A lightweight and anonymous copyright-protection protocol

Tzung-Her Chen a,⁎, Gwoboa Horng b

a Department of Computer Science and Information Engineering, National Chiayi University, 300 University Rd., Chia-Yi City, Taiwan 600, ROC
b Department of Computer Science, National Chung-Hsing University, Taiwan, ROC

Received 15 November 2005; accepted 25 March 2006
Available online 30 May 2006

Abstract

Gradually, copyright-protection protocols have attracted much attention in that they provide effective copyright protection mechanisms. Asymmetric copyright-protection protocols allow the buyer to know and possess the protected content yet the seller has no idea about it. Subsequently, if an illegal copy is found, the seller can identify the buyer by cooperating with a trusted third party. Most copyright-protection protocols adopt public-key cryptosystems to achieve asymmetry. However, both encryption and decryption of multimedia based on public-key cryptosystems have the drawbacks of requiring high computational complexity and suffering from the burden of maintaining Public Key Infrastructure. Hence, enhancement and further development of these protocols are both necessary and central to the development of future e-commerce. In this paper, a lightweight copyright-protection protocol, benefiting from combining secret-key cryptosystems and a tamper-resistant device, is proposed to provide not only asymmetry of the protocol but also transaction anonymity of the buyer. Since the tamper-resistant device, generally speaking, provides a higher security level and is more and more commonly used, the schemes based on a tamper-resistant device are more practical than before. Moreover, the proposed protocol is computationally efficient and the key management is simple.

© 2006 Elsevier B.V. All rights reserved.

Keywords: Anonymous; Asymmetry; Copyright-protection protocol; Watermarking; Fingerprinting; Tamper-resistant machine

1. Introduction

Copyright protection, aimed to encourage the creator of contents to promote the societal and cultural evolution, has been a well-known policy for several centuries now. Due to the rapid growth of broadband networks, distribution of digital contents, such as online video, audio and e-books, over the Internet is a must way to go. Digital content is easier and faster to be duplicated, modified and redistributed than before. Hence, digital content protection has become one of the most important and urgent issues.

Traitor tracing is a cryptographic system which can be used to trace an adversary for illegal redistribution by tracking the individual decryption key [1,2]. When a pirate decoder is confiscated, the pirate decryption key is exposed. Therefore, the content provider can identify the traitor and thus the traitor is found guilty. The major drawback is that once the decoder decrypts and outputs the decrypted contents in the customer end, the customer is able to duplicate and redistribute the contents without being identified. This implies that traitor tracing schemes lack the capability of copyright protection.

Recently, digital watermarking techniques, a complement to cryptography, are growing at an exponential rate. Watermarking based on steganographic systems can embed information directly into digital contents. Basically, there are two classes of robust digital watermarking: copyright watermarking and fingerprint watermarking.

Copyright watermarking embeds an identical copyright message, so-called watermark, which indicates the owner’s or creator’s identification, into each copy of the digital content. Copyright watermarking is used to declare the copyright. Therefore, this technique cannot be used to trace the person who distributes illegal copies.

Fingerprint watermarking (also called fingerprinting) embeds a unique fingerprint message, so-called fingerprint, into an individual copy. Therefore, it can be used to track illegal customers. It’s noteworthy that fingerprinting can be quite expensive in order to resist collusion attacks. Nevertheless there are researches that claimed to have successfully addressed collusion attacks [3]. Furthermore, the essential challenge of both
copyright watermarking and fingerprinting is that robustness to
digital watermarking is still an open problem.

Most fingerprinting schemes suffer from that there is no
lawful basis for content suppliers to sue the illegal customers. This
is because almost all proposed fingerprinting schemes assume
that the owners themselves, who embed fingerprints into
digital contents, are trustworthy. Unfortunately, this is not al-
ways true. Because both the seller and the buyer know the same
fingerprinted content, there is no way, from the technical aspect,
to distinguish who actually distributes the fingerprinted copy
illegally. That is, they fail in solving the dispute of copyright
protection. Therefore, copyright watermarking or fingerprint
watermarking alone is not sufficient to resolve the rightful
copyright of the digital content.

Thus, a copyright-protection protocol relying on the well-
deﬁned cryptographic tools is necessary. From the application
point of view, copyright-protection protocols could be further
classified as follows:

1. Symmetry: The seller knows the embedded fingerprint which
is uniquely linked with the buyer. That is, the seller knows the
protected contents sold to the buyer. Therefore, the judge
cannot determine who is guilty of illegal distribution due to
ambiguity.

2. Asymmetry: In an asymmetric copyright-protection protocol,
only the buyer knows and possesses the protected content.
Subsequently, if an illegal copy found by the seller, the seller
can identify the buyer and prove to the judge that the buyer is
guilty for illegal distribution.

3. Anonymous asymmetry: Other than having the advantage of
asymmetric schemes, an anonymous scheme can further
guarantee the buyer’s privacy. Nevertheless if his subsequent
illegal distribution is found then his identity will be revealed
according to the clue embedded in the distributed copy.

In 1998, Qian and Nahristedt [4] proposed an owner–custom-
er copyright-protection protocol. In their scheme, the owner or
seller still possesses the exact protected copy that the buyer
received. Hence, the buyer can still claim that the found unau-
thorized copy is distributed by the owner or the seller. Memon
and Wong [5] proposed an asymmetric buyer–seller copyright-
protection protocol in which the seller does not know the exact
protected copy that the buyer received. Unfortunately, as pointed
out in [6] the Memon–Wong scheme suffers from unbinding
problems, failing to provide the mechanism on binding a chosen
watermark to a speciﬁc digital content or a speciﬁc transaction.
Thus, when the seller ﬁnds a pirated copy, it is possible for the
seller to transplant the watermarks embedded in the pirated copy
into another copy of a higher-priced content to form piracy in
such a way he/she illegally proﬁts more. With the anonymity of
the buyer in addition, Lei et al., not only provide a ﬁx to the
Memon–Wong scheme but also form a new one. Inspired by [5],
Chen et al. recently proposed an anonymous buyer–reseller
watermarking protocol to address the digital contents redistrib-
ution in the second-hand markets [7]. Tomsich and Katzen-
beisser also proposed another asymmetric copyright-protection
protocol using a trusted tamper-proof hardware [8].

Unfortunately, the major common drawback of [4–8] is
that encryption or decryption of the whole content based on a
public-key cryptosystem gives rise to the drawback of high
computation complexity. Moreover, since each entity including
the seller and the buyer owns a pair of keys, a private key and a
corresponding public key, their schemes suffer from the expe-
sive complexity of public-key infrastructure (PKI) [9].

It’s worthwhile to note that in the ﬁeld of security more and
more researches show that tamper-resistant machine (hereafter
TRM for short) hardware provides higher security level than
software technique [8,10]. TRM has been studied for many
years and used in realistic applications, such as Cable TV box,
DVD and applications with smart cards, etc.

Since tamper-resistant hardware is claimed to be the most
obvious solution to the digital rights management (DRM) prob-
lem [10], how to beneﬁt from combining a copyright-protection
protocol with TRM with low overhead is the main focus of this
chapter. An anonymous and asymmetric copyright-protection
protocol will be proposed. The protected content received from
the seller contains both a watermark, indicating the copyright,
and a ﬁngerprint, indicating the unique serial number of the
TRM which is registered to a trusted registration authority and
bound to the individual buyer. Cooperating with a trusted third
party, the identity of the buyer with the TRM will be revealed
and accused of his illegal redistribution.

With asymmetry, the seller has no idea about any sold ﬁn-
gerprinted content associated with the buyer. Hence, the seller
cannot proﬁt from reselling the content sold to the buyer and
subsequently accuse the buyer of illegal redistribution.
On the other hand, the buyer has no excuse to deny his illegal
redistribution.

Furthermore, the proposed protocol enables anonymous
transactions between a buyer and a seller in order to further
protect the privacy of the buyer. Compared with [4–8], en-
encrypting or decrypting the content with secret-key cryptosys-
tems [9] clearly makes the proposed protocol efﬁcient. Since the
tamper-resistant device, generally speaking, provides a higher
security level and is more and more common, the scheme is more
practical than before. Moreover, the burden of maintaining PKI
is removed, i.e., the key management is simple.

The rest of this paper is organized as follows. The proposed
protocol is described in the next section. Security analysis and
further discussions are given in Sections 3 and 4, respectively.
Finally, conclusions are presented in Section 5.

2. The proposed new copyright protection protocol

2.1. Framework and deﬁnitions

In this section, the infrastructure of the proposed anonymous
and asymmetric protocol for copyright protection is defined.
For simplicity, a scenario with the following participants is
defined:

1. Tamper-Resistant Machine (TRM): The TRM conducts de-
encryption and determines a ﬁngerprinted content in which the
embedded ﬁngerprint message indicates the serial number of
the TRM. The content is fingerprinted before outputting from the TRM.

2. Registration Authority (RA): The trusted third party with a public-key pair provides the registration service of the TRM for a special buyer and keeps the information associated with the identity of the buyer and his TRM. Aside from this, RA is also involved in the illegality tracing phase to prove the dishonesty of the buyer by revealing the buyer’s identity.

3. Seller (S): The seller sells copyright-protected contents and is equipped with the capability of robustly embedding messages into his contents.

4. Buyer (B): Each buyer equipped with a TRM must first register his TRM to RA.

Both the seller and the buyer are completely untrusted participants who might profit from reselling the protected content and illegally redistributing the content he has bought, respectively.

We will assume the existence of a robust embedding function involved in both a copyright watermarking scheme [11] and a fingerprinting scheme resistant against c-collusion attacks [3]. Therefore, there are some functional definitions below.

**Definition 1.** An embedding scheme includes two functions: an embedding function \( \hat{X} = W(k, X, w) \) and an extracting function, \( w' = \hat{W}^{-1}(k, Y) \) where

- \( k \): an embedding and extracting secret key derived from the seller’s long-term secret key;
- \( X, \hat{X}, Y \): the original content, the protected content, and the test content; and
- \( w = \{w_i|w_i \in [0,1]^m, i=1,\ldots, n\} \).

**Definition 2.** The similarity of two objects is a Boolean function, \( \text{sim}(\cdot, \cdot) \). More precisely, \( \text{sim}(\text{msg}, \text{msg}') = \text{YES} \) means that the original message \( \text{msg} \) is still so close to the extracted message \( \text{msg}' \) from a redistributed illegal copy that the seller wants to identify the original buyer.

For example, the “Normalized Correlation”, denoted as NC, is usually used to evaluate the quality between the original watermark and the extracted watermark with the size \( HW_0 * W_h \). Here \( \text{sim}(\cdot, \cdot) \) is defined as

\[
\text{sim}(w, w') = \begin{cases} 
\text{yes, if NC}(w, w') > \text{threshold} \\
\text{no, otherwise}
\end{cases}
\]

where threshold is a pre-defined threshold value and

\[
\text{NC}(w, w') = \sum_{i=0}^{W_h-1} \sum_{j=0}^{W_w-1} w_{i,j} \cdot w'_{i,j}
\]

\[
\text{NC}(w, w') = \frac{\sum_{i=0}^{W_h-1} \sum_{j=0}^{W_w-1} w_{i,j} \cdot w'_{i,j}}{\sum_{i=0}^{W_h-1} \sum_{j=0}^{W_w-1} (w_{i,j})^2}
\]

**Definition 3.** A robust copyright watermarking scheme, based on an embedding scheme with robustness, is the method resisting against attacks, intending to remove the embedded watermark, including common image processing and geometric distortion under the base line of still keeping the commercial values of the digital contents. More precisely, under reasonable distortion, \( \text{sim}(\cdot, \cdot) \) still returns yes if the tested version has the exact watermark in it.

To trace an illegal distributor, the design of a serial number of TRM is not trivial by assigning a unique binary sequence chosen at random and keeping hidden from users. On the contrary, a well-designed anti-collusion fingerprinting code [3] should be adopted into the proposed protocol. To this end, an assumption and a definition of a fingerprint code generator should be clear.

**Definition 4.** A c-collusion-secure fingerprinting scheme is a method resisting a collusion of c buyers. That is, even if up to c colluding buyers aim to fail the valid detection of embedded fingerprinting by mixing their bought protected contents from the same content, the scheme should enable the seller to find at least one of c buyers. Furthermore, a fingerprint watermarking scheme is composed of how to determine a unique fingerprint code (will be defined later) for an intended buyer and an embedding scheme with robustness.

2.2. The proposed protocol

Our copyright-protection protocol can be divided into four phases: (1) Registration, (2) Initialization, (3) Transaction, and (4) Illegality Tracing.

2.2.1. Registration

In the beginning, the registration authority RA must generate a series of fingerprint codes according to a sophisticated fingerprint code generation method (FCGM) which is inspired of the most cited [3] here. Before describing FCGM, A so-called marking assumption must be made.

**Assumption 1.** Taking collusion into account, users in a coalition can detect a specific mark, a position in the protected content, if it differs between their copies; otherwise, a mark will not be detected. On the other hand, the marks should satisfy the condition that users cannot change the state of an undetected mark without rendering the content useless. However, it is considered possible for a coalition to change a detectable mark to any state.

It’s critical for RA to construct a well-designed a fingerprint code as a sequence number of TRM. The construction of c-secure fingerprint code is divided into two phases: a base-codebook construction and a combination-codebook construction.

2.2.1.1. Base-codebook construction. The first stage is intended to construction a primitive codebook \( \Gamma_0(n, d) \), \( n \)-secure code, consisting of \( n \) possible codewords of length \( n - 1 \). Let \( c_i \) be a column of height \( n \) in which the first \( i \) bits are 1 and the rest are 0. An example of the primitive codes for \( n = 4 \) (for user A, B, C, and D) is given in Fig. 1(a). The code \( \Gamma_0(n, d) \) consists of all columns \( c_1, c_2, \ldots, c_{n-1} \), each duplicated \( d \) times, arriving at a code for a total length of \( (n-1)d \). \( d \) determines the error probability. The larger \( d \), the lower error probability is.
Carry on the above example, let $d$ be 3 and the codes $\Gamma_0$ (4, 3) are changed as shown in Fig. 1(b). Before dispatching a codeword in $\Gamma_0(n, d)$ to a registered TRM as a fingerprint code, each codeword should be randomly permuted using a distinct secret key. Permutation helps in hiding the relationship between the positions of digital content and the fingerprint bits. Repetition and permutation make it harder for a coalition of users to remove fingerprint bits at will. Up to now, we construct a $n$-secure codebook $\Gamma_0(n, d)$.

2.2.2.2. Combination-codebook construction. To accommodate a large number of users, the constructed base codebook $\Gamma_0(n, d)$ is used to construct a combination codebook $C(L, N)$ of $N$ codebooks, where each codeword has a length $L$. The $N$ codewords are chosen independently and uniformly at random over the $n^L$ possibilities. Extending the above example, one random code $C(5, 9)$ with 9 codewords (for users I, II, ..., and VIII) and the first codeword is shown in Fig. 2.

Up to now, RA constructs $N$ sequence numbers to support at most $N$ users (TRM). The point is that the codewords of the $C(N, L)$ should be kept secret from the users.

When a buyer $B$ sends his identity $ID_B$ and TRM to RA and asks for registration. RA assigns a codeword of $C(N, L)$, a random $m$-bit sequence, as $SN_B$.

Then RA stores $\{ID_B, SN_B, T_B, Sign_{RA}(H(ID_B, SN_B), T_B)\}$ into TRM, where $T_B$ indicates the valid period, $H(.)$ is cryptographic one-way hash function and $Sign_{RA}(.)$ is a signature generated by RA, into TRM. RA also stores $\{ID_B, SN_B, T_B\}$ in a table. Fig. 3 shows the algorithm for registration.

2.2.2. Initialization

The initialization phase is composed of two stages: copyright watermarking and fingerprint watermarking.

2.2.2.1. Copyright watermarking. The seller $S$ first embeds a common copyright message $o$ into an original content $X$ to form a watermarked copy $C$ using an embedding function $W(.)$.

$C = W(k, X, o)$, where $o$ is a watermark indicating the copyright.

2.2.2.2. Fingerprint watermarking. Then the seller fingerprints it by performing the following operations.

1. Blocking: $S$ splits a digital content $C$ to be fingerprinted into $n$ disjoint subblocks, denoted $C_1, ..., C_n$, of the same size all of which must be concatenated to reconstruct the content $C$. For examples, an image is decomposed into non-overlapped subblocks or a stream of video is regarded as sequential frames.

2. Embedding: Then a bit string with the length of $\log_2 l$ is embedded into each subblock $C_i$ to form $C_i^0, C_i^1, ..., C_i^{l-1}$ using an embedding function $W(.)$ as follows: $C_i^j=W(k, C_i, w_i^j)$, where $i=1, ..., n$ and $w_i^j$ is a $\log_2 l$-bit binary-string form of $j$, $j=0, 1, ..., (l-1)$. That is, each block $C_i$ exists $l$ versions.

Hence, the protected subblocks are grouped into $l$ sets $C_i = \{C_i^0\}_{j=1}^n$. There exist $l$ slightly different versions of each subblock. Without lose of generality, let $l$ be 2.

\[
\begin{align*}
C_i^0 &= W(k, C_i, 0) \\
C_i^1 &= W(k, C_i, 1), \quad i = 1, ..., n; \\
C_0 &= \{C_i^0\}_{i=1}^n \quad \text{and} \quad C^1 = \{C_i^1\}_{i=1}^n.
\end{align*}
\]

For the sake of robustness, making subblock embedding resilient to intentional modification, a redundancy method may be used and given below.

Assumption 2. The existence of $l$ versions of $i$-subblock allows one to embed $\log_2 l$-bit binary string in the subblock. A simple redundancy method can be to replicate the bit string embedded in a subblock an odd number $p$ of times. Hence, $n = \frac{m}{\log_2 l} p$.

Fig. 4 shows the processes of the initialization phase.

2.2.3. Transaction

If $S$ successfully verifies the validity of $\{H(ID_B, SN_B), T_B, Sign_{RA}(H(ID_B, SN_B), T_B)\}$ received from $B$ by the RA’s public key, then $S$ transmits the blocks to $B$. Before transmitting the
Algorithm Registration

Input: $ID_B, TRM$

Output: $TRM storing \{ID_B, SN_B, T_B, \text{Sign}_B(H(ID_B, SN_B, T_B))\}$

\[ B \rightarrow RA: ID_B, TRM \]

\[ RA: \text{generates } SN_B, T_B \]

\[ RA: \text{computes } \text{Sign}_B(H(ID_B, SN_B, T_B)) \]

\[ RA: \text{stores } \{ID_B, SN_B\} \text{ into a database} \]

\[ RA \rightarrow TRM: \{ID_B, SN_B, T_B, \text{Sign}_B(H(ID_B, SN_B, T_B))\} \]

\[ RA \rightarrow B: TRM \]

Fig. 3. The processes of registration.

protected blocks, the session key $sk$ shared between $S$ and $B$ must be generated by a key exchange protocol [12].

1. Transmitting: $S$ generates $[C_i^0, \ldots, C_i^{l-1}]_{sk}$, where $[.]_{sk}$ is a secret-key encryption function with the key $sk$. Then $S$ sends it to $B$’s $TRM$.

2. Extracting: Upon receiving the blocks, $TRM$ deterministically reveals only one of $(C_i^0, \ldots, C_i^{l-1})$ to $B$ according to the bit string of $SN_B$. However, $S$ doesn’t know which one $B$ gets.

3. After $n$ rounds by repeating above two steps, $B$ gets the unique-version fingerprinted content: $C_{\bar{i}^j} = \{C_i^j | i=1, \ldots, n, j_1=0, 1, \ldots, l-1\}$, where $j_1||j_2||\ldots||j_n$ is the same as $SN_B$.

Fig. 5 shows the processes of the transaction phase.

2.2.4. Illegality tracing

This phase is divided into two stages: copyright proof and fingerprint tracing.

2.2.4.1. Copyright proof. Once $S$ finds an illegal copy $\tilde{C} = \{\tilde{C}_i^j | i=1, \ldots, n, j_i=0, 1, \ldots, l-1\}$, he can extract the watermark $\tilde{o}$, the copyright message, where

\[ \tilde{o} = W^{-1}(k, \tilde{C}) \]

$S$ shows his copyright to $RA$ by $\text{sim}(o, \tilde{o})$.

2.2.4.2. Fingerprint tracing. He goes on extracting the fingerprint $SN'_V$, indirectly indicating the identity of $B$, from the illegal copy as follows.

\[ \tilde{w}_j = W^{-1}(k, \tilde{C}_j^i), \text{ and} \]

\[ SN'_V = \tilde{w}_1||\tilde{w}_2||\ldots||\tilde{w}_n. \]

$S$ sends $SN'_V$ to $RA$ and thus $RA$ can determine with high probability who is the dishonest buyer according to $\text{sim}(SN'_V)$.

Algorithm Initialization

Input: $X$

Output: $l$ sets $C'^l_j = \{C'^l_j | i=0, 1, \ldots, (l-1)\}$

// Copyright watermarking

\[ C = W(k, X, o) \]

// Fingerprint watermarking

Create $\{C'_i\}_i=1$ from $C$.

For $i=1$ to $n$

For $j=0$ to $(l-1)$

\[ C'_i = W(k, C_i, w'_j) \]

Fig. 4. The processes of initialization.
As remarked in [5], for robust embedding schemes, this would generally be accepted by correlating $SN'_B$ with every stored $SN_B$ in the table and selecting the one with the highest correlation beyond a confidence threshold. The protocol returns failure if no such user can be found. Fig. 6 shows the processes of the illegality tracing phase.

3. Security analysis

The security of the proposed copyright-protection protocol is based on the following security assumptions. First of all, robust copyright watermarking and fingerprinting with $c$-collusion security are defined above. Secondly, the related cryptosystems used by the proposed protocol are defined as follows.

Definition 5. A secure secret-key algorithm is an algorithm for cryptography that uses the same cryptographic key to encrypt and decrypt the message. An encryption scheme is composed of the sets of encryption and decryption transformations. Without knowing the key, there is no feasible way to reveal the encrypted message.

Definition 6. A digital signature is an algorithm for cryptography that is used for signing messages. A digital signature scheme consists of the sets of signature generation and signature verification. Let $B$ be the recipient of a message $m$ signed by $A$. Then the secure signature scheme must satisfy the following requirements: (1) $B$ must be able to validate $A$’s signature on $m$. (2) It must be impossible for anyone, including $B$, to forge $A$’s signature. (3) If $A$ denies signing a message $m$, it must be possible for a trusted third party to resolve the dispute arising between $A$ and $B$.

Definition 7. A hash function is a function that takes a variable-size input and returns a fixed-size result called hash value. If a hash function is one-way, it is also called a message-digest function, and its result is called a message digest. The message digest computed from a large message can be treated as a “digital fingerprint” of the original message. It is usually used for digital signature in the way that, a message is first hashed to its message digest, and then the message digest is to be signed in place of the original message. It can be helpful to prevent known attacks on all digital signature schemes, and to save both the time and space requirements for manipulating signatures. The secure hash function $H(.)$ used for digital signature must satisfy the following conditions:

(1) The hash function can take input of any size, and the result (hash value) should be fix-sized.
(2) For any message $m$, it is easy to compute $m$’s hash value $H(m)$.
(3) It is computationally infeasible to find a message $m$ from its hash value $H(m)$.
(4) For any message $m_1$, it is computationally infeasible to find another message $m_2$ such that $H(m_1)=H(m_2)$.
(5) It is computationally infeasible to find a pair of different messages $m_1$ and $m_2$ such that $H(m_1)=H(m_2)$.

Definition 8. A secure key exchange protocol is a key establishment technique in which a shared secret is derived by two parties (or one party creates or otherwise obtains a secret value, and securely transfers it to the other) as a function of information contributed by each of these, such that no party can predetermine the resulting value.

Third and final assumption is that TRM and RA are trustworthy basically.

Based on the above definitions and assumptions, further analyses are described below.

Proposition 1. (Collusion security)

The probability of each subblock whose fingerprint can be detected by a collusion of $c$ buyers is $(1 - \frac{1}{\tau^c})$. 
Proof. As pointed out in Definition 4, c colluding buyers can remove all fingerprints in the i-subblock if and only if they can contribute l versions \((C_i^0, \ldots, C_i^{l-1})\) of the original subblock. The probability that all c buyers were given the same version is \(\frac{1}{l!c^{l-1}}\). Therefore, the probability that they can contribute l versions is \(\frac{1}{l!c^{l-1}}\). □

Proposition 2. (Anonymity)

In the transaction phase, an honest buyer will not be identified if breaking a cryptographic one-way hash function is infeasible.

Proof. In the transaction phase, B sends \(\{H(ID_B, SN_B), T_B, \text{Sign}_{RA}(H(ID_B, SN_B), T_B)\}\), like a ticket signed by RA, to convince S its legitimacy. What S sees is \(\{H(ID_B, SN_B), T_B, \text{Sign}_{RA}(H(ID_B, SN_B), T_B)\}\). If S wants to obtain ID_B from H \((ID_B, SN_B)\), he faces the hard problem of breaking a cryptographic one-way hash function. □

Proposition 3. (Traceability)

The identity of the dishonest buyer will be revealed by the cooperation of the registration authority and the seller if a robust copyright watermarking scheme and a collusion-secure fingerprinting scheme, both hypothetically based on a robust embedding function, exist.

Proof. Based on the assumption that a robust copyright watermarking scheme exists, S can extract the copyright message \(\delta = W^{-1}(k, \tilde{C})\) from the suspicious copy \(\tilde{C}\) to show his copyright to RA by \(\text{sim}(\delta, \tilde{C})\). On the other hand, since a secure fingerprinting scheme exists, S hands RA \(\text{SN'} = W^{-1}(k, \tilde{C}'_i) \{W^{-1}(k, \tilde{C}'_i), \ldots, W^{-1}(k, \tilde{C}'_n)\}\) and thus RA can determine with high probability who is the dishonest buyer according to \(\text{sim}(\text{SN'}, \text{SN}_B)\). If \(\text{sim}(\cdot, \cdot)\) is set to be very loose, this means that the system wishes to identify the specious buyer of any redistributed copy that vaguely resembles an copy on sale. Of course, identification may often fail in such cases. On the contrary, if \(\text{sim}(\cdot, \cdot)\) is tight, the system also may fail. □

Proposition 4. (Asymmetry)

If the seller intends to cheat someone for some reasons, he must distribute a fingerprinted copy that has already been sold to someone. But he does not know who the buyer is and which the exact sold copy is even if he has the list of his customers. Since the seller does not know the fingerprinted copy, the buyer cannot claim that the unauthorized copy is resold or distributed by the seller.

Proof. For each subblock \(C_i\) of a digital content, S creates l fingerprinted subblocks \(C_i^0, C_i^1, \ldots, C_i^{l-1}\). In the transaction phase, S sends \(\{C_i^0, \ldots, C_i^{l-1}\}\) in the encrypted form to TRM. Upon decrypting them, TRM deterministically reveals only one of \(\{C_i^0, \ldots, C_i^{l-1}\}\) to B. Based on the assumption of a trustworthy TRM, only the buyer knows the fingerprinted content, but the seller doesn’t know which one the buyer gets. □

Proposition 5. (Confidentiality)

The confidentiality of transmitted contents is guaranteed based on the secret session key created and shared by both the seller and TRM.

Proof. According to Definition 8, a secure session key can be generated dynamically to securely transmit the content between the seller and TRM in an encryption form using the shared session key. Under Definition 5, a secret-key encryption guarantees the confidentiality of the transmitted contents. □
For example, if the key exchange protocol in [12] is used, the security is based on that the so-called Diffie–Hellman problem is as hard as computing discrete logarithms [13].

**Proposition 6. (Counterfeit security)**

A malicious buyer cannot forge an illegal TRM to cheat the seller.

**Proof.** In the transaction phase, the seller first successfully verifies the validation of the authentication information including \(\{H(ID_B, SN_B), T_B, \text{Sign}_{RA}(H(ID_B, SN_B), T_B)\}\) received from \(B\) by the RA’s public key. If a malicious buyer forges a TRM without registering to RA, he must generate a “valid” \(\text{Sign}_{RA}(H(ID_B, SN_B), T_B)\) which will pass the verification by the seller. However, he faces the hard problem of forging a signature. □

4. Discussions

In spite of the above requirements of security, there are several added valuable merits discussed as follows. Table 1 summarizes the analyses of efficiency and functionality comparisons.

### 4.1. Computational efficiency

As [14] has shown, the speed of secret-key operations is about 1000 times faster than that of public-key operations. Compared with the schemes adopting the public-key operations on the whole multimedia content [4–8], the proposed protocol involving the secret-key cryptosystem is much more efficient. Compared to [8] in which TRM is required to perform both public key operation and watermarking on the intended content, in the proposed scheme TRM only perform secret key operation on the content. That is, the proposed scheme requires low computation capability for TRM.

### 4.2. Simple secret key management

It is obvious that if the system maintains a secret database, it will be the target of numerous attacks from networks. In general, the schemes based on a secret-key cryptosystem likely suffer this challenge, the secret key management problem, and limit scalability of a system. In the proposed scheme, there is no sensitive information stored centrally in the system. On the contrary, the one-time-used secret key used in the proposed scheme is dynamically generated based on a key exchange. Hence, maintenance cost is low, security problem decreases, and key management is simple.

#### 4.3. Simple public key management

In the proposed protocol, the public key management is very simple since only the public key and the long-term private key of RA are maintained in the system. Since only RA’s public key is used by the seller to verify the information sent from TRM, there is no public key infrastructure (PKI) required. Yet in the systems of [4–8], the public key management is just a different case. Each entity including the seller, the buyer and TRM owns a pair of keys, a private key and a corresponding public key; hence, the burden of PKI is not avoided.

#### 4.4. Low trust

It is reasonable to assume that RA is trustworthy since the buyers must register their TRMs prior to utilizing these devices and RA is responsible for illegality tracing. Furthermore, since a trustworthy TRM has been used widely in Cable TV box, DVD, smart cards, etc., the proposed protocol is practical nowadays and particularly suitable for the network environments providing membership.

#### 4.5. Of wide use

Blocking the content may be adopted in both spatial and frequency domains. The above presented method is an example of the former. The latter is, for example, that the wavelet coefficients of the content are embedded according to the sequence of a progressive transmission scheme. Generally speaking, the encryption and embedding model for multimedia contents must meet the specific property for displaying.

5. Conclusions

We believe that the anonymity and asymmetry of copyright protection protocols can benefit from a skillful combination of cryptography and watermarking techniques. Based on this idea, an anonymous asymmetric protocol based on a tamper-resistant device for copyright protection of multimedia contents is proposed without the involvement of the public-key encryption/decryption of the whole content. The identity of the dishonest buyer will be revealed by the cooperation between the seller and a trusted third party based on a robust copyright watermarking scheme and a collusion-secure fingerprinting technique. The scheme not only benefits from several valuable advantages but also is more efficiently practical than that of the existing schemes. Hence, the proposed scheme provides an ingenious integrated service for a copyright protection protocol.
References


Tzung-Her Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received a B.S. degree in Department of Information and Computer Education from the National Taiwan Normal University in 1991 and an M.S. degree in the Department of Information Engineering from Feng Chia University in 2001. In 2005, he received his Ph.D. degree in the Department of Computer Science from the National Chung Hsing University. He has been with the Department of Computer Science and Information Engineering at the National Chiayi University as Assistant Professor since August 2005. His research interests include information hiding, multimedia security, digital rights management, and network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.

Gwoboa Horng received a B.S. degree in Electrical Engineering from the National Taiwan University in 1981 and his M.S. and Ph.D. degrees from the University of Southern California in 1987 and 1992, respectively, all in Computer Science. Since 1992, he has been on the faculty of the Institute of Computer Science at the National Chung-Hsing University, Taichung, Taiwan, R.O.C. His current research interests include artificial intelligence, cryptography and information security.