AN EFFECTIVE AND SECURE WATERMARKING PROTOCOL FOR DIGITAL RIGHTS PROTECTION OVER THE SECOND-HAND MARKET

Ibrahim M. Ibrahim, Sherif Hazem Nour El-Din
Information Technology Industry Development Agency (ITIDA), Egypt

Abdel Fatah A. Hegazy
Arab Academy for Science and Technology and Maritime Transportation, Cairo, Egypt

Keywords: Buyer-seller watermarking protocol, E-commerce, public key cryptosystems, copyright protection, customer's rights, digital rights management.

Abstract: Different buyer-seller watermarking protocols have been proposed to address preserving the digital rights of both the buyer and the seller over the first-hand market. However, the support of the digital rights over the second-hand market is still rarely addressed. This paper proposes an effective and secure watermarking protocol for digital rights protection over the second-hand market. This protocol achieves customer's rights protection, copy deterrence, protocols' practice applicability, preventing the buyer's participation in the dispute resolution and defending man in the middle attack along with solving the unbinding and conspiracy problems over the second-hand market. The protocol's security is based on the public key infrastructure (PKI) and exploits the existence of the certification authority (CA) that is considered the only trust anchor between the buyer and the seller.

1 INTRODUCTION

In the last few years, the internet has seen dramatic growth in the demand of the digital contents in different forms. This led to the evolution of different e-commerce models such as Business-to-Consumer (B2C), Consumer-to-Consumer (C2C) and Business-to-Consumer-to-Consumer (B2C2C). However, the ease of illegal copying and distributing of the digital objects over the internet represents a major threat to these models. This leads to the evolution of a great challenge represented in preserving the digital rights of the seller (business) and the buyer (consumer). In order to tackle this challenge over the first-hand market, several buyer-seller watermarking protocols have been proposed (L.Qian, 1998), (Memon N., 2001), (Ju, H.S., 2002), (Chin-Chen Chang, 2003), (Lei C.-L, 2004) and (J.Zhang, 2006).

On the other hand in order to support the rights protection of the digital objects over the second-hand market, S.C.Cheung and Hanif Curreem (Shing-Chi Cheung, 2002) have proposed buyer-seller watermarking protocol for digital contents redistribution over the internet (second-hand market). In this protocol, the buyer requests a valid watermark from watermark certification authority (WCA) with his/her public key (Pk_B). The watermark certification (WCA) then issues the buyer a valid watermark (W) and its digital signature of the encrypted watermark ($Sign_{WCA}(E_{PkB}(W))$) named as watermark certificate. When the buyer requests to purchase a digital object (X) from the reseller, the buyer sends the reseller his/her watermark certificate. The reseller then sends his/her copy of the digital object (X) along with the buyer's watermark certificate to the content distributor (CD) and requests transfer of ownership. Finally, the content distributor (CD) transfers the ownership from the reseller to the buyer and sends the result to the reseller who will in turn send it to the buyer. This protocol supports the change of ownership and relaxes the requirement of confidentiality of encrypted watermarks (Shing-Chi Cheung, 2002). Furthermore, the protocol prevents the buyer from

M. Ibrahim I., Hazem Nour El-Din S. and Fatah A. Hegazy A. (2007).
AN EFFECTIVE AND SECURE WATERMARKING PROTOCOL FOR DIGITAL RIGHTS PROTECTION OVER THE SECOND-HAND MARKET.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 263-268
DOI: 10.5220/0002121202630268
Copyright © SciTePress

the participation in the dispute resolution. However, the proposed protocol has not protected the customer's rights totally since it allows a malicious content distributor (CD) to access the reseller's copy of the digital object. This will allow the malicious content distributor (CD) to illegal resell that copy and the reseller has no way to prove his/her innocence. The protocol's practice applicability has not been achieved totally since the buyer has to contact more than one party (i.e. the reseller and the watermark certification authority) to complete the purchase transaction which is considered inconvenient in practice. In addition, the protocol has not solved the unbinding problem (Lei C.-L, 2004) since a malicious seller is able to intentionally transplant a watermark initially embedded in a copy of certain digital object into another copy of a completely different digital object provided both copies are sold to the same innocent buyer. Furthermore, the protocol has not solved the conspiracy problem (J.Zhang, 2006) since a malicious seller may cooperate with an untrustworthy watermark certification (WCA) to fabricate piracy to frame an innocent buyer; on the other hand, a malicious buyer may collude with an untrustworthy third party to confound the tracing of piracy by removing the watermark from digital digital object.

In this paper an effective and secure watermarking protocol for digital rights protection over the second-hand market that overcomes all the previously mentioned shortcomings along with preventing the man in the middle attack is proposed. The proposed protocol exploits the idea of the buyer's dual signature of the purchase order and the associated buyer's unique watermark to solve the unbinding problem along with its dependence on the existence of the trusted certification authority (CA) to solve the conspiracy and the buyer's participation in the dispute resolution problems.

The rest of this paper is organized as follows. In section (2) the proposed watermarking protocol is elaborated. Section (3) discusses how the proposed protocol achieves its goals. Section (4) concludes the achievements done.

2 PROPOSED SCHEME

The proposed protocol composes of two sub-protocols which are watermarking generation/insertion protocol and dispute resolution protocol. The proposed protocol assumes that each of the buyer, the seller, the reseller and the judge has a key pair (Pk_I, Sk_I) such that (Pk_I) is the public key of party (I) and (Sk_I) is the private key of party (I). Each key pair is associated with a valid X.509-compliant digital certification (R.Housley,2002) issued by trusted certification authority (CA). This will help to establish the public key infrastructure (PKI). In addition, the protocol can deploy any invisible and private watermarking technique taken into consideration that the attacks of watermarking technique are out of scope of this paper. Furthermore, the proposed protocol assumes that the encryption function used in the public key infrastructure is a privacy homomorphism with respect to the watermark insertion operation ($\oplus$) (D.Stinson, 1995). The privacy homomorphism property states that for every *(a)* and *(b)* in the message space, there exists an encryption function (E_{PkI}) and watermark insertion operation ($\oplus$) that satisfy equation (1).

$$E_{PkI}(a \oplus b)=E_{PkI}(a) \oplus E_{PkI}(b) \qquad (1)$$

For example, the well known RSA cryptosystem (R.Rivest, 1978) is a privacy homomorphism with respect to the multiplication (D.Stinson, 1995).

The proposed protocol assumes for the first-hand market that the reseller (R) purchases a copy of the digital object (X) from the seller (S) associated with a digital object's license *(OL)*. The digital object (X) contains the seller's unique watermark *(Q)* and the reseller's unique watermark *(W)*. On the other hand, the digital object's license *(OL)* contains the reseller's unique customer number, the index number of the original digital object. The index number is the storage identification of the original digital object (X) in the seller's digital contents database. In addition, the digital object's license *(OL)* also contains the reseller's number of the resells allowed that counts down with every purchase transaction. In order to prevent the reseller (R) from tampering with the digital object's license *(OL)*, the seller (S) maintains a copy of the reseller (R) digital object's license *(OL)* in his/her rights management database (RMDB).

The parties involved in the proposed protocol are:

- (B): The buyer of the digital object (X).
- (R): The reseller of the digital object (X) who was a buyer in the first-hand market.
- (S): The seller and the owner of the digital object (X).

2.1 Watermarking Generation / Insertion Protocol

In order to support the digital rights protection over the second hand market, the following steps which are illustrated in figure (1) are conducted:

1. (B) sends (R) a request to purchase the digital object (X).
2. (R) responds to (B) with his/her digital certificate *($Cert_{CA}(R)$)*.
3. (B) and (R) set up a common agreement *(ARG)* between them. This *(ARG)* identifies the digital object (X) to be purchased and states explicitly the rights and obligations of (B), (R) and (S). Furthermore, this *(ARG)* is considered as a purchase order that binds the digital object (X) to the specified purchase transaction.
4. (B) computes the message digest of *(ARG)*, i.e. *(H(ARG))*, and encrypts the output with his/her private key *($E_{SkB}(H(ARG))$)* to be sent later to (R) in step (8) who will in turn send it to (S) in step (10). The result *($E_{SkB}(H(ARG))$)* is used by other participants (i.e. (S) and the judge) to verify that (B) has done the purchase order *(ARG)*.
5. (B) generates for this transaction a unique watermark *(W_B)*. This watermark will be used twice during this protocol. First, (B) will encrypt this watermark *(W_B)* with (B)'s private key and the result is then encrypted with (CA)'s public key *($E_{PkCA}(E_{SkB}(W_B))$)*. This will be used by the judge in case of dispute to know (B)'s watermark *(W_B)* without (B)'s participation in the dispute resolution as explained in the dispute resolution protocol (section (2.2), step (3)).
6. The second usage of (B)'s unique watermark *(W_B)* is to allow its embedding into the digital object (X) without allowing neither (R) nor (S) to access *(W_B)*. This can be achieved by encrypting the watermark *(W_B)* with (B)'s public key *($E_{PkB}(W_B)$)* to be sent later to (R) in step (8) who will in turn send it to (S) in step (10). It is worth mentioning that (S) will be able to embed (B)'s watermark *(W_B)* in the digital object (X) without having access to *(W_B)* by exploiting the privacy homomorphism property of the encryption function used with respect to the watermark insertion operation as shown in step (17).
7. (B) computes his/her dual signature by calculating the message digest of the watermark *(W_B)*, i.e. *($H(W_B)$)*, and concatenates it with the message digest of the *(ARG)* (i.e. *(H(ARG))*) computed earlier. The result is then hashed and encrypted with (B)'s private key. The output of this process *($E_{SkB}(H(H(W_B)+H(ARG))))$* is considered as (B)'s dual signature of *(ARG)* and *(W_B)*. This dual signature will prevent a malicious seller from intentionally transplant (B)'s unique watermark *(W_B)* into another higher-priced copy and hence solving the unbinding problem.
8. (B) sends (R) the results of step (4) *($E_{SkB}(H(ARG))$)*, step(5) *($E_{PkCA}(E_{SkB}(W_B))$)*, step (6) *($E_{PkB}(W_B)$)* and step (7) *($E_{SkB}(H(H(W_B)+H(ARG))))$* along with his/her certificate (*$Cert_{CA}(B)$*).
9. (R) computes the message digest of *(ARG)*, i.e. *(H(ARG))*, and encrypts the output with his/her private key *($E_{SkR}(H(ARG))$)*. The result *($E_{SkR}(H(ARG))$)* will be used by the judge in the dispute resolution protocol to compare it with *($E_{SkB}(H(ARG))$)* to validate the agreement of both (B) and (R) on the purchase order *(ARG)*.

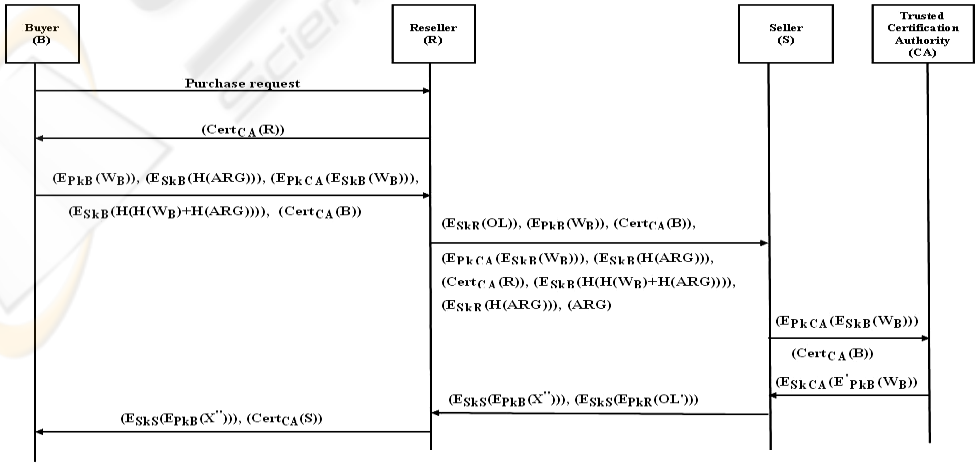

Figure 1: Watermarking generation/insertion protocol.

10. (R) encrypts his/her digital object's license *(OL)* with his/her private key *($E_{SkR}(OL)$)* and sends it to (S) along with the result of step (9) *($E_{SkR}(H(ARG))$)*, the purchase order *(ARG)* and his/her certificate *($Cert_{CA}(R)$)*. In addition, (R) forwards to (S) the following items received from (B) *($E_{SkB}(H(ARG))$)*, *($E_{PkCA}(E_{SkB}(W_B))$)*, *($E_{PkB}(W_B)$)*, *($E_{SkB}(H(H(W_B)+H(ARG))))$* and *($Cert_{CA}(B)$)*
11. In order for (S) to ensure that (B)'s watermark *(W_B)* used in *($E_{PkCA}(E_{SkB}(W_B))$)* is the same as (B)'s watermark *(W_B)* used in *($E_{PkB}(W_B)$)*. This will prevent malicious (B) from fabricating piracy to frame (S). (S) performs two steps. Firstly, (S) sends *($E_{PkCA}(E_{SkB}(W_B))$)* and *($Cert_{CA}(B)$)* to (CA). (CA) then decrypts *($E_{PkCA}(E_{SkB}(W_B))$)* using its private key followed by decrypting the output *($E_{SkB}(W_B)$)* with (B)'s public key resulting in *(W_B)* as illustrated in equations (2) and (3). (CA) then encrypts *(W_B)* with (B)'s public key obtained from *($Cert_{CA}(B)$)* followed by encrypting the output with (CA)'s private key. Finally (CA) sends the result *($E_{SkCA}(E'_{PkB}(W_B))$)* to (S).

$$E_{SkB}(W_B) = D_{SkCA}(E_{PkCA}(E_{SkB}(W_B))) \quad (2)$$

$$W_B = D_{PkB}(E_{SkB}(W_B)) \quad (3)$$

12. Secondly, (S) decrypts *($E_{SkCA}(E'_{PkB}(W_B))$)* using (CA)'s public key and then computes the message digest of the result *($E'_{PkB}(W_B)$)* (i.e. *$H'((E'_{PkB}(W_B)))$*) and computes the message digest of *($E_{PkB}(W_B)$)* sent earlier by (R) in step (10) (i.e. *$H((E_{PkB}(W_B)))$*) and compares them. If they are equal the protocol continues else the protocol throws exception and terminates.
13. In order to validate the agreement between both (B) and (R) on the purchase order *(ARG)*, (S) decrypts *($E_{SkR}(H(ARG))$)* using (R)'s public key then decrypts *($E_{SkB}(H(ARG))$)* using (B)'s public key and computes the message digest of the *(ARG)* sent by (R), i.e. *($H'(ARG)$)*, and compares the three outputs. If they are equal the protocol continues else the protocol terminates
14. (S) decrypts *($E_{SkR}(OL)$)* using (R)'s public key to get (R)'s digital object's license *(OL)*. (S) uses *(OL)* to obtain the reseller's unique customer number and the index number of the original digital object (X) then uses these information to search his/her rights management database (RMDB) for the number of resells allowed for (R).
15. (S) checks the number of the resells allowed for (R) against the number of copies of the digital object (X) requested by (B) specified in the purchase order *(ARG)*. If valid the protocol continues else the protocol terminates.
16. (S) uses the index number of the original digital object (X) to retrieve it from his/her digital contents database. (S) then generates for this transaction a unique watermark *(V)* and inserts it in the digital object (X) by using equation (4) resulting in *(X')*.

$$(X') = (X) \oplus (V) \quad (4)$$

17. (S) encrypts *(X')* with (B)'s public key *($E_{PkB}(X')$)* and inserts (B)'s encrypted watermark *($E_{PkB}(W_B)$)* in it through calculating equation (5) that exploits the privacy homomorphism property of the encryption function used (E_{PkB}) with respect to the watermark insertion operation($\oplus$).

$$E_{PkB}(X'') = E_{PkB}(X') \oplus E_{PkB}(W_B) \quad (5)$$

18. (S) then updates the number of resells allowed for (R) in (S)'s rights management database (RMDB) (counts down the number of resells allowed) and generates a new digital object's license *(OL')* for (R). In order to send the updated version *(OL')* to (R) while preventing man in the middle attack, (S) encrypts *(OL')* with (R)'s public key and then encrypts the result with (S)'s private key (i.e. *($E_{SkS}(E_{PkR}(OL'))$)*) In addition, (S) encrypts *(E_{PkB} (X''))* using his/her private key *($E_{SkS}(E_{PkB}(X''))$)* and sends (R) *($E_{SkS}(E_{PkB}(X''))$)* and *($E_{SkS}(E_{PkR}(OL'))$)*.
19. (S) stores in his/her sales database the following items *(V)*, *(ARG)*, *($E_{SkR}(H(ARG))$)*, *($E_{SkB}(H(ARG))$)*, *($E_{PkCA}(E_{SkB}(W_B))$)*, *$Cert_{CA}(B)$*, *$Cert_{CA}(R)$*, *($E_{SkB}(H(H(W_B)+H(ARG))))$*. Since *(V)* is unique for each purchase order, (S) can retrieve any purchase order's information using *(V)*.
20. (R) obtains his/her updated digital object's license *(OL')* by using equation (6) and (7).

$$E_{PkR}(OL') = D_{PkS}(E_{SkS}(E_{PkR}(OL'))) \quad (6)$$

$$(OL') = D_{SkR}(E_{PkR}(OL')) \quad (7)$$

21. (R) sends (B) *($E_{SkS}(E_{PkB}(X''))$)* and *($Cert_{CA}(S)$)*. It is worth mentioning that (R) has obtained *($Cert_{CA}(S)$)* during the first-hand market purchase transaction with (S).
22. Finally (B) obtains the final digital object (X'') by using equation (8) and (9).

$$E_{PkB}(X'') = D_{PkS}(E_{SkS}(E_{PkB}(X''))) \quad (8)$$

$$X'' = D_{SkB}(E_{PkB}(X'')) \quad (9)$$

2.2 Dispute Resolution Protocol

When a pirated copy (Y) of an original digital object (X) owned by (S) is found in the market. (S) starts gathering the required information to specify the original buyer (copy deterrence). In order to represent to the judge the needed clues to declare the responsible buyer guiltiness, the following steps are conducted:

1. (S) runs the corresponding watermark detection and extraction algorithm to extract his/her watermark *(V)* from the pirated copy (Y). (S) uses *(V)* which is unique for each purchase order to search his/her sales database for the matching record. Upon finding it, (S) retrieves the associated following items *(V)*, *(ARG)*, $(E_{SkR}(H(ARG)))$, $(E_{SkB}(H(ARG)))$, $(E_{PkCA}(E_{SkB}(W_B)))$, $Cert_{CA}(B)$, $Cert_{CA}(R)$, $(E_{SkB}(H(H(W_B)+H(ARG))))$ and sends them along with (X') (i.e.$(X'=X \oplus V)$) and (Y) to the judge.
2. In order to make sure that (B) has purchased the digital object (Y) from (R) with (S)'s agreement, the judge decrypts $(E_{SkR}(H(ARG)))$ with (R)'s public key by using equation (10) then decrypts $(E_{SkB}(H(ARG)))$ with (B)'s public key by using equation (11) and finally computes the message digest of the *(ARG)* sent by (S) (i.e. $(H'(ARG))$) and compares the three outputs. If they are equal the protocol continues else the protocol terminates with declaring (B) as innocent.

$$H(ARG) = D_{PkR}\,(E_{SkR}(H(ARG))) \quad (10)$$

$$H(ARG) = D_{PkB}\,(E_{SkB}(H(ARG))) \quad (11)$$

3. In order to validate (B)'s ownership of the pirated copy (Y), the judge performs two steps. First, the judge obtains (B)'s watermark without (B)'s participation by sending $(E_{PkCA}(E_{SkB}(W_B)))$ to the certification authority (CA) along with the judge's certificate $(Cert_{CA}(J))$. The certification authority (CA) decrypts $(E_{PkCA}(E_{SkB}(W_B)))$ using its private key and then encrypts the output with the judge's public key obtained from his/her certificate and sends the result $(E_{PkJ}(E_{SkB}(W_B)))$ to the judge. The judge then obtains (W_B) by using equation (12) and (13).

$$E_{SkB}(W_B) = D_{SkJ}(E_{PkJ}(E_{SkB}(W_B)) \quad (12)$$

$$W_B = D_{PkB}(E_{SkB}(W_B) \quad (13)$$

4. The second step to validate (B)'s ownership of the pirated copy (Y) is done by the judge by running the corresponding watermark detection and extraction algorithm taken (X'), (W_B) and (Y) as inputs. If (W_B) is detected the protocol continues to prove (B) guiltiness else the protocol terminates with declaring (B) as innocent.
5. Finally, the judge needs to validate that (B) has purchased the digital object (Y) from (R) with (S)'s agreement and that (B)'s watermark (W_B) is used with this purchase order *(ARG)*. This can be achieved by computing (B)'s dual signature of the *(ARG)* and (W_B) through calculating the message digest of *(ARG)* (i.e. $(H'(ARG))$) and the message digest of (W_B) (i.e. $(H'((W_B)))$) and concatenating them and then computing the message digest of the result (i.e. $(H'(H'(ARG)+(H'(WB))))$. Furthermore, the judge decrypts $(E_{SkB}(H(H(W_B)+H(ARG))))$ using (B)'s public key and compares the result $(H(H(WB)+H(ARG)))$ with $(H'(H'(ARG)+(H'(WB))))$. If the comparison fails then (B) is declared as innocent otherwise (B) is declared as guilty.

3 DISCUSSION

In this section, the capabilities of the proposed protocol to achieve the desired features over the second-hand market are elaborated as follows:

- The proposed protocol is fair enough for the buyer achieving the customer's rights protection. Since the buyer is the only one who has access to both his/her watermark (W_B) and the final digital object (X''). Therefore, a malicious seller is prevented from fabricating piracy to frame an innocent buyer either by illegally reselling his/her digital object (X'') or using the buyer's watermark (W_B) in any illegal way. In addition, the protocol prevents a malicious buyer from removing his/her watermark (W_B) from the final digital object (X'') since he/she does not have access to either the original digital object *(X)* or knowledge of the embedding watermarking algorithm used by the seller. Furthermore, the protocol secures the reseller since his/her copy of the digital object *(X)* is not revealed to any party during the protocol's procedures.
- The protocol solves the copy deterrence problem. Since the proposed protocol enables an honest seller to trace the pirated copies to the original buyer by allowing the seller to insert his/her unique watermark *(V)* which is unique for each purchase order in the digital object *(X)* and then storing *(V)* with the buyer's identity

and all the purchase transaction information in the seller's sales database.

- The buyer's participation in the dispute resolution is not required since the protocol exploits the existence of the certification authority (CA) as the only trust anchor between the buyer and the seller.
- The buyer has to contact only one party (the reseller) in order to complete the purchase transaction which is considered more convenient in practice than contacting more than one party and therefore increases the protocol's practice applicability.
- The protocol has been secured against the man in the middle attack based on exploiting the public key cryptography in all the communication between the different parties (the seller, the reseller, the buyer and the judge).
- The buyer's dual signature of the *(ARG)* and his/her unique watermark (W_B) has been used to solve the unbinding problem. For example, if a malicious seller intentionally transplants an innocent buyer's watermark (W_B) initially embedded in a copy of certain digital object into a copy of another digital object provided both copies are sold to the same innocent buyer, then a different (ARG') is formulated and hence this will lead to different buyer's dual signature $(H(H(W_B)+H(ARG')))$ and as a result step (5) in the dispute resolution protocol will fail declaring the buyer's innocence.
- The proposed protocol solves the conspiracy problem by eliminating the need of the participation of any untrustworthy third party. Since the protocol only requires the participation of the certification authority (CA) in the dispute resolution which is considered the only trust anchor between the buyer and the seller.

4 CONCLUSIONS

In this paper an effective and secure watermarking protocol for digital rights protection over the second-hand market has been proposed. The protocol preserves the customer's rights and allows an honest seller to trace a pirated copy to the original buyer (copy deterrence). In addition, the buyer has to contact only one party (the reseller) during the purchase transaction that increases the protocol's practice applicability. The protocol has also supported over the second-hand market that the buyer is not required to participate in the dispute resolution which is more convenient in practice. Furthermore, the protocol is secured against the man in the middle attack based on the public key infrastructure (PKI) along with solving the unbinding and conspiracy problems in effective, secure and yet convenient manner.

REFERENCES

R. Rivest, A. Shamir and L. Adelman, 1978. "A method for obtaining digital signatures and public key cryptosystems". In *Commun. ACM*, Vol. 21, pp. 120–126.

J. D. Cohen and M. J. Fischer, Oct. 21–23, 1985. "A robust and verifiable cryptographically secure election scheme (extended abstract)". In *Proc. IEEE 26th Annu. Symp. Foundations Computer Science, Portland, OR*, pp. 372–382.

D. Stinson, 1995. In *Cryptography: Theory and Practice*. Boca Raton, FL: CRC.

L.Qian and K.Nahrstedt, Seprember 1998. "Watermarking schemes and protocols for protecting rightful ownership and customer's rights". In *J. Visual Commun. Image Represent.*, Vol. 9, pp. 194–210.

Memon N. and Wong P.W., 2001. "A buyer–seller watermarking protocol". In *IEEE Trans. Image Process.*, Vol. 10, No. 4, pp. 643–649.

S. Katzenbeisser, Sept. 2001. "On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking". In *Proc. 12th Int. Workshop Database and Expert Systems Applicat.*, pp. 815–819.

Ju, H.S., Kim, H.J., Lee, D.H., and Lim, J.I., 2002. "An anonymous buyer–seller watermarking protocol with anonymity control", In *Lee, P.J., and Lim, C.H. (Eds): Proc. ICISC*, LNCS 2587, pp. 421–432.

Shing-Chi Cheung and Hanif Curreem, 2002. "Rights Protection for Digital Contents Redistribution Over the Internet". In *COMPSAC 2002: 105-110.*

R. Housley, W. Polk, W. Ford, and D. Solo, Apr. 2002. "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile". In *RFC 3280*.

Chin-Chen Chang, Chi-Yien Chung, 2003. "An Enhanced Buyer Seller Watermarking Protocol". In *Proceedings of ICCT.*

Lei C.-L., Yu P.-L., Tsai P.-L., and Chan M.-H., 2004. "An efficient and anonymous buyer–seller watermarking protocol". In *IEEE Trans. Image Process*, Vol. 13, No. 12, pp. 1618–1626.

J.Zhang, W.Kou and K.Fan, March 2006. "Secure buyer-seller watermarking protocol". In *IEE Proc.-Inf. Secur.*, Vol. 153, No. 1.