An Efficient and Anonymous Buyer-Seller Watermarking Protocol


Multimedia Security
Outline

• Customer’s Right Problem
• Buyer-Seller Watermarking Protocol
• Unbinding Problem
• The Proposed Watermarking Protocol
• Discussion
Customer’s Right Problem

• In traditional watermarking scenarios, the seller is entitled to the responsibility of generating and inserting digital watermarks. As a result, the seller is granted access to each watermarked copy.

• A malicious seller can easily frame the buyer by releasing corresponding watermarked copy afterwards.
Memon and Wong’s Protocol

\[ E_B(W') = P(E_B(W)) \]
\[ E_B(X') = E_B(X + W') = E_B(X) + E_B(W') \]

Privacy Homomorphism

\[ \text{Sign}_{WCA}(E_B(W)) \]

\[ \text{Sign}_{WCA}(E_B(W)) \]

(II) Returning the watermark generated

(III) Sending out the purchase order

(IV) Making the Delivery

(I) Requesting for a valid watermark

\[ X' = DB^{-1}(E_B(X')) \]

B & ID_B

W
1) The buyer sends his identity and public key $B$ to WCA and requests a valid watermark. Upon receiving the request, WCA randomly generates a watermark $W$ with its vector representation being $\{w_1, w_2, w_3, \ldots, w_n\}$, and encrypts it as $E_B(W) = \{E_B(w_1), E_B(w_2), E_B(w_3), \ldots, E_B(w_n)\}$, where $E_K$ denotes the privacy-homomorphic encryption function with respect to the watermark insertion operation of the underlying watermarking scheme using public key $K$. Then, WCA signs $E_B(W)$ and sends it back to the buyer.
2) The buyer forward $E_B(W)$ and WCA’s signature to the seller. After verifying that $E_B(W)$ is perfectly signed and, hence, $W$ is, indeed, a valid watermark generated by WCA, the seller chooses a permutation function $\sigma$ to shuffle the elements in $E_B(W)$ to get $E_B(W') = \sigma(E_B(W)) = E_B(\sigma(W)) = \{E_B(w'_1), E_B(w'_2), E_B(w'_3), \ldots, E_B(w'_n)\}$ and inserts the permuted watermark into $X$, the image to be sold, in the encrypted domain by computing $E_B(X') = E_B(X \oplus \sigma(W)) = E_B(X) \oplus E_B(\sigma(W)) = E_B(X) \oplus E_B(W')$, where $\oplus$ is the watermark insertion operation of the underlying linear watermarking scheme, and $X'$, or $X \oplus \sigma(W)$, is the watermarked copy of $X$ in its final form (not known to the seller). After the seller finishes the computation, she sends $E_B(X')$ to the buyer.
3) When the buyer receives $E_B(X')$, he decrypts it with his private key $B^{-1}$ by computing $X' = D_{B^{-1}}(E_B(X'))$, where $D_{K^{-1}}$ denotes the decryption function using private key $K^{-1}$, and gets the correctly watermarked copy $X'$. 
• Remarks:

• (1) In step 1), $E_K$ is required to be privacy homomorphic wrt. the watermark insertion operation. In step 2), the underlying watermarking scheme is required to be linear.

• (2) If the buyer refuses to or cannot decrypt $E_B(w)$, he is considered guilty.

• (3) Memon and Wong’s protocol successfully solves the custom’s right problem but not the Unbinding problem.
Unbinding problem

• What is Unbinding problem:
  fail to provide proper mechanisms on binding a chosen watermark to a specific digital content or a specific transaction.

Once the seller discovered a pirated copy, it is possible for her to transplant the watermark embedded in the pirated copy into another copy of a higher-priced digital content to produce made-up piracy so that she can get compensation more.
Assume that the buyer has bought $U'$ and $V'$ from the same seller. Where $U' = U \oplus \sigma_1(W_1)$ and $V' = V \oplus \sigma_2(W_2)$ are two watermarked images of two different still images $U$ and $V$, respectively, and $U$ is much more expensive than $V$, $\sigma_1$ and $\sigma_2$ are two different permutation functions and $W_1$ and $W_2$ are two different watermarks.
• S’pose some time later the seller gets a pirated copy $V'$, which the buyer distributes without authorization.

• Since the seller has the corresponding original image $V$, it is trivial for her to derive $\sigma_2(W_2)$ from $V'$. Thus, she is able to insert $\sigma_2(W_2)$ into $U$ and encrypts the resulting watermarked image with the buyer’s public key $B$ to obtain $U'' = E_B(U \oplus \sigma_2(W_2))$. 
• With $E_B(W_2)$, WCA’s signature associated with $E_B(W_2)$, and $\sigma_2$ in hand, now the seller has all the evidence needed and is ready to claim that the buyer illegally distributes $U'' = U \oplus \sigma_2(W_2)$, which is actually never sold to the buyer.
Another point of view:

- Following Memon and Wong’s protocol, the seller keeps records of $E_B(W)$, WCA’s signature associated with $E_B(W)$ and $\sigma$ after a successful transaction.

- The next time the same buyer comes to purchase another image, the ill-behaved seller simply ignores the newly generated and encrypted watermark forwarded by the buyer and inserts the same permuted watermark $\sigma(W)$ into the copy of the requested image in the encrypted domain.
• Under this circumstances, the same $E_B(W)$, WCA’s signature associated with $E_B(W)$, and $\sigma$ can be used to testify against the particular buyer regardless which still image actually being pirated, provided that the buyer has committed piracy.

• As a result, when a pirated image is found, the seller can always claim that the buyer also illegally distributes copies of other images purchased by him.
Roles

• S: seller
• B: buyer
• CA: A trusted certification authority, issuing anonymous certificate
• WCA: a trusted **watermark** certificate authority
• ARB: arbiter
• The existence of WCA asserts the validity of **watermarks** and ensures that the watermarks generated are not revealed to S.
Before a transaction is carried out, B applies to CA an anonymous certificate. In this case, B’s public key serves as his *Pseudonym*, and the anonymous certificate is used to certify that the pseudonym is correctly registered to CA, and CA actually knows about the real identity behind the pseudonym. The existence of CA provides the possibility of B’ anonymity as well as the assurance to S.
Notations

- \((pk_I, sk_I)\): a public-private key pair for owner I
- \((pk^*, sk^*)\): a one-time key pair
- \(\text{Sign}_I(M)\): digital signature of message M signed by I
- \(D_{skI}/E_{pkI}\): Decryption and encryption function
- \(X+W\): watermarked version of X, + standards for watermark insertion
- \(\text{ARG}\): common agreement between buyer and seller, negotiated in advance
Registration Protocol

• B first sends a randomly selected $pk_B$ to CA. When CA receives $pk_B$, it generates an anonymous certificate $\text{Cert}_{CA}(pk_B)$ and sends it back to B.

• The registration process can be skipped if anonymity is not a concern
The Proposed Protocol

(I) Sending out the purchase order
(II) Requesting for a valid watermark
(III) Returning the watermark generated
(IV) Making the Delivery
The Proposed Protocol

\[ X' = X + V \]

\[ E_{pk^*}(X') = E_{pk^*}(X + W) = E_{pk^*}(X') + E_{pk^*}(W) \]

Store sales records
1) To acquire a copy of digital content $X$, $B$ first negotiates with $S$ to set up a common agreement, ARG, which explicitly states the rights and obligations of both parties, and specifies the digital content of interest. ARG uniquely binds this particular transaction to $X$ and can be regarded as a purchase order. Note that $B$ may use his pseudonym in the negotiation to keep his identity unexposed. Alternatively, since ARGs are different only in the part specifying the digital content of interest, it is possible for $S$ to generate ARGs beforehand and put them in a public place (e.g., her Web site), along with the catalog of the digital contents to be sold, so that $B$ may have anonymous access to ARGs.
2) After the initial negotiation, B randomly selects a one-time key pair \((pk^*, sk^*)\) and generates an anonymous certificate, \(\text{Cert}_{pk_B}(pk^*)\), with \(pk^*\) being the associated pseudonym, on the honor of \(pk_B\), B’s pseudonym associated with \(\text{Cert}_{CA}(pk_B)\). In this case, CA assures the legality of \(pk_B\), and \(pk_B\), in turn, assures the legality of \(pk^*\). Then, B transmits \(\text{Cert}_{CA}(pk_B)\), \(\text{Cert}_{pk_B}(pk^*)\), ARG, and \(\text{Sign}_{pk^*}(\text{ARG})\) to S.
3) Upon receiving $\text{Cert}_{CA}(pk_B)$, $\text{Cert}_{pk_B}(pk^*)$, ARG, and $\text{Sign}_{pk^*}(\text{ARG})$, $S$ verifies the validity of the certificates and the signature, and aborts the transaction if any of them is invalid. Otherwise, she generates a unique watermark $V$ for this particular transaction and computes $X' = X \oplus V$, where $X'$ is the watermarked digital content. In this step, $S$ may employ any watermarking scheme she likes, provided that it is able to resist various possible distortions resulted from malicious attacks and still can be successfully extracted sometime later. The existence of $V$ in $X'$ is to produce a key of search for $S$ to quickly locate a specific entry in her sales records when a pirated copy is found. It is not meant for proving the involvement of a cheating buyer. Then, $S$ sends $\text{Cert}_{pk_B}(pk^*)$, ARG, $\text{Sign}_{pk^*}(\text{ARG})$, and $X'$ to WCA.
4) When **WCA** receives $\text{Cert}_{pk_B}(pk^*)$, ARG, $\text{Sign}_{pk^*}(\text{ARG})$, and $X'$ from $S$, it verifies the validity of the certificate and the signature, and aborts the transaction if any of them is invalid. Otherwise, it generates a watermark $W$ specific to this transaction. Since $X'$ is also transmitted to **WCA**, it is possible for **WCA** to create a more robust watermark according to the characteristics of $X'$ so that the well-tailored watermark can be more difficult to disrupt and cause less perceivable defects when later inserted into $X'$. If $S$ has concerns about sending $X'$ to **WCA**, she may offer a profile describing $X'$ instead. After $W$ is successfully generated, **WCA** computes $E_{pk^*}(W)$, $E_{pk_{WCA}}(W)$, and $\text{Sign}_{WCA}(E_{pk^*}(W), pk^*, \text{Sign}_{pk^*}(\text{ARG}))$, and sends them back to $S$. 
5) Upon receiving the response, S performs the second-round watermark insertion in the encrypted domain by computing $E_{pk^*}(X'') = E_{pk^*}(X' \oplus W) = E_{pk^*}(X') \oplus E_{pk^*}(W)$, without knowing the actual watermark, $W$. S also has no idea about the doubly watermarked copy of $X$ in its final form, $X''$, or $X' \oplus W$. Note that the computation of $E_{pk^*}(X'')$ is possible because $E_{pk^*}$ is privacy homomorphic with respect to $\oplus$. Afterwards, S delivers $E_{pk^*}(X'')$ to B and stores $V_1, \text{Cert}_{CA}(pk_B), \text{Cert}_{pk_B}(pk^*), \text{ARG}, \text{Sign}_{pk^*}(\text{ARG}), E_{pk^*}(W), E_{pk_{\text{WCA}}}(W)$, and $\text{Sign}_{\text{WCA}}(E_{pk^*}(W), pk^*, \text{Sign}_{pk^*}(\text{ARG}))$ in a new entry of Table$_X$, her sales records with respect to digital content $X$. 
6) After receiving $E_{pk^*}(X'')$, B decrypts it with $sk^*$ by computing $X'' = D_{sk^*}(E_{pk^*}(X''))$ and obtains the correctly watermarked copy $X''$. Note that S cannot intentionally alter the value of $E_{pk^*}(X'')$ via any kind of post processing after it is computed. Otherwise B may fail to restore $X''$ in the process of decryption and decide to abort the transaction.
Identification and Arbitration

A Pirated Copy, Y, of Digital Content X

Table $\lambda$ (The Seller’s Sales Records with Respect to Digital Content X)

<table>
<thead>
<tr>
<th>Watermark for First-Round Insertion (Key)</th>
<th>One-Time Anonymous Certificate</th>
<th>Encrypted Watermark for Second-Round Insertion</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_1$</td>
<td>$\text{Cert}<em>{pk</em>{m_1}}(pk_1^*)$</td>
<td>$E_{pk_1^*}(W_1)$</td>
</tr>
<tr>
<td>$V_2$</td>
<td>$\text{Cert}<em>{pk</em>{m_2}}(pk_2^*)$</td>
<td>$E_{pk_2^*}(W_2)$</td>
</tr>
<tr>
<td>$V_3$</td>
<td>$\text{Cert}<em>{pk</em>{m_3}}(pk_3^*)$</td>
<td>$E_{pk_3^*}(W_3)$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$V_n$</td>
<td>$\text{Cert}<em>{pk</em>{m_n}}(pk_n^*)$</td>
<td>$E_{pk_n^*}(W_n)$</td>
</tr>
</tbody>
</table>

Y, X’, Cert$_{CA}(pk_B)$, Cert$_{pk_B}(pk^*)$, ARG, Sign$_{pk^*}(ARG)$, $E_{pk^*}(W)$, $E_{pk_{WCA}}(W)$, Sign$_{WCA}(E_{pk^*}(W), pk^*, \text{Sign}_{pk^*}(ARG))$

Seller → Arbiter → WCA

Buyer using pk*
Solving Unbinding Problem

- \( \text{Sign}_{WCA}(E_{pk^*}(W), pk^*, \text{Sign}_{pk^*}(\text{ARG})) \) explicitly binds \( W \) to \( \text{ARG} \)

- By introducing the one-time key pairs, it is impossible for \( S \) to fool \( B \).
Accomplishment of Other Goals

- Buyer’s privacy is well protected by using anonymous certificate.
- Only one communication with seller is required for the buyer now.
- Trusted third parties are capable of making appropriate adjudications, no cooperation from buyer is required.
- The WCA gets information about the digital content, thus a more robust watermark may be tailored.