An efficient buyer-seller watermarking protocol based on proxy signatures

Mohammad kazem nasab haji
Ziba Eslami

8'th iscisc

September 2011

Outline

- Customer's Right Problem
- Buyer-Seller Watermarking Protocol
- The proposed scheme
- Implementation of the proposed protocol
- Security analysis

customer's rights

- Digital content can easily be edited, transformed and perfectly reproduced.
- Traditional watermarking techniques combine digital watermarking and fingerprinting.
- seller is responsible for generating and inserting digital watermarks.
- A malicious seller can easily frame the buyer
- Therefore, these techniques do not preserve the customer's rights.

Buyer-Seller Watermarking Protocol

- Combines encryption, digital watermarking, and fingerprinting.
- Seller and buyer are responsible for watermark generation and embedding
- The first known buyer-seller watermarking protocol was introduced by Memon and Wong, 2001.

Buyer-Seller Watermarking Protocol: Security problems

- The piracy tracing problem
- The customer's rights problem
- The unbinding problem
- The anonymity problem
- The conspiracy problem

The proposed scheme

- Consists of three protocols:
  - Registration protocol
  - Watermark generation and embedding protocol
  - Identification and arbitration protocol
- Entities are: Seller(S), Buyer(B), Certificate Authority(CA), Judge(J).

Notations

(pk_i, sk_i)	The public and private key of participant entity i
ARG_X	The purchase agreement between S and B for the content X
ID_B	The identity of B,
PID_B	he proxy identity corresponding to IDB
$E_k(m)$	Encryption of m with the key k using Paillier cryptosystem
$H(.)$	A hash function
W_A	The watermark corresponding to the entity A
$Wrnt_{O\to P}$	The warrant given by O to P
$dKey_{O\to P}$	The delegation key that O assigns to the proxy signer P
$psKey_{O\to P}$	The proxy signing key which the proxy signer P computes from $dKey_{O\to P}$ and his own private key sk_O
$Sign(psKey_{O\to P}, m)$	The proxy signature of P on behalf of O on message m
$\|$	The concatenation operation

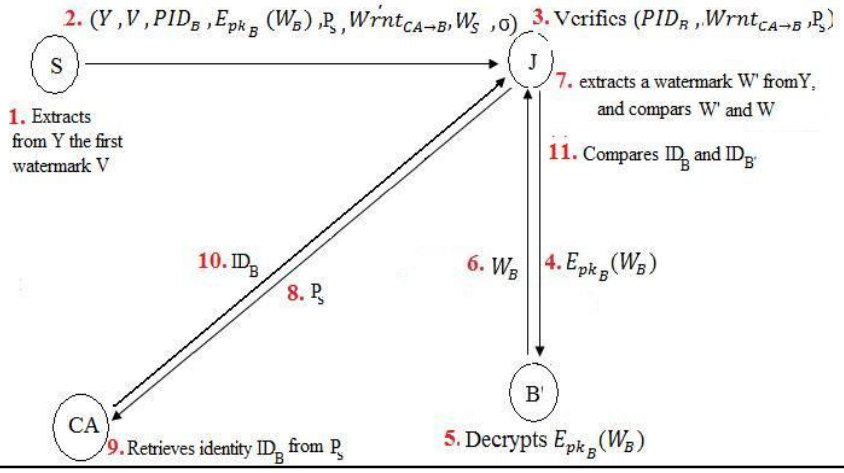
Registration protocol

Buyer(B)		Certificate Authority(CA)
1.	(ID_B, pk_B) →	
		Compute PID_B , $dKey_{CA\to B}$, **.2** $Wrnt_{CA\to B}$ from $(ID_B, pk_B$ $sk_{CA})$ and store (PID_B, ID_B)
	← $(dKey_{CA\to B}, Wrnt_{CA\to B}, PID_B)$	
3. If verify($Wrnt_{CA\to B}$, $dKey_{CA\to B}$) = True then compute proxy signing key $psKey_{CA\to B}$		

Watermark generation and embedding protocol

Seller(S)		Buyer(B)
	ARG_X →	
		Generate W_B and compute .1 P_s= Sign($psKey_{CA\to B}$, $[E_{pk_B}(W_B)\|\|H(ARG_X])$
	← P_s, ARG_X , $E_{pk_B}(W_B)$, $Wrnt_{CA\to B}$	
2. If P_s and $Wrnt_{CA\to B}$ are verified then generate V, W_S , σ, X' = X + V $C = E_{pk_B}(X') \cdot E_{pk_B}(W_S) \cdot \sigma(E_{pk_B}(W_B))$ Store (V, W_S , σ , P_s , $E_{pk_B}(W_B)$).		
	C →	Decrypt C with sk_B and obtain .3 X'' = X' + W_S + $\sigma(W_B)$

Identification and arbitration protocol



Implementation of the proposed protocol

- Robust spread spectrum watermarking technique
- The Paillier cryptosystem
- Collusion-secure fingerprinting code

Security analysis

- The piracy tracing problem: YES
- The customer's rights problem : YES
- The unbinding problem : YES
- The anonymity problem : YES
- The conspiracy problem : YES

THE END

Thank you for your attention