Multiparty Multilevel Watermarking Protocol for Digital Secondary Market based on Iris Recognition Technology

Jie Sang[1], Xiaojun Wu[1], Chunlin Song[1*], Sud Sudirman[2]

1. School of Computer Science, Jiangnan University, Wuxi, China
2. Department of Computer Science, Liverpool John Moores University, UK

sarlly2016@hotmail.com; xiaojun_wu_jnu@163.com;
songchunlin@jiangnan.edu.cn, s.sudirman@ljmu.ac.uk

Abstract: In order to design a secure digital right management architecture between different producers and different consumers, this paper proposes a multiparty and multilevel watermarking protocol for primary and secondary market. Comparing with the traditional buyer-seller watermarking protocols, this paper makes several outstanding achievements. First of all, this paper extends traditional buyer-seller two-party architecture to multiparty architecture which contains producer, multiply distributors, consumers etc. Secondly, this paper pays more attention on the security issues, for example, this paper applies iris recognition technology as an advanced security method. Finally, this paper also presents a second-hand market scheme to overcome the copyright issues, that may happen in the real world.

Keywords: second-hand market, iris recognition technology, watermarking protocol, multilevel, multiparty.

I. INTRODUCTION

With the rapid development of communication and internet technology, e-commerce products, digital media products and other digital entertainment products are in harmony with our lives and become new life styles [1]. However, new life style brings new problems, such as information security problem, copyright and authorization problem etc which have been paid more attention [2]. Under this situation, digital watermarking protocol as a potential solution integrates with encryption algorithm, digital watermarking algorithm, XML, meta-data and digital payment method [3-4]. Therefore, designing an effective and secure watermarking protocol for preventing copyright and solving security issues are very important [5-6].

For achieving the above targets, this paper proposes a multiparty and multilevel digital watermarking protocol to design a scheme for digital products in first-hand and second-hand market. Multiparty refers as producer, distributor, first-hand consumer and second-hand consumer. Multilevel refers as five sub-protocols which are listed as followed:

- Security production sub-protocol.
- Distribution rights sub-protocol.
- Transaction protection sub-protocol.
- Second-hand transaction protection sub-protocol.
- Identification and arbitration sub-protocol.

For designing an efficient and secure watermarking protocol, there are several aspects which need to be considered:

- First of all, the watermarking protocol should protect the copyright of each entity.
- Secondly, in order to avoid the watermark-overlaid problem, the joint-information watermark signal will be applied[7-8].
- The next aspect is related to security issues, in this protocol, all of the transmitted messages are encrypted through the encipher algorithm. Furthermore, the secure sockets layer (SLL) communication technology is applied in this protocol.
- Digital right management (DRM) system [9] integrates with different functions is applied in this protocol. Different entities are endowed with different permissions.
- The iris recognition technology will be used in watermarking protocol to identify different consumers.
- At last, this paper tries to apply a proposed watermarking protocol to digital secondary market under the consideration of solving digital product depreciation problems, such as the number of embedding times, ambiguity problem, transparency and capacity problem etc.

This paper is organized as follows, section II describes the background of watermarking protocol, section III introduces the innovations and preliminaries, section IV discusses the specific process of the proposed watermarking protocol, section V analyses and discusses the protocol and finally, a brief conclusion is presented.

II. RELATED WORKS

The research of watermarking protocol is developed rapidly with the increasing contradiction between supply and demand of digital copyright issues [10]. The first watermarking protocol was proposed by Memon and Wong in 2001(MW scheme), this protocol applied homomorphic public key encryption system in the watermarking protocol to protect both buyer's and seller's copyright. However, MW scheme did not solve the binding and buyer's anonymous problems [11].

In 2003, Choi proposed a digital watermarking protocol without trusted third party by applying a commutative cryptosystem structure to defense collusive attack [12]. However, this protocol did not completely solve the problem of collusion attack. After that, Chang and Chung produced a buyer-seller watermarking protocol using digital time-stamp to solve the problem of middle attack[13]. However, the protocol did not provide a solution of binding and anonymity issues.

In 2004, Lei improved the original MW scheme and proposed a novel system [14]. This scheme used disposable key to encrypt the digital content and established a contract between buyer and seller to bind both digital contents and watermark signals in the transaction process. This protocol also provided an updated version of MW scheme, to resolve consumers' rights problem, binding problems, anonymous problem etc.

In 2005, Kuribayashi and Tanaka produced a fingerprint protocol based on the homomorphic characteristic [15], this protocol improved the robustness of digital watermarking to a certain context. However, there was no specific solution to the security problem, such as conspiracy attack, binding problem and so on.

In 2006, Zhang proposed another secure buyer-seller watermarking protocol for solving the problem of collusion attack [16], but the anonymity problem was still a question. In 2007, Ibrahim proposed a practical and secure buyer-seller watermarking protocol based on Public Key Infrastructure (PKI), which applied the credible authentication center to resist collusion attack [17]. Another scheme [18] proposed by Zhang could avoid embedding multi-watermarking signals in order to enhance the robustness of the watermark.

In 2008, Katzenbeisser argued that it was not feasible to conduct cryptography calculation in the traditional seller-buyer watermarking protocol and he created a new secure-embedding seller-buyer watermarking protocol [19]. Such an approach was based on a 'secure' watermark embedding algorithm, which was implemented by using symmetric ciphers and 'partial encryption'.

In 2009, Fan proposed a buyer-seller watermarking protocol with an offline trusted third party, which can resist collusion attack [20]. In 2010, Hu proposed an effective digital watermarking protocol to generate multiple watermarks through watermark generation authentication [21]. This approach asked the buyer to select the watermark signals randomly in order to avoid collusion attack.

In 2011, Mehra and Shandilya proposed an anonymous and privacy-protected buyer-seller watermarking protocol [22], this protocol focused on buyer's anonymity and convenience. However, the protocol was also easy to suffer collusion attacks.

In 2013, Terelius proposed a second-hand watermarking protocol, which focused on the process of second-hand transactions [23]. However, the protocol hypothesized that all of the participants were fully trusted. Although the protocol solved the problem of second-hand market on digital product, but it was hard to achieve in practice.

To sum up, most of the watermarking protocols do not support multiparty architecture and second-hand market. Therefore, it is necessary to produce a more flexible and hierarchical distribution network for business model. Hence, a multiparty architecture involving multiple levels of distributors for digital secondary market needs to be considered.

III. PRELIMINARIES

A. Multiparty Multilevel DRM Architecture

The architecture of multiparty and multilevel watermarking protocol is a flexible and efficient distribution frame which faces different environments and sale systems [24]. The primary task of this scheme is to protect the digital contents and prevent piracy effectively, the overall structure is shown in **Fig.1**. As can be seen in **Fig.1**, producer, distributors, consumers and second-hand consumers are four different entities in this scheme. These four different entities take part in the transactions process to make a great contribution to accomplish multi-time sales, multi-place sales, multiparty sales, multilevel sales, piracy tracking and identity authentication. Transaction information authority (TIA) as a trusted third party which is responsible for exchanging the trading information. In addition, the direct selling license, usage license and reselling license are used in this protocol for achieving different targets, the details of these license will be described in the following context.

B. Structure of Licenses

There are three kinds of licenses which are applied in this protocol: direct selling license, usage license and reselling license. Different licenses play different roles in this protocol:

Direct selling license is issued by producer which is used for allowing distributors to sell digital contents legally. The direct selling license is also named as the trading license which specifies the sales time, sale place and sale contents.

Usage license is created by DRM systems which allows consumer and second-hand consumer to use a digital product. Moreover, if anyone who wants to use the digital product, he needs to provide the private key and public key.

Reselling license limits the number of transaction times in digital secondary market. The maximum number of transaction times are up to three according to the quality of watermarked digital

product and its corresponded economic value. The transaction times will be upgraded automatically by the DRM system.

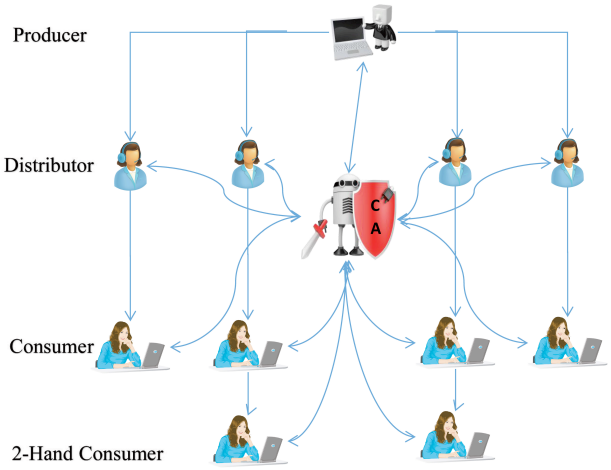


Fig.1. The communication between different entities and the certification authority in the multiparty multilevel architecture.

C. Iris Recognition Technology

Under the consideration of anonymity problem, this protocol will collect consumer's iris information to replace the traditional technology. Iris recognition technology is mainly used for identity confirmation, anonymous purchase and piracy tracking. It contains many advantages such as universality, uniqueness, stability, reliability, non-aggression, acquisition with low false acceptance rate and low false rejection rate [25]. In practice, iris recognition is usually divided into four steps: iris image acquisition, iris image pretreatment, iris feature extraction and feature recognition which is shown in **Fig.2**.

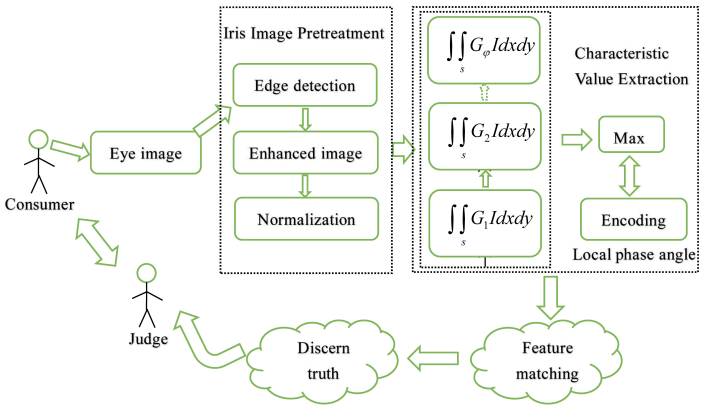


Fig.2. The flowchart of iris recognition technology operation.

- The primary task of iris recognition technology is to collect the high quality of the eye image [26]. In the tradition scheme, 6 inches camera-device is needed to collect consumer's iris information, however, in this protocol, we will apply mobile camera to collect eye image [26]. It uses infrared radiation (IR) illuminators and an IR pass filter to capture iris patterns. Cold mirror is attached to reflect light. **Fig.3** illustrates the mobile camera and its basic elements.
- The next task is iris pretreatment. In this stage, it contains three main steps which are edge detection, enhanced image and normalization. The main task of this stage is to separate iris texture

from eye image, remove the eyelid, eye-liquid and noise interference. Finally, in the end of this process, we decompose the eye image and extract the iris feature information.

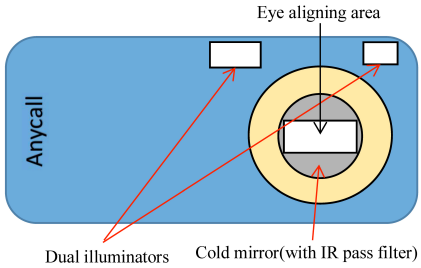


Fig.3[26]. The mobile phone used for capturing iris pattern.

- The third step is encoding. In this step, the binary code is generated by using feature extraction routine. After the encoding module, the system stores the encoding features into its related database.

In the process of feature extraction process, we encode the iris feature information using various algorithms such as 2-D complex Gabor wavelet algorithm [27], the formula is listed as (1):

$$G(x, y, f, \varphi) = \exp\left\{-\pi[(x-x_0)^2\alpha^2 + (y-y_0)^2\beta^2\right\} \exp\left\{-2\pi i f[(x-x_0)\cos\varphi + (y-y_0)\sin\varphi]\right\} \quad (1)$$

In this formula, α and β indicate the scale factor, f represents the frequency of the sinusoidal surface. ϕ is the filtering direction. By adjusting the parameters of Gabor wavelet, the local phase information can be obtained.

- Finally, the matching algorithm is used to identify two iris feature-codes.

IV. Proposed Watermarking Protocol

In this section, we introduce a multiparty, multilevel watermarking protocol based on iris recognition technology for second-hand market. The proposed protocol includes several entities which is listed in **Tab.I**, the definitions of different symbols are showed in **Tab.II** and the definitions of different functions in DRM system are listed in **Tab.III**.

TABLE I. DEFINITIONS OF SIX DIFFERENT ENTITIES

Entity	Definition
P	The producer, who creates digital products.
D	The distributor, who sales digital product to consumers.
C	The first hand consumer, who purchases a digital product from the distributor.
2-C	The second-hand consumer, who purchases a digital product from another consumer.
IA	Iris authority, a fully trusted third party, which is responsible for storing and protecting consumers' personal identity and iris information. IA stores the consumers' information unless the consumer is adjudicated to be guilty.
J	The judge, who judges lawsuits against the infringement of copyright. Only the judge has the right to require the identify information.
TIA	Transaction information authority, a trusted third party which verifies certifications, exchanges and stores the trading information from distributor, consumer and second-hand consumer.

TABLE II. DEFINITIONS OF ALL SYMBOLS

Symbol	Definition
X	The digital products, which is created by P.
L_X	The label with a unique copy number of X.
$E_{pub}(\bullet \mid K)$	The encrypted contents with a public key K.
$D_{pub}(\bullet \mid K)$	The decrypted content with a public key K.
$E_{sym}(\bullet \mid K)$	The classic encryption algorithms such as AES or 3DES.
$D_{sym}(\bullet \mid K)$	The classic decryption algorithms, corresponding to the encrypted algorithm.
$Sig(\bullet \mid K)$	The digital signature generated with public key K.
$Ver(\bullet \mid K)$	The digital signature verified with public key K.
(e_i, d_i)	The pairs of the public-private-key, i∈〈0, 4).
K_{DRM}	A secret key generated by producer, which is embedded in the DRM system.
$Cert_i$	The certificate of different entities, i is producer or distributor or consumer or second-hand consumer, the certificate makes a record of transaction information.
CS_i	The content server of different entities, i is producer or distributor or consumer or second-hand consumer.
$H(\bullet)$	A standard hash function, such as SHA1 or MD5.
$W_{gen}(\bullet \mid K)$	A standard watermarking signal generation algorithm with a public key K.
$W_{emd}(\bullet \mid K)$	A standard watermarking embedding algorithm with a public key K.
$W_{\det}(\bullet \mid K)$	A standard watermark detection algorithm with a public key K.
$W_{ext}(\bullet \mid K)$	A standard watermark extraction algorithm with a public key K.
I_i	The joint information, i is consumer or second-hand consumer.
W	The watermarking signal, which is composed of joint information.
W_P	The detection-watermarking signal generated by producer.
UL_i	The usage licenses of different entities, i is producer or distributor or consumer or second-hand consumer.
DL_P	The direct selling licenses issued by producer.
RSL_k	The reselling licenses, k is represented as the number of reselling times and the max number is up to 3.
IR_i	The iris information, i denotes as consumer or second-hand consumer.
$Identity_i$	The personal information containing name, sex etc, i is consumer or second-hand consumer.
Z_i	The encrypted trading information, i is producer or distributor or consumer or second-hand consumer.
DRM system	A digital right management system developed by producer under the supervision of TIA, which integrates several algorithms, such as security communication mechanism, encryption and decryption algorithms, watermarking generation, embedding, detection and extraction algorithm.

TABLE III. FUNCTIONS OF DRM SYSTEM IN DIFFERENT ENTITIES

Function	Entity	Detail

Encryption/decryption	Producer, distributor, consumer, second-hand consumer	For the security reasons, the trading information needs to be encrypted before communication. As the same reason, the receiver need to decrypt the encrypted information.
Watermarking generation, embedding	Producer	Producer generates the detection watermark W_P and embeds it into digital content.
	Consumer and second-hand consumer	In the trading process, consumer/second-hand consumer apply watermark generation function to generate watermark signals and embed it into digital product.
Watermarking detection	Producer	When illegal copy is found, the watermark detection algorithm is applied to detect and verify the pirate.
Watermarking extraction	Judge	When illegal copy is found, the watermark extraction algorithm is applied to extract watermark content.

The transaction starts from security production sub-protocol and the details are described below. In addition, **Fig.4** shows the transaction process of the first three sub-protocols, the security communication technology SSL is used as an addition level of protection.

A. Security production sub-Protocol.

1) P sends $Cert_P$ with public key e_P to TIA.

2) TIA verifies the validity of $Cert_P$, and aborts the transaction if it is invalid. Otherwise, TIA generates a random key k_P and sends the encrypted content $k_{P-P} = E_{pub}(k_P \mid e_P)$ to P.

3) P decrypts $k_P = D_{pub}(k_{P-P} \mid d_P)$, generates UL_P, DL_P and RSL_k. P uses k_P to encrypt them $Z_P = E_{sym}(UL_P, DL_P, RSL_k, L_X, H(X) \mid k_P)$ and sends to TIA.

4) TIA decrypts the above information $D_{sym}(Z_P \mid k_P) = (UL_P, DL_P, RSL_k, L_X, H(X))$ and verifies UL_P, DL_P, RSL_k. If everything is corrected, TIA stores $(Cert_P, UL_P, DL_P, RSL_P, L_X, H(X))$ to its database and sends the feedback to P.

5) P integrates L_X with random pseudo code to generate a specific watermark signal W_P and embeds L_X into the digital product X to get watermarked digital product X'. At last, P encrypts X' and uploads to its content server CS_P.

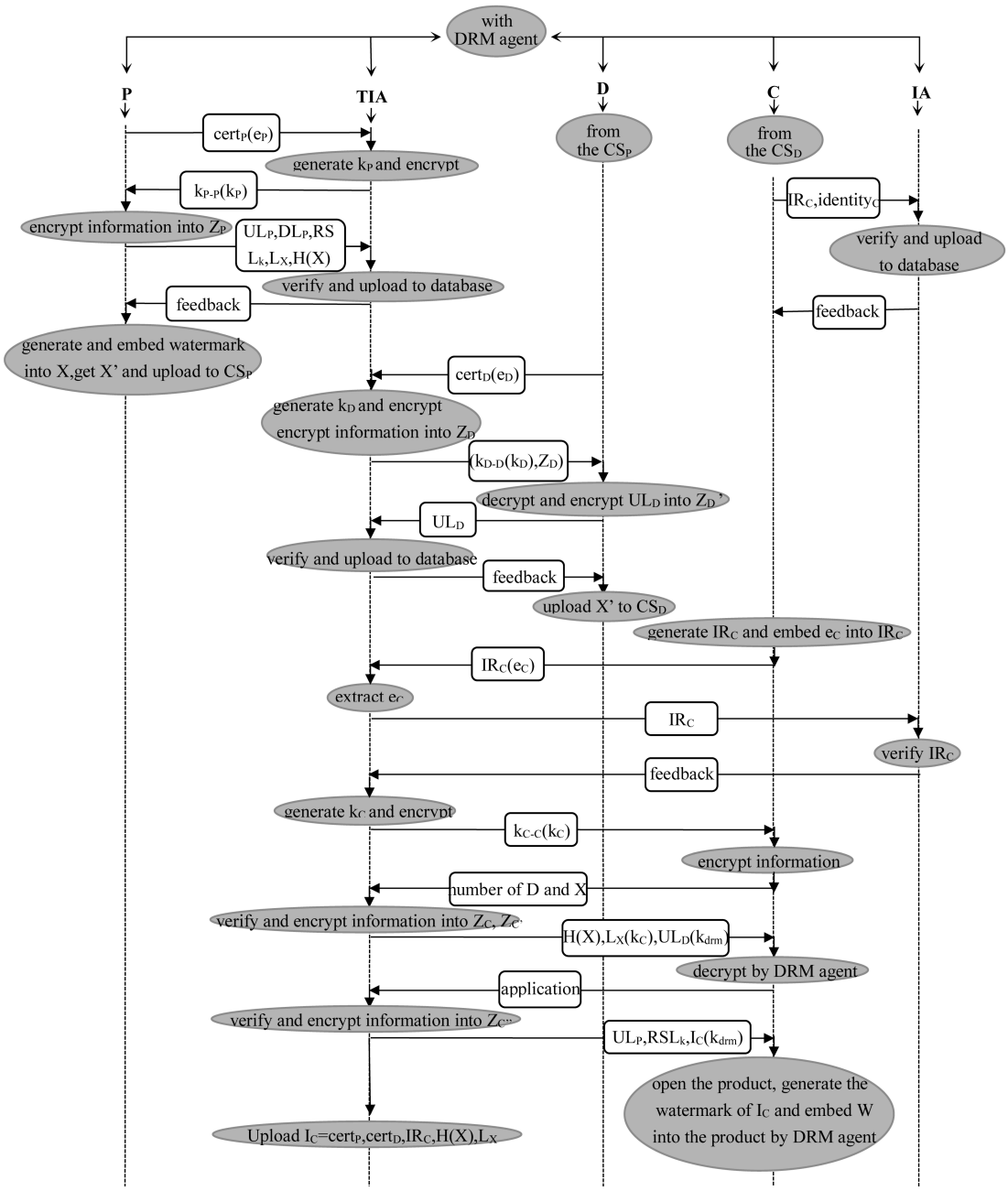


Fig.4. Details of a transaction in the first three sub-protocols.

B. Distribution rights sub-protocol.

1) D downloads the encrypted product X' from CS_P, contacts and purchases distribution-certificate $Cert_D$ with a public key e_D from P, and sends $Cert_D$ to TIA.

2) TIA verifies $Cert_D$ and extracts the public key e_D to generate a random key k_D. Then, TIA encrypts the above information to produce $k_{D-D} = E_{pub}(k_D \mid e_D)$. Next, TIA also encrypts the distribution licenses and other information $Z_D = E_{sym}(DL_P, RSL_k, H(X), L_X \mid k_D)$ and sends ($k_{D\text{-}D}$, Z_D) to D.

3) D decrypts $k_D = D_{pub}(k_{D-D} \mid d_D)$ and $D_{sym}(Z_D \mid k_D) = (DL_P, RSL_k, H(X), L_X)$, generates its

usage license in DRM system and sends the encrypted $Z_D^{'} = E_{sym}(UL_D \mid k_D)$ to TIA.

4) TIA decrypts the encrypted information $D_{sym}(Z_D^{'} \mid k_D) = (UL_D)$ and verifies the UL_D. If it is corrected, TIA uploads $(Cert_D, UL_D)$ to its database and sends feedback to D.

5) D uploads the encrypted X' to its own content server CS_D.

C. Transaction protection sub-protocol.

1) C collects and gets his own iris information IR_C though his mobile camera. Then, C sends IR_C and $Identity_C$ to IA to register personal information. IA verifies the consumer's personal information and add (IR_C, $Identity_C$) to its database. After that, IA sends a feedback to C.

2) C uses IR_C as his user-name to download the encrypted product X' from CS_D anonymously. Then, C makes a payment to D. After that, D returns a e-receipt to C. Finally, C embeds a public key e_C into IR_C to get IR_C' through DRM system and sends IR_C' to TIA.

3) TIA extracts the public key e_C from IR_C' and sends IR_C' to IA.

4) IA verifies the validity of IR_C', and aborts the transaction if it is invalid. Otherwise it sends the feedback to TIA.

5) If IR_C' is corrected, TIA generates a random key k_C and sends the encrypted $k_{C-C} = E_{pub}(k_C \mid e_C)$ to C.

6) C decrypts $k_C = D_{pub}(k_{C-C} \mid d_C)$.

7) After that, C encrypts L_X and the transaction information between D and C, and sends them to TIA.

8) TIA decrypts the information, searches its database and verifies whether there exists such a trade. If everything is correct, TIA encrypts the information separately as $Z_C = E_{sym}(H(X), L_X \mid k_C)$ and $Z_{C'} = E_{sym}(UL_D \mid k_{drm})$ and sends to C.

9) C decrypts Z_c as $D_{sym}(Z_C \mid k_C) = (H(X), L_X)$ and his DRM system applies k_{drm} to decrypt $D_{sym}(Z_{C'} \mid k_{drm}) = UL_D$. Then, C applies UL_P and RSL_k from TIA.

10) TIA receives the notification from C and it arranges the joint watermarking information, $I_C = (Cert_P, Cert_D, IR_C, H(X), L_X)$ to uploads to its database, then it encrypts UL_P, RSL_k, I_C as $Z_C = E_{sym}(UL_P, RSL_k, I_C \mid k_{drm})$ and sends to C.

11) C decrypts Z_C through DRM system as $D_{sym}(Z_C \mid k_{drm}) = (UL_P, RSL_k, I_C)$ and releases the content using UL_P, RSL_k and UL_D. DRM system utilizes the standard watermark generation algorithm $W_{gen}(I_c)$ to generate watermark signal W, and embeds W into X' through embedding algorithm W_{emd}(W, X'). Then, X' becomes the watermarked product X_1'.

D. Second-hand transaction protection sub-protocol.

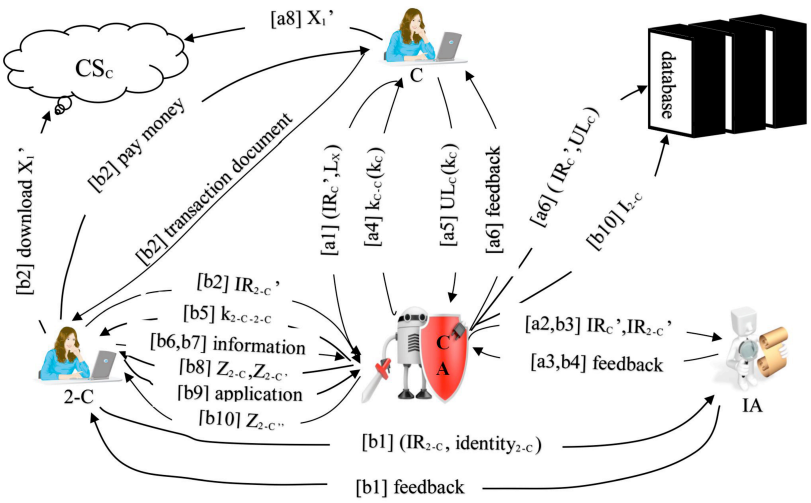


Fig.5. Details of a second-hand transaction process in the sub-protocol.

In this sub-protocol, we use iris information as the identity for each consumer, which achieves the anonymity and uniqueness of the consumer. It is worth emphasizing that the transaction information as a new watermark which is embedded into the watermarked X_1' due to the depreciation idea of the second-hand products.

This sub-protocol will be divided into two processes: consumer-releasing-products and second-hand-consumer-purchasing-products. **Fig.5** illustrates the details of this sub-protocol.

(a) Consumer-releasing-products

1) C sends L_X and IR_C' with the public key e_C to TIA.

2) TIA extracts the public key e_C from IR_C' and sends IR_C' to IA.

3) IA verifies IR_C' and sends the feedback to TIA if everything is corrected.

4) If TIA confirms IR_C', TIA searches and checks the trading information of IR_C' from the database and confirms whether the k in RSL_k is greater than 0. If k = 0, TIA notifies that the digital product cannot be traded anymore, otherwise, if k>0, TIA generates a random key k_C and sends the encrypted $k_{C-C} = E_{pub}(k_C \mid e_C)$ to C.

5) C decrypts $k_C = D_{pub}(k_{C-C} \mid d_C)$ and generates usage license UL_C, then consumer encrypts it as $Z_C = E_{sym}(UL_C \mid k_C)$ and sends to TIA.

6) TIA decrypts $D_{sym}(Z_C \mid k_C) = UL_C$ and verifies the validation of UL_C. If UL_C is corrected, TIA adds (IR_C',UL_C) to the database.

7) C encrypts X_1' and uploads to its content server CS_C.

(b) Second-hand-Consumer-Purchasing-Products

1) 2-C collects his own iris information $IR_{2\text{-}C}$ through mobile camera. 2-C sends $IR_{2\text{-}C}$ and

$Identity_{2\text{-}C}$ to IA to register personal information. IA verifies the authenticity of the information and adds ($IR_{2\text{-}C}$, $Identity_{2\text{-}C}$) to its database.

2) 2-C uses $IR_{2\text{-}C}$ as his user-name to login and download the encrypted product X_1' from CS_C anonymously. Then, 2-C makes a payment to C. C transfers a e-receipt to 2-C. C embeds the public key $e_{2\text{-}C}$ into $IR_{2\text{-}C}$ to get $IR_{2\text{-}C}$', 2-C sends to TIA.

3) TIA extracts the public key $e_{2\text{-}C}$ and sends $IR_{2\text{-}C}$' to IA.

4) IA verifies $IR_{2\text{-}C}$' and sends the feedback to TIA if it is corrected.

5) If TIA confirms that $IR_{2\text{-}C}$' is corrected, TIA generates a random key $k_{2\text{-}C}$ and sends the encrypted $k_{2-C-2-C} = E_{pub}(k_{2-C} \mid e_{2-C})$ to 2-C.

6) 2-C decrypts $k_{2-C} = D_{pub}(k_{2-C-2-C} \mid d_{2-C})$.

7) 2-C encrypts the transaction information between C and 2-C and the label of X_1', then sends to TIA.

8) TIA decrypts the information, searches in his database and verifies whether there exists such a trade. If everything is corrected, TIA encrypts the information separately as $Z_{2-C} = (H(X), L_X \mid k_{2-C})$ and $Z_{2-C'} = (UL_C \mid k_{drm})$, after that, TIA sends the encrypted information to 2-C.

9) 2-C uses $k_{2\text{-}C}$ to decrypt $Z_{2\text{-}C}$ as $D_{sym}(Z_{2-C} \mid k_{2-C}) = (H(X), L_X)$. DRM system uses k_{drm} to decrypt $Z_{2\text{-}C}$ as $D_{sym}(Z_{2-C'} \mid k_{drm}) = UL_C$. Then, 2-C applies UL_P, UL_D and RSL_k from TIA.

10) TIA verifies the validation of 2-C's application, arranges the joint watermark information including C, 2-C as $I_{2-C} = (IR_C, IR_{2-C}, H(X), L_X)$, uploads to the database. In addition, TIA decreases k to k-1, changes RSL_k into $RSL_{k\text{-}1}$, encrypts UL_P, UL_D, $RSL_{k\text{-}1}$, $I_{2\text{-}C}$ as $Z_{2-C''} = E_{sym}(UL_P, UL_D, RSL_{k-1}, I_{2-C} \mid k_{drm})$ and sends to C.

11) 2-C decrypts $Z_{2\text{-}C''}$ as $D_{sym}(Z_{2-C''} \mid k_{drm}) = (UL_P, UL_D, RSL_{k-1}, I_{2-C})$ and releases the content using UL_P, RSL_k and UL_D by DRM system. DRM system computes the watermark signal from $I_{2\text{-}C}$ using the standard watermark generation algorithm $W_{gen}(I_{2\text{-}C})$ to generate watermark signal $W_{2\text{-}C}$, and embeds that into X_1' by $W_{emd}(W_{2\text{-}C}, X_1')$. Then, X_1' becomes the watermarked product X_2'.

Commonly, there will be third-hand-consumer, four-hand-consumer and so on, who uses the protocol according to the above sub-protocol.

Throughout the sub-protocol, second-hand reselling license RSL_k restricts the number of transfer times. Meanwhile, the number of embedding times k is advised to be less than or equal to 3 due to the Muhammad Imran Khan's research [28], which will be described in detail in section V.

E. Illegal arbitration protocol

We assume that all the watermark contents have been fully inserted into the digital product X. Next, if producer has discovered a pirated product Y, which requires the following steps to track piracy:

1) P verifies that W_P is presented in Y. If the case is undertaken, the P continues the following steps; otherwise, J rejected the case.

2) P presents Y, H(X), L_X and W_P to J.

3) J checks whether the W_P is present in the Y. If it is present, proceed; else end the sub-protocol.

4) J uses the watermark detection algorithm $W_{det}(Y)$ and extraction algorithm $W_{ext}(Y)$ to extract the joint watermarking signals. If I_C is discovered, J continues to extract the $I_{2\text{-}C}$ until no watermark existing anymore.

5) J extracts the iris information from I_C or $I_{2\text{-}C}$, and compares this iris information with the one that is stored in IA.

6) Finally, J applies the personal information of C or 2-C to IA in order to find out the pirate.

In this sub-protocol, producer has the rights to determine whether the product is pirated or not, so the tracking watermark W_P is embedded by producer. Distributor could not be the traitor because D cannot get UL_P from P. Therefore, the piracy process will only be generated in the first-hand consumer or the other multi-hand consumer. In addition, the entire transaction process is carried out by DRM system, it is hard for consumers to get in touch without the keys.

V. EXPERIMENT

In this section, two experiments are carried out to prove the feasibility of our protocol, the first experiment is called iris recognition experiment and the second experiment is named as watermarking experiment under different attacks.

A. Iris recognition.

The first experiment simulates the whole process of iris recognition including iris segmentation, iris normalization, iris feature encoding and matching [29]. The iris experiment database are composed by ten groups of iris images of different person, which are collected from the iris database of Chinese Academy of Sciences Institute of Automation(CASIA)[30]. The original image is named 'S2003L03' which is showed in **Fig.6**. In addition, all experiment images are sized by 640×480.

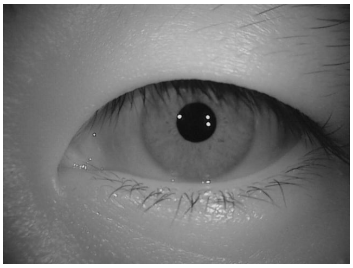
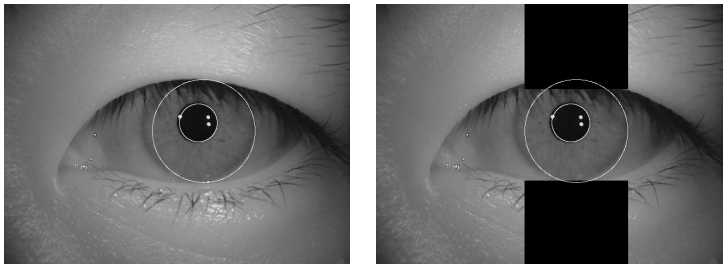


Fig.6. The original iris image

(a) Iris Segmentation.

The first step is iris segmentation which aims to isolate the iris region from a digital eye image. It is designed to apply circular Hough transform to find the boundaries of pupil and iris. In particular, a modified version of Canny algorithm [31] is applied to get an edge map and then, the circular Hough transform [32] can be employed to locate the regions of circular pupil and iris. Finally, we use eyelash detection algorithm [33] to isolate eyelash regions. The iris segmentation results can be seen in **Fig.7**. As can be seen in **Fig.7**, we can find that the regions of iris and pupil are separated successfully, which proves the segmentation step being acceptable to be applied.

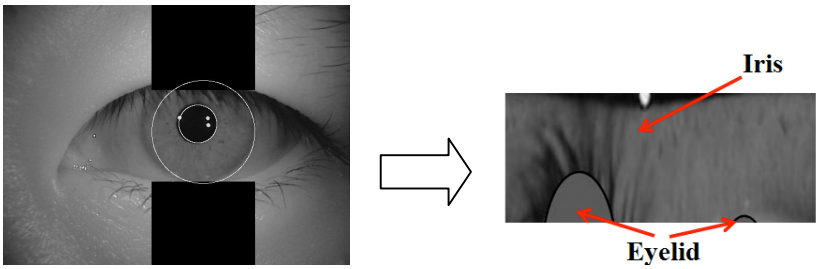


(a) (b)

Fig.7. The segmentation result of iris image named 'S2003L01': (a) The original iris image after segmentation; (b) The segmented iris image after eyelash detection technique.

(b) Normalization.

After the progress of segmentation step, the next stage is called normalization. This step transforms the iris region into a fixed dimension for comparing different iris information before the final stage. In this step, the Daugman's rubber sheet model [34] is applied to achieve the new iris region as a uniformed dimension. The experiment results are showed in **Fig.8**. As can be seen in **Fig.8**, the segmented iris region is re-scaled into a constant dimension successfully, the region of iris and eyelid are separated effectively.

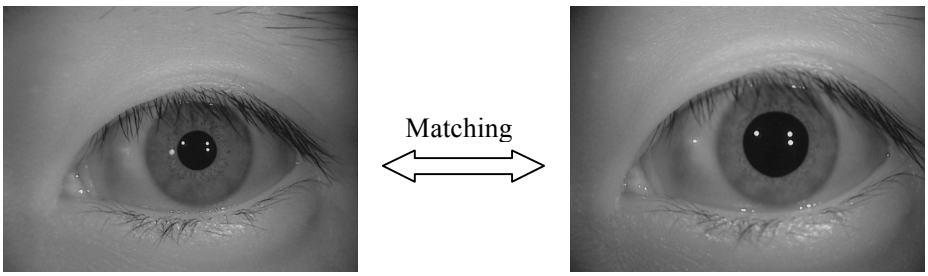


(a) (b)

Fig.8. The normalization result of iris image: (a) The segmented iris image; (b) The normalized iris result.

(c) Feature encoding and matching.

Once the iris images have the same dimension, the features are extracted to encode. In this step, we employ 1D Log-Gabor wavelets to encode the iris region [35] which transfers the 2D normalized pattern to 1D signal.



(a) (b)

Fig.9. The two iris images from the same person (a) the original iris image; (b) the tested iris image

The final stage is matching, in this step, the Hamming distance [36] is calculated to measure how many bits are similar between two different iris patterns. The value of Hamming distance is close to 0, the more similar of two iris images are. **Fig.9** compares two iris images and the result indicates that the two iris images from the same person.

From a series of experiments described in this section, we can conclude that the iris recognition technology can solve the anonymous problem and it will be applied in the proposed watermarking protocol.

B. Applied watermarking algorithm

The proposed watermarking protocol could apply any embedding and extraction watermarking algorithms. Meanwhile, the protocol is also suitable for most of the digital products such as digital videos, digital audios, digital images or digital games etc. For testing the robustness of the proposed protocol, in this experiment, we applied the DCT-DWT watermarking technique to digital videos. The host digital video is called 'tempete.yuv'. **Fig.10** is the first frame of the original video. In addition, there are another two different watermark contents shown in **Fig.11 which is** represented the first watermark signal and the second watermark signal.

Fig.10. The first frame of the original video.

(a) (b)

Fig.11. (a)The first watermark signal; (b) The second watermark signal.

(a) Watermark embedding and extraction.

For measuring the quality between original video frame and watermarked video frame, the peak signal to noise ratio(PSNR) is applied. The formula of PSNR is presented as below:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \tag{6}$$

MSE is mean square error and its formula is shown in (7):

$$MSE = \frac{1}{MN}\sum_{m,n}(W_{m,n} - W'_{m,n})^2 \tag{7}$$

In addition, the normalized correlation(NC) is used to compare the similarity between the extracted watermark image and original watermark image. The formula of NC is shown in (8):

$$NC = \frac{\sum_{i=1}^{i=M} \sum_{j=1}^{j=M} W(i,j)W'(i,j)}{\sum_{i=1}^{i=M} \sum_{j=1}^{j=M} W(i,j)^2} \tag{8}$$

If the PSNR is greater than 30, it means the watermarked content is close to original content. Furthermore, if the NC value is close to 1, it represents the extracted watermark is similar to the original one. The experiment result is shown in **Fig.12** and **Tab.IV**. The first watermark will insert into the original host frame and the second watermark will insert into the first watermarked video frame.

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

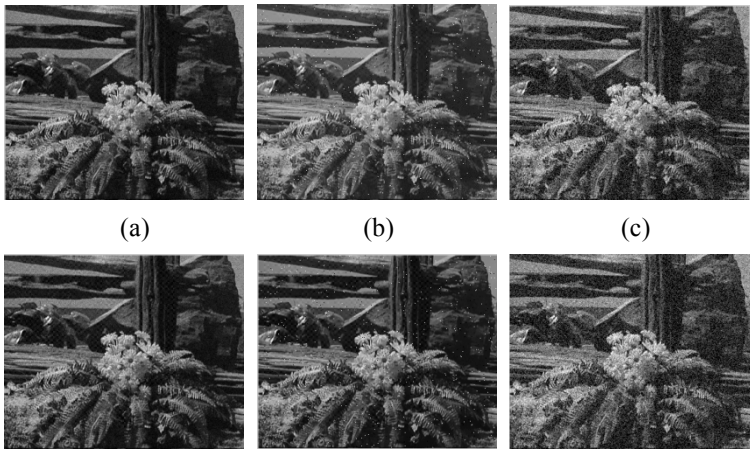
Fig.12. (a) The first watermarked video; (b) The second watermarked video; (c) The first watermark signal; (d) The second watermark signal.

TABLE.IV THE PSNR AND NC VALUES BETWEEN THE ORIGINAL CONTENT AND WATERMARKED CONTENT INTHE FIRST-HAND MARKET AND SECOND-HAND MARKET

Category	**The Watermarking Progress for First Hand Market**	**The Watermarking Progress for Second Hand Market**
PSNR	44.2176	37.6334
NC	0.9568	0.9919

(b) Watermark attacks.

In addition, for testing the robustness of the watermarking algorithm, several watermark attacks are applied. The testing results are shown in **Tab.V**, **Fig.13** and **Fig.14**.



(a) (b) (c)

(d) (e) (f)

Fig.13. Watermarked video under different attack: (a) and (d) is first and second watermarked content under Poisson Filter; (b) and (e) is first and second watermarked content under Salt-Pepper

Filter(0.02); (c) and (f) is first and second watermarked content under Gaussian Filter(0.05).

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

Fig.14. The extracted watermark under different attack: (a) and (d) is first and second extracted watermark under Poisson Filter; (b) and (e) is first and second extracted watermark under Salt-Pepper Filter(0.02); (c) and (f) is first and second extracted watermark under Gaussian Filter(0.05).

TABLE.V THE PSNR AND NC VALUES OF WATERMARKED VIDEO UNDER ATTACKS

Watermark Attack	**The Watermarking Progress for First Hand Market**		**The Watermarking Progress for Second Hand Market**	
	PSNR	NC	PSNR	NC
Poisson Filter	33.2257	0.9248	32.6149	0.9541
Salt-Pepper Filter(0.02)	41.1492	0.8908	36.8109	0.9078
Gaussian Filter(0.05)	31.4400	0.8068	31.3645	0.8110
Cutting frames(5)	42.6009	0.8984	36.5512	0.8985
Cutting frames(10)	41.0479	0.8390	35.5284	0.7851

From **Tab.IV**, we can find out that the PSNR value in the second-hand market process is lower than the first-hand market. This represents that the more watermark embedded, the poorer quality of the digital video is. Furthermore, the NC values between the extracted watermark content and original watermark content in the first and second hand market are both exceeded 0.9500 which is shown in Table IV, it means that both of the extracted watermarks are similar to the original content. From the results in **TABLE.V** and **Fig.13&14**, we can find that the PSNR values in the second watermarked content are lower than the first watermarked content after different watermark attacks, and the result of the NC value in the latter is better than the former one, this indicates that the first watermark content suffers from not only removal attack, but also ‘ambiguity attack’. The results are suitable to realities in the second-hand market, which proves the proposed protocol is reasonable.

VI. ANALYSIS

This section analyses the innovations, characteristics, security issues and achievements of this proposed protocol. First of all, the iris recognition technology is applied in this scheme to replace the traditional consumer's personal identification system, which is in order to solve the security and anonymous problem. It achieves the target of anonymity because the entities cannot recognize the iris information without the help of IA. In addition, the scheme requires IA to be a trusted third authority to store and protect consumers' information, including identity information and iris information. TIA could validate the certificates, transfer trading information and store trading information. This can effectively avoid the collusion attacks because the trading information and identity information are stored in two different trusted authorities. If the personal information and the trading information are stored in the same authority, it may suffer from collusion attacks because the authority will get to know who you are and what you buy. Moreover, the iris information is collected and managed by mobile phone, which is benefited for the consumers. It makes the protocol reality.

Secondly, it creates a watermark protocol for second-hand market and proposes the solution in

detail. The RSL_k restricts number of the trading times in second-hand market which protects the producer's and distributors' prohibits. The number of trading times is set to 3 because embedding three watermark signals would cause 2.97% degradation of digital product. Moreover, embedding more than three watermark signals would degrade over 17% on the quality of digital product [28]. Next, comparing with the traditional buyer-seller watermarking protocol, this protocol proposes another 2 entities: distributors and second-hand consumer. These new entities constitute the multiparty and multilevel watermarking protocol for digital secondary market. In real life, the quality of second-hand products will be worse than the original one. Therefore, in the digital second-hand market, we need to decrease the quality of the second-hand products, which aims to protect the producers' and distributors' prohibits The digital watermarking technology as one of the best solutions achieves these purposes, it does not only protect the copyrights of different entities, but also decrease the quality of the digital product. Finally, there are four different entities and two authorities involved in the protocol and all the communications are conducted by content server.

In the first hand trading process, the joint watermark content is embedded into digital product. Moreover, once a second-hand trading occurs, a new joint watermarking information will be embedded into the digital product.

DRM system in this protocol helps different entities to transfer the trading information, which makes a great contribution to different parties' securities. The DRM system is developed by producer and supervised by TIA. Consumer and second-hand consumer download the DRM systems from producer's content server. Therefore, DRM system plays a very important role in this protocol and different entities have different functions, which is aimed to achieve different goals. The functions of DRM system in different entities are listed in **Tab.III**. Although DRM system is developed by producer, producer would not collude with distributor, consumer or second-hand consumer, because producer would not take part in any transactions with them. Consumer and second-hand consumer do not have any opportunity to interfere in the process of tracking and copying the product X, because they can only download the encrypted X. At least, if the consumer and second-hand consumer get the secret keys of the encrypted X, they also need UL_P and UL_D to use the product. Finally, TIA could inspect all the DRM functions before the system is put in use.

The delivery process of digital product X is secure because the crypto-system and the security communication channel SSL are used in the whole process. First of all, producer and distributor encrypt digital product X before uploading to their content server. Secondly, in the second-hand market, consumer or second-hand consumer also encrypt X and upload to their content server, which force the next consumer to make a payment.

TIA is a trusted third party who runs through the whole trading process in the protocol. TIA is an important entity in this protocol to ensure the colluding behavior not occurring. TIA should verify and store the trading information. When any piracy copy is found, the information stored in TIA as the key evidence to determine the traitor. IA is a trusted third party who keeps the consumer's identity and iris information. Therefore, IA does not have any chances to collude with consumer or second-hand consumer, because IA does not know the trading information in detail. In other words, IA does not have any idea about the trading information, including which digital product the consumer buys. The responsibility of IA is storing and protecting consumer's information in detail.

From the viewpoint of producer, the proposed protocol is secure. Distributor, consumer and second-hand consumer could not access the unprotected digital product X. Moreover, distributors sell digital products without producer's usage license UL_P and keys. Consumer leaves the trading

information in TIA and identity information in IA.

Distributor stands in a same camp with producer, because distributor's sale rights will be protected when distributor keeps the power of distributing. Producer cannot frame distributor because distributor cannot decrypt the encrypted X.

Consumer and second-hand consumer could not know each other because they use iris information as their nickname. IA would not let anybody know about the consumers' information only when producer find the pirate copy. Furthermore, the most important sub-protocol in the proposed protocol is the second-hand transaction of digital product between consumer and second-hand consumer. The trading information is kept in TIA. In each second-hand transaction, the protocol will generate a new joint watermark signal and embed that into X. This step is necessary for the illegal arbitration.

All of the entities get their cryptographic credentials from the upper-level entity. SHA-1 is chosen as the one-way hash function for encrypting. The DRM system generates the watermark signals from the joint-information watermarking contents and inserts that into digital product. In addition, the watermark detection and extraction process is applied if the pirate copy is found, thus, the watermark generation, watermark embedding, extraction and detection are all arranged.

At last, the proposed protocol contains the following characteristics:

- Confidential data is managed by DRM systems and stored in two independent trusted authorities: TIA and IA.
- SLL technology is used to achieve the secure communication between different entities. In addition, communications between the entities are authenticated and encrypted.
- The whole transactions are divided into several steps and the trading information is encrypted/decrypted through different entities, which effectively prevents the "replay" attack.
- Consumer communicates with TIA by DRM system. The watermark signals are generated and embedded by DRM system.
- The second-hand consumer downloads the second-hand digital product from consumer's content server and their trading information needs another watermark.
- It is impossible for any entities to be a traitor because every step is under the supervision of TIA.

VII. CONCLUSION

In recent years, the multiparty and multilevel digital watermarking protocol has become a hot research topic due to the complex business model. In this paper, we propose a multiparty and multilevel watermarking protocol for digital second-hand market based on iris recognition technology. The protocol is composed by five sub-protocols including security production sub-protocol, distribution rights sub-protocol, transaction protection sub-protocol, second-hand transaction protection sub-protocol and identification and arbitration sub-protocol, and different sub-protocols have different functions between different entities. This protocol solves a number of problems such as pirate tracing problem, consumers' rights problem, consumers' anonymous problems, collusion attacks problem and so on. In addition, the iris recognition technology as a creatively mechanism is proposed. we also design a second-hand trading sub-protocol of digital product, which makes the whole business model more reliable. Finally, all of the transacted information is encrypted through different entities and TIA, which improves the security of the whole protocol.

In the future, the bio-technology is more and more considered to apply in the field to solve remuneration problems , multiple goods problems etc.

ACKNOWLEDGEMENTS

The work was sponsored by Jiangnan University of Science & Technology Young Scholar Grant (No.JUSRP11462), National Natural Science Foundation of China (No. 61305017)

REFERENCE

[1] B. Terelius. Towards transferable watermarks in buyer-seller watermarking protocols. 2013 IEEE International Workshop on Information Forensics and Security (WIFS). 197-202, 2013.

[2] A. Rial,J. Balasch,B. Preneel. A privacy-preserving buyer–seller watermarking protocol based on priced oblivious transfer. IEEE Transactions on Information Forensics and Security, 6(1),202-212, 2011.

[3] I. Cox,J. Bloom,M. Miller. Digital watermarking: principles & practice, 1558607145, San Francisco: Morgan Kaufman, 2002.

[4] A. Sachan, S. Emmanuel, A. Das, M. S. Kankanhalli. Privacy preserving multiparty multilevel DRM architecture. Networking Conference on Consumer Communications. 1-5, 2009.

[5] F. Franco. Watermarking protocols: problems, challenges and a possible solution. The Computer Journal, bxu015, 944-960, 2014.

[6] R. Naskar,A. Raju, R. S. Chakraborty. A single pass, high throughput reversible watermarking scheme for audio based on redundant embedding. 2013 International Conference on Signal Processing and Communication (ICSC).303-308, 2013 .

[7] J. W.Lee, T. W.Oh, M. J.Lee, H. K.Lee, H. Y.Lee. Video watermarking on overlay layer. 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). 85-88, 2011.

[8] V. Mehan,R. Dhir, Y. S. Brar. Joint watermarking and fingerprinting approach for colored digital images in double DCT domain. 2013 IEEE International Conference on Signal Processing& Computing and Control (ISPCC).1-6, 2013.

[9] M.Feng and B. Zhu. A DRM system protecting consumer privacy. 2008 IEEE Conference on Consumer Communications and Networking. Las Vegas, 1075-1079, 2008.

[10] A. Piva, F. Bartolini, M. Barni. Managing copyright in open networks. IEEE Transactions on Internet Computing,6(3), 18-26, 2002.

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

[12] J. G. Choi, K. Sakurai, J. H. Park. Does it need trusted third party? Design of buyer-seller watermarking protocol without trusted third party. Springer Berlin Heidelberg on applied cryptography and network security. 265-279, 2003.

[13] C. C. Chang, C. Y.Chung. An enhanced buyer seller watermarking protocol.2003 International Conference on Communication Technology Proceedings.2(9-11), 1779-1783, 2003.

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

[15] M. Kuribayashi, H. Tanaka. Fingerprinting protocol for images based on additive homomorphic property. IEEE Transactions on Image Processing, 14(12), 2129-2139, 2005.

[16] J. Zhang,W. Kou, K. Fan. Secure buyer-seller watermarking protocol. IEEE Proceedings

on Information Security, 153(1),15-18, 2006.
[17] I.M.Ibrahim, S.H.N.El-Din, S.H.N. Hegazy. An effective and secure buyer-seller watermarking protocol. 2007 Third International Symposium on Information Assurance and Security. 21-28, 2007.
[18] J. Zhang, W. Kou, K. Fan, L.Ye. Watermarking protocol of secure verification. Journal of Electronic Imaging, 16(4), 043002-1-043002, 2007.
[19] S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, M. Maas. A buyer–seller watermarking protocol based on secure embedding. IEEE Transactions on Information Forensics and Security, 3(4), 783-786, 2008.
[20] C. I. Fan, M. T. Chen, W. Z. Sun. Buyer-seller watermarking protocols with off-line trusted parties.2007 International Conference on Multimedia and Ubiquitous Engineering, 1035-1040, 2007.
[21] Y. Hu, J. Zhang. A secure and efficient buyer-seller watermarking protocol. Journal of Multimedia, 4(3), 161-168, 2009.
[22] N. Mehra, M. Shandilya. Pseudonymous privacy preserving buyer-seller watermarking protocol. International journal of computer science issues,8(3), 215-219, 2009.
[23] B. Terelius. Towards transferable watermarks in buyer-seller watermarking protocols. 2013 IEEE International Workshop on Information Forensics and Security (WIFS). 197-202, 2013.
[24] T. Thomas, S. Emmanuel, A. V. Subramanyam, M. S. Kankanhalli. Joint watermarking scheme for multiparty multilevel DRM architecture. IEEE Transactions on Information Forensics and Security, 4(4), 758-767, 2009.
[25] A. Hematian, A. A. Manaf, S. Chuprat,R. Khaleghparast, S. Yazdani. Field programmable gate array system for real-time IRIS recognition. 2012 IEEE Conference on Open Systems (ICOS), 1-6, 2012.
[26] K. R. Park, H. A. Park, B. J. Kang, E. C. Lee, D. S. Jeong. A study on iris localization and recognition on mobile phones. EURASIP Journal on Advances in Signal Process. 1-12, 2008.
[27] R. Raghavendra, K. B. Raja, C. Busch. Exploring the usefulness of light field camera for biometrics: An empirical study on face and iris recognition. IEEE Transactions on Information Forensics and Security, 99,1-1.
[28] M.I. Khan, V. Jeoti, A. S. Malik, et al. A joint watermarking and encryption scheme for DCT based codecs. 17th Asia-Pacific IEEE Conference on Communications (APCC), 816-820, 2011.
[29] L. Masek. Recognition of human iris patterns for biometric identification. The University of Western Australia, 2,2003.
[30] Chinese Academy of Sciences Institute of Automation. CASIA Iris Image Database Version 4.0. http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris, 2010.
[31] P. Kovesi. MATLAB functions for computer vision and image analysis. Available at: http://www.cs.uwa.edu.au/~pk/Research/MatlabFns/index.html
[32] M. Rizon, Y. Haniza, S. Puteh, et al. Object detection using circular hough transform. 2005.
[33] B. J. Kang, K. R. Park. A robust eyelash detection based on iris focus assessment. Pattern Recognition Letters, 28(13): 1630-1639, 2007.
[34] S. Sanderson, J. Erbetta. Authentication for secure environments based on iris scanning technology. IEEE Colloquium on Visual Biometrics, 2000.
[35] D. Field. Relations between the statistics of natural images and the response properties of cortical cells. Journal of the Optical Society of America, 1987.
[36] H. Yang, Y. Wang. A LBP-based face recognition method with hamming distance constraint. 2007 IEEE Conference on Image and Graphics, 645-649, 2007.