Pseudonymous Privacy Preserving Buyer-Seller Watermarking Protocol

Neelesh Mehra[1], Dr. Madhu Shandilya[2]

[1] Department Of Electronics and Communication, S.A.T.I(Engg.)College, Vidisha, M.P, India.

[2] Department Of Electronics, M.A.N.I.T, Bhopal, M.P, India.

Abstract

A buyer-seller watermarking protocol utilize watermarking along with cryptography for copyright and copy protection for the seller and meanwhile it also preserve buyers rights for privacy. Up to now many secure BSW protocol has been suggested but the common problem with all of them is that in all of them is the buyer's involvement in generation of some cryptographic key or watermark or digital signature what happened if buyer is not capable or is a layman and does not understand what cryptography and watermarking means. In this paper we proposed the use of open access identification concept for this buyer has to get registered with some trusted third party which after registration provide an open access ID which is unique. This not only provide anonymity to buyer but the seller can also provide some benefit to his loyal customers. In our scheme non of the watermark or cryptographic key is generated by buyer so a layman buyer can also use it. It also enables a seller to successfully identify a malicious seller from a pirated copy, while preventing the seller from framing an innocent buyer and provide anonymity to buyer.

Keywords: **Buyer-Seller watermarking protocols; watermarking; copy protection; copyright protection**

1. Introduction

Now a days multimedia data is floating throughout the world wide web . The ease by which digital content can be stored and processed without any loss of quality resulted in illegal replication and distribution of digital content To prevent this Digital Right Management Technologies(DRM) has been developed. DRM utilize special properties of cryptography and watermarking for copyright protection of multimedia data and to prevent unauthorized use of digital content. But due to lack of implementation rule a uniform DRM system is not possible yet. Earlier research on fingerprinting schemes have been conducted by Pfitzmann etal. [1], and by Camenisch et al. [2]. The shortcoming of these schemes lies in their inefficiency. A buyer-seller watermarking protocol is one that combines encryption, digital watermarking, and other techniques to ensure rights protection for both the buyer and the seller in e-commerce. The first known buyer-seller watermark protocol was introduced by Memon et al. [3].Since the first introduction of the concept, several alternative design solutions have been proposed in [4,5,6,7].

The main feature of a buyer-seller watermarking protocol is to enable a honest seller to successfully identify a traitor from a pirated content copy, while preventing the dishonest seller from framing an innocent buyer and also preserve anonymity of buyer. A buyer-seller watermarking scheme may involves the two steps[10].

(I) A watermark is embedded by seller to identify the buyer of a digital product, such as an image.

(II) When a pirated copy is found, the seller will detect the watermark of the pirated copy and verify the buyer with the help of some trusted third party. A secure buyer-seller watermarking protocol is must consist of following properties

Traceability: A copyright violator should be able to be traced and identified. Non-framing: Nobody can accuse an honest buyer.

Non-repudiation*:* A guilty buyer cannot deny his responsibility for a copyright violation caused by him.

Dispute resolution: The copyright violator should be identified and adjudicated without him revealing his private information, e.g. private keys or secret watermark.

Anonymity*:* A buyer's identity is undisclosed until he is judged to be guilty.

Most of the proposed protocols has the above said properties, these protocols are infeasible as most of the protocols underlying the assumption that the buyer has the knowledge of cryptography and watermark. However, the buyer may have or have-not any knowledge of cryptography and watermark so the involvement of buyer must be reduced in the generation of watermark and cryptographic Key without neglecting his rights. Second, a buyer must interact with different parties many times and exchange different keys and store them this is very inconvenient to the buyer and accuse a high communication load.

Almost many of the above mentioned technical problems are solved in the scheme proposed by Alfredo Rial et al in their Privacy preserving Buyer-Seller watermarking Protocol(PBSW) based on Price Oblivious Transfer(POT) besides this some practical problem remain unsolved and need to be discussed. Firstly in this protocol Buyer has to interact many times with seller and Trusted third party making system more complicated for buyer. Secondly buyer is anonymous for seller so seller cannot give some advantage to his loyal customers this may be against the marketing policy of many companies. Thirdly seller doesn't learn items bought by customer so he cannot planned strategically to improve his business. fourth short comes of this scheme is what happened if seller deliver wrong item in place. Lastly if buyer is corrupt and claiming the deliver items are not that item which he actually ordered there is no counterparts suggested to deal such types of practical problem. In this paper we propose a novel pseudo privacy preserving buyer-seller watermarking protocol which is capable to solve all the technical problem along with all practical problems mentioned above and overcome the drawbacks existing in the present protocols. Our protocol is easy to implement and accomplished in fewer steps causing no extra computation burden on the buyer The rest of this paper is organized as follows. In Section II, we describe our proposed watermarking protocol in detail. In Section III, we discuss the working of proposed scheme , in Section IV we analyze proposed method. Finally, in Section V, we summarize our work.

2. PROPOSED SCHEME

Our buyer-seller watermarking protocol consist of a buyer denoted by "B", a seller "S" trusted third party called as copyright Certification Authority (Bank) is a certification and registration authority which is responsible for registration of buyers($B_{1,}B_2$…….B_n) and seller (S_1,S_2….S_n)and to embed second watermark which is invisible and used to verify the misbehavior of any buyer or seller also verify the payment condition ,So it can be any commercial bank so this trusted third party can be said as "Bank" .Finally An Judge "J", who adjudicates lawsuits against the infringement of copyright and intellectual property. The buyer-seller watermarking protocol we proposed in this section has four sub protocols: registration protocol, watermark generation protocol, watermark insertion protocol, copyright violation and dispute resolution protocol. In our protocol, we assume the following assumptions hold. (1) A public key infrastructure PKI is well developed. (2) The TTP is assumed to be trustworthy. (3) The encryption function used in the PKI, i.e. (Ek), is assumed to be a privacy homomorphism with respect to watermark insertion operation $\oplus$. By privacy homomorphism with respect to $\oplus$ we mean it has the property that $\mathrm{Ek}\,(a \oplus b) = \mathrm{Ek}\,(a) \oplus \mathrm{Ek}\,(b)$.

Our algorithm has been accustomed of following signs

B:Buyer of certain multimedia content
S: seller of certain multimedia concept
CCA :Copyright certifying authority
sKB: private key of CCA
pKB: public key of buyer issued by CCA
TID: Transaction ID
CA: Certificate of authenticity

2.1 Registration

Registration process has two phase both are mutually explicit one is for customer and another is for seller

The registration protocol, performed between the buyers($B_{1,}B_2$…….B_n) and the copyright Certification Authority (Bank) the registration process as follows:

Step 1. If the buyer B wants to remain anonymous during transactions, he asks Bank for an anonymous certificate and get himself registered with Bank.

Similar to above the Seller has to get registered with Certification authority and request a certificate of authenticity from the bank

Step 2. Bank now provide an open access identity which will act as pseudo-identity for the buyer and will be the identity of buyer for seller .

This registration is one time process and will be valid until any of the party involve will refuse to continue.

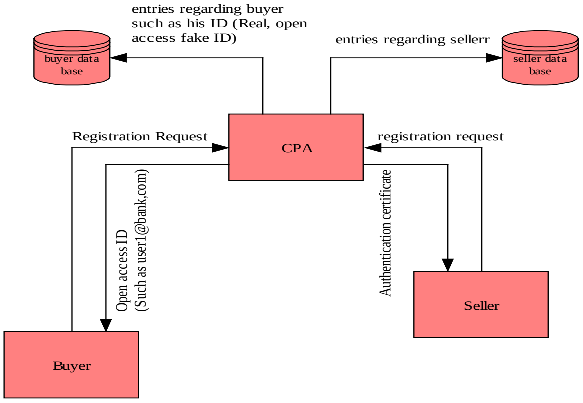
entries regarding buyer such as his ID (Real, open access fake ID)
entries regarding sellerr
buyer data base
seller data base
Registration Request
CPA
registration request
Open access ID (Such as user1@bank,com)
Authentication certificate
Seller
Buyer

Figure 1

2.2 Initialization

The initialization of protocol starts as the buyer wish to purchase a message (m_1 to m_n), this process performed between the buyer(B) and the Certification Authority (Bank) the Initialization process as follows:

Step 1. buyer asks Bank for an anonymous certificate and sends detail of items and seller to Bank,

Step 2. Bank verify from seller about the items availability and their price and confirm the amount deposit in account of buyer .

Step 3. After confirmation Bank selects a key pair (pkB , skB) randomly, then he generates an anonymous certificate $\mathrm{Cert}_{\mathrm{CCA}}$(pkB) and an anonymous transaction

ID (TID) which can identity B. Bank sends certificate Cert CA(skB), skB (TID) to B and Cert CA(pkB) to S.

2.3 Watermark Generation and embedding Protocol At Seller End

Seller S generates a watermark V which can be used to identify the guilty user. This is a protocol between Buyer Seller and Trusted Third Party

Step 1. When B wants to buy a digital content X from the seller" S", B first negotiates with seller"S" to set up an agreement (ARG) which explicitly states the rights and obligations of both parties and specify the digital content X . The ARG uniquely binds this particular transaction to X and can be regarded as a purchase order.Buyer B sends his transaction ID (TID) to Seller

Step 2. Upon receiving transaction ID (TID) from B, S verify it with the TID provide by Bank, If it is valid, S generate or select (from his database) a unique watermark "VW" which is visible watermark and unique key pair(pkS , skS) for this particular transaction.

Step 3. Now this watermark is embedded by S in digital content X such that

$X' = X \oplus skS(VW)$

Step 3. Now X' is encrypted with the Private key send by buyer and send it to bank ie.S sends EpkB(X'), to bank and the public Key pkS to buyer.

2.4 Watermark Embedding Protocol At Bank End

Step 1. When Bank receives the encrypted digital product EpkB (X') from S, It decrypt it with the help of his private key afterwards bank generates or select (from his database) a watermark(IW) and a symmetric key(pKt) to insert a invisible watermark(IW) in X', buyer is anonyms of this watermarking. Seller may knows about invisible watermark but he doesn't know about what generated watermark

Such as: $X'' = EpkB [X' \oplus EpKt((IW)]$

Step 2. After that, X'' is send to B along with TID.

When B receives the encrypted watermarked X'' he decrypt and remove visible watermark by using public key pkS. The entire protocol can be summarized by seeing figure 1 and 2

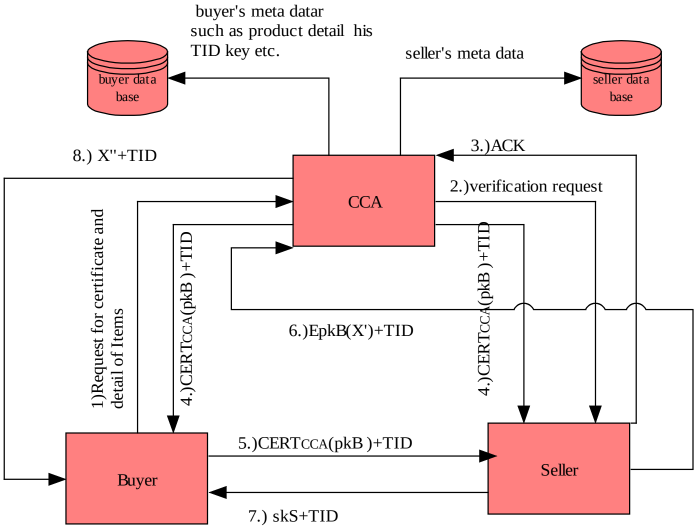

Figure 2.

Identification and Dispute Resolution:

When Seller found an unauthorized copy of content X, seller raises the matter to CCA.

1) Seller sends the pirated copy to CCA.

2) CCA extract invisible watermark and match with the database of buyer's .

3) if both invisible watermark is same then buyer is guilty and can be challenged in front of judge

4) If seller tries to frame innocent buyer then no invisible watermark is found or it will not match with the database of buyer since for every transaction CCA will choose different watermark.

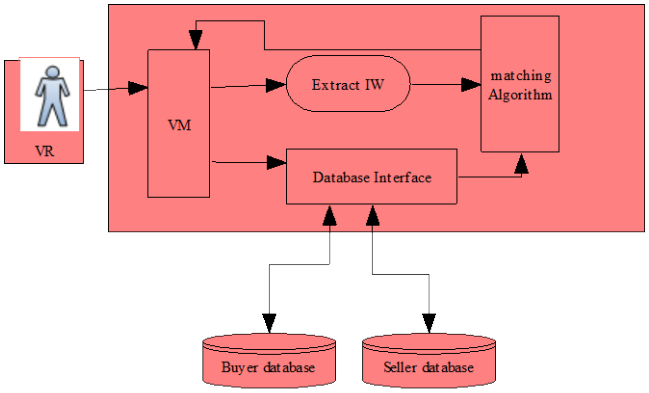

Figure 3.

3. Accountability Analysis

Ownership Right Protection : Owner of the digital work embed visible watermark with his private key into the image for owner authentication. The buyer can remove this with his public key for restriction free use of this digital work. The ownership right is now protected by the invisible watermark which is inserted by the bank which is semi fragile in nature thus helpful in tracing malicious buyer to trace if pirated copy found. A semi-fragile watermark is sensitive to non-permitted modifications. Ideally, a semi-fragile watermark would gloss over innocent alterations on the image (for example postproduction editing, mild compression, filtering or contrast enhancement) but it should give alarm when content change occurs or in case of high compression rates. So, if a client tries to do any kind of malicious manipulations such as the addition or removal of a significant element of the image, would invalidate the image. Also an owner can prove his ownership with the help of copyright Certification Authority (Bank) . In case of any dispute copyright Certification Authority (Bank) extracts the copyright watermark from the disputed digital product and verifies the watermark and copyright information submitted by the valid requester with the information stored in the owner's database.

Client's Right Protection : If the seller wants to frame the innocent buyer he can sell the digital content with his own visible watermark but it cannot insert the invisible watermark, since the bank issue the certificate for the deal he cannot cheat buy supplying the wrong digital content. In case of any dispute, the right verification of a valid-requester (a client in this case) is done by the verification module in the CPA. CPA uses its verification module to extract the client certificate and watermark for any dispute.

Pirate Root Identification : The Pirate root identification is provided by the CPA. When a suspicious copy of the digital image is submitted to CPA, the CPA uses its verification module to extract invisible watermark using watermark extraction algorithm and match it with client database

Anonymity problem : The anonymity of the buyer can be retained during the transaction unless the buyer is judged by ARB to be guilty of piracy. In our proposed protocol, the dispute resolution protocol can be carried out well without the buyer's participation, so the buyer's privacy right is well protected.

Buyer's participation in the dispute resolution problem : Buyer's participation is not required in dispute resolution protocol with the assistance of Trusted Third Party(TTP) It can prevent malicious seller from annoying innocent buyer by repeatedly enforcing the buyer to participate in the dispute resolution.

4. CONCLUSION

In this paper we try to build a Buyer-Seller watermarking protocol which is capable to solve the common problems. Since none of the cryptographic key and watermark is generated or embedded by buyer it reduces computational cost at buyer end and make it easy to use by a laymen buyer also. Since buyer is using open access ID issued by CCA thus remain anonymous and since this ID is unique so seller can give some reward to it's loyal customer. No need of buyer's involvements in any kind of dispute until he is found guilty. Lastly the number of times of buyer's interaction with seller is less then other protocol.

References

[1] B. Pfitzmann and A.-R. Sadeghi. Anonymous fingerprinting with direct non-repudiation. In Advances in Cryptology ASIACRYPT '00, LNCS 1976, pages 401–414. Springer-Verlag, 2000.

[2] J. Camenisch. Efficient anonymous fingerprinting with group signatures. In ASIACRYPT, LNCS 1976, pages 415– 428. Springer-Verlag, 2000.

[3] N. D. Memon and P. W. Wong. A buyer-seller watermarking protocol. IEEE Transactions on Image Processing, 10(4):643–649, 2001.

[4] J.-H. P. Jae-Gwi Choi, Kouichi Sakurai. Does it need trusted third party? design of buyer-seller watermarking protocol without trusted third party. In Applied Cryptography and Network Security, LNCS 2846, pages 265–279, 2003.

[5] B.-M. Goi, R. C.-W. Phan, Y. Yang, F. Bao, R. H. Deng, and M. U. Siddiqi. Cryptanalysis of two anonymous buyer seller watermarking protocols and an improvement for true anonymity. In Applied Cryptography and Network Security,
LNCS 2587, pages 369–382, 2004.

[6] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan. An efficient and anonymous buyer-seller watermarking protocol. IEEE Transactions on Image Processing, 13(12):1618–1626, 2004.

[7] J. Zhang, W. Kou, and K. Fan. Secure buyer-seller watermarking protocol. In IEE Proceedings Information Security, volume 153, pages 15–18, March 2006.

[8] M.-H. Shao. A privacy-preserving buyer-seller watermarking protocol with semi-trust third party. In Trust, Privacy and Security in Digital Business, LNCS 4657, pages 44–53, August 2007.

[9] Mina Deng, Bart Preneel,"On secure and anonymus buyer-seller watermarking protocol",in proceeding of IEEE International Conference ICIW,pages 524-529,June2008

[10] Defa Hu, Qialiang Li," A secure and practical buyer-seller watermarking protocol",in proceeding of IEEE International Conference MINES,pages 105-108,Nov.2009

[11]Huang Daren et al," A DWT Based Image Watermarking Algorithm, in proceeding of IEEE International Conference on Multimedia and Expo,pages 429-432,Aug..2001

[12] S.C.Ramesh ,M.Mohamad Ismail Majeed," Implementation of a visible watermarking in a secure still digital camera using VLSI design",in proceeding of IEEE

International Conference AFRICON,pages 798-801,Sept.2009