A Buyer-Seller Watermarking Protocol for Digital Secondary Market

Chunlin Song[1*], Jie Sang[1] and Sud Sudirman[2]
1. School of Computer Science, Jiangnan University, Wuxi, China
2. Department of Computer Science, Liverpool JMU, Liverpool, UK
chunlin.song@hotmail.com, sarlly2016@hotmail.com, s.sudirman@ljmu.ac.uk

Abstract—**In the digital right management value chain, digital watermarking technology plays a very important role in digital product's security, especially on its usage tracking and copyrights infringement authentication. However, watermark procedures can only effectively support copyright protection processes if they are applied as part of an appropriate watermark protocol. In this regard, a number of watermark protocols have been proposed in the literature and have been shown to facilitate the use of digital watermarking technology as copyright protection. One example of such protocols is the anonymous buyer-seller watermarking protocol. Although there are a number of protocols that have been proposed in the literature and provide suitable solutions, they are mainly designed as a watermarking protocol for the first-hand market and are unsuitable for second-hand transactions. As the complexity of online transaction increases, so does the size of the digital second-hand market. In this paper, we present a new buyer-seller watermark protocol that addresses the needs of customer's rights problem in the digital secondary market. The proposed protocol consists of five sub-protocols that cover the registration process, watermarking process for the first, second and third-hand transactions as well as the identification & arbitration processes. This paper provides analysis that compares the proposed protocols with existing state-of-the-arts and shows that it has met not only all the buyer's and seller's requirements in the traditional sense but also accommodates the same requirements in the secondary market.**

Keywords—**Digital watermarking, watermarking protocols, digital products, copyright protection, digital secondary market, cryptography**

I. INTRODUCTION

Recent years have seen a rapid growth in the availability of multimedia products in digital form due to the increase in people's needs. Digital multimedia products have been widely bought and sold online in the past two decades. As the size of the market increases so does the complexity of the needs of the customers to include second-hand transactions. Second-hand transactions of physical goods date back several decades or even millennia in many cases and they are relatively straightforward. Second-hand transactions of digital goods, however, is relatively new but their volume is increasing rapidly. The growth in the second-hand market of digital goods can be attributed to two important factors. First of all, digital goods do not deteriorate with use. This makes used digital goods be as good as new ones. Secondly, because digital goods are immaterial they do not impart strong emotional attachment to their owner as physical goods would. This factor will increase the chance of resale of digital goods compared to the latter.

The second-hand market of digital goods, however, has introduced many of its own legal and practical challenges. In 2012, for example, the first online marketplace for pre-owned digital products called ReDigi was launched. ReDigi is a marketplace, which means it does not buy the pre-owned digital products for reselling itself but rather provides a platform that allows its users to buy and sell pre-owned products directly from one another. ReDigi has been the subject of a lawsuit by a music company which alleged that it is liable for copyright infringements that take place as a result of such transactions. In 2013, a United States District Court has ruled that ReDigi has engaged in illegal activity by vicariously infringing on copyrights of digital goods [1].

At the heart of this problem is the copyright protection of digital products. There has been a steady increase in interest to develop better copy protection and copy deterrence mechanisms. One such solution is the digital watermarking technology.

Over the years, this technology has evolved and developed into a key technology that allows authentication of the ownership of copyrighted digital products and provides forensic proofs through the detection/decoding of the pre-embedded imperceptible watermark [2-5]. Digital watermarking is realized in a transaction by embedding signature signal into a digital product that is imperceptible to the human visual system which can be used to identify the buyer with that particular copy of digital product being transacted [6-9]. Thus, if such procedures are characterized by a good degree of robustness against a wide range of common and non-intentional attacks models including signal processing attack, cryptographic attack, as well as different types of intentional and malicious attacks such as conspiracy attack [10-11], it should be possible to track any copyrights infringement hence protect the copyright of the digital product.

It should be noted that watermarking algorithms alone cannot be used solely as a solution to copyright protection. To effectively support copyright protection processes, they should be applied as part of a suitable watermark protocol as Katzenbeisser in [12] put it: *"Watermarking alone is not sufficient to resolve rightful ownership of digital data; a protocol relying on the existing public-key infrastructure which is also used for digital signatures is necessary"*.

The work on designing suitable watermark protocols, such as those detailed in [13-17], have been proposed in the past. However, most of the current schemes in the literature are designed using the 'first sale doctrine' of the traditional two-party buyer-seller architecture. As evidenced by the emerging popularity of second-hand marketplace such as ReDigi, there is a constant need for a robust watermarking protocol that does not just address the buyer-seller requirements but also addresses them as part of the second-hand business model.

In this paper, we detail the design of our novel buyer-seller watermark protocol for the digital secondary market. The proposed watermark protocol addresses the issues facing Lei's scheme [16] with regards to the conventional buyer-seller requirements and further provides additional protocols to accommodate those requirements in the secondary market. The rest of paper is organized as follows. In section II, a number of contemporary and state-of-the-art, as well as some pioneering watermarking protocol are reviewed. Section III describes the main goals of the proposed watermarking protocol whereas section IV details the stages of the proposed watermarking protocol. Section V provides analysis and comparison between the proposed protocol and the state-of-the-art protocols. Section VI discusses the issues related to practicality and security. The paper summary is provided in section VII.

II. Related Work

More traditional watermarking protocols attempt to solve the issue of copyright protection solely through identification of unauthorized copy. In these protocols, the seller embeds their own watermark in the digital product to identify the buyer during the transaction. The identity of the watermark is known only by the seller, and the seller is the only party that has the ability to embed and extract the watermark. In such schemes, it is then assumed that sellers are trustworthy and always perform the watermark embedding honestly. However, in practice, this assumption cannot fully be guaranteed. The seller could maliciously try to frame a buyer by embedding a certain watermark and distributing the contaminated product as an unauthorized copy. On the other hand, a buyer whose watermark has been found in an unauthorized copy could claim that the unauthorized copy is created maliciously by the seller to frame the buyer. In the absence of sufficient safeguards to avoid such issues and legally sound procedures to confirm or deny that such infringements have taken place, watermarking is a useless technology for copyright protection. This problem is popularly known in the literature as the *Customer's Rights* problem. In this section, we will review a number of solutions to this problem and more current solutions which address other types of requirements and problems such as the *unbinding* problem and the *anonymous* problem.

A. Customer's Rights problem and solutions.

The first protocol that attempts to solve the Customer's Right problem is the Owner-Customer Watermark protocol [18] proposed by Qiao and Nahrstedt in 1998. In this protocol, the customer first provides the owner with an encrypted predetermined bit-string which is then embedded as the unique watermark into the digital product. The watermarked product is then sent to the customer. The customer will be able to prove to a third party the legitimate ownership of the copy in the customer's possession by decrypting the watermark to extract the unique bit-string. This protocol, while provides some sort of solution to the Customer's Right problem, does not protect the customers fully from subsequent potential problems that may arise from unauthorized use of the watermarked products. The main drawback of this protocol is that it does not solve the problem that irrevocably binds the customer to that specific copy, which in turn can hold the customer responsible for any unauthorized exact copies found elsewhere. Similarly, this uncertainty also affects the sellers' case. In the event of a circulation of an unauthorized copy of the product, and in the event of the original buyer, whose watermark has been found on unauthorized copies, is identified, the buyer can claim that the unauthorized copy was created or caused by the original seller either intentionally (or maliciously to discredit the buyer) or unintentionally (through security breach).

One of the subsequent protocols that attempt to fully solve the Customer's Right problem is proposed in [15] by Memon and Wong. This protocol applies encryption during the watermarking stage and incorporates additional, fully trusted, third party namely Watermark Certification Authority (WCA). In this protocol, the buyer requests a valid watermark from WCA which then generates a valid watermark and encrypts it with the buyer's public key. This encrypted watermark is then sent to the buyer. The buyer then sign this encrypted watermark by adding its own digital signature into it before sending it to the seller. The seller is free to add additional information, such as the buyer’s ID and encryption parameter etc., into this signed and encrypted watermark. The seller is then required to encrypt the product using the buyer’s public key before embedding the encrypted and signed watermark into it. Upon completion of the payment, the seller sends the watermarked product to the buyer. This protocol addresses the customer rights problem more satisfactorily than the previous protocol, however, it still has not addressed the unbinding problem and anonymous problem.

B. Unbinding and Anonymous Problem

The unbinding problem refers to the failure of a watermarking protocol to provide proper mechanisms to bind a specific watermark to a specific transaction or a specific copy of the product. This problem could result in a situation where a dishonest seller transplanting a watermark found in a pirated copy of a digital product into another copy of higher-priced digital product to fabricate piracy. The anonymous problem, on the other hand, refers to the failure of a watermarking protocol to protect the buyer’s identity until any guilt has be proven. This requires additional third-party certification, provided by Certification Agency (CA) that binds the buyer’s identity to a unique certificate unknown to the seller or any other third parties and will only be revealed when robust criteria of guilt have been established.

C.Lei et. al first addresses the issue and produces the first solution [16] based on Memon and Wong's protocol. This protocol contains three sub-protocols namely registration sub-protocol, watermarking sub-protocol and arbitration sub-protocol. In the first sub-protocol, the buyer applies to the CA for an anonymous certificate with Public Key Infrastructure (PKI) system. Afterwards, CA generates an anonymous certificate with an appropriate encryption and sends it to the buyer. This sub-protocol is then followed by the watermarking sub-protocol which steps are summarized as follows:

- The buyer first negotiates with the seller to set up a common agreement, ARG, which states the rights and obligations of both parties.
- After that, buyer generates an encrypted anonymous certificate with private key sk^*. Then, B transmits encrypted anonymous certificate and his digital signature to the seller.
- After receiving the above package, the seller generates a unique watermark V after she verifies the validation of the certificate and signature. Then, the seller performs the first round watermark insertion by computers $X' = X \oplus V$, where X and X' are original digital product and watermarked digital product. The seller sends X', encrypted anonymous certificate and the seller’s digital signature to WCA.
- When WCA receives the above document, it generates another watermark W and encrypts it with buyer's public key pk^* which it then sends back to the seller.
- Seller performs the second round watermark insertion in the encrypted domain by computing $E_{pk*}(X'') = E_{pk*}(X' \oplus W)$. It is possible because E_{pk*} is privacy homomorphic with respect to the watermark. Afterward, the seller delivers the encrypted watermarked product to the buyer.
- Lastly, the buyer decrypts the encrypted watermarked product and obtains the watermarked copy.

Whenever a suspected pirated copy of the product is found in the market, the arbitration sub-protocol can be conducted to ascertain the facts. The main aim is to determine the identity of the responsible distributor of the pirated copy, who is assumed to be the buyer in the transaction, with undeniable evidence.

Although the protocol had been shown to have solved both the unbinding and the anonymous problems, it has several other issues. As was touched upon earlier, the protocol lacks supports for second-hand transactions in which the buyer from the previous transaction becomes the seller of the current transaction. Furthermore, in this protocol, the buyer is required to carry out some necessary security steps before they can participate in the transactions. The third problem associated with this protocol is the requirement to perform double watermark insertions by different entities involved in the protocol. This could result in an unexpected and unintentional degradation in quality of the digital product as well as the watermarked data.

III. Main Goals and Design Decisions

In light of all the issues discussed in the previous section, we present in this section a new watermark protocol that solves the aforementioned issues. The main goals of the proposed watermarking protocol are:

1. To fulfil the buyer-seller requirement in the second-hand market
2. To solve the Customer's Right problem, the unbinding problem as well as the anonymous problem.
3. To allow all the buyers, including subsequent buyers after the first transaction, to keep their identities anonymous during transactions.
4. To avoid double watermark insertion in the first transaction which could lead to an unnecessary degradation in quality.
5. To avoid as much as possible collusive behaviors among the entities involved in the protocol.

One of the major hurdles in implementing a secondary market for owners of digital products to resell their property is to ensure that the seller relinquishes and deletes all copies of the product in their possession once the transaction has concluded. However, as noted in [1] there is no way to guarantee all the original files have been deleted. Therefore, this protocol will not put any assumptions that the sellers have deleted the original files but instead, it puts a limit on the number of times the product can be resold.

To achieve these goals, as well as making the proposed watermarking protocol flexible to suit the needs of the second-hand market, three main design decisions have been made: the first decision makes a regulation for proposed watermark protocol after discussing the differences between digital product & non-digital product at second hand market; the second decision is to limit the number of redistribution times of digital product at the same grade of market; whereas the last decision is in regard to the number of grades of market of digital product during transaction.

As for the first design decision, the proposed watermark protocol need to consider the differences between digital product & non-digital product. The price of non-digital used product in a second hand market is usually lower than the corresponding new product because of the degradation in quality suffered from using the product. Therefore, the non-digital product at second-hand market does not significantly affect the first hand market. However, the situation in the digital product is different. Digital products do not suffer from usage as physical products do, but the price of a used digital product at the second hand market is usually lower than the new one. Therefore, this situation could damage the economic interest of the publishing company.

In order to solve this problem, this paper would like to lay out the guideline when inserting the watermark to the digital product being redistributed. Our philosophy follows that suggested in [19] which states that the embedding of the watermark into the digital product not only to protect the ownership of copyrighted products, but should also serve as a means to degrade the quality of the digital product to some extent. Thus, cheap price of used watermarked digital products at a second-hand market is balanced by their slightly inferior quality compared to the new version.

As for the second design decision, unlike with the non-digital products, digital products are very easily duplicated and redistributed, therefore, the proposed protocol puts a limit on number of times the digital product can be resold. This limitation could be enforced softly through the watermarking process which gradually degrades the quality of the product as it is sold multiple times.

This then leads to the final design decision. In this protocol, there are three grades of market considered namely first hand market, second hand market and third hand market. In each grade, the seller embeds their watermark into the digital product. Therefore, at the third hand market, the digital product contains three different watermark signals and this contributes 2.97% visual degradation [19], and if further watermark is embedded, the quality of the product will decrease significantly. Therefore, the proposed protocol have three different watermark signals at most and set up three grades of market correspondingly.

IV. Watermark Protocol

In this section, we propose a novel watermarking protocol for second hand market. To achieve this goal, there are five sub-protocols comprised: 1) registration sub-protocol; 2) watermarking sub-protocol for first hand market; 3) watermarking sub-protocol for second hand market and 4) watermarking sub-protocol for third hand market and 5) identification & arbitration sub-protocol. In particular, the structure of proposed scheme is shown in Fig.1 and a number of actors and roles which are described in Table I. The notations and the meanings of the symbols used to describe the sub-protocols are defined in Table II.

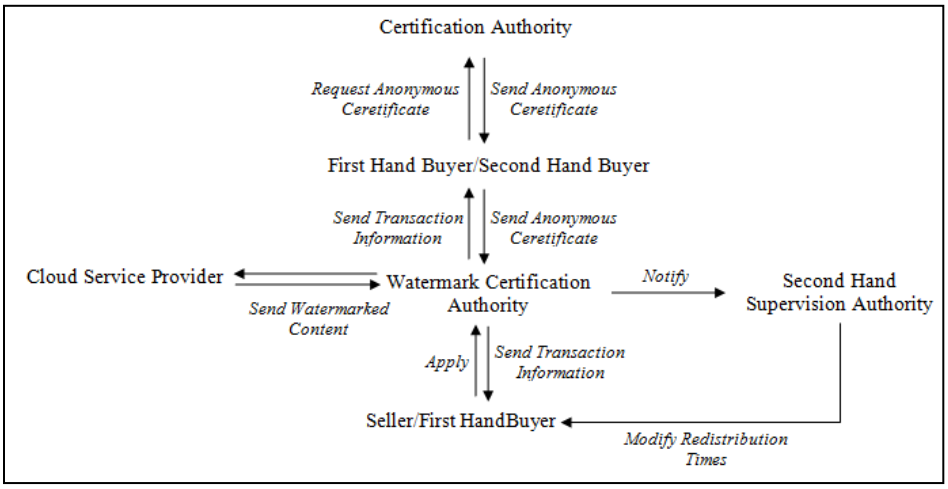

Certification Authority
Request Anonymous Ceretificate
Send Anonymous Ceretificate
First Hand Buyer/Second Hand Buyer
Send Transaction Information
Send Anonymous Ceretificate
Cloud Service Provider
Send Watermarked Content
Watermark Certification Authority
Notify
Second Hand Supervision Authority
Apply
Send Transaction Information
Seller/First HandBuyer
Modify Redistribution Times

Fig. 1. The structure of proposed watermark protocol

In this proposed protocol, we assume that the buyer must have established a secure sockets layer (SSL) connections when purchasing a copy of the digital product. In addition, sensitive information is passed between actors as encrypted tokens and through secure connection such as SSL. The use of such tokens does not intend to increase the security level of the communications but rather to allow each entity involved in the protocol to validate each other's information.

Table I. The parties considered in this protocol and their notations

Notations	Description
B_i	The ith buyer who wants to purchase the digital products (i = 1, 2)
S	The seller who wants to sell the digital products.
CSP	Cloud service provider which will enable the integration of cloud services with web application for more reliable and secure transactions. The cloud service provider, it is assumed to supply trusted and specialized watermarking and security service.
CA	The trusted certification authority is an entity that issues anonymous digital certificates to provide anonymity of B and assurance to D
WCA	The fully trusted watermark certification authority responsible for generating valid and random watermark.
SHSA	The fully trusted second hand supervision authority

Table II. Notations used in the watermarking protocol description

Symbol	Meaning
AGR_i	the ith common agreement, which represents the purchase order (i = 1, 2)
TID_i	the ith transaction identifier which is a code used by seller (i = 1, 2)
XD	brief description of digital product X
SC	sale certification
AC_i	the ith anonymous certification (i = 1, 2)
UD_i	the ith type of data used by WCA to identify B_i during the secure transaction (i = 1, 2)
CD	data used by WCA to identify S during the secure transaction
RDL_i	the ith redistribution license (i = 1, 2)
NWS	number of watermark signals
T_{entity}	time stamp, generate by different entity to identify date and time of day
W_{first_hand}	the first hand watermark signal
$W_{second\text{-}hand}$	the second hand watermark signal
X	digital product
$\overline{X_{first\_hand}}$.	watermarked X after embedding one watermark signal at first hand market
$\overline{\overline{X_{second\_hand}}}$.	watermarked X after embedding two watermark signals at second hand market
$E_{entity}(data)$	Information whose data are encrypted with the entity's security key
$Eh_{entity}(data)$	Enciphered token whose data are encrypted homomorphic
$\overline{Content}$	watermarked digital product/content
(pk_N, sk_N)	A public-private key pair belonging to entity N.
$Cert_N(pk)$	Product certificate issued by entity N and encrypted using pk key

A. Registration Sub-protocol

This sub-protocol only applies if B_i would like to be anonymous during the transaction. Prior to commencing a transaction, B_i is required to apply for an anonymous certificate to the CA. This type of certificate is a normal digital certificate except that the content of its subject field is a pseudonym rather than the real identity of B_i. This sub-protocol starts with B_i randomly selecting a public-private key pair (pk_B, sk_B) and sends the public key pk_B to a trusted CA. Upon receiving the key, CA generates an encrypted anonymous certificate, $Cert_{CA}(pk_B)$, and sends it to B_i. It is also important to note that B_i could forgo the option to remain anonymous by using his or her own valid digital certificate in the transaction.

This sub-protocol achieves the anonymity requirement of the protocol if B_i desires it but at the same time ensure the traceability of the buyer in the event of piracy being committed and proven. This is because CA is responsible for binding a unique anonymous certificate to B_i, and it also guarantees that the binding will not be revealed to any other entity unless requested after a phase of dispute resolution, when the buyer is proven to have committed piracy.

B. Watermark Sub-protocol for First Hand Market

The steps in this sub-protocol is detailed as the following:

1. The transaction starts with B_1 who visits the S's website and chooses a digital product X. B_1 creates an anonymous certificate through the registration sub-protocol detailed previously. B_1 then negotiates with S to set up a common agreement AGR_1, which explicitly states the rights and obligations of both parties, and specifies the digital product of interest, its price and redistribution times. The AGR_1 can be regarded as a 'purchase order' whose generic form can be also published by S on its website. After the initial negotiation, B_1 sends AGR_1 to S.
2. Upon receiving AGR_1, S generates the token-1 denoted as $E_S(TID_1, AGR_1, XD, SC, T_S)$ and send it to WCA with these plain information. In addition, S also sends the token-1 to SHSA with this plain information.
3. After receiving token-1, SHSA verifies the validity of the certificate, and aborts the transaction if any of them is invalid. Otherwise, SHSA generates RDL_1 and NWS to set an initial values. In this case, we assume the initial value of RDL_1 is n, in the other worlds, B_1 could transfer his digital product to the other buyer n times until n is 0. NWS indicates the number of watermark signals which embeds into the digital product and the initial value is 3.
4. B_1 sends AC_1 to WCA.
5. Upon receiving token-1 and the plain information from S and AC_1 from B_1, WCA verifies the validity of both certificates, and aborts the transaction if any of them is invalid. Otherwise, WCA derives UD_1 from the data contained in the anonymous certificate and CD from the data contained in the sale certificate. Afterwards WCA generates token-2 which is denoted as $E_{WCA}(TID_1, AGR_1, XD, UD_1, CD, T_{WCA})$. T_{WCA} is a time-stamp that allows anyone to check when the token last updated. WCA then sends E_{WCA} and AC_1 to B_1 and sends E_{WCA} and SC_1 to S as a temporary transaction certificate.
6. After receiving the temporary sale certificate, S sends WCA the watermarking request.
7. WCA generates two specific functions Ψ and Φ, which can generate two binary codes, μ and σ, respectively. The former identifies the buyer on the basis of UD_1 and CD, whereas the latter is a bit string depending on XD and T_{WCA}. Hence, $\mu = \Psi(UD_1+CD)$ and $\sigma = \Phi(XD + T_{WCA})$. Whereas f is a unique m-bit random value.

$$W_{first\_hand} = E_{WCA}(\mu + \sigma + f) \tag{1}$$

   The first hand watermark signal is obtained by enciphering the concatenation of μ, σ and f, with the secret key. After that, the watermark signal is enciphered by using a full homomorphic cryptosystem [20]. The resulting is denoted as $Eh_{WCA}(W_{first\_hand})$.

8. S also encrypts digital product X using the same cryptosystem to produce $Eh_S(X)$. Then, S sends $Eh_S(X)$ to WCA. WCA forwards it together with $Eh_{WCA}(W_{first_hand})$to CSP. Then CSP can directly watermark, such operation is possible because the encryption function applied by S and WCA is assumed to be homomorphic with respect to the watermark.
9. Once $Eh_S(X)$ has been watermarked, CSP sends WCA the watermarked product $\overline{Eh_S(X)}$. After that, WCA sends a notification to SHSA and S to inform the digital watermarked product is produced.
10. Upon receiving the notification, SHSA modifies the NWS from 3 times to 2 times which means these digital products could embed another 2 watermark signals at most in another two different grades of market. After that, SHSA generates a specific function Ω to produce a specific code λ_1 and sends the encrypted code $E_{SHSA}(\lambda_1)$ back to S, in which $\lambda_1 = \Omega(NWS + RDL_1)$. SHSA stores the relevant information to its database.
11. Once S receives $E_{SHSA}(\lambda_1)$ from SHSA, she requires B_1 to make a payment. After successful receives the payment

from B_1, S sends $E_{SHSA}(\lambda_1)$to B_1. In addition, S notifies the availability of the watermarked product to B_1 with the decryption key.

12. B_1 downloads and decrypts $\overline{Eh_s(X)}$to generate the final version of the watermarked copy of X denoted as $\overline{X_{\text{first\_hand}}}$.
13. Once generated $\overline{X_{\text{first\_hand}}}$, B_1 notifies the availability of the purchased product to WCA. Then WCA can generate the token-3 $E_{WCA}(TID_1, AGR_1, XD, UD_1, CD, W_{\text{first\_hand}}, T_{WCA})$ which represents the definitive version of transaction and send to B_1 and S respectively. In addition, WCA stores UD_1, CD, TID_1 and $W_{\text{first\_hand}}$ in a new entry of TableX.

C. *Watermark Sub-protocol for Second Hand Market*

The steps in this sub-protocol is detailed as the following:

1. If B_1 wants to sell his digital watermarked product $\overline{X_{\text{first\_hand}}}$, he exhibits $\overline{X_{\text{first\_hand}}}$ on its own website or online second hand marketplace. We assume his anonymous certificate as his sale certificate which is applied in this sub-protocol.
2. We assume B_2 is the first buyer who is interested in $\overline{X_{\text{first\_hand}}}$ at second hand market. He wants to purchase digital product $\overline{X_{\text{first\_hand}}}$ and then he creates his own anonymous certificate through registration protocol. After that, he negotiates with B_1 to set up a new a common agreement AGR_2 and sends it to B_1. AGR_2 not only states the rights and obligations of both parties but also specifies the digital product of interest, its price and redistribution times for next grade of market.
3. Upon receiving AGR_2, B_1 generates token-4 denoted as $E_{B1}(TID_2, AGR_2, XD, AC_1, T_{B1})$ and send it to WCA with this plain information. In addition, B_1 sends $E_{SHSA}(\lambda_1)$ and token-4 to SHSA with these plain information.
4. After receiving token-4, SHSA verifies the validity of the certificate, and aborts the transaction if any of them is invalid. Otherwise, SHSA decrypts $E_{SHSA}(\lambda_1)$ by his decryption key and apply Ω to extract RDL_1 and NWS. At the same time, SHSA retrieves the related content from its database to view record. In addition, SHSA generates another redistribution license RDL_2 for B_2 at second hand market. RDL_2 is redistribution times for B_2 and it is valid if B_2 sell his digital product for third hand market.
5. B_2 sends AC_2 to WCA.
6. Upon receiving the plain information from B_1 and B_2, WCA verifies the validity of both certificates to make sure any of them is valid. Then, WCA creates UD_2 and retrieves UD_1 for generating token-5 which is denoted as $E_{WCA}(TID_2, AGR_2, XD, UD_1, UD_2, T_{WCA})$. Then WCA sends token-5, AC_2 to B_2 and token-5, SC_2 to B_1 as a temporary transaction certificate.
7. After receiving the temporary sale certificate, B_1 sends WCA the watermarking request.
8. WCA generates another two specific functions α and β, which can generate two binary codes, γ and δ, respectively. The former identifies the buyer on the basis of UD_1 and UD_2, whereas the latter is a bit string depending on XD and T_{WCA}. Hence, $\gamma = \alpha(UD_1 + UD_2)$ and $\delta = \beta(XD + T_{WCA})$. Whereas r is a m-bit random value.
$$W_{\text{second\_hand}} = E_{WCA}(\gamma + \delta + r) \tag{2}$$
9. The second hand watermark signal is obtained by enciphering the concatenation ofγ, δand r, with the secret key. After that, the watermark signal is enciphered by using a full homomorphic cryptosystem. The resulting is denoted as $Eh_{WCA}(W_{\text{second\_hand}})$.
10. B_1 also encrypts $\overline{X_{\text{first\_hand}}}$ using the same cryptosystem to produce $Eh_{B1}(\overline{X_{\text{first\_hand}}})$. Then, B_1 sends $Eh_{B1}(\overline{X_{\text{first\_hand}}})$ to WCA. WCA forwards it together with $Eh_{WCA}(W_{\text{second\_hand}})$ to CSP. Then CSP can directly watermark,the watermark embedding algorithm in this sub-protocol is same as the algorithm which is applied in first hand market.
11. Once $Eh_{B1}(\overline{X_{\text{first\_hand}}})$ has been watermarked, CSP sends WCA the watermarked product. After that, WCA sends a notification to SHSA and B_1 to inform the digital watermarked product is produced.
12. Upon receiving the notification, SHSA modifies the NWS from 2 times to 1 time and amends RDL_1 from n times to n-1 times. After that, SHSA updates the latest content and applies function ζ to produce another specific code λ_2 and sends it as an encrypted version $E_{SHSA}(\lambda_2)$ back to B_1, in which $\lambda_2 = \zeta(NWS + RDL_1 + RDL_2)$. In addition, SHSA informs B_1 of the rest about redistribution times and stores the pertinent information to its database.
13. If B_2 is the last buyer who purchases $\overline{X_{\text{first\_hand}}}$ at second hand market legally. At this step, SHSA modifies the NWS from 2 times to 1 time and amends RDL_1 from 1 time to 0. Then, SHSA updates the latest content and applies ζ to produce the final specific code λ_n and sends it as an encrypted version $E_{SHSA}(\lambda_n)$ back to B_1, in which $\lambda_n = \zeta(NWS + RDL_2)$. In addition, SHSA informs that B_1 losses his authority to redistribute and stores the pertinent information to

its database.

14. If B_2 is the x^{th} buyer, neither the first buyer nor the last buyer who purchases $\overline{X_{first\_hand}}$ at second hand market. As same as before, SHSA first modifies the NWS from 2 times to 1 time and amends $RDL_1$from m times to m-1 times, in which m is equivalent to (n - x) times. Then, SHSA updates the latest content and applies ζ to produce the new specific code λ_m and sends it as an encrypted version $E_{SHSA}(\lambda_m)$ to B_1, in which $\lambda_m = \zeta(NWS + RDL_1 + RDL_2)$. In addition, SHSA informs B_1 about the rest of redistribution times and stores the relevant information to its database.
15. Once B_1 receives $E_{SHSA}(\lambda_1)$or $E_{SHSA}(\lambda_n)$ or $E_{SHSA}(\lambda_m)$ from SHSA, he requires B_2 to make a payment. After successful receives the payment, B_1 notifies the availability of the watermarked product to B_2 with the decryption key and B_1also sends $E_{SHSA}(\lambda_1)$ or $E_{SHSA}(\lambda_n)$ or $E_{SHSA}(\lambda_m)$ to B_2.
16. B_2 downloads and decrypts $\overline{Eh_{B1}(X_{first\_hand})}$ to generate the final version of the watermarked copy of X_{first_hand}, denoted as $\overline{\overline{X_{second\_hand}}}$.
17. Once generated $\overline{\overline{X_{second\_hand}}}$, B_2 notifies the availability of the purchased product to WCA. Then WCA can generate the token-6 $E_{WCA}(TID_2, AGR_2, XD, UD_1, UD_2, W_{second\_hand}, T_{WCA})$ which represents the definitive version of transaction and send to B_1 and B_2 respectively. In addition, WCA stores UD_1, UD_2,TID_2 and W_{second_hand} in a new entry of TableX.

D. *Watermark Sub-protocol for Third Hand Market*

If B_2 wants to sell his digital material to another buyer B_3, he will need to follow this sub-protocol. This sub-protocol is similar to the sub-protocol for Second Hand Market with a few differences as detailed below:

1. This sub-protocol does not consider B_1 as a seller and B_2 as a buyer. Instead, B_2 is considered as a seller and B_3 is a potential buyer.
2. As with the second hand market sub protocol, this sub protocol also involves producing another, albeit different, set of tokens by the different entities and uses similar set of notations. However, there are two main differences:
3. In the second step, if B_3 wants to purchase digital product $\overline{\overline{X_{second\_hand}}}$, he creates an anonymous certificate and set up a new a common agreement AGR_3 after negotiating with B_2. The most important prevision in AGR_3 states that B_3 has no rights to resell digital product any more. Therefore, in the next step, SHSA do not need to generate another redistribution license for next grade of market.
4. In the eleventh step, SHSA modifies the NWS from 1 time to 0 and amends RDL_2. After that, SHSA applies τ to specific code λ_3 and sends it as a encrypted version $E_{SHSA}(\lambda_3)$ back to B_2. Finally, SHSA informs B_2 of the rest about redistribution times and stores the pertinent information to its database

E. *Identification and Arbitration Sub-protocol*

Whenever a pirated copy of a protected product is found in the market. The main aim is to determine the identity of the responsible distributor, who was the buyer in some earlier transaction with undeniable evidence. Therefore, when a pirated copy X' is found. WCA can ask CSP for starting this protocol by sending it X'.

1. The first thing for CSP to do is to run the corresponding detection and extraction algorithm on X' to extract the watermark. Let V' denote the watermark extracted.
2. CSP transfer V' to WCA. Then WCA use V' as a key to search TableX for a match.
3. WCA access its database and use V' to search them for a match. When a possible is found, WCA retrieves transaction ID, seller and buyer's information.
4. WCA requires the corresponding seller to deliver the transaction certificate.
5. Seller deliveries the transaction certificate $E_{WCA}(TID_n, AGR_n, XD, UD_n, UD_n, W_{first\_hand}$ or $W_{second\_hand}, T_{WCA})$ to WCA which n = 1 or n = 2.
6. Then WCA then decrypts it to obtain Wand compares it with V'. If they match, WCA then retrieve the buyer's anonymous certificate $Cert_{CA}(pk_B)$ from UD_n. WCA will request CA to retrieve and reveal the identity of the buyer using that certificate. WCA will then adjudicate that the buyer is guilty. On the other hand, if the two watermarks do not match or if seller failed to retrieve a valid transaction certificate then no buyer's identity will be revealed.

V. Comparison of the Proposal

In this section, we compare our approach with the extensions of buyer-seller watermarking protocols to the digital secondary market architecture.

A. Comparison with other protocols

In [16], Lei *et al*. describes a buyer-seller watermarking protocol using homomorphic public-key cryptosystem. This protocol exploits trusted WCAs in order to carry out watermark insertions and to ensure a correct copyright process. The protocol implements the correct authentication of buyers without exposing their identities during the transaction. Thus, the protection of the buyers' privacy from the sellers is guaranteed, and the sellers will not be able to collect sensitive information about buyers during the transaction.

This design principle is widely accepted as a good solution to the unbinding problem and has since been adopted by a number of subsequent watermark protocols including [14, 26]. However, these protocols suffer from the *double watermark insertion problem* [25]. In these protocols, double watermark insertion is crucial in solving the unbinding problem. However, a digital product, especially when coded in a compressed format, has a limited capacity for including hidden information without suffering deteroration in its perceptual quality. In contrast, a single watermark insertion, whilst can provide a secure and robust outcome, should also allow insertion of long fingerprint codes that could be particularly useful in achieving the anti-collusion objective.

The first solution on single watermark insertion schemes is introduced in [33]. This protocol solves the major and most common problems documented in the literature, it does not require the buyer to have any knowledge of cryptography and watermarking, and it avoids the double watermark problem by adopting a single-watermark approach, and is not limited to linear watermarking schemes. Subsequently, a number of watermarking protocols have been developed based on this protocol [25, 28].

In this respect, the proposed protocol achieves all the above objectives and more. It avoids collusion attack and protects different entities' copyright by applying different encryption algorithms. The proposed protocol also employs single watermark insertion scheme at each grade market. In addition to those, and as the main unique selling point, the proposed protocol provides supports for the digital secondary market.

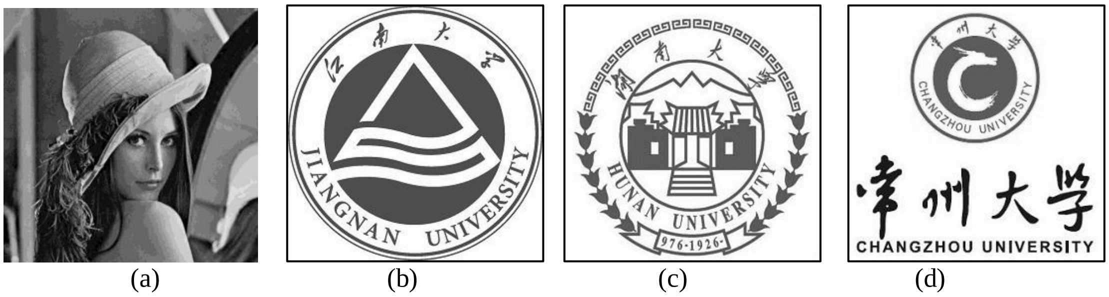
In this protocol, a single watermark insertion approach is adopted to securely link the product, buyer, seller and transaction. Two specific functions are used to generate two binary codes which are then combined to produce a single watermark. In addition, WCA delivers the watermark and the digital product to another trusted third party, namely the CSP, to embed. CSP cannot collude with other entities of which the details are described in section VI.

The second advantage of this protocol is its support for the digital secondary market. The proposed watermarking scheme protects the first hand buyer's (seller) and the second hand buyer's (buyer) copyright. The main goals of this level is to balance the economic value of digital product and the quality of digital product, therefore, embedding multi-watermark signals are perferred, and a trusted third party SHSA is employed to limit the maximum number of redistribution to three. The summary of prominent watermark protocols and their fulfillment of the buyer's and seller's requirement is given in Table III.

Table III.The summary of watermark protocols

Requirements fulfilled	**Lei [16]**	**Peng [14]**	**Chen [26]**	**Hu [33]**	**Our Protocol**
Traceability	√	√	√	√	√
No Repudiation	√	√	√	√	√
Anonymity	√	√	√	√	√
No framing	√	√	√	√	√
Collusion Tolerance	√	√	√	√	√
Unbinding	√	√	√	√	√
One Watermark Insertion	×	×	×	√	√
Digital Secondary Architecture	×	×	×	×	√

B. Watermark Experiment



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

Fig. 2 (a) The host image (b) the first watermark image (c) the second watermark image (d) the third watermark image

The proposed protocol could be applied to protect copyright of any digital products including digital videos, digital audios, digital images or digital games etc. It could use any robust watermarking algorithms to achieve its objective of gradual degradation in digital product's quality. In this section, we will present the result of our experiment when we use DWT-SVD technique [29] as the watermarking algorithm and will show that it does allow our protocol to meet its requirements. The experiment applies this to digital images as the type of digital product under consideration using also digital images as the watermark data. The images used in this experiment are shown in Figure 2.

Figure 2a is the host image and the other three images are the first, second and third watermark image respectively. The host image is 1024 x 1024 pixels in size and the watermark images are 64 x 64.

The embedding stage of the DWT-SVD on each level is summarized as follows:

1. First of all, the host image is divided into non-overlapping blocks.
2. Secondly, sum the entropy and edge entropy for each block. Arrage the blocks in ascending order and select the first 1024 blocks that have the lowest values as the appropriate blocks for watermark embedding.
3. Apply DWT algorithm to the selected blocks and then apply SVD algorithm on LL subband of each block.
4. Examine the $U_{2,1}$ and $U_{3,1}$ entries of matrix **U** to embed the watermark by updating the relationship.
5. Perform an inverse SVD and an inverse DWT to obtain the watermarked image.

The watermark extraction procedure is a series of inverse steps of embedding procedure.

The experiment also performs a number of different attacks to the watermarked images to simulate activities that could happen intentionally in real life to destroy the watermark data.

As a quantitative measure of the quality degradation caused by the attacks we use Peak-Signal-to-Noise Ratio (PSNR). The PSNR between the original watermarked I(t) and the attacked watermarked J(t) signals is calculated using equations (3) and (4). High PSNR values indicate lower degradation or high quality.

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{255}{\mathrm{RMSE}}\right) \tag{3}$$

RMSE is the square root of mean square error is defined as:

$$\mathrm{RMSE} = \sqrt{\frac{1}{\mathrm{T}}\sum_{\mathrm{t}}^{\mathrm{T}}(\mathrm{I(t)} - \mathrm{J(t)})^2} \tag{4}$$

Once the watermarked images have been exposed to the different attacks, their corresponding watermark image is extracted. To measure the similarity between the original watermark w(i,j) and the extracted watermark w'(i,j) we use the Normalized Correlation (NC) which is calculated using equation (5)

$$\mathrm{NC} = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} w(i,j)\cdot w'(i,j)}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} w^2(i,j)} \tag{5}$$

Two experiments are conducted to test the robustness of proposed watermarking protocol. The first experiment is aimed to verify that inserted watermarks images can be extracted with minimal distortion. The second experiment measures the robustness and suitability of the DWT-SVD technique for the proposed protocol.

B.1 Watermark insertion and extraction verification

The first experiment will show that watermark images could be inserted and extracted completely by using DWT-SVD technique, the embedding strength is set to 0.04. Figure 3 shows the experiment results of the watermark insertion process. The PSNR value between original watermarked image and host image is illustrated in Table IV.

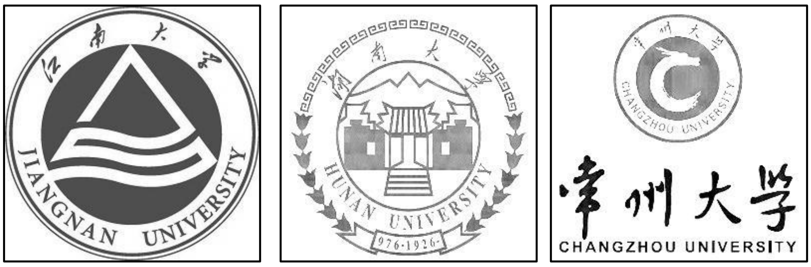
Table IV PSNR value between the watermarked image and host image after different insertion process

The insertion process	PSNR value
The first insertion process	37.8
The second insertion process	32.3
The third insertion process	28.6

(a) (b) (c)

Fig. 3 The watermarked image (a) after the first insertion process (b) after the second insertion process (c) after the third insertion process

As can be seen from Figure 4, the extracted watermark images are similar to the original watermark images shown in Figure 2. The NC value between original watermark image and the extracted watermark image is listed in Table V. It is important to note that the watermark images are extracted in the reversed order of the embedding process. This means the first watermark image is extracted last and vice versa. Table V has shown that the extraction process yields identical third watermark image and degraded second and first watermark images.



(a) (b) (c)

Fig. 4 The extracted watermark image (a) after the final extraction process (b) after the second extraction process (c) after the first extraction process

Table V NC value between the original watermark image and the extracted watermark image

The extraction process	NC value
The first extraction process (third watermark)	1.0000
The second extraction process (second watermark)	0.9949
The third extraction process (first watermark)	0.9884

B.2 Robustness Comparison

To test the robustness of the DWT-SVD watermarking algorithm and its suitability for use in the proposed protocol, nine watermark attacks are applied to the watermarked image. They are Gaussian noise attack, sharpen attack, median filter attack, affine transformation (rotation and translation) attacks and cropping attacks. Table VI shows the NC values between the extracted watermark images after different attacks and original watermark image.

Table VI NC value between the extracted watermark image after different attack and the original extracted watermark image

Attacks	The extraction process	NC value
Gaussian Noise Attack (mean = 0, variable = 0.005)	The first extraction process	0.9385
	The second extraction process	0.9808
	The third extraction process	0.9694
Shapen Attack	The first extraction process	0.8467
	The second extraction process	0.9297
	The third extraction process	0.9162
Median Filter Attack (3*3)	The first extraction process	0.9964
	The second extraction process	0.9859
	The third extraction process	0.9580
Rotation Attack (30 degree)	The first extraction process	0.3707
	The second extraction process	0.4507
	The third extraction process	0.6672
Rotation Attack (45 degree)	The first extraction process	0.3778
	The second extraction process	0.4395
	The third extraction process	0.6328
Rotation Attack (50 degree)	The first extraction process	0.3842
	The second extraction process	0.4467
	The third extraction process	0.6398
Translation Attack	The first extraction process	1.000
	The second extraction process	1.000
	The third extraction process	1.000
Cropping off 20%	The first extraction process	0.9242
	The second extraction process	0.9668
	The third extraction process	0.9498
Cropping off 50%	The first extraction process	0.9160
	The second extraction process	0.9563
	The third extraction process	0.9331

Watermark attacks can be categorized as either removal attacks or geometric attacks. Removal attack includes Gaussian noise attack, sharpen attack and median filter attack. Geometric attack includes rotation attack, translation attack and cropping attack. As can be seen in Table VI, we can conclude that in our algorithm, most of the NC values are greater than 0.9, which means most of the watermarks are detected with minimal distortion, therefore, it proves that the DWT-SVD watermark algorithm is robustness against the most of various watermark attacks.

B.3 Degradation Test

As was previously discussed, in most cases digital products do not suffer from quality degradation over time or after each use. Therefore, a second-hand or a third-hand digital product has as much usage value as a brand new digital product. Since a used digital product is often sold cheaper than its brand new counterpart, this fact reduces the economic value of the latter. This provides a disincentive for the original copyright owner to approve or support any subsequent sale of their products in secondary market. Therefore, it is imperative that a gradual degradation in quality is introduced to the digital products as more secondary sales occur. This protocol introduces such concept through its process of watermarking. The quality of the product is expected to degrade as the product is watermarked and sold for multiple times. The protocol dictates that by the fourth time the degradation should exceed acceptable threshold.

It is understood that different types and usage of digital products have different tolerance in quality degradation. It is impossible to cover all possible combinations there are, however for this specific experiment we will provide a case of digital image for high quality print publication.

In order to prove that the usability of the digital image and the watermark is damaged on the fourth-hand market, we continue the experiment by embedding another watermark image. The plot of the NC values of the extracted watermark images and the PSNR values of the digital image is shown in Fig. 5 and 6 respectively. The experiment shows that the 4th insertion of the watermark introduces considerably worse effect on the quality of the extracted watermarks even without subjecting them to additional attacks. The NC value of the first watermark, for example, drops from around ~0.98 (as shown in Table V) to ~0.91 when extracted.

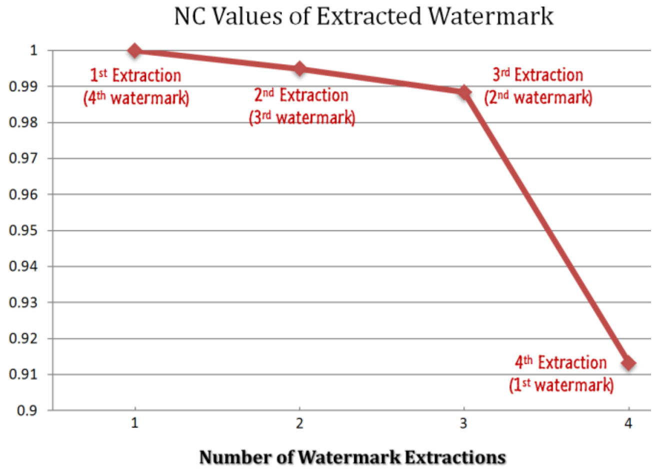


Fig 5. The degradation of the watermark images

With respect to the degradation in the watermarked image quality, the DWT-SVD has shown good result. As a measure of quality degradation, we use PSNR value between the original unmarked image and the watermarked images. The result is shown in Fig. 6. The figure shows that the image quality degrades gracefully as the image is watermarked multiple times and by the third time it falls slightly below 30dB and considerably after the fourth watermarking. This results is in line with the expectation that the quality should drops gradually and also with the suggestion in [35] which implies that excellent PSNR values (suitable for print publication use of digital images) range from 30 to 50 dB, while an acceptable range (suitable for online transmission or publication) settles around 25dB.

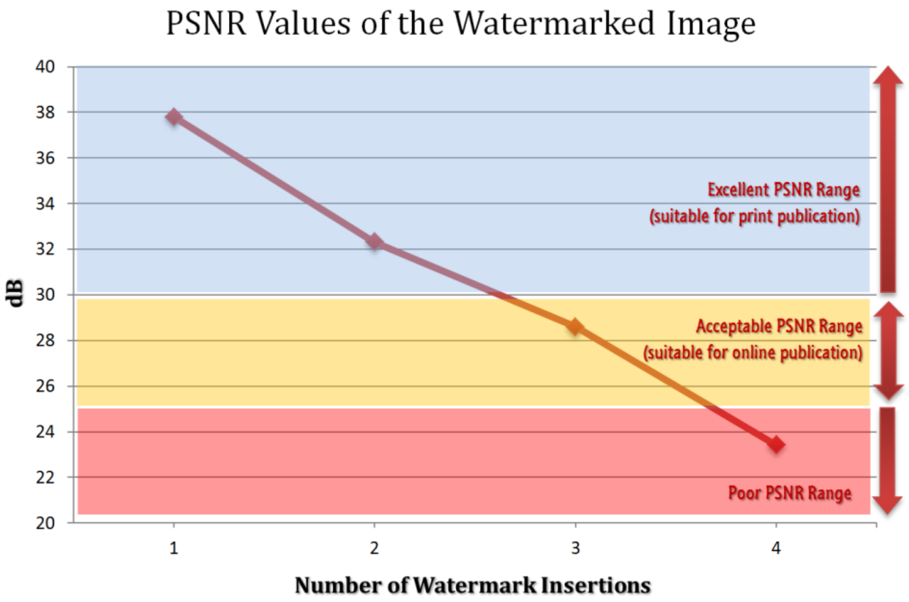


Fig 6. The degradation of watermarked image

Additive watermarking algorithm is the most popular embedding technique. In additive watermark embedding process, the tradeoff between robustness and degradation is achieved by means of adjusting the embedding strength α in Equation 6.

$$I_w = I_H + \alpha.W \tag{6}$$

Where I_w is the resulting watermarked image, I_H is the host (original) image and W is the watermark signal. Larger value of α often means more robust watermarked image but more degraded quality. The resulting degradation in quality and robustness level, however, does not only depend on the value of α alone. They are affected by the features of the host image and the watermark images used. Furthermore, the DWT-SVD watermarking algorithm, which is specifically used in this paper, is a region-based watermarking technique which inserts watermarks only in certain parts of the host image selected after meeting specific criteria.

The above factors make it almost impossible to have a closed-form solution in getting degradation and robustness levels from just the embedding strength alone. Therefore, to do so, the authors suggest the users of this technique to experiment with the embedding process to get the level of protection and quality degradation they want.

B.4 Time complexity

Each program has been run on a a desktop computer equipped with a CPU AMD A8-7650K Radeon R7, 10 computer cores 4C+6G at 3.30 GHz, 8GB of RAM and SS disk of 400GB. All desktop computers have been connected by a Fast Ethernet at 72MB/s.

The proposed protocol is applicable to use on different sized images and using different settings/values for the security parameters such as the watermark length, the length of security key etc. Therefore, the execution times could vary depending on the data and setting used. In this experiment, we use a 1024 x 1024 sized digital image, 64 x 64 sized watermark images, and a 1024-bit long encryption key. The mean results of the execution time of main tasks in first hand market are shown in Table VII, and the total execution time is 388.3 seconds. The execution time of second hand market and third hand market have the similar results.

Table VII Execution times of main tasks

Task	Execution time
Catalogue navigation	Variable time
Seller generates token-1	2.1s
SHSA generates RDL$_1$ and NWS	1.5s
WCA verifies the certificates and generates token-2	2.5s
WCA generates and encrypts two specific functions	100.8s
Seller encrypts digital products	98.6s
The watermarked product is generated	135.7s
SHSA modifies the NWS and generates a specific function Ω	1.8s
Buyer downloads and decrypts watermarked product	45.3s

VI. Security Analysis and Discussion

The proposed protocol has been designed for second hand market, taking into account the results of the security analysis. Therefore, the basic principles that characterize the design of the proposed protocol are:

1. Communications among the entities involved in the protocol are all basically enciphered and authenticated.
2. Buyer is the sole entity that is allowed to obtain access to the final watermarked product
3. Seller and CSP cannot collude since there is never any contact between them

Due to the realistic situation of digital multimedia product on secondary hand market [1], the copyright protection becomes a special and important problem. In this question, how to make a tradeoff between digital product quality and economic value is a vital issue, based on this, the paper proposed a pioneering technique in designing a buyer-seller watermark protocol for digital secondary market. This protocol first considers the regular and common problems such as customer's right problem, anonymous and binding problem, and security problems amongst other issues. There are three main design decisions studied and made. The first decision deals with the issue of quality and cost of second hand digital products. Digital products do not suffer from usage as physical products do, but the cost of a used digital product at the second hand market is usually lower than the new one. This situation could impact economically on the publishing company. In order to solve this problem, this protocol proposes a concept that inserts a watermark every time the product is being sold. In each grade level of the market, a watermark is inserted into the digital product. The benefit of this approach is not only for the protection of the seller's copyright but also to intentionally reduce the economic values of digital product to simulate degradation in quality as more watermarks are embedded [25-28].

The proposed watermarking scheme enables the seller to embed watermark sequence into multimedia product with flexible watermarking capacity, in order to adaptively satisfy different requirements in a variety of practical applications. In addition, this protocol can exploit different robust watermark embedding and extraction schemes, such as the 'asymmetric' and 'secure' algorithms. Specifically for this paper, we show that the block-based DWT-SVD image watermarking algorithm [29] is particularly suitable watermarking algorithm that achieves all of the intended objectives. This algorithm starts by dividing the image into different non-overlapping blocks. After that, some of these blocks are selected to ensure the embedding process would only affect specific regions of the image. Finally, a combination of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) algorithms are applied to embed watermark into a digital image. The DWT-SVD method has been shown to have provided high robustness to attack as well as introduce relatively low distortions and watermark perceptibility. This algorithm however has a disadvantage of not being a zero-knowledge watermarking scheme [36]. The use of such algorithms would not be suitable for this protocol because zero-knowledge watermarking algorithms do not change any original data, but rather utilize some features of the product to construct the watermark, hence the intended quality degradation objective could not be achieved.

Secondly, this protocol limits the redistribution times on the digital secondary market. By designing this factor because the digital product would not be redistributed without restricting to disrupt the market. The publishing company will set up the redistribution times at the very beginning and after that, the seller, the first buyer, and the second buyer will follow the redistribution rules.

In theory, unlimited number of watermarks could be inserted into a digital product but in practice this leads to severe deterioration of quality. Therefore, there is a question of how many watermark can a digital product can store before it becomes unusable. The answer is not straightforward as because different types and usage of digital products have different tolerance in quality degradation. For example, a digital image used for high quality print publication has a much lower tolerance to degradation than images used as thumbnail online. While embedding too many watermark could degrade the quality of digital product significantly, embedding fewer watermarks than needed may not be sufficient in achieving the goals of the proposed protocol. Khan in [19] indicates that embedding 3 different watermarks are the best choice in this protocol.

One of the major contribution of the proposed protocol is the gradual degradation in quality of the digital product through embedding multiple watermark products for the economic reasons. A specific case of product degradation is illustrated in section B.3. As can be seen from the experimental result, the DWT-SVD watermarking algorithm can be used with this protocol to achieve this objective and provide good quality watermarked product (in the region of 30-50 dB) in the first hand, second hand and third hand market and a lower quality watermarked product (sub 25 dB) after subsequent and fourth watermarking.

The protocol imposes an explicit requirement that messages are always interchanged over secure and anonymous communication channels between parties through an SSL connection, which are widely provided by web browsers and guarantee a high security level. This enables us to achieve the level of communication security that is commonly considered sufficient for communications in web contexts. Furthermore, transaction identifiers, timestamps and digital signatures are exploited according to prevent possible transaction attacks to enable different entities involved in the protocol to control the ongoing transactions. Then, the exchange of redundant enciphered tokens enables each party to validate their communication in a single phase rather than in multiple phases. These two characteristics ensure the proposed watermark protocol to be efficient and secure.

CSP is a service delivering mode based on the Internet. It can provide users with scalable services as required through the Internet and has been widely recognized and applied. In our proposed scheme, CSP plays a very important role for embedding watermark. However, one of the top threats to cloud computing is malicious insiders. An insider can be a rogue administrator employed by a cloud service provider, or an employee of the victim organization who exploits vulnerabilities to gain unauthorized access. The multitenant nature of the cloud computing environment makes it difficult to detect and prevent insider attacks. In order to solve this problem, the proposed protocol applies fully homomorphic encryption which is produced by Craig Gentry in 2009 to allow computations to be carried out on encrypted data [20]. Homomorphic encryption generates an encrypted result, which, when decrypted, matches the result of the same operations performed on the original data. The rest of the security issues on CSP is server availability problem, multitenant services problem, data storage problem, access control problem and so on that is not described in this paper, the related solutions are introduced in [21-23].

The product to be protected is sent from WCA to CSP in an enciphered form, and so CSP cannot access the digital product. Therefore, CSP cannot collude with sellers. From the seller's viewpoint, the proposed protocol is secure, because buyer and CSP cannot gain access to an original copy of X. In addition, buyer can neither know which watermarking algorithm has been used to protect digital product nor calculate the watermark signal, because the signal is not always the same for a given buyer. In other words, the protocol ensures that the identity of the buyer can be traced via the AGR stored contained in the transaction certificate, using the stored data to extract the watermark in the illegal copy of the product. A guilty buyer cannot deny responsibility or claimed that they have been framed by a third party since no single party could plant a malicious watermark because a valid watermark is unique to each transaction, securely encrypted from all parties. To put it bluntly, the only case where a malicious but valid watermark can be inserted into the product is when all parties, including the buyer, colluded for it.

In our proposed watermarking protocols, WCA plays a very important role to control and directly manage all the phases. Therefore, WCA is a fully trusted third party in different kinds of watermarking protocols to generate watermark signals and prevent different parties. In addition, our protocol proposes another fully trusted third party SHSA which is responsible for manage the redistribution times.

On the buyer’s right requirement, seller, WCA and CSP cannot obtain access to the final watermarked copy, and this prevents them from directly distributing illegal replicas, thus solving the customer's right problem. Furthermore, the transaction certificates bind the watermark signal to the buyer's identity, the purchased product and the transaction by which the product is bought. In addition, the transaction certificate is stored by buyer and seller in an enciphered and signed form, and so seller, buyer, CSP cannot generate, access, or modify them and therefore, solving the unbinding problem.

In order to improve the efficiency of the watermark protocol. In a period of ‘first sale doctrine’, the scheme employs one watermark signal instead of two or more watermark signals usually employed in traditional methods [9][11]. This requires that the digital product to be transferred from the seller, to WCA, to CSP before returning back to WCA, which is the site which buyer can download the product from. In fact, such a solution forces the product to follow a route characterized by several hops. After that, the protocol inserts different watermark signals at second hand market and third hand market. Therefore, on the premise of quality in watermarked digital products assurance, this protocol designs tertiary online digital product market if buyers want to resell their goods.

The protocol also meets the anonymity requirement by making sure that buyer's privacy is well protected. The protocol takes advantage of anonymous certificates to preserve the anonymity of buyer during transactions. The anonymity achieved in the proposed watermarking protocol is asserted by a trusted third party, CA. Under the assumption of CA's existence, buyer can keep his real identity unexposed unless he is adjudicated to be guilty by the arbiter.

Finally, the protocol assumes that the burden of storing necessary information is mainly put on the sellers and WCAs, and this can be considered reasonable since they are very likely to already have their databases needed to manage their activities.

Although this protocol achieve the goals on designing a buyer-seller watermark protocol for digital secondary market it is also characterized by some drawbacks and it requires improvements in future. The first problem is digital certificate problem. Digital certificate issued by CAs are widely used for e-commerce transactions by buyers who reside within specific area, such as Western Europe, the American and Japan, but their spread and adoption within many other geographical areas with high population densities are still a slow process [15-16] thus restricting the protocol deployment to developed countries. So the improved version for future research should provide a 'multiple negotiation mechanism'. Secondly, the watermark protocol mechanisms for digital secondary market can be further improved by using more up-to-date watermarking technologies such as the zero-knowledge watermark algorithm.

VII. Conclusion

We have presented a watermarking protocol for second hand market that has met all the entities requirement, satisfactorily addressed the requirements of the second hand business models for content or product delivery by supporting enciphered transaction, as well as being efficient in carrying out the transaction. The technique achieved this by employing five sub-protocols namely registration sub-protocol; watermarking sub-protocol for first hand market; watermarking sub-protocol for second hand market and watermarking sub-protocol for third hand market and identification & arbitration sub-protocol.

We have provided a thorough analysis and discussion on how the proposed technique meets the all the requirements of modern watermarking protocols as well as overcoming the main drawbacks affecting the major solutions existing in the literature without requiring a double watermark insertion. Finally, the proposed protocol follows a number of design principles that help its success in term of practical acceptance in web context.

Acknowledgement

The work was sponsored by Jiangnan University of Science & Technology Young Scholar Grant (No.JUSRP11462); Key Project of Jiangnan University Fund Grant (No. JUSRP51414A); National Natural Science Foundation of China (No. 61305017); Natural Science Foundation of Jiangsu Province (No. BK20130154); the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) and Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAEET).

References

[1]. K. Gittleson, "US court to rule on ReDigi's MP3 digital music resales", Oct 2012, http://www.bbc.com/news/technology-19842851.

[2]. I. Cox, J.Bloom and M.Miller, "Digital watermarking: principles & practice". San Mateo, CA:Morgan Kaufman, 2001.

[3] C. Qin, C. Chang, Y. Chiu. "A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting", IEEE Transactions on Image Processing, 23(3), 969-978, 2014.

[4] C. Qin, X. Zhang. "Effective reversible data hiding in encrypted image with privacy protection for image content", Journal of Visual Communication and Image Representation, 31(C), 154-164, 2015.

[5]. Z. Xia, X.Wang, X.Sun, Q.Liu, and N.Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels," Multimedia Tools and Applications, 75(4), 1947-1962, 2016.

[6]. C. Song, S. Sudirman and M.Merabti, "A robust-adaptive dual image watermarking technique", Journal of visual communication and image representation, 23, 549-568, 2012.

[7]. X. Zhang, S. Wang, Z. Qian and G. Feng. "Reference sharing mechanism for watermark self-embedding", IEEE Transaction on Image Processing, 20(2), 485-495, 2011.

[8] C. Qin, C. Chang, P. Chen. "Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism", Signal Processing, 92(4), 1137-1150, 2012.

[9]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing", IEEE Transactions on Information Forensics and Security, 2016.

[10]. Z. Hu, K. She, J. Wang, J. Tang. "Game theory based false negative probability of embedded watermark under unintentional and steganalysis attacks", Communication, China. 11(5), 114-123, 2014.

[11]. Z. Zhou, Y. Wang, J. Wu, C. Yang, X. Sun, "Effective and efficient global context verification for image copy detection", IEEE Transactions on Information Forensics and Security, 2016.

[12]. S. Katzenbeisser. "On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking", 12thInternationalworkshop on database and expert systems applications, 815-819, 2001.

[13]. A. Rial, J. Balasch, B. Preneel. "A privacy-preserving buyer-seller watermarking protocol based on priced oblivious transfer", IEEE transaction on information forensics and security, 6(1), 202-212. 2011.

[14]. Y. Peng, C. Wang, Y. Fang and W. Li. "Anonymous watermarking protocol for vector spatial data", International conference on computer science & service system, 2095-2098, Nanjing, 2012.

[15]. N. Memon and P. W. Wong, “A buyer-seller watermarking protocol”, IEEE transaction on image process, 10(4), 643–649, 2001.

[16]. C. L. Lei et al., “An efficient and anonymous buyer-seller watermarking protocol,” IEEE transaction on image process,13(12),1618–1626, 2004.

[17]. A. Rial, M. Deng, T. Bianchi, A. Piva and B.Preneel. "A provably secure anonymous buyer-seller watermarking protocol", IEEE transaction on information forensics andsecurity, 5(4), 920-931, 2010.

[18]. L. Qiao, K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights", Journal of visual communication and image representation, 9(3), 194-210, 1998.

[19]. M. Khan, V. Jeoti, A. Malik et al. "A joint watermarking and encryption scheme for DCT based codecs. 17th Asia-pacific conference on communications, Malaysia, 2011.

[20]. C. Gentry. "A fully homomorphic encryption scheme". PhD dissertation, Department of Computer Science, Stanford University, 2009.

[21]. KM. Khan, Q. Malluhi. "Establishing trust in cloud computing". IT Professional, 12(5), 20-27, 2010.

[22]. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement", IEEE Transactions on Parallel and Distributed Systems, 27(9), 2546-2559, 2016

[23]. Y.Ren, J.Shen, J.Wang, J.Han, and S.Lee, "Mutual verifiable provable data auditing in public cloud storage," Journal of Internet Technology, 16(2), 317-323, 2015.

[24]. F. Frattolillo. "Watermarking protocol for web context". IEEE Transaction on Information Forensics and Security, 2(3), 350-363, 2007.

[25]. F. Frattolillo. "Watermarking protocol: problems, challenges and a possible solution". The Computer Journal, 58(4), 944-960, 2014.

[26]. C. Chen, C. Chen, D. Li and P. Chen. "A verifiable and secret buyer-seller watermarking protocol". IETE Technical Review, 32(2), 104-113, 2015.

[27]. J. Huang, F.Jeng, T.Chen. "A new buyer-seller watermarking protocol without multiple watermarks insertion". Multimedia Tools and Applications, 1-13, 2016.

[28]. F. Frattolillo. "A buyer-friendly and mediated watermarking protocol for web context". ACM Transactions on the Web, 10(2), Article 9, 2016.

[29]. N. Makbol, B. Khoo, T. Rassem. "Block-based discrete wavelet transform-singular value decoomposition image watermarking scheme using human visual system characteristics". IET Image Processing, 10(1), 34-52, 2016.

[30]. G. Zhang, Y. Ma. "Analysis on influence factors of digital preservation sustainability". Information Science (Chinese Journal), 28(11), 1737-1740, 2010.

[31]. H. Ochi, T. Ota, A.Yamaoka, H. Watanabe, Y. Kondo, N. Tokuda, H. Taguchi, T. Matsumoto, H. Kobayashi, S. Imai. "Sealed mask ROM wafer with 5mm magnetic resonant coupling for long-term digial data preservation". IEEE 26th International SOC Conference, 262-266, Erlangen, 4-6 Sep, 2013.

[32]. D.Langr, P.Tvrdik. "Evaluation criteria for sparse matrix storage formats". IEEE Transaction on Parallel and Distributed System, 27(2), 428-440, 2016.

[33]. D. Hu, Q. Li. "A secure and practical buyer-seller watermarking protocol". International Conference on Multimedia Information Networking and Security, 105-108, November, 2009.

[34]. M. Nematollahi, S. Haddad. "An overview of digital speech watermarking". International Journal of Speech Technology, 16(4), 471-488, 2013.

[35]. W.Zhou, A.C.Bovik. "Mean square error: love it or leave it? A new look at signal fiedlity measures". IEEE Signal Processing Magazine. 26(1), 98-117, 2009.

[36]. J. Waleed, S. Hameed and D. Huang. "A robust optimal zero-watermarking technique for secret watermark sharing". International Journal of Security & Its Application. 8(5), 349-360, 2014.