A High Security Buyer-Seller Watermark Protocol based on Iris Biometric

Chunlin Song[1,*], Jie Sang[1] and Bo Zhou[2]

[1]*Department of IOT Engineering, Jiangnan University, Wuxi, China and* [2]*Department of Computer Science, Liverpool JMU, Liverpool, UK*

Abstract: With the development of digital watermarking technology, digital watermarking protocol is now drawing the attention for protecting copyrights of digital products. However, the copyright protection is fully protected by watermark technology if it is employed a suitable protocol between the rights owner and the customer. Therefore, currently, there are a number of buyer-seller watermarking protocols proposed, however, an anonymous problem and collusion problem are still unsolved completely. Thus, this paper proposes a high security watermark protocol based on iris biometric for resolving these problems. In addition, this paper also produces watermarking generation mechanism which aims to improve the efficiency of the whole mechanism. Finally, the investigation indicates that the proposed buyer-seller watermark protocol takes care of the security concerns of all parties involved, and the proposed scheme could also find an illegal copy of the content, the violators can be traced back.

Keywords: Copyright protection, iris biometric, security, buyer-seller, watermark protocol, watermark algorithm.

I. INTRODUCTION

Currently, the communication and computer technologies are rapid by developed, networking and globalization have become irresistible trends of the world. Consequently, digital resources and services can be easily accessed in anytime, anywhere, which are much more convenient than before. Under these circumstances, digital products such as electric books, digital images, movies, music etc. are very easily duplicated, reproduced, distributed or exhibited without authorization. Thus, the copyright problems are paid more and more attention by researchers

In order to solve the above problems, digital watermarking technology plays a very important role to authenticate the rights of copyrighted digital contents. A watermark algorithm can be classified as fragile watermarking algorithm, robust watermarking algorithm and semi-fragile watermarking algorithm. The use of a fragile watermarking technique is important when people want to verify whether the protected media has been tampered with or not. This type of watermark is especially designed to be as delicate as possible, so that even the slightest modification to the marked media can destroy it, indicating that someone tampered with the media in question. On the other hand, robust watermarking algorithm is designed to withstand such modifications, and its use mainly provide proof of ownership of the media in question, even after such media has been subjected to several attempts to remove the watermark. A semi-fragile watermarking system should provide an application-driven trade-off between robust and fragile. Semi-fragile watermarking system fragile to malicious modifications while robust to incidental manipulations.Therefore, the illegal copy of digital product could be proved through the decoding the imperceptible watermark.

*Address correspondence to this author at the Department of IOT Engineering, Jiangnan University, Wuxi, China; E-mail: songchunlin@jiangnan.edu.cn

The effectiveness of copyright protection process is supported by watermarking technique if a suitable watermark protocols relying on the existing public-key infrastructure and digital signatures is employed. Nowadays, there are several representative buyer-seller watermark protocols introduced [1-5]. Briefly speaking, when a digital content is displayed online and ready to sell, watermarking protocol is typically used to embed specific watermark content which contains both buyer's and seller's information in order to protect copyrights of both of them. After that, the watermark protocol arbitrates the guilty person when an illegal distribution is detected. Watermark protocol aims at resolving the issues related to implementing watermarking as a solution to QoS estimations [6], bill purposes [7] and digital rights management in real life e-commerce application [8]. In particular, it should:

- Watermark protocol should be efficient and effective
- A customer's identity is protected until he/she is proven guilty.
- Watermark protocol should identificate and arbitrate illegal copy or distribution
- A host buyer should be protected from malicious action.

This paper designs an improved version of buyer-seller watermark protocol to provide secure, flexible and convenient solution. The proposed scheme provides a high security authentication mechanism using iris biometric. In addition, this protocol also improves the efficiency of whole system compare with the traditional mode. The structure of this paper is organized as follows. Section 2 reviews background and some important watermark protocols. Section 3 introduces iris collection, iris image pre- processing, feature extraction and in section 4, the proposed watermarking protocol is described. Finally, section 5 discusses security and accomplishment of main goals.

2352-0965/16 $58.00+.00

2. RELATED WORK

In 1998, Qian and Nahrstedt proposed the first watermarking protocol [9]. This protocol attempted to solve *customer's copyright problem*. This problem referred as a buyer who owned a watermarked digital product that had been found in unauthorized copies claiming that the seller created unauthorized copy. Therefore, the author proposed a solution to apply watermark algorithm and exchange data between different entities. A buyer first applied an encrypted function to his personal information and send to seller. After that, when seller received this encrypted message, he applied any watermark algorithm to watermarked. Then, this watermarked digital product was transmitted back to buyer. The consumer decrypted the watermarked content and proved the ownership of this copy to trusted third party. However, the other researchers pointed out this scheme could not solve customer's right problem because the watermarked copy can still be accessed in its final form. The above problem was successfully solved by Memon and Wong [10]. This watermarking protocol worked by ensuring that the seller did not get to know the exact watermarked copy that the buyer received hence the seller cannot create copies of the original content, containing the buyer's watermark. In addition, the protocol also involved another two fully trusted actors for the transaction and arbitration, which named as the watermark certification authority and arbiter, respectively. The transaction in this protocol can be illustrated in Fig. (**1**).

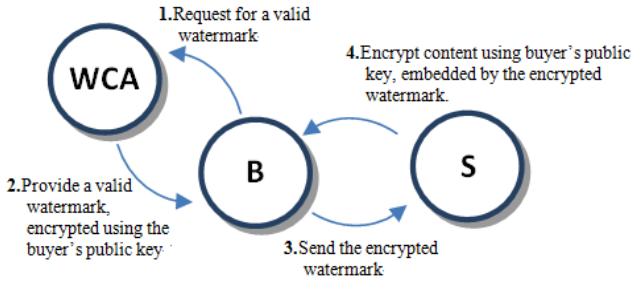

Fig. (1). Transaction in Memnon & Wong's buyer-seller watermarking protocol.

Upon discovering an illegal copy of the content, the seller can use the arbiter to verify whose watermark was contained in it. The arbiter would be able to determine this by using the private key of each buyer.

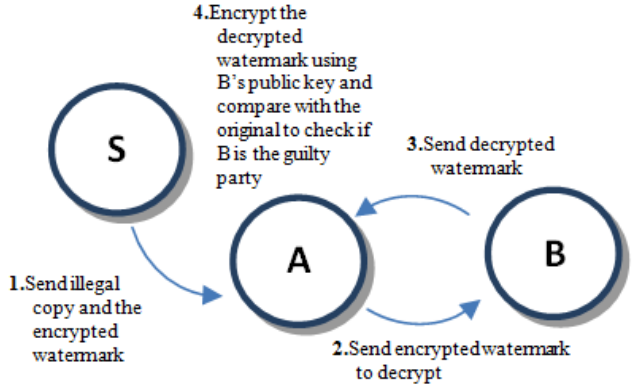

Fig. (2). Arbitration in Memnon & Wong's buyer-seller watermarking protocol.

An unbinding and anonymous problem is when the buyer's secrecy is not be protected against collusion in the event of malicious arbiter. This problem was sorted out by Lei's proposal [11]. This protocol first set up a certificate authority (CA) as a trusted third party. In this protocol, buyer first applied a unique common agreement (ARG) from CA's and a particular transaction was bind between ARG and a piece of digital product. Besides that, the customer could stay be anonymous status during transaction via the help of CA. Thus, the anonymous problem was solved. After that, the buyer-seller watermark protocol becomes the hot topic, and a number of watermark protocols have been proposed.

In 2005, Kuribayashi and Tanaka introduced an anonymous buyer-seller fingerprint scheme based on the Okamoto-Uchiyama encryption algorithm to improve the enciphering rate [12]. In 2007, another secure buyer-seller watermark protocol was proposed, this scheme indicated that a seller first generated an original permuted watermark to embed into digital content in an encrypted domain. And then, when an unauthorized digital product was found in the market, the seller first extracted and recovered the watermark signal and forwarded it to the arbitrator [13]. In 2008, there was another anonymous watermark protocol proposed to improve the computational cost by applying a secure watermark embedding algorithm [14]. Recently, an offline trusted third parties buyer-seller watermark protocol was proposed by Fan, this protocol improved the efficiency of trusted third parties and resisted against conspire attack [15]. Neelesh proposed a buyer-seller watermark protocol that aimed to reduce computational cost at buyer's end [16]. In [17], another protocol was presented for transplanting the digital watermarked content between buyers, this protocol also ensured that each copy was unique to identify its recipient. Furthermore, the seller's communication complexity was proportional to the size of the watermarks rather than the size of the content.

The requirement of having a multiparty architecture was first identified in [18] where a protocol utilizing multiparty multilevel Digital Rights Management architecture was proposed. In this protocol, different parties were considered as distributors (sub-distributors), owner, consumer, and license server. The distribution level was assumed as a multi-levels architecture, where the top level was for the right owner, the medium level was distributors, and their sub-distributors, and the bottom level was for the customers. Furthermore, there were two types of licenses introduced in this protocol named as redistribution license and usage license. The protocol applied a joint digital watermarking algorithm using Chinese Reminder Theorem (CRT) where each party generated its individual watermark signals and these watermark signals are combined together using CRT algorithm.

An interesting watermarking protocol was described in [19]. The protocol was based on three cryptographic building blocks: group signature, homomorphic encryption and zero proof of knowledge. The first block allowed buyers to sign the purchase messages when they are sent to the seller. The second block allowed the buyer and the seller to encrypt the watermark content and embedded into the digital product in such a way that none of the parties knows about it. The third blockI was a two-party protocol between a 'prover' and a

'verifier', which allowed the prover to verify the knowledge of the secret input which fulfilled the some statement.

Finally, Ashwani compared the difference between different buyer-seller watermarking protocols to integrate with different digital watermarking algorithms and cryptography techniques for copyright protection [20].

Even though there are a number of watermark protocols presented above and solve a number of issues, however, some main drawbacks and problems also existed.

- In the above examples, CA as a trusted third party issues digital certificates. Buyers need to provide their real identity to apply digital certificate [11]. However, although CA is assumed as a trusted third party in watermark protocol, but if CA is untrustworthy, CA could collude with a malicious seller to fabricate piracy to frame innocent buyer.
- The watermark protocol is inefficient because there are a large number of data exchanged among different entities.

For solving the above mentioned problems, in this paper, we will introduce iris biometric in our watermark protocol to improve the security level of CA. In addition, the watermark pool will be generated by WCA in order to improve the efficiency of the whole system.

3. IRIS BIOMETRIC AUTHENTICATION SYSTEM

Authentication system is the act of confirming the personal identification claimed to be true by an entity and security identity authentication is the kernel of authentication system. Furthermore, remote authentication is one of the most commonly used methods to determine the identity. Generally speaking, password authentication, smart card authentication and biometric authentication are the three most popular authentication methods.

Password authentication systems are used frequently as the most early authentication mechanisms [21]. While the advantage of password authentication is easy to implement, however, the disadvantage of password authentication is indicated that such anauthentication system has many vulnerabilities. Therefore, smart card with password authentication mechanism provides two-factor authentication which gives stronger security than the password authentication [22]. However, both of the authentication schemes are not suitable for buyer-seller watermark protocol.

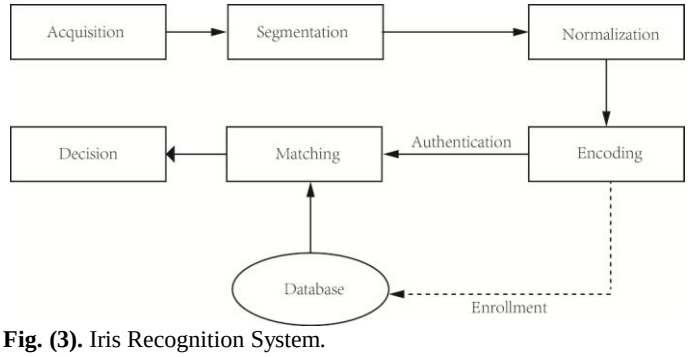

Fig. (3). Iris Recognition System.

Another authentication mechanism is a biometric authentication which aims to apply in the buyer-seller watermark protocol. Biometric authentication could verify or recognize the identity of a person by scanning their physiological characteristics, such as fingerprint, voiceprint, iris scan etc. [23]. Biometric characteristics are regarded as a reliable authentication factors because they own a unique and invariance property which cannot be easily lost or forgotten. Recently, iris biometric authentication systems have attracted extensive attention worldwide because the improvements in the machine matching algorithms and the progress in sensor technologies, thus making the systems both secure-protected and cost-effective [24]. They are ideally appropriated for remote authentication application such as buyer-seller watermark protocol.

In iris biometric authentication system, most of the iris recognition systems contains five basic modules: acquisition, segmentation, normalization, encoding and matching, the process is illustrated in Fig. (**3**).

- Acquisition: there is a 6 inches camera-device needed to acquisite his/her iris information in most of the iris recognition systems [25] and part of iris recognition systems applies built-in camera-device such as mobile camera and its corresponding iris recognition software without requiring any additional hardware component [26]. In the proposed protocol, the latter scheme is preferred with mobile camera or web camera [26] which can achieve our target in the case of user with glasses.
- Segmentation: In this module, iris segmentation algorithm is used in the collected eye image by isolating iris from other structures [27].
- Normalization: In normalization module, a rubber-sheet model is applied to transform the iris texture from Cartesian to polar coordinates [28].
- Encoding: The binary code is generated by using feature extraction routine. After encoding module, the system stores the encoding features into its related database.
- Matching: This module produces a match score by comparing the presented iris image against the encoded features to identify an individual.

4. PROPOSED SCHEME

In this section, the proposed watermark scheme will be introduced, the roles and notations are defined first in this section and the goals are explained in the next section. Then we continue to elaborate the five sub-protocols: the *seller registration sub-protocol*, the *watermark generation sub-protocol*, the *buyer registration sub-protocol*, the *watermark sub-protocol* and the *identification and arbitration sub-protocol*. Fig. (**4**) illustrates the relationship of different roles and sub-protocols and the details are explained later in this section.

In the proposed watermark protocol, there are several different roles described below:

- **S**: The seller, who wants to sell certain digital content to buyer.
- **B**: The buyer, who wants to purchase the digital content.
- **CA**: A certification authority is an entity that generates anonymous digital certification.
- **WCA**: A trusted third party watermark certification authority responsible for generating random and valid watermark.

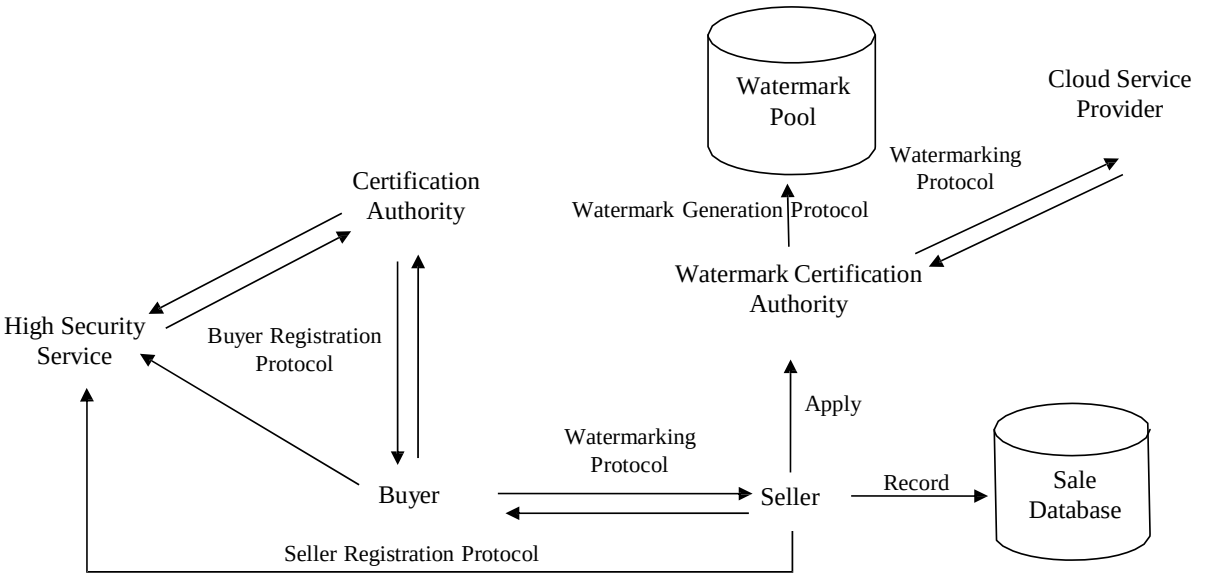

Fig. (4). The overall structure of proposed watermark protocol.

- **ARB**: An arbiter, who arbitrates lawsuits against the violation of copyright and intellectual property.
- **HS**: Government-oriented high security department such as police security department, which is responsible for iris collection, analysis and storage.
- **CSP**: The 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.

The notations are defined as follows:

Table 1. Notations Used to Describe the Watermarking Protocol.

Symbol	Meaning
AGR	a common agreement, which represents the purchase order
TID	the transaction identifier is a code used by S
XD	brief description of digital product X
SOI	seller's original iris image
SIC	seller's iris code
BOI	buyer's original iris image
BIC	buyer's iris code
B_Cert	seller's business certification
$Sign_I(M)$	the signature of message M signed by I with his privacy key
$Cert_J(I)$	the digital certificate issued to subject I by certification authority J
$SIC_{HS}(pk_{S1})$	HS encrypts seller's iris code using key pk_{S1}
T_I	time stamp, generate by I to identify date and time of day
X	digital content
X'	primer watermarked content
X''	final watermarked content

There are four main goals to be achieved in the proposed protocol:

- The proposed buyer-seller watermark protocol is considered to solve the conspiracy problem if CA is untrustworthy. In particular, government-oriented high security company is introduced in this protocol.
- The proposed watermark protocol considers to fulfill both B's and S's requirements. Particularly, in the point of B's view, seller should be an honest and trustworthy vendor which could not frame B by any means, and in the point of S's view, B should not try to remove the watermark which is embedded in purchased by him.
- For the purpose of improving the efficiency of WCA, the watermark pool is generated before transaction. In addition, watermark insertion is not performed by WCA in order to reduce the overload of WCA.
- B's privacy needs to be protected very well. The proposed protocol promises to preserve the anonymity of buyer's identity unless he is proved guilty.

A. Seller Registration Sub-protocol

To update a security level of whole protocol in order to protect S's copyright, S collects his original iris information to HS to apply iris encoding features.

To apply iris encoding features, S first acquire his original iris image SOI using build in camera such as web or mobile camera. S then generates a key pair (pk_{S1}, sk_{S1}) and encrypts SOI and his business certificate B_Cert by sk_{S1}, and sends to HS with pk_{S1}. When the HS receives encrypted information, it decrypts with pk_{S1}first and then it proves the business certificate, if the business certificate is invalid, HS aborts the transaction, otherwise HS analyzes the original iris image to generate the iris code SIC using feature extraction routine which is described in the previous section. After that, HS encrypts the biometric information with pk_{S1}, $SIC_{HS}(pk_{S1})$and sends back to S.

B. Watermark Generation Sub-protocol

Before new digital product released, S is responsible for generating and sending new product information to WCA to register new products. WCA verifies the information of digital product, if the digital product is already registered, the request is declined, and otherwise, WCA generates a production certificate and generates watermark pool afterwards.

In the first step, S generates a key pair (pk_{S2}, sk_{S2}) and the new product information were reported. The report, $E_{REPORT}(XD, T_S)$, is encrypted by the sk_{S2}, and sends to WCA with pk_{S2}. When the WCA receives encrypted report, it decrypts E_{REPORT} with pk_{S2}. Next, WCA generates a product certificate, encrypted with pk_{S2}, $Cert_{WCA}(pk_{S2})$, and sends back to S with related information which is described in Table **2**.

Table 2. Product Certificate.

Information
Product certification identification
Product model number (k bits)
Production description
n numbers of watermark signals
Updated timestamp by WCA

One of the most important things in this sub-protocol is to create a watermark pool by WCA after product registration. Watermark pool involves a number of m-bit fingerprinting codes f_i, each fingerprinting code contains k bits product model number and m-k bits pseudo random serials, which is listed in Fig. (**5**). After that, each fingerprinting code will be encrypted for another security level and uploaded to watermark pool database.

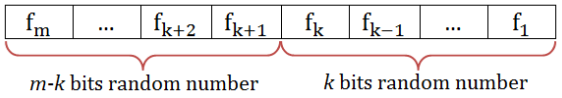

Fig. (5). Fingerprinting codes used in the watermark pool.

C. Buyer Registration Sub-protocol

This sub-protocol assumes that CA is not a trusted third party however, HS is a government oriented high security department which is responsible for buyer's security. It collects buyer's iris information and guarantees that the information is secured and not disclosed to anybody unless the buyer is provided as a guilty person.

This sub-protocol only applies if B would like to be anonymous during the transaction. Prior to commencing a transaction, B is required to apply for an anonymous certificate to the CA. The anonymous certificate is a normal digital certificate and CA is responsible for issuing and binding anonymous certificate to B after buyer registers personal information at HS.

Before acquiring a copy of digital content, each buyer B needs to register with CA to apply his own anonymous certificate. For achieving this target, B first makes an application to CA, CA generates a notification and forwards to B, the notification requires B original iris image to HS. Then B collects his original iris image BOI using web/mobile camera. After that, B generates a key pair (pk_{B1}, sk_{B1}), encrypts BOI by sk_{B1}, and sends the encrypted packet to HS with pk_{B1}. When the HS receives encrypted information, it decrypts with pk_{B1}, analyzes the BOI to generate the buyer's iris code BIC and stores the encrypted information $BIC_{HS}(pk_{B1})$ into its own database. Finally, HS sends key pk_{B1} and notice of completion to CA. When CA receives the notification and key from HS, an anonymous certification, $Cert_{CA}(pk_{B1})$is generated which is sent back.

D. Watermark Sub-protocol

The steps in this sub-protocol are illustrated in Fig. (**6**) and the details are described as follows:

(1). First of all, B would like to purchase digital product X and visit the S's website. B sets up an anonymous certification through buyer registration protocol and after negotiating with S, B sets up AGR, which describes both the rights and obligations clearly to the buyer and seller, and states the digital content of interest and its price.

(2). After that (pk*, sk*), as a one-time key pair is selected and $Cert_{pkB1}(pk^*)$as an anonymous certificate is generated. While pk_{B1}'s pseudonym is associated with pk* and $Cert_{CA}(pk_{B1})$ is the associated pseudonym on B. Then, B transmits $Cert_{CA}(pk_{B1})$, $Cert_{pkB1}(pk^*)$, ARG, $Sign_B(ARG)$, T_B to S.

(3). Upon receiving $Cert_{CA}(pk_{B1})$, $Cert_{pkB1}(pk^*)$, ARG, $Sign_B(ARG)$, T_B, S confirms the authority of both certificates and signature, if all of them are valid, S generates a transaction ID, TID, and integrates with BIC to produce a unique watermark V and computers $X' = V \oplus X$, where X' is the watermarked digital product and X is the digital product. Within this step, any watermarking algorithm might be applied to digital product to provide that it is able to resist different watermark attacks and still can be extracted later if it is required. Moreover, S transmits $Cert_{pkB1}(pk^*)$, ARG, $Sign_B(ARG)$, TID,XD, $Sign_S(ARG)$ and T_S to WCA. In addition, S sends TID and $E_{pk^*}(X')$ to CSP.

(4). When WCA receives the above information, it verifies the validity of the certificates and signature, and aborts the transaction if any of them is invalid. Otherwise, WCA finds out and withdraws the corresponding fingerprint code f through XD from watermark pool, decrypts it, computers $E_{pk^*}(f)$ and sends $E_{pk^*}(f)$, TID to CSP, sends $E_{pkWCA}(f)$ to S.

(5). After receiving the enciphered information above, CSP matches between $E_{pk^*}(f)$ and $E_{pk^*}(X')$ through TID transaction. After that, CSP can directly watermark $E_{pk^*}(X'') = E_{pk^*}(f) \oplus E_{pk^*}(X')$. Such an operation is possible because the encryption function is assumed to be homomorphic with respect to the watermark.

(6). When digital contents are watermarked, CSP uploads the watermarked content E(X'') into designated database. CSP also informs the availability of digital watermarked content to S and S requires B to make a payment. S stores V, $Cert_{pkB1}(pk^*)$, ARG, $Sign_B(ARG)$, TID,XD, $E_{pkWCA}(f)$, $Sign_S(ARG)$in a new entry of Table **X**.

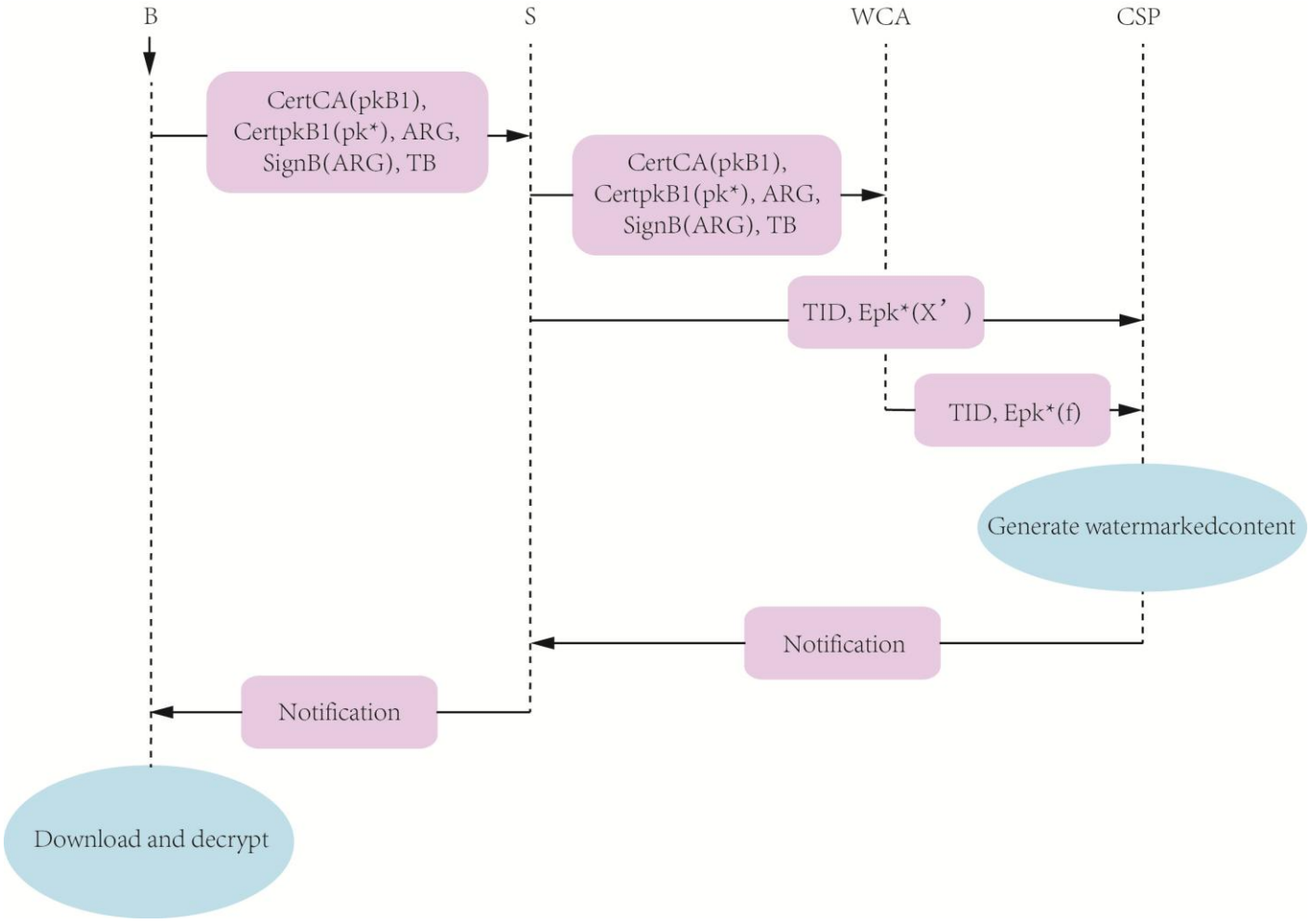

Fig. (6). Details of transaction in the proposed watermark sub-protocol.

(7). When B successfully makes a payment for digital content, S will allow B to download watermarked content E(X''). Next, B can decrypt it with sk* and gets the correctly watermarked copy X''.

E. Identification and Arbitration Sub-protocol

In the event of a pirated copy, denoted as Y of the product being found in the market, the identification and arbitration protocol plays an important role in this section to determine the identity of guilty person with undeniable evidence.

(1). First of all, CSP extracts the watermark signals by running the extraction algorithm on Y. Let V' denotes the extracted watermark content. Then, S searches her sale records Table **X** by using V, for a match. Then, S collects the related information after a match is found, X', $Cert_{pkB1}(pk^*)$, ARG, $Sign_B(ARG)$, TID,XD, $Sign_S(ARG)$, sends ARB with Y.

(2).When ARB receives the above information, it verifies the validity of them. If all of them are valid. ARB asks WCA to decrypt $E_{pkWCA}(f)$ and obtain f. Next, ARB executes the second round of verification on $E_{pk^*}(f)$. If $E_{pk^*}(f)$ is correct, ARB applies the corresponding watermark extraction technique to determine the existence of f in Y. If f is discovered in Y, ARB requests HS to provide the real identity behind pseudonym pk*. The ARB decides the buyer to be guilty only because the identity for the buyer who owns pk* is revealed, and then closes the case. Otherwise, if f is not found in Y, the buyer is considered as innocent, and his identity remains unexposed.

5. SECURITY ANALYSIS AND DISCUSSION

In this section, we will analyze the security issues and discuss whether the design goals are achieved or not.

There are three main design goals which have been described in section III, and all of the three aims are achieved by the proposed scheme.

(1). First of all, this buyer-seller watermark protocol considers to fulfill both B's and S's requirements. On the seller's point of view, buyer is ignorant about which type of watermark has been inserted into the copy he purchased,

therefore he can not get rid of the watermark. The proposed watermark protocol also provides an explicit mechanism, which identified the guilty buyer when the illegal copy is found.

From the perspective of B, the proposed watermark scheme is a secure and fair protocol, because S gets no authority to access the final form of digital watermarked content, and S cannot allocate illegal replicas to frame the buyer. Therefore, the customer's right problem is avoided.

(2). The operations of watermark insertion are not performed by WCA to improve the efficiency of WCA. Watermark is generated before transaction and CSP are responsible for embedding watermarks, and therefore, WCA is relieved from excessive computations.

(3). B's privacy is well protected. The proposed watermarking protocol designs a high security scheme to preserve the identity of B during transactions. Compared with Lei's protocol, CA has no idea about the buyer's real identity, therefore, a malicious seller cannot collude with CA to fabricate piracy to frame an innocent buyer. Instead, HS as a highly trusted third party, a government-oriented security service department is responsible to collect, analyze and verify buyer status though iris recognition. HS is considered to be a trusted third party because this is a government-led organization, entitled with protected power, supervision power and law enforcement power. Under this assumption, B can keep his real identity unexposed unless he is adjudicated to be guilty by ARB

(4). 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. 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 are server availability problem, multitenant services problem, data storage problem, access control problem and so on, that are not described in this paper, the related solutions are introduced in [16].

(5). This paper assumes CA as an un-trusted third party to issue anonymous certificate. Therefore, CA could collude with a malicious seller to fabricate piracy to frame an innocent buyer. In order to solve this problem, we apply iris biometric authentication system to make the whole protocol secure. HS as a government oriented high security and fully trusted third party is responsible for buyer's security. It collects buyer's iris information and guarantees that the information is secured and un disclosed to anyone.

(6). In most of the 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. It is for this reason that WCA becomes a bottleneck in a realistic large-scale distribution system because it manages all transactions and the bandwidth usage is prohibitively high especially on transaction protocol. As a result, this problem is the critical question as we considered, in the proposed watermarking protocol, WCA generates a number of watermark signals in the first-phase preparations in product registration sub-protocol. Consequently, the utilization is reduced in transaction sub-protocol, so the bandwidth usage is optimized as well. Thus, the effectiveness of the whole distribution system is improved.

The availability of WCA is critical to the availability of the whole system. In general, the availability of WCA requires the reliability if WCA itself and the stability of WCA, cluster-based solutions can be used to construct a single node of WCA. On the other hand, deploying a distributed system with multiple nodes of WCA over the Internet solves the problem of network failures that may cause temporary or permanent disconnection from a particular node.

Even if the availability of WCA is assured by the distributed system techniques mentioned above, it may also be necessary for the party who must communicate with WCA to possess multiple physical connections to the Internet so that the party will have less chance to suffer from complete disconnection from the network. In the proposed watermarking protocol, only S and CSP are required to contact WCA during transactions. We argue that it is more practical for S and CSP to have multiple network connections rather than for B to do so.

(7). The protocol is a modular and flexible scheme, because it is defined as four different sub-protocols and this

Table 3. The summary of prominent watermark protocols and their fulfilment of the buyer's and seller's requirement

Requirements fulfilled	Memon [10]	Ju[3]	Choi[4]	Lei[11]	Zhang[13]	Kuribayashy[5]	Proposed Scheme
Traceability	√	√	√	√	√	√	√
No Repudiation	√	√	√	√	√	√	√
Anonymity	×	√	×	√	×	√	√
No framing	√	√	√	√	√	√	√
Collusion Tolerance	×	×	×	×	√	×	√
Unbinding	×	×	×	√	√	√	√

protocol can exploit different watermark embedding and extraction schemes, such as the 'asymmetric' and 'secure' algorithms, or 'zero-knowledge' watermark algorithms.

(8). In this protocol, we presented a buyer-seller watermark protocol that ensures only one watermark signal is embedded into the content as compared to the embedding of two watermark signals into the content with most of the approaches. Thus, this approach minimizes the possible degradation of the quality of a digital content due to embedding of watermark signal. In other words, a single watermark insertion can result in being secure and robust, and enables the insertion of long fingerprinting codes, particularly useful to exploit 'anti-collusion' techniques.

Finally, the summary of prominent watermark protocols and their fulfillment of the buyer's and seller's requirement is given in Table **3**. As we can see from Table **3**, the proposed watermark protocol is achieved in all the design requirements especially on collusion tolerance.

6. CONCLUSION

In this paper, we have presented a high security watermarking protocol that has met not only all the buyer's and seller's requirements, but also satisfactorily addressed the requirements of the present-day business models. This protocol includes five sub-protocols, 1) seller registration sub-protocol, 2) watermark generation sub-protocol, 3) buyer registration sub-protocol, 4) watermark sub-protocol and 5) identification and arbitration sub-protocol. Before a transaction, each buyer registers with CA and HS with buyer's iris information through the registration protocol and watermark pool which are also generated in order to improve the efficiency of WCA. Then, a watermarked version of the digital content is generated from a seller and WCA via the watermark sub-protocol and delivered to buyer. Finally, if any dispute can be found and identified by using the identification arbitration protocol.

We have provided a thorough analysis and discussion on how the proposed technique meets all the requirements of modern watermarking protocols as well as overcoming the main disadvantages, affecting the major solutions existing in the literature. Finally, this protocol follows a number of design principles that help its success in terms of practical acceptance in web context.

CONFLICT OF INTEREST

The authors have declared no conflict of interest.

ACKNOWLEDGMENTS

The work was sponsored by Jiangnan University of Science & Technology Young Scholar Grant (No.JUSRP11462), and Key Project of Jiangnan University Fund Grant (No.JUSRP51414A)

REFERENCE

[1] H.S. Juet, "An anonymous buyer-seller watermarking protocol with anonymity control", *Inform. Sec. Cryptol., —ICISC*. Springer, pp. 421–432, 2003.

[2] J.-G. Choi, K. Sakurai and J.-H Park, "Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party", In: *Appl. Cryptograh. Network Secur.*, pp. 265–279, 2003.

[3] M. Kuribayashy and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property", *IEEE Transact. Image Process.*, Vol. 14, pp. 2129–2139, 2005.

[4] M. William, H. Treharne and C. Cuknane, "Using a formal technique to identify an unbinding attack on a buyer-seller watermark protocol", *ACM Workshop Multimedia Secur.*, pp. 205-214, 2008.

[5] Y. Peng, C. Wang, Y. Fang and W. Li, "Anonymous watermarking protocol for vector spatial data", *Inter. Conf. Comput. Sci. Service Syst.*, pp. 2095-2098, 2012.

[6] F. Benedetto, G.Giunta and A.Neri, "A Bayesian business model for video-call billing for end-to-end Qos provision", *IEEE Transact. Vehicular Technol*., Vol. 58, pp. 836-842, 2009.

[7] F. Benedetto, G.Giunta and A.Neri, "Qos assessment of 3G video-phone calls by tracing watermarking exploiting the new colour space YST", *IET Communicat.*, Vol.1, pp. 696-704, 2007.

[8] F. Frattolillo, "Watermarking protocol for web context", *IEEE Transact. Inform. Foren. Secur*, Vol. 2, pp.350-363, 2007.

[9] L. Qiao and K. Nahrstedt. "Watermarking schemes and protocols for protecting rightful ownership and customer's rights", *J. Vis. Commun. Image Represent.*, Vol. 9, pp. 194-210, 1998.

[10] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol", *IEEE Transact. Image Process*, Vol. 10, pp. 643–649, 2001.

[11] C. L. Lei, "An efficient and anonymous buyer-seller watermarking protocol", *IEEE Transact. Image Process*., Vol. 13, pp. 1618–1626, 2004.

[12] M. Kuribayashi and H. Tanaka. "Fingerprinting protocol for images based on additive homomorphic property", *IEEE transact. on image processing*, 14(12), pp. 2129-2139, 2005.

[13] J. Zhang, W. Kou, K. Fan. "Watermarking protocol of secure verification". *Journal of electronic imaging*, 16(4), 043002-043002-4, 2007.

[14] S, Katzenbeisser, A. Lemma. "A buyer-seller watermarking protocol based on secure embedding". *IEEE Transact. Inform. Foren. Secur*, 3(4), pp.783-786, 2008.

[15] C. Fan, T. Chen and Z. Sun, "Buyer-seller watermarking protocols with off-line trusted third parties". *Inter. J. Ad Hoc Ubiquitous Comput.*, Vol. 4, pp. 36-43, 2009.

[16] N. Mehar and M.Shandilya, "Pseudonymous privacy preserving buyer-seller watermarking protocol", *Inter. J. Comput. Sci. Issues*, Vol. 8, pp. 215-219, 2011.

[17] B. Terelius, "Towards transferable watermarks in buyer-seller watermarking protocol". *IEEE Inter. Workshop Inform. Foren. Secur*., Guangzhou, China, pp. 197-202, 2013.

[18] T. Thomas, S. Emmanuel, A. Subramanyam, M. Kankanhalli, "Joint watermarking scheme for multiparty multilevel DRM architecture", *IEEE Transact. Inform. Foren. Secur*., Vol. 4, pp. 758-769, 2009.

[19] A. Rial, J. Balasch and B. Preneel. "A privacy-preserving buyer-seller watermarking protocol based on priced oblivious transfer", *IEEE Transaction. Inform. Foren. Secur*., Vol. 6, pp. 202-212. 2011.

[20] A. Kumar, P. Ghrera and V.Tyagi, "A comparison of buyer-seller watermarking protocol based on discrete cosine transform and discrete wavelet transform", *Emerging ICT for bridging the future-proceedings of the 49th annual convention of the computer society of India*, Vol. 1, pp. 401-408, 2015.

[21] R. Reeder and S.Schechter, "When the password doesn't work: secondary authentication for websites", *IEEE Security Privacy*, 9(2), pp.43-49, 2011.

[22] C. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card", *IET Inform. Secur.*, Vol. 7, pp. 3-10, 2013.

[23] W. Meng, D. Wong, S. Furnell and J. Zhou, "Surveying the development of biometric user authentication on mobile phones". *IEEE Commun. Survey Tutor*., pp. Vol. 17, pp. 1268-1293, 2015.

[24] N. Schmid, M. Ketkar, H. Singh, and B. Cukic. "Performance analysis of iris-based identification system at the matching score level". *IEEE Transact. Inform. Foren. Secur*, Vol. 1, pp.154–168, 2006.

[25] X. He, J. Yan, G. Chen and P. Shi, "Contactless auto-feedback iris capture design", *IEEE Transact. Instrument. Measure.*, Vol. 57, 2008.

[26] K. R. Park, H.-A. Park, B. J. Kang, E. C. Lee, and D. S. Jeong."A study oniris localization and recognition on mobile phones", *EURASIP journal on Advices in signal process*, vol. 2008, pp. 1-12, 2008.

[27] A. Radman, K. Jumari and N. Zainal, "Fast and reliable iris segmentation algorithm", *IET Image Process.*, Vol. 7, pp. 42-49, 2013.

[28] A. Hilal, P. Beauseroy and B. Daya, "Elastic strips normalisation model for higher iris recognition performance", *IET Biometric*., Vol. 3, pp.190-197, 2014.

Received: November 11, 2015 **Revised: April 11, 2016** **Accepted: April 13, 2016**