A Practical Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform

Ashwani Kumar
Dept of Computer Science & Engg, Jaypee University of Information Technology Waknaghat, Distt. Solan, H.P., India

Vipin Tyagi
Dept of Computer Science & Engg, Jaypee University of Information Technology Waknaghat, Distt. Solan, H.P., India

Mohd Dilshad, Kapil Kumar
Dept of Computer Science & Engg, Jaypee University of Information Technology Waknaghat, Distt. Solan, H.P., India

ABSTRACT
Digital watermarking is the key technology of digital copyright protection. An efficient digital watermarking solution must tackle the problems of copyright protection and trace of pirate copy. Digital water marking is a promising technology to embed information as unperceivable signals in digital contents. It plays a very important role in E-commerce. Buyer-seller watermarking protocols based on Discrete Wavelet Transform (DWT) integrate multimedia watermarking and fingerprinting with cryptography, for copyright protection, piracy tracing, and privacy protection. It uses the public key encryption schemes. In this paper we propose a Practical Buyer Seller watermarking protocol based on Discrete Wavelet Transform (DWT) which is secure and flexible and gives more security from previous watermarking protocols to both buyer and seller. In this we use Public Key Infrastructure (PKI), arbitrator and watermarking certificate authority (WCA) for better security. The protocol has better security property and higher efficiency.

Keywords
public key infrastructure; copyright protection; Digital watermarking;

1. INTRODUCTION
The development of information technology, more and more multi-media information is stored, processed and transmitted on Internet. The models of information distribution, transmission and sharing experience drastic changes. There arises an important problem concerning copyright protection of digital production [1]. The rapid growth of computer networks increased use of multimedia data via the Internet have resulted in fast and convenient exchange of digital information. In digital watermarking an imperceptible signal "mark" is embedded into the host image, which uniquely identifies the ownership. Copyright marking [3] is a relatively new technique for hiding information in multimedia content with the aim of tracing any traitor who redistributes the content illegally. Digital watermarking [4] has been proposed, complementing encryption techniques, to establish and prove ownership rights by embedding the seller's information in the redistributed content. A number of watermarking protocols have been proposed in [5] to track down the distributors of illegal replicas.

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. In general, the watermark could be visible or invisible. A visible watermark typically consists of visible text message or a company logo indicating the ownership of the digital content. In contrast, invisible watermarked content appears identical to the original. The only way to find out the existence of the invisible watermark is to examine the digital content with appropriate watermark detection and extraction algorithms. A complete and sound buyer-seller watermarking protocol is used to solve the following problems:

1.1 The customer's rights problem
When a watermark is inserted solely by the seller, the seller may benefit from framing attacks to an innocent buyer.

1.2 The piracy tracing problem
The seller should be able to trace and identify the copyright violator. The unbinding problem- The seller may fabricate piracy by transplanting the buyer's watermark into other contents.

1.3 The anonymity problem
The buyer should be anonymous during transactions until he is adjudicated to be guilty.

1.4 Certification authority obligation problem
This problem occurs in existing watermarking protocol. The problem is to provide a certificate for both buyer and seller.

In general, a buyer-seller watermarking scheme for traitor tracing involves three steps. First, a seller embeds a watermark that identifies the buyer into a digital product, such as an image. Second, when a pirated copy is found, the seller will detect the watermark of the pirated copy. At last, once the watermark of a specific buyer is identified, the seller will take the case to a court. A buyer-seller watermarking protocol combines encryption, digital watermarking, and fingerprinting, in order to ensure copyrights protection, privacy, and security for both the buyer and the seller simultaneously in e-commerce. Digital watermarking is a promising technology employed by various digital rights management (DRM) systems to achieve rights management. Watermarking techniques can be broadly classified into two categories: such as spatial domain methods [4][6] and transform domain methods [8]. Spatial domain methods are less complex as no transform is used, but are not robust against attacks. Transform domain watermarking techniques are more robust in comparison to spatial domain methods. Among the transform domain watermarking techniques discrete wavelet transform (DWT) based watermarking techniques are gaining more popularity because DWT has a number of advantages over other transform such as progressive and low bit-rate transmission, quality scalability.

2. RELATED WORK

There are many watermarking protocols which have been proposed using cryptography techniques. The intuitive idea of watermark-based fingerprinting has been implemented by a number of schemes using cryptographic techniques before the customer's right problem was first identified in [8]. Recent researches show that a secure watermarking protocol is protecting the participants' digital content during transaction using digital watermarking technique and a public key cryptosystem. The first known buyer-seller watermark protocol was introduced by Memon et al. [6], and it was improved by Ju et al. [7]. Since the first introduction of the concept, several alternative design solutions have been proposed in [8, 10, 11]. I Memon and Wong proposed a buyer-seller watermarking protocol in [7] to deal with the customer's right problem, but also introduced a new issue, the unbinding problem, in their solution. We propose a practical buyer-seller watermarking protocol based on discrete wavelet transform (DWT) to fulfill the design requirements, Different from the predecessors, our approach makes improvements on the many aspects such as anonymous communication between buyer and seller, it support multi-transaction and dispute resolution and avoid double watermark insertion. This paper proposes a practical buyer-seller watermarking protocol with DWT based on public key encryption standard, which is secure and flexible, to solve all the problems which are defined above.

Using the concept of discrete wavelet transform it results that it may increase the security of the protocol hence the efficiency will increase. The previous protocols were having problems describes above.

3. PROPOSED PROTOCOL

In the proposed protocol we have used DWT to provide more security for the buyer and the seller during the transmission of digital content. In this section we first define the role and notations which are given in table-1. In the rest of paper we have given assumptions and a watermark protocol. We also define the wavelet decomposition and determination of watermarking location. Figure 2 shows the sub-band distribution. We cover our entire proposed protocol with figure 4 & 5.which explain the transaction in proposed protocol.

In our proposed protocol we use robust watermark technique proposed by L Qiao [15] with the RSA cryptosystem [16]. In this, there are four roles where one is buyer, another is a seller, and other is a WCA device, the fourth is DWT. The seller provides the watermark embedding operation and sells the watermarked product to the buyer. The WCA device is integrated into the seller's computer system and it will generate the watermark with the help of DWT for the buyer. We assume that every seller in transaction has unique water marking embedded function algorithm in the software. In the proposed protocol we use watermarking embedding with discrete wavelet transform (DWT), and group signature (GS), arbiter (ARB) and watermarking certificate authority (WCA). We also assume that all messages are transferred in a secure manner and digital content is still image.

3.1 Watermark generation and extraction protocol with Discrete Wavelet transform (DWT)

The watermark generation and extraction protocol using discrete wavelet transform (DWT), as depicted in fig 1 & 2. The process of watermarking embedding includes wavelet decomposition of original image, features extraction, watermarking embedding and wavelet reconstruction. Original image is decomposed by using 2-demension discrete wavelet transformation (DWT) and coefficients of each sub-band from which the features are extracted. Coefficients that meet some specific conditions are selected for watermarking embedding. Then, watermarking is embedded by changing these coefficients according to specific regulation. Finally the modified coefficients are reconstructed with other coefficients to watermarked image by using inverse 2-DWT (IDWT).

The process of watermarking extraction includes wavelet decomposition of watermarked image, feature extraction and watermarking extraction, and correlation resolving. After wavelet decomposition of watermarked image, features that meet specific requirements are extracted and watermarking are embedded in these locations.

3.1.1 Watermark Insertion using DWT

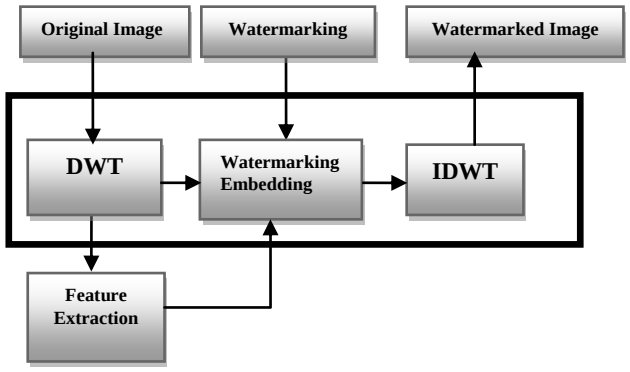

Figure 1: DWT Based Encoder

3.1.2 Watermark Extraction using DWT

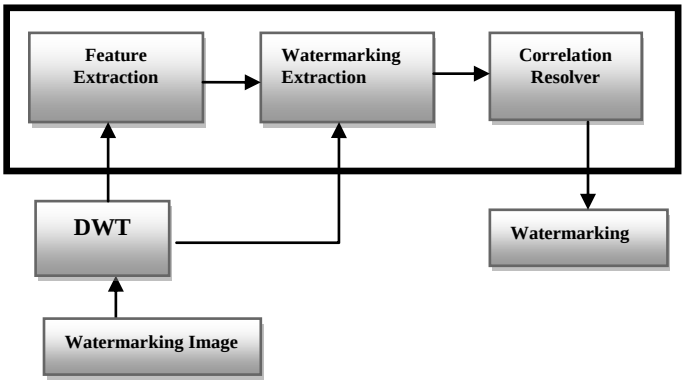

Figure 2: DWT Based Decoder

3.2 Wavelet decomposition

After 3-level wavelet transform decomposition, the original image is decomposed into 10 sub-bands with different resolution and directions shown in Fig. 3. These sub-bands include one low frequency sub band labeled as LL3 and nine intermediate and high frequency sub-bands labeled as LH1-3, HL1-3 and HH1-3. LL3 is selected in this algorithm as locating reference sub-band and LH2, HL2, HH2, LH3, HL3 and HH3 as watermarking embedding sub-bands.

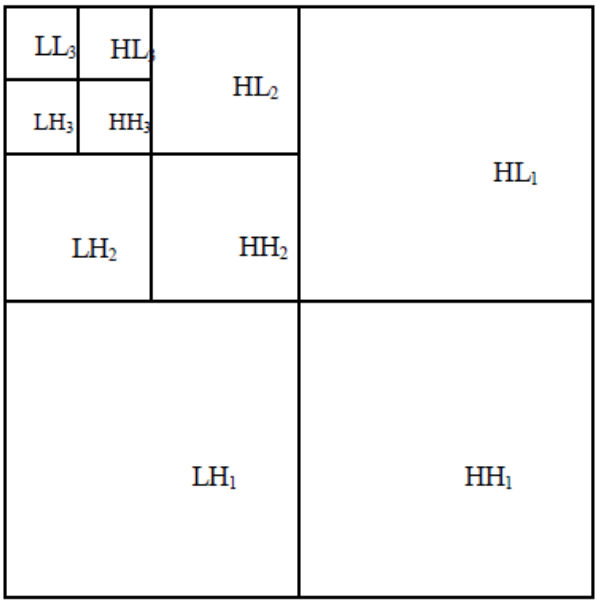

Figure 3: Sub-band Distribution

3.3 Determination of watermarking locations

Watermarking locating is a critical technique of blind watermarking. To accurately detect watermarking, the location of embedding point must be stable. It is required that the feature points should have features preventing against noise, image processing and geometric distortion.

In Wavelet watermarking, Xia et al. [9] firstly proposed that significant large intermediate frequency coefficients could be chosen as embedding carrier and the locations of these coefficients were locations where watermarking were located at the time of embedding and indexed at the time of extraction. However, these coefficients change significantly due to watermarking embedding and noise, image processing and image compression. It is difficult to locate precisely and will result in high probability of detection failure. Watermarking can be located by means of recording the watermarking locations when embedding [2]. This method makes high accuracy of watermarking locating and prevents watermarking against noise and image compression and processing which are specially used to attack digital watermarking. However, this kind of algorithm needs large amount of memory. It is apparently impractical because each image requires special memory to record the locations of watermarking. Using secret key and special algorithm to create watermarking embedding locations is an effective method. This kind of method can avoid too many memory spending. However, because of random-city of watermarking embedding locations, the inherent features of image are not sufficiently used and results in bad harmony between transparency and robustness for watermarking. Although watermarking embedding locations need not to be record or create when embedding in the form of sequential blocks, lack of random-city will result in security problems. Watermarking locating is realized by mapping spatial coordinates from low frequency to intermediate frequency. Because above 99 percent of energy of image is concentrated in, the low frequency coefficients present very good ability in anti-interference and anti-compression. Watermarking locating completely meet the requirements of inflexibility. Proposed spatial coordinates relationship between locating reference sub-band (LL3) and embedding sub-bands (LH1-3, HL1-3, HH1-3) is shown in Fig. 4.

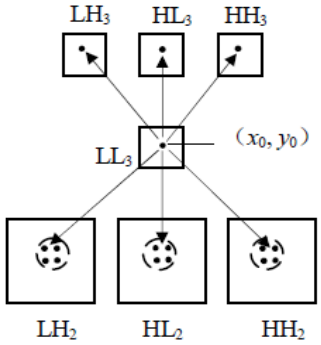

Figure 4: spatial coordinates relationship between LL3 and embedding sub-bands.

4. WATERMARKING PROTOCOL

Figure 5 shows the proposed practical buyer-seller watermarking protocol based on DWT, which is secure than its predecessors. The proposed model based on any public key cryptosystem has five different roles as follows.

S: The Seller, from where the buyer purchases the digital content. The seller may be the original owner of the digital content, or an authorized reselling agent or dealer.

B: The Buyer, who wants to purchase a digital content from the seller S.

WCA: Watermark Certification Authority, responsible for issuing public and secret key for anyone who likes to take part in commerce via internet. CA also issues the digital signature certificate based on private key in such a way that anyone in the electronics commerce transaction will be able to check the authenticity to avoid any future repudiation. WCA can also be viewed as trusted watermark certification authority, which is responsible for generating valid watermark for any digital contents registered to it.

ARB: An Arbiter, who adjudicates lawsuits against the infringement of copyright and intellectual property with the help of WCA.

DWT: Discrete Wavelet Transform is used for embedding the watermark into the image or video or audio, for transfer the digital content between the buyer and seller.

S → Seller
B → Buyer
WCA → Watermark Certificate Authority

4.1 Analyses of Current Protocols

In this we discuss our practical buyer seller watermarking protocol based on discrete wavelet transform (DWT). It should be mentioned that the protocols here are theoretical results other than application oriented protocols. The capabilities of the proposed practical buyer-seller watermarking protocol based on DWT to solve the previously common problems which are defined above.

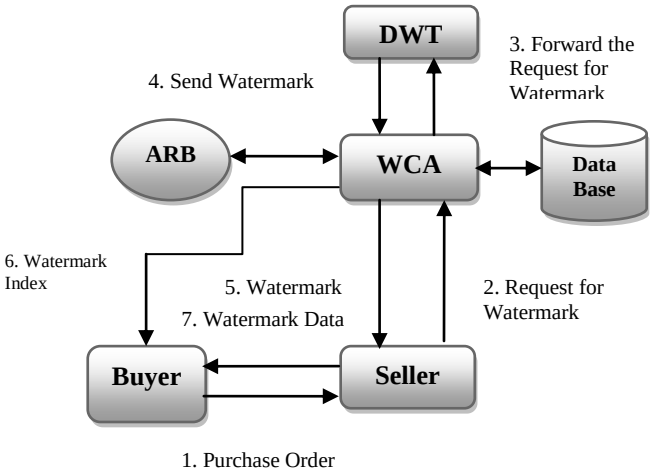

Figure 5: A Practical Buyer Seller Watermarking protocol with DWT

The figure 6 shows the details of possible transactions in the proposed watermarking protocol. Step-by-step procedures of the Transactions are given below:

1. When B wants to purchase a digital content from S, after negotiation B will place the purchase order (PO) by encrypting SB, ESB(PO), along with digitally signing the PB using SB, DSSB(PB).

2. S checks the authenticity by analyzing the digital signature using B's public key and decrypts the PO using PB. S places request for valid digital watermark (WR), buyer contact information (BI) such as IP address and other details to CA, along with encrypted PB using SS key, ESS(WR+BI+PB), and with digitally signing the PB using SS, DSSS(PB).

3. Forward the request for watermark to the DWT device.

4. Receiving the request for generating the watermark W from WCA, to DWT will do so after checking the digital signature. It generates a watermark with the help of DWT which is DWTWID and sends it to a WCA device.

5. Upon receiving the request for generating the watermark W from S, CA will do so after checking the digital signature. Watermark W directly depends on B's and S's public keys and Product-Copy ID number (PB, PS and PCID). Following conditions are satisfied when the watermark W is generated:

$$\Gamma(\mathrm{PB}, \mathrm{PS\ PCID}) \rightarrow \mathrm{W} \quad (1)$$

$$\mathrm{f}(\mathrm{W}, \mathrm{SB}) \rightarrow \mathrm{PS} \quad (2)$$

$$\mu(\mathrm{X'}\Phi(\mathrm{W}, \mathrm{PB})) \rightarrow \mathrm{X'} \quad (3)$$

$$\mu'(\mathrm{X'}©(\mathrm{PB})) \rightarrow \mathrm{W} \quad (4)$$

$$\mu''(\mathrm{X'}\emptyset(\mathrm{SB})) \rightarrow \mathrm{W'} \quad (5)$$

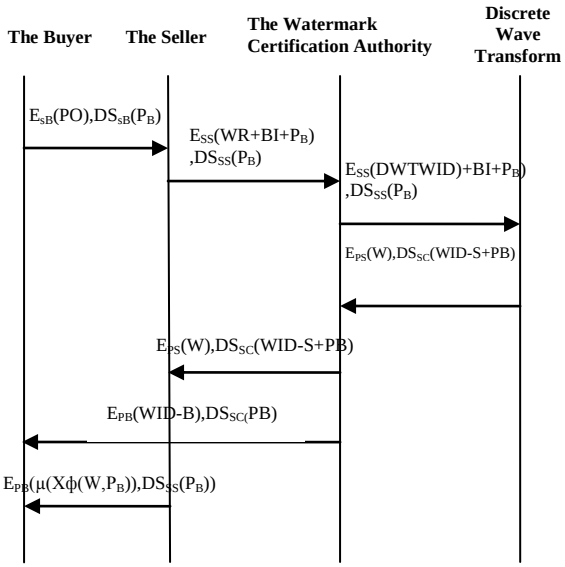

Figure 6: Transactions in the proposed watermarking

Where Γ, f, μ, μ', and μ'' are homomorphism functions to generate or check the digital content or watermark. A privacy homomorphism with respect to the binary operator © is applied to extract the watermark W from any original copy of the watermark embedded digital content X'. This homomorphism binary operator © and function μ' is only known to the WCA.

$$\delta(\mathrm{W}, \mathrm{SS})\_\mathrm{WID} - \mathrm{S} \quad (6)$$

$$\delta'(\mathrm{WIS} - \mathrm{S}, \mathrm{SS})\_\mathrm{W'} \quad (7)$$

$$\sigma(\mathrm{W'}, \mathrm{SB})\_\mathrm{WID} - \mathrm{B} \quad (8)$$

$$\sigma(\mathrm{WID} - \mathrm{B}, \mathrm{SB})\_\mathrm{W} \quad (9)$$

6. Generated watermark, W, is encrypted, EPS(W), by CA is send to S along with digitally signing the WID-S and PS, DSSC(WID S+PB).

7. The encrypted Watermark Identification number for B, EPS(WID-B), and DSSC(PB) is send to B. This will help B to check the originality of the purchased digital content in a later stage of the transaction.

8. Upon receiving (EPS(W), DSSC(WID-S+PB)) from CA, S checks the authenticity by decrypting the digital signature using PC to get WID-S and PB. The equation (6) is applied to generate WID-S to crosscheck, with the one that is received from CA, originality of the watermark. S decrypts, DSB(EPS(W)), to get the watermark W, which will be embedded using the secrets homomorphism function μ.

9. Digitally signed PB, DSSS(PB), and encrypted watermarked digital content, EPB(μ(XΦ(W, PB)) or X', is now forwarded to B.

10. Upon receiving (EPB(μ(XΦ(W, PB)), DSSS(PB)) from S, B checks the authenticity by analyzing the digital signature. W' is generated from X¢ and SB from the equation (5) and WID-B is from the equation (8) to crosscheck-with the one that is received from CA, the originality of the digital content purchased.

Table-1. The notation used in this defined below.

NOTATION	DESCRIPTION
X	Original copy of digital content.
W	Watermark information to be embedded, generated based on public keys of buyer and seller.
X'	Watermarked digital content.
WID	Generated watermark information's Index Identity number, which is to be embedded in the digital content.
DWTWID	Generated watermark information's Index Identity number using Discrete Wavelet Transform (DWT).
ϕ	Insertion of Watermark information into the original copy of digital content.
(P_B, S_B)	A public-secret key pair, where PB is buyer's (or B's) public key and SB is B's secret key.
$DS_{SB}(M)$	The message M is digitally signed by B's private key.
$E_{PB}(M)$	The message M is encrypted using B's public key.
$E_{SB}(M)$	The message M is encrypted using B's private key.
$D_{PB}(C)$	The cipher text C is decrypted using B's public key.
$D_{SB}(C)$	The cipher text C is decrypted using B's private key.

5. CONCLUSION

This paper proposed a Practical Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform (DWT) that solves many problems which were found in previous watermarking protocol. These improvements enable our protocol feasible and suitable for web context. Discrete wavelet transform (DWT) based watermarking techniques are gaining more popularity because DWT has a number of advantages over other transform such as progressive and low bit-rate transmission, quality scalability and region-of-interest (ROI) coding demand more efficient and versatile image coding that can be exploited for both, image compression and watermarking applications.

This protocol provides a property that the seller does not get to know the exact watermarked copy that the buyer receives. We use group signature, arbitrator, public key infrastructure and watermark certificate authority (WCA) for providing the efficient security for the buyer and seller. This is designed for public key crypto system and the operations of watermark insertion are performed by the seller rather than the watermark certification authority. The protocol has higher efficiency, and it is very safe. The security of this protocol lies on the security and robustness of the encryption standard and different group signature, and technique used in this protocol, which can further be modified and developed to improve the efficiency of the proposed protocol. Our protocol is simple and can be used with different watermark techniques.

6. ACKNOWLEDGEMENTS

First of all I would like to thank Almighty God the merciful, the gracious who has given me the ability, intelligence and energy to accomplish this research works.

Many people have contributed, directly or indirectly, to the successful completion of this thesis. They will all be remembered in my heart. First, I would like to thank my advisor, Dr. Vipin Tyagi and Brig. (Retd.) Satya Prakash Ghrera for his guidance from conducting to writing this research work and support that he has extended to me.

7. REFERENCE

[1] I Hartung F, Kuter M. Multimedia Watermarking Techniques, Proceeding of the IEEE, 1999,87(7):1079-1107.

[2] M. Kutter, S. K. Bhattacharjee, T. Ebrahimi. Towards Second Generation Watermarking Scheme. Image Processing, 1999. ICIP 99. Proceedings. vol.1: 320 – 323.

[3] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?" in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '99), vol. 4, pp. 2067–2069, Phoenix, Ariz, USA, March 1999.

[4] I. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12):1673–1687, 1997.

[5] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1593–1601, 2001.

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

[7] H.-S. Ju, H.-J. Kim, D.-H. Lee, and J.-I. Lim. An anonymous buyer-seller watermarking protocol with anonymity control. Information Security and Cryptology - ICISC, pages 421–432, November 2002.

[8] 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.

[9] X. G. Xia, C. G. Boncelet, G. R. Arce, A Multiresolution Watermark for Digital Images. Image Processing 1997 Proceedings. International Conference. vol.1 :548 – 551.

[10] 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.

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

[12] Mina Deng, Bart Preneel, "On Secure and Anonymous Buyer-Seller Watermarking Protocol" ,Third International Conference on Internet and Web Applications and Services ,pp. 524-529, June 2008.

[13] Vinu V Das and Nessy Thankachan, "A Buyer-Seller Watermarking Protocol for an Efficient and Secure Digital Transaction," in Proc. jSt Int. Conf. on Information System and Technology, India, 2007, pp. 127-132.

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

[15] L Qiao and K Nahrstedlt, "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Right," Journal of Visual Communication and Image Representation, Vol. 9, pp. 194-210, Sept. 1998.

[16] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of ACM, vol. 21, pp.120-126, 1978.