Pertanika J. Sci. & Technol. 25 (1): 57 - 76 (2017)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection

Ashwani Kumar[1]*, S. P. Ghrera[1] and Vipin Tyagi[2]

[1]*Department of CSE, Jaypee University of Information Technology, Waknaghat, P.O. Waknaghat, Teh Kandaghat, Distt. Solan, 173234, India*

[2]*Department of CSE, Jaypee University of Engineering and Technology, A-B Road, Raghogarh, 473226, India*

ABSTRACT

Digital watermarking protocols are the one, which have combined fingerprinting technique with watermarking, for embedding digital signal or watermark into an original multimedia object. Buyer-seller watermarking protocol is fundamentally applied to continue the digital rights of both buyers and seller. We proposed an identity-based buyer-seller watermarking protocol that encounters various weaknesses of Zhang et al.'s watermarking protocol. We ensured that by pointing out these weaknesses, inaccuracy can be minimised for further implementing the buyer-seller watermarking protocol. The suggested protocol uses ID-based public key cryptography and digital watermarking scheme to place the ownership of digital content. Hence, copyright protection is attained. We claim that our suggested protocol is efficient and has adequate security as compared to traditionally proposed protocols, and therefore suitable for any practical buyer-seller watermarking scheme.

Keywords: Digital content, Identity-based technique, Public key cryptography, Digital watermarking, Copyright protection

INTRODUCTION

The speedy development of internet and e-commerce needs a copyright protection mechanism for multimedia data. Digital watermarking becomes an important technique for protecting the digital rights. The principal object of digital watermarking technique is: (Mintzer & Braudaway, 1999) to retain digital copyright or watermark, embedded into the cover object. The desirable secure digital watermarking scheme is one, which integrates public key cryptosystem and digital watermarking technique for protecting the buyers and seller in a digital content transaction. Digital watermarking

Article history:
Received: 14 January 2016
Accepted: 26 July 2016

E-mail addresses:
ashwani.kumarcse@gmail.com (Ashwani Kumar),
sp.ghrera@juit.ac.in (S. P. Ghrera),
dr.vipin.tyagi@gmail.com (Vipin Tyagi)
*Corresponding Author

ISSN: 0128-7680

(Memon & Wong, 2001) techniques use encrypted domain for embedding and extracting the watermarks. The rapid growth of the internet encourages some bad usage too; these include operations such as transformation, duplication and redistribution of digital content. With the avail of some software tools, we can easily identify these bad users and redistribution of digital content can also be placed. In general, secure digital watermarking (Zeng et al., 2011) scheme should satisfy the following requirements:

Robustness
The capability of the watermark to resist various image processing attacks such as rotation, scaling, cropping, etc.

Imperceptibility
The optical aberration of the watermarked image should not bear on the characters of the original picture.

Effectiveness
The algorithms for embedding and extracting the watermark from the digital content should be effective.

Memon et al. (2001) proposed the very first buyer-seller watermarking protocol in 2001, and Ju et al. (2002) modified this protocol with various advances. In history, various protocols have been proposed (Choi et al., 2003; Goi & Phan, n.d; Hu & Zhang, 2009; Hu & Li, 2009). Digital watermarking (Zeng et al., 2011) algorithm is divided into two parts; first non-blind watermarking scheme and second, blind watermarking scheme. The non-blind watermarking scheme needs original cover object as well as watermark and watermark key for extracting the watermark, while blind watermarking scheme does not require cover object, watermark key and watermark for detection or extraction of the watermark. The buyer-seller watermarking protocol (Kumar et al., 2011a; Kumar et al., 2011b) is a three-party protocol among a service provider, a customer, and a trusted watermark certificate authority. This protocol combines fingerprinting and encryption techniques for protecting the participants into any transaction. A very common buyer-seller watermarking protocol consists of four sub-protocols the registration protocol, the watermarking protocol, the identification and arbitration protocol, and the dispute resolution protocol. The buyer-seller watermarking protocol (Kumar et al., 2011a; Kumar et al., 2011b) is expected to solve the problems, which are given below.

Certification authority problem
In this, a digital certificate is given for the participants involving in a transaction.

The conspiracy problem
Malicious parties may collude with each other and mount attacks to cast an innocent buyer or to confound the tracing by removing the watermark from the digital content.

The customer's rights problem
Customer's right problem states that when the service provider embeds a watermark information into digital content, and have the advantage to frame the customer.

The piracy-tracing problem
In this, the service provider is supposed to trace illegal copies of digital content. Therefore, the redistribution of digital content can be controlled by the seller.

The unbinding problem
Unbinding means unable to bind watermark for the digital rights. In this problem, service providers can fabricate piracy of the customer by manipulating customer's watermark.

The anonymity problem
In the anonymity problem, during the transaction, the customer identity should be hidden until the customer is declared as the culprit.

According to history, Hwang et al. (2005) introduced a time stamping protocol in 2005. In their protocol, a TTP (trusted third party) was introduced for checking the verification and signing phase. Ju et al. (2002) proposed an anonymous buyer-seller watermarking protocol with anonymity control in 2002. In the paper, the authors have identified the anonymity problem. They discussed that a buyer could purchase digital content anonymously, but the anonymity can be controlled. Zhang et al. (2006) proposed a secure buyer–seller watermarking protocol in 2006. In his paper, no assistance is needed, so that it avoids the conspiracy problem, piracy tracing problem and customer's right problem. There are only two participants, a seller and a buyer. The protocol can simultaneously resolve many problems. However, there is a drawback in Zhang et al.'s protocol, i.e. the buyer's assistance is needed to solve the piracy dispute. Therefore, dispute resolution and unbinding problems exist in the protocol by Zhang et al. (2006).

We proposed an identity-based buyer-seller watermarking protocol and encountered various existing weaknesses of Zhang et al.'s (2006) protocol such as dispute resolution and unbinding problem. Here, we proposed a new identity-based buyer-seller watermarking protocol to prove the ownership of digital content. Our proposed protocol enables the seller to produce the watermarked content with their private key. The watermark certificate authority (WCA) is responsible for issuing the digital signature that corresponds to ID of the seller, timestamp (Hwang et al., 2005) used for watermark content, watermark and cover object. WCA is maintaining its own table and keeping the requested IDs of both buyer and seller; suppose if dispute occurs, the buyer can communicate or confirm to the WCA to checkout that whether he/she is the original buyer or not. If any dispute occurs at a later stage, with the help of arbiter, it can also be resolved to check the correctness of information used by the seller. Timestamps are compared by the arbiter to identify the appropriate seller of digital content and with the help of timestamps, the unbinding problem is also solved. Some key details of our proposed watermarking protocol are identified below:

1. In our proposed protocol, we adopt wavelet and principal component analysis based techniques (kumar et al., 2015) with identity-based public key cryptography.
2. This watermarking protocol must be autonomous of all watermarking schemes.
3. Our protocol makes use of a tamper resistance device, which is embedded into seller's computer and reduces the overhead on WCA as TTP.

The rest of the paper is structured as follows. In Section Two, we review the scheme of Zhang et al. (2006) and identify previously unpublished problems. Section Three describes the proposed ID-based buyer-seller, watermarking protocol. Section Four discusses the security analysis. Section Five shows the experimental results. Finally, Section Six concludes our paper.

REVIEWING THE SCHEME OF ZHANG *ET AL.*

Zhang et al. (2006) proposed a secure buyer-seller watermarking protocol in 2006. The authors proposed a secure buyer-seller watermarking protocol without the assistance of a TTP in which there are only two participants, the seller and buyer. Zhang et al.'s paper is based on the Lei et al. (2004) and in this, no third party is brought in; therefore, the proposed protocol is more childlike and more dependable than the existing watermarking protocol. Zhang et al.'s protocol resolves the conspiracy problem, piracy tracing problem and customer's right problem. However, there is a drawback in Zhang et al.'s protocol, i.e. the buyer's assistance is needed to solve the piracy dispute problem.

The protocol of Zhang et al. composes of three sub-protocols: the registration protocol, the watermarking protocol and the identification and arbitration protocol. Here, we show the notations of Zhang et al.'s protocol.

$E_{pk*}(X')$ = encrypted watermark image

$E_{pk*}(X'')$ = second round encrypted watermark image

$E_{pk*}(W)$ = encrypted watermark

$Cert_{CA}(pk_B)$ = digital certificate of CA

pk_B, sk_B = random key pair

ARB = Arbiter

SEC_B = secret key of buyer

SEC_S = secret key of seller

$E_{pk^*}(SEC_B)$ = encrypted secret key

$Sign_{sk^*}(E_{pk^*}(SEC_B))$ = sign encrypted secret key

$Cert_{pk_B}(pk^*)$ = anonymous certificate

In the protocol of Zhang et al., a seller randomly generates a secret $\mathrm{SEC_S}$ key. In the encrypted domain, the seller obtains the encrypted watermark $\mathrm{E_{pk*}(W)}$, as follows.

$$E_{pk*}(W) = E_{pk*}(SEC_S) \otimes E_{pk*}(SEC_B)$$
$$E_{pk*}(SEC_S \oplus SEC_B) \quad (2.1)$$

Seller S then inserts the second round watermark through the following formula:

$$E_{pk*}(X'') = E_{pk*}(X') \otimes E_{pk*}(W)$$
$$E_{pk*}(X' \oplus W) \quad (2.2)$$

Zhang et al. claimed that their proposed secure buyer-seller watermarking protocol provides a solution for conspiracy problem, piracy-tracing problem and customer's right problem. We have identified that the protocol is unable to solve the dispute resolution problem and unbinding problem. Figure 1 shows a simplified trading model, based on the protocol by Lei et al.

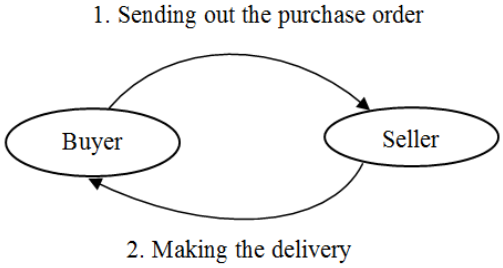


Figure 1. A simplified trading model

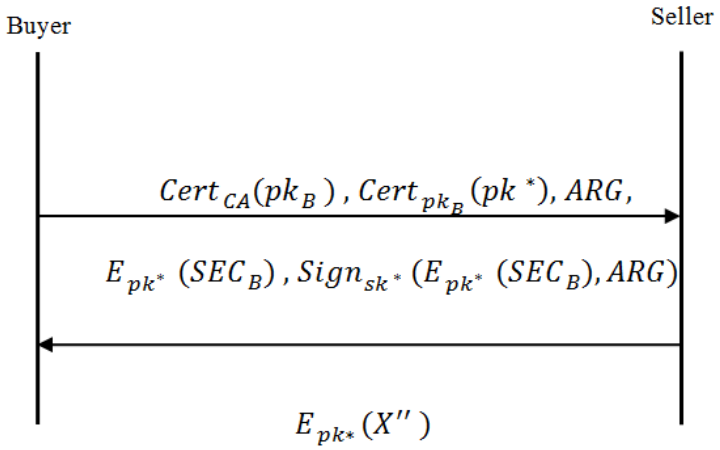


Figure 2. The encryption phase of J. Zhang secure buyer-seller watermarking protocol (Zhang et al., 2006).

In Zhang *et al.*'s protocol, the unbinding problem arises because once the seller finds out a pirated copy, there is a potential for a seller to transplant the watermark embedded in the pirated copy into another copy of digital content. Dispute resolution problem also exists because the data encrypted by the judge may not be equal to the data furnished by the seller. To level out these topics, we have proposed identity-based cryptographic scheme (Zeng et al., 2011) into the watermarking algorithm. ID-based techniques were introduced by Shamir in 1984.

PROPOSED ID-BASED BUYER-SELLER WATERMARKING PROTOCOL

This paper is an extension of our previous work (Kumar et al., 2011a; Kumar et al., 2011b). In our suggested protocol, the same trust model used by Memon et al. (2001) and Lei et al. (2004) is employed. The proposed protocol is based on public key infrastructure, arbiter, ID-based public key cryptography (Cox et al., 1997; Paillier, 1999) and digital watermarking scheme. The watermarking scheme involves secret key and digital signature certificate issued by WCA. WCA maintains its own table and keeps the requested IDs of both buyer and seller because it contains a database. Our protocol is flexible because it makes use of tamper resistance device, which is utilised to reduce the overhead on WCA and also solves the problems listed in section 1. Now, in the digital signature verification phase, someone else can use the WCA public keys to validate that the watermarked content embedded at a certain time into the digital content. Our proposed digital watermarking protocol consists of three sub-protocols: the watermark embedding and signing protocol; watermark detecting and verifying protocol; and registration protocol, as presented in Figure 4. We first determine the roles and notations for various participants in our proposed protocol, as presented in Figure 3.

Seller

The owner of the digital content or from where the buyer wants to purchase the digital content.

Spurious buyer

Th person who wants to learn the rightful side of the digital capacity that does not belong to him.

WCA

Public, private, and shared secret key is issued by this authority. The valid watermark and digital signature are also generated by *WCA*.

ARB

ARB stands for an arbiter; if any dispute occurs between the buyer and seller, that dispute is resolved by arbitration. ARB also verifies the correctness of the digital certificates.

Tamper-resistant device

This device is detached from seller's computer and used to produce necessary watermarks and digital signature.

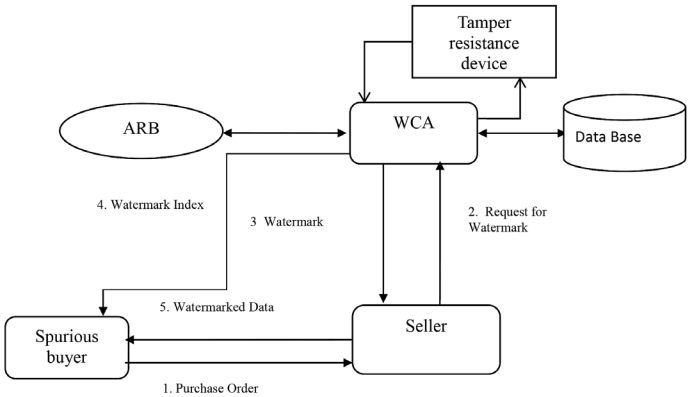


Figure 3. ID-based buyer-seller watermarking protocol.

We have shown assumptions of our suggested protocol.

1. Buyer-seller and *WCA* contain a matched clock. This clock is held securely.
2. The cover object is an image in which the watermark is applied.
3. WCA is assumed to be trustworthy.
4. The buyer-seller communicates through a secure channel.
5. The valid watermark is generated by the seller and WCA.

The goals of the proposed watermarking scheme are described below:

1. Our protocol solves the unbinding problem, the dispute resolution problem and it also identifies the spurious seller who claims the ownership of digital content.
2. The buyer interacts with the seller but one time.
3. The buyer does not possess any knowledge of cryptosystem and the embedded watermark.
4. Our protocol avoids the double watermark insertion and *WCA* is responsible for the generation of the watermark.

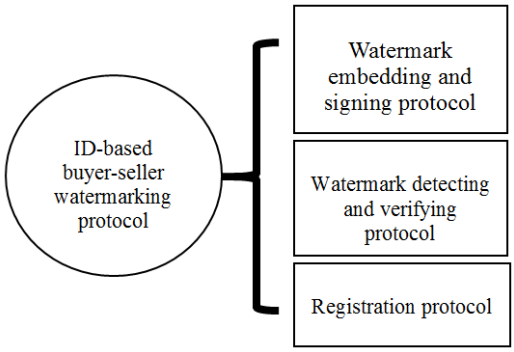


Figure 4. Three sub-protocols of ID-based buyer-seller watermarking protocol.

We have shown the roles and notations of our proposed ID-based secure and flexible buyer-seller watermarking protocol.

X	= original image
W	= watermark
W'	= forge watermark
Z	= forged digital content
X_W	= watermarked image or data
$E_{H(w_k)}$	= encrypted watermark key
$D_{H(w_k)}$	= decrypted watermark key
C	= cipher text

t = timestamp

$SE_{PC_{wca}}$ = seller performs encryption using WCA public key

ARG = arbiter

ID_S = seller credential

$SD_{K_{wca}}$ = seller performs decryption using WCA public key

$Ver_{PC_{wca}}(Ds)$ = verification of digital signature

$Ds(Sig_{K_{wca}})$ = digital signature Ds generated by WCA using its private-key.

Watermark embedding and signing protocol

The watermark embedding and signing protocol are described in Figure 5. The protocol is being executed multiple times for authentication of a buyer between the seller and WCA. If the seller wants to establish the lawful ownership of their digital content, i.e. image X, then the seller can carry out the embedding and then sign a protocol with WCA, as given in Figure 5. The deal between the seller and WCA is given below.

1. The seller selects a random and robust watermark *W*.

2. The seller embeds the watermark *W* into digital content *X* to obtain watermarked data X_w.

$$X_W = E_{H(w_k)}(X, W) \tag{3.1}$$

where *E* is the watermark embedding algorithm and $H(w_k)$ is the watermark key.

3. The seller then converts plaintext *P* into ciphertext *C* using the public-key cryptosystem, PC_{wca}.

$$C = SE_{PC_{wca}}(ID_S, t, X, W, X_W) \tag{3.2}$$

where X_W is provided by the seller and t is the creation of time of the watermarked content, i.e X_W.

4. The seller sends the ciphertext C to the WCA.

5. After receiving C, WCA performs some decrypt operation.

$$(ID_S, t, X, W, X_W) = SD_{K_{wca}}(C) \tag{3.3}$$

where K_{wca} is the private key of WCA and *D* is the decryption.

6. WCA checks whether ID_S is legitimate or not. If not, WCA aborts the sub-protocol.

7. If the time t is accepted, WCA then checks to confirm that the watermarked content X_W has been constructed by embedding the watermark W in X.

8. If watermark content X_W is valid, then WCA generates the digital signature Ds using WCA private key K_{wca}.

$$Ds = Sig_{K_{wca}}(ID_S, t, W, H(w_k)) \tag{3.4}$$

9. WCA sends this digital signature to the seller.

10. After receiving the digital signature Ds, seller verifies it using the public key of WCA.

$$Ver_{PC_{wca}}(Ds) = (ID_S, t, W, H(w_k)) \tag{3.5}$$

11. If the digital signature is valid, then the seller keeps Ds, t and W in their local database. After successfully completing the watermark embedding and signing protocol, the Seller can publicise the digital watermarked content X_W.

Watermark detecting and verifying protocol

The watermark detecting and verifying protocol is described in Figure 6. This protocol takes place between the buyer and the arbiter (ARB). If the arbiter receives a forge digital content, let say, Z and seller consist K_S, t, Ds, W, X. Then, seller can claim the rightful ownership of Z by executing the watermark detecting and verifying protocol.

1. The seller sends $ID_S, t, W, H(w_k), Ds$ and X to arbiter.

2. After getting all information from the seller, arbiter uses the watermark detection algorithm:

$$D_{H(w_k)}(Z, X, W) \tag{3.6}$$

Where D belongs to watermark detecting scheme. If we receive the result of the above equation, equal to 1, then Z consist watermark W and if the effect of above equation equal to 0 then Z does not contain watermark W and arbiter performs next step.

3. After step 2, arbiter verifies the validity of the digital signature Ds using the following equation:

$$Ver_{PC_{wca}}(Ds) = (ID_S, t, W, H(w_k)) \tag{3.7}$$

where PC_{wca} is the public-key cryptosystem of WCA. If Eq. (3.7) is true, the arbiter returns their own key $ID_S, t,$ otherwise, arbiter returns 0.

Registration Protocol

The registration protocol takes place between the customer and the WCA. If a buyer wants to hide his identity to a transaction of digital content, then the buyer randomly selects a pair of key Rpk_B, Rsk_B and sends Rpk_B to a trustworthy WCA [11]. After receiving Rpk_B, WCA generates an anonymous digital certificate $Cert_{WCA}(Rpk_B)$ and sends it to the buyer. If the buyer does not require anonymity, the entire registration process can be skipped and normal digital certificate can be practiced by the buyer.

Seller		WCA
1. Seller select watermark W 2. $X_W = E_{H(w_k)}(X, W)$ 3. $C = SE_{PC_{wca}}(ID_S, t, X, W, X_W)$	4. C →	5. $(ID_S, t, X, W, X_W) = SD_{K_{wca}}(C)$ 6. WCA checks ID_S, t 7. Checks X, X_W
10. $Ver_{PC_{wca}}(s) = (ID_S, t, W, H(w_k))$	9. Ds ←	8. $Ds = Sig_{K_{wca}}(ID_S, t, W, H(w_k))$
11. Stores Ds, t, W into the database		

Figure 5. Watermark embedding and signing protocol

Seller		Arbiter (ARB)
1. Seller sends $(ID_S, t, W, H(w_k), Ds, X)$		2. Perform decryption $D_{H(w_k)}(Z, X, W)$ 3. Arbiter verifies $Ver_{PC_{wca}}(s) = (ID_S, t, W, H(w_k))$

Figure 6. Watermark detecting and verifying protocol

Table 1
A comparison of our proposed scheme with the existing protocols.

	[11]	**[6]**	**[4]**	**[12]**	**[Our Scheme]**
The customer's rights problem	Solved	solved	solved	solved	solved
The piracy-tracing problem	Solved	solved	not tested	solved	solved
The unbinding problem	Solved	not solved	not solved	solved	Solved
The anonymity problem	partially solved	solved	not solved	partially solved	Solved
The dispute resolution problem	Solved	not solved	not solved	solved	Solved
Tamper-resistant WCA device With Database	No	No	No	No	Yes

SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, the security of the proposed ID-based secure and flexible buyer-seller watermarking protocol is analysed. The security of the proposed protocol depends on the security and robustness of the underlying watermarking embedding and detecting scheme. We have examined the security of our protocol and compared it with the scheme (Memon & Wong, 2001; Choi et al., 2003; Lei et al., 2004; Zhang et al., 2006). The proposed watermarking protocol is secure and flexible for the reason that buyer has no idea about the original digital content **X**, and hence, is unable to remove the watermark. Since seller gets no access to the watermarked copy of the digital content **X**, hence, the seller cannot distribute illegal replicas

of digital content X. Our proposed protocol has successfully solved the problems identified in the protocol of Zhang et al., which are listed in section 1. The security of the proposed protocol is examined and compared with the previously published work (Memon & Wong, 2001; Choi et al., 2003; Lei et al., 2004; Zhang et al., 2006) in tabular form.

Table 2
A comparison of computation cost with existing protocol

Encryption Operation	3	2k+1	2	3	1
Decryption Operation	1	4	1	1	1
⊕ operation	2	2	2	2	2
Signing Operation	1	k	2	2	1
k is the number of watermarks					

Table 1 and Table 2 show the comparison of various results. In Table 1, the seller uses a tamper resistant device, which produces necessary watermarks and digital signature. Table 1 shows that our protocol can withstand all of the known problems which are listed above and identify the true owner of the digital content. Table 2 shows the various encryption and decryption operation used in our proposed protocol. We used three sub-protocols watermark embedding and signing the protocol, watermark detection and verifation protocol and registration protocol. In our scheme, the number of communication rounds takes one encryption, one decryption, two watermark embedding, and one signing operation respectively, which minimises the passing time and also reduces overhead on WCA, and hence is better when compared to others such as that of Memon & Wong, 2001; Choi et al., 2003; Lei et al., 2004; Zhang et al., 2006. Furthermore, if buyer sends a request to purchase a product with anonymity, the then seller publishes the encrypted product to the buyer and the seller is not able to trace the identity of the buyer. Hence, during the entire transaction, the privacy of the buyer is protected against the seller. In the case of WCA, it only has the credentials of the buyer, but WCA is not aware of the product or digital content which the buyer has bought, and hence, the buyer is also protected against WCA.

Dispute resolution problem

In the dispute resolution problem, if the seller takes evidence to the judge, i.e. arbiter that the buyer is responsible for copyright violation. The seller does not know exactly where the watermark is embedded in the digital content, X. The seller is unable to frame the buyer. When the arbiter asks the buyer for the watermark, W, the buyer can send some random watermark $W_{\square'}$ instead of original, W. The seller has presented the Judge with a signed and encrypted copy of the watermark W and this watermark W will not match the watermark W′ presented by the buyer. Then, the buyer would be considered as the spurious buyer. For that, WCA finds the value of watermark W in place of watermark W′ with the help of Equation 3.3. WCA takes the final decision based on this equation.

$$(ID_S, t, X, W, X_W) = SD_{K_{wca}}(C)$$

Unbinding problem

The unbinding problem is solved because in this, first, the seller does not know the buyer's watermark W_B, because the watermark is embedded by a trusted third party, i.e. WCA under encryption algorithm. The buyer's signature binds to the ARG that uniquely identifies a particular digital content, X. These aspects make it impossible for the seller to transplant the watermark into another copy of the forged digital content.

When both buyer and seller argue to prove the ownership of a similar media *Z*, then the arbiter executes the watermark detecting and verifying protocol to specify the lawful possessor of the digital content *Z*. For determining the robustness of the underlying watermarking algorithm, we check the result of equation 3.6. If the digital signature, i.e. Ds is generated by the WCA then the equation no. (3.7) should be reliable.

$$D_{H(w_k)}(Z, X, W)$$

$$Ver_{PC_{wca}}(Ds) = (ID_S, t, W, H(w_k))$$

In the case of watermark embedding and signing protocol ciphertext C and digital signature Ds are transmitted between WCA and seller. As ciphertext C is encrypted using the public key of PC_{wca} of WCA, an unauthorised person cannot obtain the digital content X and X_W from the ciphertext C and digital signature Ds because the original digital content X and watermarked data X_W are kept secret in the watermark embedding and signing protocol. Hence, the buyer can obtain X_W only if after seller publicises the watermarked data, and then arbiter can determine whether that the seller is the rightful owner or not.

From the above analysis, our proposed protocol can solve the common problems, which are presented in Section 1 and design goals are also achieved, which are given in Section 3. Our protocol has come at some modification based on the previously published protocol. We did not embed the second watermark into the original digital content, the buyer needs to interact with the seller, arbiter and the WCA in the transaction process and the seller and WCA are used for issuing the valid watermark. Hence, the seller is unable to bind a watermark for framing the innocent buyer i.e. the unbinding problem is resolved and if any disputed occurs between buyer and seller, and then WCA and arbiter can solve that issue using time stamp based technique to establish the use of timestamp at what time the digital content or signal was created, signed or verified, i.e. dispute resolution problem is resolved.

EXPERIMENTAL RESULTS

All previously proposed buyer-seller watermarking protocol uses Cox (Cox et al., 1997) method to gain robust watermarking. In our proposed protocol, however, we adopted wavelet and principal component analysis based techniques (Kumar et al., 2015) with identity-based public key cryptography for achieving high robustness. Hence, we claimed the novelty of our proposed scheme as our protocol is more robust and has very high imperceptibility. We have presented various parameters for analysing the performance of the proposed protocol.

Peak Signal-To-Noise Ratio (PSNR)

Peak Signal-To-Noise Ratio is generally applied to analyse the quality of a picture.

$$PSNR = 10 * log \frac{255^2}{MSE} \tag{5.1}$$

Mean Square Error (MSE)

The MSE represents the cumulative squared error between the compressed image and the original image. In order to calculate the PSNR, first, the mean-squared error (MSE) is calculated using the following equation.

$$MSE = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{i,j} - B_{i,j}|)^2}{x * y} \tag{5.2}$$

Where x is the width of the image and y is height, and $x * y$ is the number of pixels.

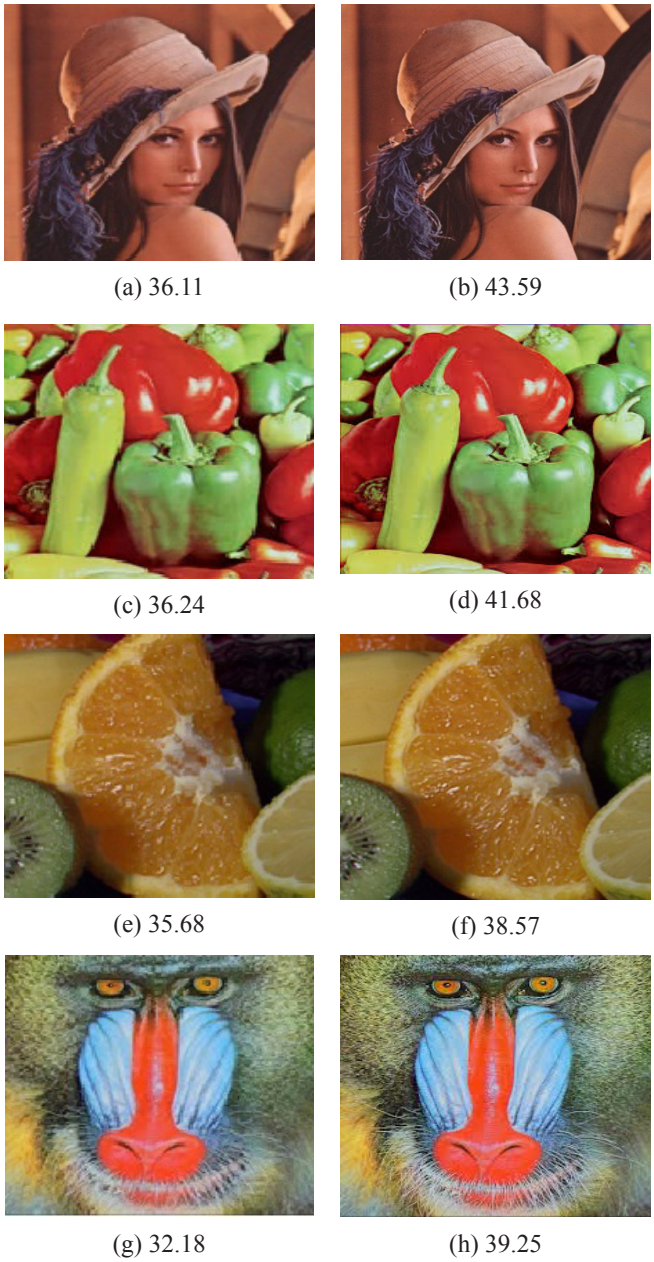
Normalized Correlation Coefficient (NCC)

It is used for calculating the robustness of the algorithm.

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{i,j} B_{i,j}}{\sum_{i=1}^{m} \sum_{j=1}^{n} A_{ij}^2} \tag{5.3}$$

Where $A_{i,j}$ and $B_{i,j}$ denote the pixel values in row i and line j of the original watermark and the exacted watermark respectively.

The correctness of our proposed approach depends on the robustness of watermarking embedding and extracting scheme. In our scheme, we set α =0.01 i.e. watermark embedding coefficient factor. For instance, we have chosen Lena and Baboon images for producing our results. Figure 8 shows the original test images and watermarked test images. The various watermark logos, i.e. JNU logo and copyright logo, are shown in Figure 9. These watermark logos are embedded into the original images to prove the owner of the digital content. Some attacks are applied to the watermarked images for checking the robustness of the proposed scheme. The primary objective of our protocol is to solve the entire problem, which is solved by Zhang *et al*., as and as well dispute resolution problem and unbinding problem. The embedding method uses wavelets and principal component analysis technique (Kumar et al., 2015) with identity-based public cryptography for getting the watermark, while the existing protocol uses Cox's embedding method (Cox et al., 1997), which is based on DCT transform. In the previously proposed protocol, each element is processed independently, and thus, the computation cost and overhead increase linearly. In our proposed scheme, however, we adopted wavelet and principal component analysis based scheme (Kumar et al., 2015), which has only one asymmetric operation by the buyer or seller and two asymmetric operations by TTP as WCA. Consequently, communication overhead is almost constant.



(a) 36.11 (b) 43.59

(c) 36.24 (d) 41.68

(e) 35.68 (f) 38.57

(g) 32.18 (h) 39.25

Figure 7. The watermarked images on the left side are created by the buyer and right sides are created by the seller.

In the watermarking process, WCA generates the valid watermark images seller using wavelet and principal component analysis transform to create correlation coefficient, and buyer executes these correlation coefficients for generating the watermarked image. Figure 7 shows the watermarked images created by both the buyer and seller. It is clear that the PSNR value of Figure 7 on the left side is lower than the right side. The left side of Figure 7

shows the watermarked images generated by the buyer and the right side of the figure show watermarked images generated by the seller. Table 3 shows that the PSNR values corresponding to seller and buyer. Here, in order to calculate the robustness of the watermark embedding scheme, we have applied several types of attacks to the watermarked images.

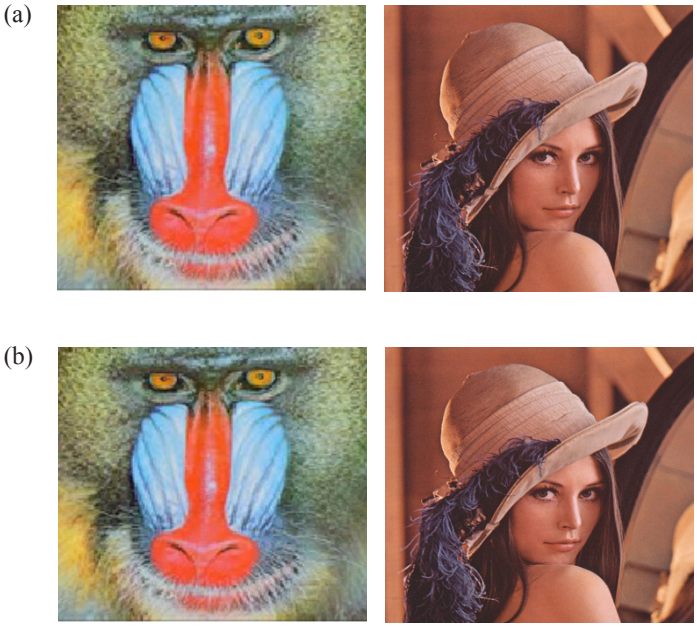
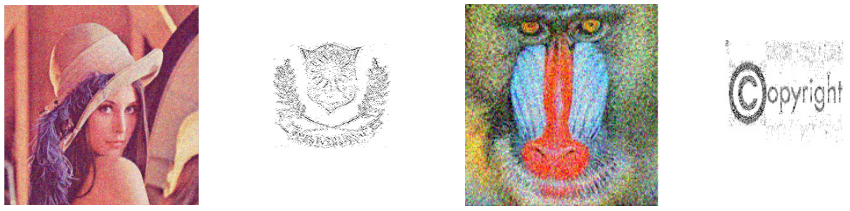


Figure 8. (a) Original Test Image; (b) Watermark Test Images

Table 3
Peak signal to noise ratio (PSNR) dB created by both buyer and seller for each original colour image.

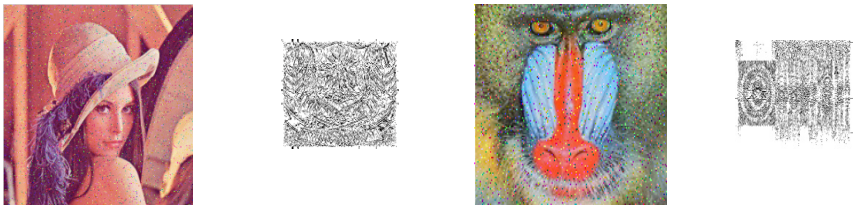
PSNR(dB)	Lena	Pepper	Fruit	Baboon
Buyer	36.11	36.24	35.68	32.18
Seller	43.59	41.68	38.57	39.25

Figure 9. Watermarks logos (a) JNU (b) Copyright (c) gray scale JNU (d) gray scale Copyright



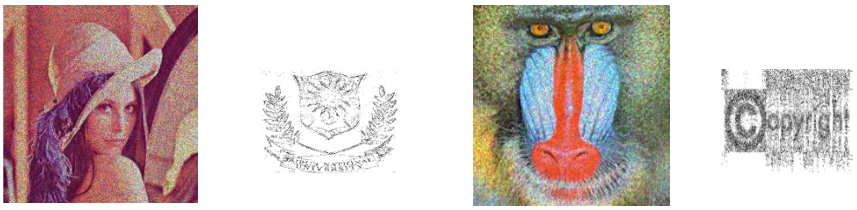
(a) (b) (c) (d)

Figure 10. (a) Watermarked Lena Image after Gaussian Noise at 0.02; (b) Extracted Watermark; (c) Watermarked Baboon Image after Gaussian Noise at 0.02; (d) Extracted Watermark.



(a) (b) (c) (d)

Figure 11. (a) Watermarked Lena Image after Salt & Pepper Noise at 0.02; (b) Extracted Watermark; (c) Watermarked Baboon Image after Salt & Pepper Noise at 0.02; (d) Extracted Watermark.

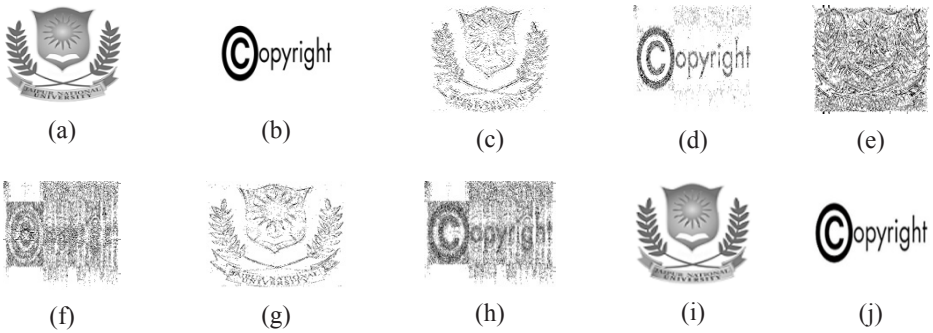


(a) (b) (c) (d)

Figure 12. (a) Watermarked Lena Image after Speckle Noise at 0.03; (b) Extracted Watermark; (c) Watermarked Baboon Image after Speckle Noise at 0.03; (d) Extracted Watermark.

(a) (b) (c) (d)

Figure 13. a) Watermarked Lena Image after Median Filter at [5 5] b) Extracted Watermark c) Watermarked Baboon Image after Median Filter at [5 5] d) Extracted Watermark.



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

Figure 14. Extracted Watermark Images

In Figure 10, we have applied Gaussian noise with a density of 0.02 to the watermarked Lena and Baboon images, with the JNU watermark logo and copyright logo are embedded respectively. The quality of the extracted watermark logos is good with the presence of attacks. To check the quality of these watermarks, we have calculated correlation coefficient by using equation 5.3. Meanwhile, the corresponding correlation coefficients are shown in Table 4.

Figure 11 shows the performance of our scheme against the salt and pepper noise. We have applied this noise with a density of 0.02 on the Lena and baboon watermarked images and then extracted the corresponding watermarks.

In Figure 12, we have applied speckle noise with 0.03 density on the Lena and Baboon watermarked images, and then the corresponding watermark are extracted. In this, we got good results and the watermarks are still extracted.

Filtering is the most common attacks on digital images. Thus, we have applied the median filter to both the watermarked images with the filter size M=5 in Figure 13. The results show that watermarks are easily recognised. If we increase the filter, size normalised correlation will also decrease. Figure 14 (a,b) shows the original watermarks and (c, d, e, f, g, h, i, j) with the extracted watermarks from the Lena and Baboon images. In order to measure the quality of watermarked images, we have PSNR by equation 5.1. Figure 8(b) shows the watermarked images and their corresponding PSNR values are shown in Table 4.

Table 4

The PSNR values of all the test images.

Images	Lena	Pepper	Fruit	Baboon
PSNR	43.59	41.68	38.57	39.25

Table 5 shows the various results of our proposed scheme. We have successfully extracted the watermark from Gaussian noise, salt and pepper noise, Speckle noise and Median filter attacks. It is noticeable that in the case of Median filter and Gaussian noise, the performance of our scheme is quite impressive. Hence, our scheme is very robust against Salt and pepper noise and Median filter attack, and it also shows a better performance. Table 5 shows that the correlation coefficient values for the extracted watermark and PSNR values for the attacked watermark images. The imperceptability and robustness our watermark embedding scheme is very high.

Table 5
PSNR values and normalised corelation coefficient of all watermarked images and extracted logos after the attacks.

Images	**Lena**		**Baboon**	
Attacks	**PSNR**	**NC**	**PSNR**	**NC**
Gaussian Noise with Noise 0.02	40.62	0.8463	37.39	0.8131
Salt & pepper Noise with density 0.02	39.63	0.6338	35.10	0.5321
Speckle Noise with density 0.03	39.72	0.7842	37.61	0.8741
Median Filter with filter size [5, 5]	41.01	0.9762	36.49	0.7153

CONCLUSION

In this paper, we have presented an identity-based buyer-seller watermarking protocol which can solve the various problems of the previously published protocol and free from all known attacks. In addition, we made use of a tamper resistance device, which is embedded into seller's computer and reduces the overhead on WCA. WCA maintains its own table and keeps the requested IDs of both buyer and seller. Hence, WCA is required to participate in each transaction of the digital contents between buyer and seller. We also adopted wavelet and principal component analysis based techniques (Kumar et al., 2015) to increase the robustness and imperceptibility of our embedding scheme. The watermark certificate authority is responsible for issuing the digital signature corresponding to ID of the seller. If the problem of multiple ownership occurs, then it is the duty of an arbiter to decide on it. The arbiter checks the correctness of data used by the seller, and then the arbiter compares the timestamps for determining the original possessor of the digital content. These changes enable our proposed protocol to become really secure, feasible and efficient.

REFERENCES

Choi, J. G. Sakurai, K., & Park, J. H. (2003). Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party. In *International Conference on Applied Cryptography and Network Security* (pp. 265-279). Springer Berlin Heidelberg.

Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Process, 6*(12), 1673–1687.

Goi, B. M., & Phan, R. C. W. (2004). Cryptanalysis of two anonymous buyer seller watermarking protocols and an improvement for true anonymity. In *International Conference on Applied Cryptography and Network Security* (pp. 369-382). Springer Berlin Heidelberg.

Hu, D., & Li, Q. (2009). A secure and practical buyer-seller watermarking protocol. In *2009 International Conference on Multimedia Information Networking and Security* (Vol. 2, pp. 105-108). IEEE.

Hu, Y., & Zhang, J. (2009). A Secure and Efficient Buyer-Seller Watermarking Protocol, *Journal of Multimedia, 4*(3), 161-168.

Hwang, M. S., Hwang, K. F., & Chang, C. C. (2005). A time-stamping protocol for digital watermarking. *Applied Mathematics and Computation, 169*(2), 1276–1284.

Ju, H. S., Kim, H. J., Lee, D. H., & Lim, J. I. (2002). An anonymous buyer-seller watermarking protocol with anonymity control. In *International Conference on Information Security and Cryptology* (pp. 421-432). Springer Berlin Heidelberg.

Kumar, A., Tyagi, V., Ansari, M. D., & Kumar, K. (2011). A Practical Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform. *International Journal of Computer Applications, 21*(8), 46-51.

Kumar, A., Ansari, M. D., Ali, J., & Kumar, K. (2011). A New Buyer-Seller Watermarking Protocol with Discrete Cosine Transform. In *International Conference on Advances in Communication, Network, and Computing* (pp. 468-471). Springer Berlin Heidelberg.

Kumar, A., Ghrera, S. P., & Tyagi, V. (2015). Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis. *Indian Journal of Science and Technology, 8*(35), 1-9.

Lei, C. L., Yu, P. L., Tsai, P. L., & Chan, M. H. (2004). An Efficient Anonymous Buyer-Seller Watermarking Protocol. *IEEE Transactions on Image Processing, 13*(12), 1618– 1626.

Memon, N. D., & Wong, P. W. (2001). Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing, 10*(10), 1593–1601.

Memon, N. D., & Wong, P. W. (2001). A buyer-seller watermarking protocol. *IEEE Transactions on Image Processing, 10*(4)*,* 643–649.

Mintzer, F., & Braudaway, G. W. (1999). If one watermark is good, are more better? In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '99)* (pp. 2067–2069).

Paillier, P. (1999). Public key cryptosystems based on composite degree residuosity classes. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 223-238). Springer Berlin Heidelberg.

Rial, A., Deng, M., Bianchi., T., Piva, A., & Preneel, B. (2010). A Provably Secure Anonymous Buyer–Seller Watermarking Protocol. *IEEE Transactions on Information Forensics and Security, 5*(4), 920-931.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 47-53). Springer Berlin Heidelberg.

Zeng, P., Cao, Z., & Choo, K. R. (2011). An ID-based digital watermarking protocol for copyright protection. *Computers and Electrical Engineering, 37*(4)*,* 526–531.

Zhang, J., Kou, W., & Fan, K. (2006). Secure Buyer-Seller Watermarking Protocol. *IEEE Proceedings of Information Security, 153*(3), 15–18.