the **ARG** that **S** prepared on the website. **ARG** can be regarded as the purchase agreement or order for **X**. Then **B** sends $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$, ARG, $Sign_{pk^*}(ARG)$ to **S,** where pk* is the anonymous key obtained in the registration protocol.

(2) When **S** receives the message $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$, **ARG**, $Sign_{pk^*}(ARG)$ from **B, S** will verify the validity of certificates and signatures. If there is a failure, **S** may suspend the protocol operation. If qualified, **S** will generate a number of digital authority certificates of **X** $Sign_{pk_S}(Sign_{CA}(W), Cert_{CA}(pk_B), Cert_{pk_B}(pk^*))$ for **B**, which can be represented by $R_B^X$. Then **S** will encrypt $R_B^X$ with **B**'s public key to obtain $E_{pk^*}(R_B^X)$ and send it back to **B** to turn off the watermarking protocol. As in Microsoft's operating system software, for software products, a digital license certificate is the most critical. **B** can

download digital work X with ftp protocol at any time at the server address provided by **S** using $R_B^X$ as permitted.

Hence, the most complex watermarking protocol can be reduced to two steps using the zero-watermark algorithm, as shown in Figure 2.

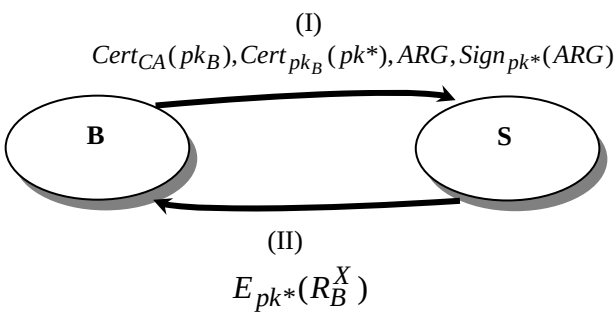


Fig. 2 Watermarking protocol based on zero-watermark

Only two steps are required to complete the transaction watermarking protocol, which corresponds with reality in a large number of real-time Internet transactions.

### *C. Arbitration Protocol*

Watermarking protocol requires only two steps to complete: solving the issue when a copyright dispute occurs, or requiring further analysis.

When a copyright dispute occurs, it cannot be assumed that **B** is cooperative. Therefore, we have to design arbitration protocol that can be executed without **B**'s participation. To this end, digital work used for commercial purposes should provide the link to the digital certificate authority by law, with any person free to download it.

Thus, when **S** suspects that digital work Y released by **B** is pirated, **S** can start the arbitration protocol from **ARB**. Then **ARB** sends Y with its online digital certificate of $Sign_{pk_S}(Sign_{CA}(W), Cert_{CA}(pk_B), Cert_{pk_B}(pk^*))$ to **WCA**. Then **WCA** will verify whether the digital signature of **S** is valid or not. If it is invalid, **WCA** will reject the application from **S**. If the signature from **S** is valid, **WCA** will construct the zero-watermark of Y by extracting the characteristics in it.

$$W' = F_{extract}(Y) \tag{3}$$

Using the above formula to obtain $W'$, **WCA** then obtains W using the public keys of **S** and **CA**. **WCA** compares $W'$ with W. If the results show the two are the same, then we can judge Y to be legitimate. Then **ARB** will stop the arbitration protocol process after obtaining confirmation from **WCA**. If there is a difference between $W'$ and W, Y can be identified as pirated. After receiving feedback from **WCA**, **ARB** will send $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$ to **CA** asking for the true identity of **B** and inform **S**.

If maturity arrives at a certain stage, the feature extraction function can make up a standard, like the PKI infrastructure. Then zero-watermark protocol can provide public free service for everyone. In this way, each Internet user can monitor the problem of digital copyright issues.

## V. DISCUSSION AND ANALYSIS

Can the *zero-watermark protocol* resolve the customer's rights problem, the client's problem of anonymity and the unbinding problem? The three problems will now be analyzed separately to determine whether they can be resolved.

For the client's problem of anonymity, because the protocol still uses the anonymous certificate of the Lei protocol, it can naturally ensure the anonymity of the user's buying habits.

For the customer's rights problem, online available digital work used for commercial purposes is required by law to bind the digital certificate, so **B**'s cooperation is not first considered when copyright disputes occur. Considering the importance of the *Digital Rights Management* (DRM) issues, requiring digital work published on the web to bind with its digital certificates should be a trend.

In fact, the unbinding problem is the most difficult for any watermarking protocol. As the *zero-watermark* protocol adopts the features of digital work to construct the watermark message, and each feature is unique; otherwise, it will lose value. Thus, the zero-watermark algorithm itself provides the proper mechanism for binding a chosen watermark to specific digital content or a specific transaction. Hence, what is very difficult for other protocols can be resolved easily with the zero-watermark algorithm.

The *zero-watermark* algorithm also has the following further advantages.

(1) It simplifies the transactions steps needed for a watermarking protocol. Only **B** and **S** participate, and only two steps are required to complete the transaction.

(2) It is no longer necessary to embed the watermark information twice; once is enough. At the same time, the zero-watermark information does not have to be embedded in the original work. It not only improves the security of the protocol but also buys high-quality digital goods.

(3) It reduces the number of transmissions of digital work in the protocol. There is only one transmission in watermarking protocol, which greatly reduces the pressure on network bandwidth and improves the usability of the protocol.

(4) It does not require **S** to complete the task of embedding the watermark, thereby reducing the technology burden on business and making the protocol easy to promote.

(5) Everyone on the network can monitor the infringement of work available online.

## VI. CONCLUSION

The digital watermarking protocol is studied in this paper. Use of the zero-watermarking method results in greater improvement for a buyer-seller watermarking protocol. Theoretical analysis shows that the improved protocol solves the customer's rights problem, the client's problem of

anonymity and the unbinding problem. The transaction steps and operations are simplified in watermarking protocol. The number of transmissions of digital work is reduced, so the practicality and security of watermark protocol are greatly improved. The further application of digital watermarking will benefit from this.

As the zero-watermark is essentially a different concept of digital watermarking, it can be applied not only in the Lei protocol but also in other digital watermarking protocols.

At present, an agent is applied to the study of digital watermarking protocol, and a digital watermarking agent (DWA) implementation framework is proposed [12][13]. In the future, a digital watermarking agent could be used in a zero-watermark protocol framework, which would further enhance its flexibility, security and usability.

## REFERENCES


[1] Fabien A.R Petiteolas, Ross J. Anderson, Markus G. Kuhn. Information hiding – A survey, Proc. of IEEE, 1999, pp. 1062-1078.

[2] Wen Quan, Sun Tan-fen, Wang Shu-xun. Concept and application of zero-watermark, Acta Electronica Sinica, Vol. 31, No. 2, 2003, pp. 214-216. (in Chinese)

[3] L. Qiao and K. Nahrstedt. Watermarking schemes and protocols for protecting rightful ownership and customer's rights, J. Vis. Commun. Image Representation, Vol. 9, Sept. 1998, pp. 194–210.

[4] N. Memon and P. W. Wong. A buyer-seller watermarking protocol, IEEE Trans. Image Processing, Vol. 10, Apr. 2001, pp. 643-649.

[5] Franco Frattolillo. Watermarking protocol for web context. IEEE Transaction on Information Forensics and Security, Vol. 2, No. 3, September 2007, pp. 350-363.

[6] Chin-Laung Lei, Pei-Ling Yu, Pan-lung Tsai, Ming-Hwa Chan. An efficient and anonymous buyer-seller watermarking protocol, IEEE Transaction on Image Processing, Vol. 13, No. 12, December 2004, pp. 1618-1626.

[7] I. Cox, J. Bloom, M. Miller. *Digital Watermarking: Principles & Practice*. San Mateo, CA: Morgan Kaufman, 2001.

[8] Jian-Hu Ma, Yu-Jing Guan, Yu-hua Zhao. A method of zero-watermark based on lifting wavelet. Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition, Beijing, China, 2007, pp. 239-243.

[9] Ye Tian-yu, Ma zhao-feng, Niu Xin-xin, Yang Yi-xian. A zero-watermark technology with strong robustness. Journal of Beijing University of Post and Telecommunications, Vol. 33, No. 3, 2010, pp. 126–129. (in Chinese)

[10] Zhang Li-bao, Ma Xin-yue, Chen Qi. Image zero-watermarking algorithm based on region of interest. Journal of Communications, Vol. 30, No. 11A, 2009, pp. 117-120. (in Chinese)

[11] Sun Jian-guo, Zhang Guo-yin, Yao Ai-hong, Wu Jun-peng. *Lossless Digital Watermarking Technology for Vector Maps*. Acta Electronica Sinica, Vol. 38, No. 12, 2010, pp. 2786-2790. (in Chinese)

[12] Quan Wen, Xiaoying Sun, Yufei Wang. *Enhance the Security of Watermarking Protocol Using Fellow Agent*[C]. International Conference on Information Security and Artificial Intelligence (ISAI), Chengdu, China, 2010, pp. 82-86.

[13] Quan Wen, Yufei Wang. *Research on Digital Watermarking Agent Based on Software Behavior*[C]. The 3rd International Conference on Networks Security, Wireless Communications and Trusted Computing, 23-24 April, Wuhan, China, 2011, pp. 714-717.