An Enhanced Watermarking Protocol for Electronic Copyright Management

Jun Zhang, Weidong Kou, Kai Fan
The State Key Laboratory of Integrated Service Networks,
Xidian University, Xi'an, 710071, P. R. China
{zhangj, wdkou, kfan}@mail.xidian.edu.cn

Abstract

In Piva et al's watermarking scheme for Electronic Copyright Management System (ECMS), authors were considered trusted potentially, so a dishonest author could authorize more than one distributor to sell her one document, named "One Document to Multi-distributor" problem, which would damage the benefit of the distributors. To resolve the problem, in this paper, we propose an enhanced watermarking protocol based on Piva et al's scheme by introducing document nature code (DNC) and register records table. In addition, our protocol offers the distributor an efficient means to verify his right to an authorized digital document.

Keywords: *copyright management, digital watermarking, watermarking protocol, e-commerce*

1. Introduction

With the development of internet and e-commerce, digital copyright protection is becoming more and more important. Digital watermarking as a promising technology for protecting digital copyright has been studied for many years [1-3]. As we know, to achieve the desirable goal of protecting digital copyright, it is needed that not only a good watermarking algorithm but also a secure watermarking protocol [4-6].

Most of existing watermarking protocols concern the security of digital document transaction between a distributor and a customer, e.g., customer's right problem [7-9], private protection [10-12], and conspiracy attack [13-14]. In [15], Piva et al. proposed a watermarking scheme, which introduced a distinct difference with respect to the previous protocols, by considering the author and distributor as independent roles. The scheme is closer to reality, as authors and distributors are usually different entities. On the other hand, the scheme allows all participants in a digital document trade to verify their ownership rights by themselves. In [16], Victoria et al presented the results of the application of a risk analysis technique (specifically 'attack trees' technique) to Piva et al's watermarking protocol.

With more analysis on the security of Piva et al's watermarking scheme for ECMS, we point out that the author being considered trusted potentially result in "One Document to Multi-distributor" problem. Based on the original scheme, we propose an enhanced watermarking protocol for ECMS to resolve the problem.

The rest of this paper is organized as follows. In Section 2, Piva et al's watermarking scheme is reviewed, and Section 3 describes the proposed watermarking protocol in detail. Section 4 analyzes the security of the proposed protocol. Section 5 concludes this paper.

2. Related works

In this section, we first define the roles and notations to be used throughout the rest of this paper. Then we summarize Piva et al's watermarking scheme and explain "One Document to Multi-distributor" problem.

2.1. Roles and notations

In the rest of this paper, some different roles and notations involved are as follow.

(1) A: author, who is the owner of an original digital document.

(2) D: distributor, who is an authorized agent on the sales of certain digital document.

(3) C: customer, who wants to purchase a copy of a digital document from a distributor.

(4) CS: collecting society. We assume CS is a trusted third party that will promise that a protected digital document is traded correctly.

(5) ARB: arbiter, who is responsible for checking the participants' right to a digital document and adjudicating lawsuits against the infringement of copyright and intellectual property.

(6) (pk_I, sk_I): public-private key pair, that is, pk_I is I's public key, while sk_I is I's private key.

(7) $Sign_I(M)$: the signature of message M signed by I with his private key.

(8) $HASH(X)$: the digest of a digital document X.

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

(10) $D_{sk_I}(C)$: the original message of ciphertext C decrypted by I with his private key.

(11) $Cert_J(I)$: the digital certificate issued to I by J. Anyone is able to verify the validity of any certificate, and the public key associated with a particular subject can be easily obtained from his certificate.

(12) $X \oplus W$: $\oplus$ denotes the operation of watermarking insertion. X is an original digital document and W is a watermark to be inserted.

(13) $u \| v$: $\|$ stands for concatenation of two strings.

2.2. Piva et al's watermarking scheme

Piva et al proposed a watermarking scheme for ECMS in [15], and Fig.1 shows a simplified trading model. The protocol involves three parties, an author (A), a distributor (D) and a customer (C), which is closer to the reality.

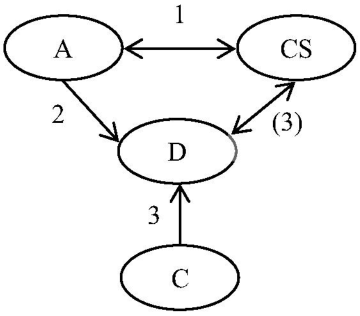
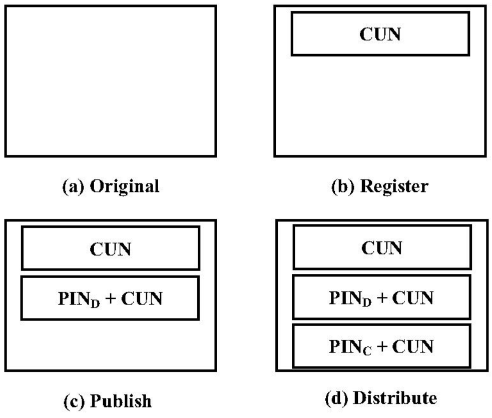


Figure 1. A simplified trading model



(a) Original

(b) Register

(c) Publish

(d) Distribute

Figure 2. A digital document at different phases

The scheme is composed of three subprotocols: the register protocol, the publish protocol and the distribute protocol. The author, the distributor and the customer's right to a digital document are proved by embedding three different identification watermarks. Figure 2. shows a digital documents in different phases.

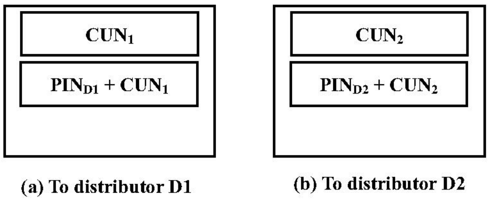
Register protocol. A registers a document in CS. First, A generates a CUN (Create Unique Number), which unambiguously identifies her document, and encrypts the CUN to get the first watermark, $W_A = E_{sk_A}(CUN)$. Then A embeds W_A into the document X, $X' = X \oplus W_A$, and transmits the watermarked document X' to CS. (Assume that the document can be identified as belong to A in some other ways).

Publish protocol. A authorizes D to sell copies of her creation. First, D sends his identifier PIN_D to A. A uses PIN_D and the document's CUN to produce the second watermark, $W_D = E_{sk_A}(PIN_D \| CUN)$. Then A embeds W_D into X', $X'' = X' \oplus W_D$, and sends the watermarked document X'' and W_D to D.

Distribute protocol. D sells a copy of the digital document to C. First, C forwards his identifier PIN_C to D. D sends PIN_C, CUN and the second watermark W_D to the CS. Then, CS uses PIN_C and CUN to create the third watermark, $W_C = E_{sk_{CS}}(PIN_C \| CUN)$, embeds it into X'', $X''' = X'' \oplus W_C$, and signs the digest of X''', $Sign = Sign_S(HASH(X'''))$. At last, CS transmits $Sign$ and W_C to D. D embeds W_C into X'', $X''' = X'' \oplus W_C$, and transmits X''', W_C, and $Sign$ to C.

2.3. One document to multi-distributor problem

In Piva et al's watermarking scheme, an author can authorize more than one distributor to sell her one document, named "One Document to Multi-distributor" problem, which will damage the benefit of the distributors. For simplicity, we describe in detail how an author can authorize two distributors to sell one document in three cases as follow.

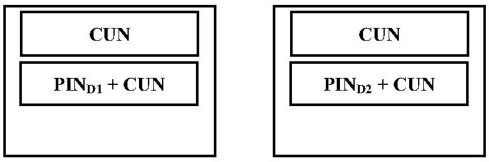


(a) To distributor D1

(b) To distributor D2

Figure 3. Case 1 of the problem

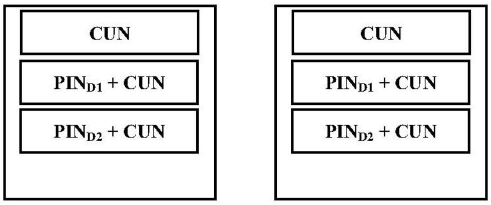
Case 1: The author generates two different create unique numbers, CUN_1 and CUN_2, for one original document. Then she registers in CS for two times, and deposits two different watermarked documents into CS archive. Other steps are the same as that in Piva et al's scheme. Thus the author can contact two distributors to publish her document. Figure 3 shows the watermarked documents to two distributors.



(a) To distributor D1 (b) To distributor D2

Figure 4. Case 2 of the problem

Case 2: The author generates one CUN for one original document. Then he registers in CS, and deposits a copy of the watermarked document into CS archive. Then, the author embeds two different distributor identifiers, PIN$_{D1}$ and PIN$_{D2}$, into the document, respectively. Other steps are the same as that in Piva et al's scheme. Figure 4 shows the watermarked documents to two distributors.



(a) To distributor D1 (b) To distributor D2

Figure 5. Case.3 of the problem

Case 3: The author generates one CUN for one original document. Then he registers in CS and deposits a copy of the watermarked document into the CS archive. After that, the author embeds two distributor identifiers, PIN$_{D1}$ and PIN$_{D2}$, into the document, simultaneously. Other steps are the same as that of Piva et al's scheme. Figure 5 shows the watermarked documents to two distributors.

In the three cases of the "One Document to Multi-distributor" problem, the author's CUN is embedded in the document, so the author can prove to ARB that she is the owner of the digital document. In addition, the distributor's identifications are embedded in the documents, so he can prove to ARB that he is authorized to sell his own watermarked document. Since the distributors are unable to find the fraudulence of the author, it is easy for the author to authorize more than one distributor to publish her document.

3. Proposed scheme

An enhanced watermarking protocol based on Piva et al's scheme is proposed to resolve the "One Document to Multi-distributor" problem by introducing document nature code (DNC) and register records. In addition, it is difficult for a distributor to verify the CUN in the second watermark is that in the first watermark in the original scheme, so we offer the distributor a simple means to achieve it in the proposed protocol.

3.1. Document nature code

Document nature code (DNC) is introduced to verify whether two digital documents are the same. In other words, if the similar degree between the DNC of two digital documents is above a judge threshold, we consider two digital documents are the same. Otherwise, two digital documents are different. Based on the algorithm proposed in [17], we propose a simple algorithm to verify whether two digital documents are the same using DNC as following.

Assume that the original document is an image X, which is a gray-level image with 8 b/pixel. X is defined as follows.

$$X = \{x_{i,j} \mid 0 \le x_{i,j} \le 255, 0 \le i < W_X, 0 \le j < H_X\} \qquad (1)$$

where W_X and H_X is the width and height of X, respectively.

1) Wavelet transforming of the original image: The original image is decomposed by performing t-level wavelet transform to obtain the subband LL_t. The size of subband $LL_t(L)$ is W_L and H_L. L is defined as

$$L = \{l_{i,j} \mid 0 \le l_{i,j} < 255, 0 \le i < W_L, 0 \le j < H_L\} \qquad (2)$$

2) Constructing DNC of X: The average value P_{av}^X of all pixels in L is calculated. Then DNC of X, DNC_X, is constructed as follows:

$$DNC_X = \{p_{m,n}^X \mid p_{m,n}^X \in \{0,1\}, 0 \le m < W_L, 0 \le n < H_L\} \qquad (3)$$

where

$$p_{m,n}^X = \begin{cases} 0, & \text{if } l_{m,n} < P_{av} \\ 1, & \text{if } l_{m,n} \ge P_{av} \end{cases} \qquad (4)$$

3) Verify whether two digital documents are the same using DNC. Assume two original digital documents are X and Y, the similar degree $Sim(X,Y)$ between them is calculated as follows:

$$Sim(X,Y) = 1 - \frac{\sum_{m=0}^{m=W_L} \sum_{n=0}^{n=H_L} p_{m,n}^X \otimes p_{m,n}^Y}{W_L \times H_L} \qquad (5)$$

where ⊗ denote XOR operation.

If $Sim(X,Y) > T$, where T is a judge threshold, we consider X and Y are the same. Otherwise, we consider X and Y are different.

3.2. An enhanced watermarking protocol

The proposed watermarking protocol contains three subprotocols like Piva et al's scheme: the register protocol, the publish protocol and the distribute protocol. We assume all participants in a digital document transaction have their digital certifications issued by CA.

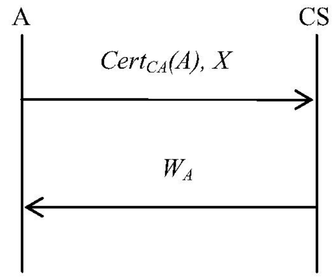


Figure 6. Data exchange in register protocol

Register protocol. A transmits her digital certificate $Cert_{CA}(A)$ and an original document X to CS for register. We assume CS manages a register records table, e.g., table.1. First, CS calculate the DNC of X , DNC_X . (Similar to Piva et al's scheme, we assume that the document can be identified as belong to A in some other ways). Then, CS uses pk_A as a keyword to search register records and gets the DNC of A's registered documents. After that, CS compares X with arbitrary A's registered documents using DNC according to the algorithm described in section 3.1. If CS finds that X is the same as one of A's registered document, that is, X has been registered before, the register protocol aborts. Otherwise, CS generates a CUN, which identifies A has the ownership of the document, and uses the CUN to create the first watermark, $W_A = E_{sk_{CS}}(CUN)$. At last, CS embeds W_A into the document X , $X' = X \oplus W_A$, calculates the digest of X' , $HASH(X')$. CS saves pk_A , CUN, $HASH(X')$ and DNC_X as a new register record, and sends the first watermark W_A to A. A embeds W_A into X to get X' , $X' = X \oplus W_A$, and decrypts W_A with CS's public key to get CUN, $CUN = D_{pk_{CS}}(W_A) = D_{pk_{CS}}(E_{sk_{CS}}(CUN))$.

Table.1 Register records

pk	CUN	PIN	HASH	DNC
pk_{A1}	CUN_{11}	PIN_{D11}	$HASH(X_{11}')$	DNC_{X11}
	CUN_{12}	PIN_{D12}	$HASH(X_{12}')$	DNC_{X12}
	…	…	…	…
pk_{A2}	CUN_{21}	PIN_{D21}	$HASH(X_{21}')$	DNC_{X21}
	…	…	…	…
	…	…	…	…
…	…	…	…	…

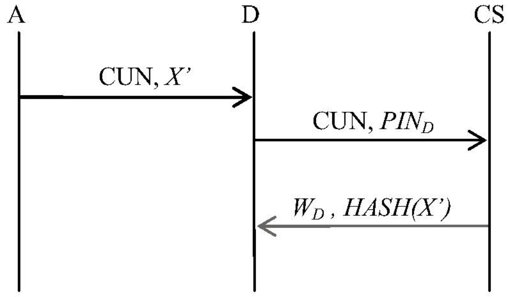


Figure 7. Data exchange in publish protocol

Publish protocol: To publish a digital document X, A sends the document identifier CUN and the watermarked document X' to a distributor (D). D sends its identifier PIN_D and CUN to CS. CS then uses CUN as a keyword to search register records, and check whether the document has been published. If PIN of a distributor has existed in X's register record, that is, the digital document has been published, the publish protocol aborts. Otherwise, CS fills PIN_D into X's register record, and uses the concatenation of PIN_D and CUN to computer the second watermark, $W_D = E_{sk_{CS}}(PIN_D \| CUN)$. Then, CS transmits $HASH(X')$ and W_D to D. D computes a digest of X' , and compares it with $HASH(X')$ offered by CS to verify whether the CUN in the second watermark is the same as that in the first watermark W_A . If two hash of X' are equal, D embeds W_D into X' , $X'' = X' \oplus W_D$. Otherwise, the publish protocol aborts.

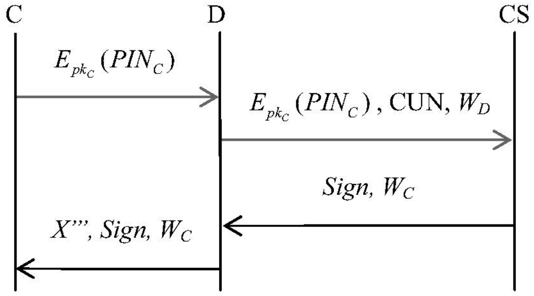


Figure 8. Data exchange in distribute protocol

Distribute protocol: To purchase a copy of a digital document, C computes $E_{pk_c}(PIN_C)$, and sends it to D. D transmits $E_{pk_c}(PIN_C)$, CUN and W_D to CS. CS produces the third watermark by encrypting the concatenation of $E_{pk_c}(PIN_C)$ and CUN, $W_C = E_{sk_{CS}}(E_{pk_C}(PIN_C) \| CUN)$, and embeds it into the watermarked document X'' , $X''' = X'' \oplus W_C$. Then CS signs a digest of X''' ,

$Sign = Sign_{CS}(HASH(X'''))$, and transmits $Sign$ and W_C to D. At last, D embeds W_C into X'' to get X''', $X''' = X'' \oplus W_C$, and transmits X''', $Sign$ and W_C to C. Figure 8 shows the details of the distributor protocol.

4. Discussion

The security of the proposed watermarking protocol relies on the security of the underlying watermarking and encryption techniques. We take particularly care to examine the protocol itself and how to resolve the problems arise in Piva et al's scheme.

(I) Similar to Piva et al's scheme, the document is self-contained in the proposed watermarking protocol. At any given instant the document contains all the information needed to verify whether the current holder is using the data legally, and ARB can check the holder's right to the document.

Suppose ARB asks A to prove that he is the original owner of a multimedia document X. The author can give the watermarked document X' and the first watermark W_A to ARB. ARB first checks the first watermark W_A for CUN, then, by applying a watermark detection engine to the document, it verifies that the watermark with CUN is actually embedded in the data.

Suppose ARB asks D to prove that he is allowed by A to publish the document. D can give the watermarked document X'' and the second watermark W_D to ARB. ARB decrypts W_D for PIN_D and CUN, and verifies that the document contains W_D and the CUN is the same as that in the first watermark W_A.

Suppose ARB asks C to prove his right to the digital document in its possession. C can give his identifier PIN_C, the third watermark W_C and digital certificate $Cert_{CA}(pk_C)$ to ARB. ARB computes $E_{pk_C}(PIN_C)$, and checks W_C for C's identifier PIN_C. Then CS can verifier X''' contains W_C by applying a watermark detection engine to the watermarked document X'''. At last, ARB can contact CS to verifier the CUN in W_C is the creation unique number of the document.

(II) The proposed watermarking protocol can avoid the "One Document to Multi-distributor" problem, which is described as following.

In case 1 of the problem, A needs to register one document in CS for two times, with different CUN. However, in the register phase of our protocol, CS will verify whether the digital original document X has been registered using DNC. If X has been registered before, the protocol aborts. So A can't achieve her goal, that is, "One Document to Multi- distributor" problem can be avoided.

In case 2 of the problem, A needs to embed different PIN into the document for different distributors. However, in the publish phase of our protocol, CS will verify whether the document has been published. If the document has been published, the protocol aborts. So A can't achieve her goal, and the problem can be avoided.

In case 3 of the problem, similar to case.2, CS can know whether A's document has been published, so A is unable to authorize more than one distributor to sell her document.

(III) The proposed protocol offers a simple means for D to verifier its right to the document. To prove his right to the document to ARB, D must prove that the document contains W_D, whose identifier PIN_D is in W_D, and the CUN in W_D is the same as that in W_A. In the proposed protocol, D gets W_D from CS, and embeds it into the document. So D can assure the document contains W_D. By decrypting W_D to get PIN_D, D can also assure that his identifier is embedded in the document. In addition, D can calculate the digest of X' by itself, and compare it with $HASH(X')$ offered by CS. If two hash is equal, the CUN in the second watermark W_D is the same as that in the first watermark W_A. Otherwise, two CUN are different. Thus, D can verify his right to the document by itself easily.

5. Conclusion

In this paper, we propose an enhanced watermarking protocol for ECMS based on Piva et al's scheme, which can resolve the "One Document to Multi- distributor" problem. We achieve some improvements over original scheme as following.

(1) In the register phase of our protocol, CS will assure that the original digital document hasn't been registered using DNC. Then CS generates unique CUN for the document.

(2) In the publish phase of our protocol, CS will assure that the document hasn't been published by searching the register records table.

(3) The distributor can easily verify that the CUN in the second watermark is the same as that in the first watermark by itself.

Acknowledgement

This work was supported by Graduate Innovation Fund of Xidian University, the NSFC Grant 90304008 and the CUDSFC 20040701001.

References

[1] Anun Kejaniwal, Watermarking, IEEE Potentials, pp.37-40, October /November 2003

[2] N. Memon and P. W. Wong, Protecting Digital Media Document, Commun. ACM, vol.41, no.7, pp.35-43, July 1998

[3] G. Voyatzis, N. Nikolaidis, and I. Pitas, Digital Watermarking: An Overview, in Proc.9th Eur. Signal Processing Conf., pp.9-12, Sept. 1998

[4] Scott Craver, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung, Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications, IEEE Journal on Selected Areas in Communication, v 16, n 4, pp.573-586, May 1998.

[5] Stefan Katzenbeisser, On the Intergration of Water- marks and Cryptography, IWDW 2003, LNCS 2939, pp.50-60, 2004.

[6] G. Voyatzis and I. Pitas, The Use of Watermarks in the Protection of Digital Multimedia Products, Proc.IEEE, vol.87, pp.1197-1207, July 1999.

[7] L. Qiao and K. Nahrstedt, Watermarking Schemes and Protocols for Protecting Rightful Ownerships and Customer's Rights, Journal of Visual Communication and Image Representation, 9(3):194-210, 1998.

[8] N.Memo and P.W.Wong, A Buyer-Seller Water- marking Protocol, IEEE Trans. Image Processing, vol.10, pp.643-649, Apr. 2001.

[9] Chin-Laung Lei, Pei-Ling Yu, Pan-Lung Tsai, and Ming-Hwa Chan, An Efficient and Anonymous Buyer-Seller Watermarking Protocol, IEEE Trans. Image Processing, vol.13, pp.1618-1626, December 2004.

[10] Shing-chi Cheung, Ho-fung Leung, and Changjie Wang, A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Documents, IEEE Proceeding of the 37th Havaii International Conference on System Sciences 2004.

[11] Hak Soo Ju, Hyun Jeong Kim, Dong Hoon Lee, and Jong In Lim, An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control, ICISC 2002, LNCS 2587, pp.421-432, Springer-Verlag Berlin Heidelberg 2003.

[12] Bok-Min Goi, Raphael C. W. Phan, Yanjiang Yang, Feng Bao, Robert H. Deng, and M.U. Siddiqi, Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity, ACNS 2004, LNCS 3089, pp.369-382, Spring-Verlag Berlin Heidelberg 2004.

[13] Jae-Gwi Choi, Kouichi Sakurai, and Ji-Hwan Park, Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party, ACNS 2003, LNCS 2846, pp.265-279, Springer-Verlag Berlin Heidelberg 2003.

[14] Bok-Min Goi, Raphael C.-W. Phan, Yanjiang Yang, Feng Bao, Robert H. Deng, and M.U. Siddiqi, Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity, LNCS 3089, pp.369-382, Spring Verlag 2004.

[15] Alessandro Piva, Franco Bartolini, and Mauro Barni, Managing Copyright in Open Networks, IEEE Internet Computing, pp.18-26, MAY/JUN 2002.

[16] M^a Victoria Higuero, Juan Jose Unzilla, Eduardo Jacob, Purificacion Saiz, and David Luengo, Application of 'attack trees' technique to copyright protection protocols using watermarking and definition of a new transactions protocol SecDP (secure distribution protocol), MIPS 2004, LNCS 3311, pp.264-275, Spring-Verlag Berlin Heidelberg 2004.

[17] Tzung-Her Chen, Gwoboa Horng and Wei-Bin Lee, A Publicly Verifiable Copyright-Proving Scheme Resistant to Malicious Attacks, IEEE transaction on industrial electronics, vol. 52, No. 1, February 2005.