A CRT BASED WATERMARK FOR MULTIPARTY MULTILEVEL DRM ARCHITECTURE

Tony Thomas, Sabu Emmanuel, Amitabha Das

School of Computer Engineering
Nanyang Technological University, Singapore

Mohan S. Kankanhalli

School of Computing
National University of Singapore, Singapore

ABSTRACT

In this paper, we propose a joint digital watermarking protocol for the multiparty multilevel DRM architecture using Garner's algorithm for the Chinese remainder theorem (CRT). Our protocol exploits the incremental nature of the computation of CRT by the Garner's algorithm. The proposed joint watermarking protocol embeds a single watermark signal into the content while taking care of the various security concerns such as proof of involvement in the distribution chain, non-repudiation of the involvement and protection against false framing of the different parties involved. Further, in the event of finding an illegal copy of the content, the identities of all the parties involved in that content distribution chain can be traced back by extracting the watermark information.

Index Terms— digital rights management, watermarking, Chinese remainder theorem

1. INTRODUCTION

The traditional two party digital rights management (DRM) architecture involving a seller and a buyer is not adequate to address the requirements of the present day business models for content delivery. Hence, multiparty multilevel digital rights management architecture (MPML-DRM-A) has been suggested as an alternative to the traditional two party (buyer-seller) DRM architecture by many authors [2, 7]. The term multiparty refers to the multiple parties such as the owner, distributors, sub-distributors and consumers and the term multilevel refers to the multiple levels of distributors/sub-distributors involved in the distribution chain of a content.

The technique of digital watermarking has been used for the purpose of ownership proving, copyright violation detection and violator identification, content tamper detection etc. [4]. In a MPML-DRM-A the watermarking scheme needs to address the security concerns of all the parties involved. This involves protecting the rights of the owner, distributors and consumers. The owner, distributors and consumers could be able to prove their role, if they were part of the distribution chain of a content. On the other hand, there should be security against false framing for any party which was not part of the delivery chain of a content. Further, it should be ensured that all the parties in the distribution chain have contributed to the watermark signal with their correct share. The naive approach for watermarking in MPML-DRM-A is that each party embeds its watermark signal individually into the content. However, this approach affects the quality of the resultant content to a greater extent (due to the presence of multiple watermark signals in the content) and the security concerns such as proof of involvement, non-repudiation of the involvement and protection against false framing of the parties will not be properly taken care as each party is embedding its watermark signal independently. Another approach to watermarking in this case is to employ a buyer-seller watermarking protocol [4] between each pair of interacting parties. However, this also can affect the quality of the resultant content due to the embedding of multiple watermark signals into the content. So, our approach is to embed one watermark signal into the content based on a watermark information jointly generated by all the parties involved with the help of a trusted third party (license server). This approach not only minimizes the size of the watermark in the content but also takes care of the security concerns of the parties involved.

In this paper, we propose a joint digital watermarking protocol for MPML-DRM-A using Chinese remainder theorem (CRT). Some previous applications of CRT in DRM include, a key distribution scheme using CRT for conditional access system in digital TV broadcast [1], a CRT based parameter distribution in the scrambling process for conditional access to Pay-TV systems [3] and a binary fingerprinting code using CRT [6]. We generate a joint watermark information as the (CRT) solution of a set of congruences corresponding to each party in the distribution chain. The Garner's algorithm [5] is used for the incremental computation of CRT, so that the joint watermark information is generated in an additive manner with each entity adding a component corresponding to its share. Our scheme guarantees that the identities of all the involved parties can be traced back using the properties of CRT.

The rest of the paper is organized as follows. We first recall the CRT and Garner's algorithm in Section 2. Then we describe our joint watermarking mechanism using CRT and its security analysis in Section 3. The paper concludes with some remarks and future directions for research in Section 4.

Thanks to the Agency for Science, Technology and Research (A*STAR), Singapore for supporting this work under the project 'Digital Rights Violation Detection for Digital Asset Management' (Project No: 0721010022).

2. CHINESE REMAINDER THEOREM (CRT)

Let $n_1, \ldots, n_k$ be pairwise coprime positive integers. Then, for any given set of integers $r_1, \ldots, r_k$, the system of k simultaneous congruences, $x \equiv r_i \mod n_i$, for $1 \leq i \leq k$, has a unique solution x such that $0 \leq x < n_1 \ldots n_k$. The solution x of the above system of congruences can be efficiently computed using the Garner's algorithm [5] given below. In the Garner's algorithm, we assume that $0 \leq r_i < n_i$, for all i.

Garner's Algorithm

1. For i from 2 to k do the following:
   (a) $c_i \leftarrow 1$.
   (b) For j from 1 to $(i-1)$ do the following:
   . $u \leftarrow n_j^{-1} \mod n_i, c_i \leftarrow uc_i \mod n_i$.
2. $u \leftarrow r_1, x \leftarrow u$.
3. For i from 2 to k do the following:
   . $u \leftarrow (r_i - x)c_i \mod n_i, x \leftarrow x + u \prod_{j=1}^{i-1} n_j$.
4. Return(x).

Using Garner's algorithm the solution x can be computed in a sequential manner. The value of x at any stage corresponds to the solution of the set of congruences considered till then.

3. CRT BASED WATERMARKING SCHEME

In this section, we describe our joint watermarking protocol based on CRT for MPML-DRM-A. The parties involved in a typical MPML-DRM-A are an owner, multiple levels of distributors, consumers and a license server [7]. The content moves from the owner to the consumers through multiple levels of distributors. The owner and distributors maintain their own content servers CS. A consumer can get the content from any of the content servers of owner/distributors. The owner and the distributors generate their redistribution licence and usage licence and send to the license server. A redistribution license allows the receiver to redistribute the content and usage licence allows the receiver to use the content. A license contains permissions, constraints and cryptographic keys. A sub-distributor can obtain the redistribution licence and a consumer can obtain the usage licences (of owner and the distributor) from the license server.

We generate a joint watermark information as the (CRT) solution of a set of congruences corresponding to each party in the distribution chain. The watermark signal is generated from this joint watermark information and then embedded into the content using any of the known robust embedding algorithms. The watermark signal is extracted using the corresponding watermark extraction algorithm. Due to space constraints, we do not elaborate on the embedding and extraction algorithms in this paper.

3.1. Generation of Individual Watermark Information

Let the parties involved in the delivery of a content X be an owner O, k levels of distributors $D_1, \ldots, D_k$ (there can be no distributor also), a consumer C and a license server L. The content moves as $O \rightarrow D_1 \rightarrow \ldots \rightarrow D_k \rightarrow C$.

Let y be a unique identifier (can be a hash) of X. Each party i involved in the content delivery generates/gets its watermark information r_i as a function of y and its identity i, either individually by computing its digital signature on y or with the help of a trusted *watermark certification authority* which generates a valid watermark information upon request, and sends it along with a time-stamp and a digital signature.

The following section describes how the individual watermark informations r_i are combined to generate a joint watermark information I using Garner's algorithm for CRT.

3.2. Generation of Joint Watermark Information

Let $r_0, r_1, \ldots, r_k$ and r_{k+1} be the individual watermark information of $O, D_1, \ldots, D_k$ and C respectively, computed by one of the methods described in the Section 3.1. Let $n_0, n_1, \ldots, n_{k+1}$ be a set of positive integers which are coprime to each other and are (publicly) assigned by a *certifying authority* to $O, D_1, \ldots, D_k$ and C respectively. The joint watermark information of these parties is the solution I of the following set of $k+2$ congruences:

$$I \equiv r_i \mod n_i, \text{ where } i = 0, 1, \ldots, k+1. \quad (1)$$

The existence and uniqueness of I is guaranteed by CRT. I is computed as a sum $I = I_0 + I_1 + \cdots + I_{k+1}$, using the Garner's algorithm as follows. Let $J_i = I_0 + I_1 + \cdots + I_i$ for $0 \leq i \leq k+1$.

I_0 is computed by O using r_0 as follows.

1. $I_0 = r_0 = J_0$.

For $1 \leq i \leq k+1$, I_i is computed by D_i (if $i \leq k$) or C (if $i = k+1$) using $r_i, J_{i-1}, n_0, n_1, \ldots, n_i$ as follows.

1. $c \leftarrow 1$.
2. For $j = 0$ to $j = i-1$ do the following:
   • $u \leftarrow n_j^{-1} \mod n_i, c \leftarrow uc \mod n_i$.
3. $u \leftarrow (r_i - J_{i-1})c \mod n_i$.
4. $I_i = u \prod_{j=0}^{i-1} n_j, J_i \leftarrow J_{i-1} + I_i$.

The following proposition is a consequence of Garner's algorithm.

Proposition 3.1. *For $0 \leq i \leq k+1$, J_i computed above satisfies the following congruences:*

$$J_i \equiv r_j \mod n_j, \text{ where } j = 0, 1, \ldots, i. \quad (2)$$

The following sections will give the joint watermark embedding, watermark extraction and identification protocols.

3.3. The Joint Watermark Embedding Protocol

Let a content X reaches a consumer C from the owner O through k distributors $D_1, \ldots, D_k$. We fix any standard public-key cryptosystem such as RSA or ECC. Let (e_i, d_i) and $Cert_i$, where $i = 0, \ldots, k+1, L$ be the public-private-key pairs and the public-key certificate of the owner, the k distributors, the consumer and the licence server respectively. Let $Enc(.|K)$, $Dcp(.|K)$, $Sig(.|K)$ and $Ver(.|K)$ be the encryption, decryption, digital signature generation and digital signature verification algorithms (with key K) respectively. Let $Enc(x_1, \ldots, x_p|K) = (Enc(x_1|K), \ldots, Enc(x_p|K))$ and $Dcp(y_1, \ldots, y_p|d) = (Dcp(y_1|d), \ldots, Dcp(y_p|d))$.

Let $H(.)$ be any standard hash function such as SHA1 and $||$ be the concatenation operator. Let l_X be a unique copy number of the content X. In our scheme, r_i is generated by the party i as its digital signature. We define $r_i = Sig(H(H(X)||l_X)|d_i)$, where $0 \leq i \leq k+1$. Now the watermark embedding protocol is as follows.

The owner O does the following with license server L.

1. O computes $r_0 = Sig(H(H(X)||l_X)|d_0)$, usage license UL_0, redistribution licence RdL_0 and then encrypts as $Y = Enc(UL_0, RdL_0, J_0, n_0, H(X), l_X|e_L)$.
2. O sends, $(Y, r_0, Cert_0)$ to the licence server L.
3. L verifies $Cert_0$, decrypts Y using its private key as $Dcp(Y|d_L) = (UL_0, RdL_0, J_0, n_0, H(X), l_X)$, verifies signature r_0, and checks J_0 by verifying the Proposition 3.1. If all verifications pass through, it adds $(Cert_0, UL_0, RdL_0, J_0, n_0, r_0, H(X), l_X)$ to its database and notifies O.
4. O uploads (encrypted) content on content server CS_0.

For $1 \leq i \leq k$, any distributor in the i-th level D_i does the following with license server L.

1. D_i downloads (encrypted) content from CS_{i-1}.
2. D_i sends the request for the redistribution licence of D_{i-1} along with its public-key certificate $Cert_i$ to L.
3. L verifies $Cert_i$ and then sends to D_i, $Y = Enc(RdL_{i-1}, J_{i-1}, n_0, \ldots, n_{i-1}, H(X), l_X|e_i)$.
4. D_i decrypts Y using its private key as $Dcp(Y|d_i) = (RdL_{i-1}, J_{i-1}, n_0, \ldots, n_{i-1}, H(X), l_X)$.
5. D_i computes its usage licence UL_i, redistribution licence RdL_i, $r_i = Sig(H(H(X)||l_X)|d_i)$ and then J_i using the algorithm in Section 3.2.
6. D_i sends $Y = Enc(UL_i, RdL_i, J_i, n_i|e_L)$ and r_i to the licence server L.
7. L computes $Dcp(Y|d_L) = (UL_i, RdL_i, J_i, n_i)$, verifies signature r_i and checks J_i using Proposition 3.1. If all verifications pass through, it adds to its database $(Cert_i, UL_i, RdL_i, J_i, n_i, r_i)$ and notifies D_i.
8. D_i uploads (encrypted) content on content server CS_i.

A consumer C (DRM agent) does the following with license server L.

1. DRM agent downloads (encrypted) content from the content server CS_k of the distributor D_k (or owner).
2. DRM agent sends the request for the usage licence of D_k along with public-key certificate $Cert_{k+1}$ to L.
3. L verifies $Cert_{k+1}$ and then sends to C, $Y = Enc(UL_k, J_k, n_0, \ldots, n_k, H(X), l_X|e_{k+1})$.
4. DRM agent decrypts Y using consumer's key as, $Dcp(Y|d_{k+1}) = (UL_k, J_k, n_0, \ldots, n_k, H(X), l_X)$.
5. DRM agent computes $r_{k+1} = Sig(H(H(X)||l_X)|d_{k+1})$ and then $I = J_{k+1}$ using the algorithm in Section 3.2. It then sends $Y = Enc(I, n_{k+1}|e_L)$ and r_{k+1} to L.
6. L computes $Dcp(Y|d_L) = (I, n_{k+1})$, verifies signature r_{k+1}, and checks I by verifying Proposition 3.1. If all verifications pass through, it adds to its database the entry $(Cert_{k+1}, I, n_{k+1}, r_{k+1})$.
7. L sends $Y = Enc(UL_0|e_{k+1})$ to C.
8. DRM agent computes $Dcp(Y|d_{k+1}) = UL_0$ and opens the content using the keys in UL_0 and UL_k to get X.
9. DRM agent computes a watermark signal W from watermark information I computed by it in Step 5. The computation of W from I and embedding into the content X can be done using any robust watermarking technique.

3.4. The Joint Watermarking Extraction Protocol

We assumed that the watermark signal is generated and then embedded using any of the well known techniques with the only restriction that the watermark information I can be extracted out from the watermarked signal. Once I is extracted out, the identity of all the parties involved can be obtained by reverse computing the CRT equations as follows.

Suppose that we need to check whether a party with public parameter n_i (corresponding to CRT equation) and public key e_i was involved in the delivery chain of the content X with copy number l_X. First extract the watermark information I from the watermarked content using the extraction algorithm. Then, compute r_i from the equation, $I \equiv r_i \mod n_i$. Now,

check whether r_i is a valid signature of that party by checking whether $Ver(r_i, H(H(X)||l_X)|e_i) = 1$. If it holds we can conclude that this party was involved.

3.5. Security Analysis

In this section, we give the security analysis of our scheme. We keep the discussion brief due to space constraints.

Any of the existing known algorithms can be used for hashing, encryption, digital signature and watermarking with the only restriction that the watermark information I can be extracted out from the watermarked content.

The individual watermark information r_i are generated by the parties themselves as their digital signature. The license server verifies the individual watermark information r_i and the partial joint watermark information J_i and stores them in the database. This prevents collusion attacks. Further, the redistribution license of the i-th party will be accepted by the license server only if the verifications of r_i and J_i pass through. In the final stage, the license server verifies the watermark information r_{k+1} of the consumer and the joint watermark information I. The usage license of the owner is given to the DRM agent only if the verifications pass through. Thus the DRM agent will be able to open the content only if the joint watermark information I was correctly generated. The watermark signal W is generated from I and then embedded into the media by the DRM agent. The DRM agent is the owner's entity residing in a consumer's machine and performing actions on contents according to the usage licenses. Since DRM agent is a trusted entity representing the owner, we can assume that these steps will be carried out correctly. If not, the owner will not be able to trace the traitors if he finds illegal copies in the future as well as he will not be able to establish his ownership.

As we described in Section 3.4, if the owner/distributor finds an illegal copy of the content, he can easily identify all the distributors and the consumer involved in the distribution chain of that content by reverse computing the CRT equations. Similarly, with the same analysis the owner or distributors can always prove their part in the content distribution. Further, the scheme offers protection for parties who were not part of the delivery chain of the content against wrong identification or false framing as follows. Let n and (e, d) be the public parameters of a party. The accuser computes r from the equation $I \equiv r \mod n$, and checks whether r is a valid signature of that party by checking whether $Ver(r, H(H(X)||l_X)|e) = 1$ holds. However, this verification will fail as its success corresponds to the *existential forgery* of the signature $Sig(H(H(X)||l_X)|d)$, which is not possible as the underlying digital signature scheme is assumed to be secure.

The i-th party in the delivery chain gets the partial watermark information J_{i-1} and $H(X)$. The license server L can prevent the misuse of this information by i-th party by checking that J_i send to L by the i-th party was preceded by a sending of J_{i-1} by L to the i-th party. Further X can not be computed from $H(X)$ as it is a one way function.

In the tracing stage of the watermark, the original watermark information I is extracted out. The security issues in this case is not different from any other watermarking scheme.

4. CONCLUSION

In this paper, we have presented a novel joint digital watermarking protocol for the multiparty multilevel DRM architecture using Garner's algorithm for the Chinese remainder theorem (CRT). The proposed joint watermarking protocol is applicable for any DRM architecture. It takes care of the security concerns of all the participants by constructing a single joint watermark for embedding into the content. Further, in the event of finding an illegal copy of the content, the identities of all the parties involved in that content distribution chain can be traced back by extracting the joint watermark information. In future, we plan to improve the protocols to reduce the workload on the license server.

5. REFERENCES

[1] B. Hu, W. Ye, Sui-Li Feng, Xiao-Liang Wang, X. Xie, "Key distribution scheme based on two cryptosystems for hierarchical access control", Advanced Communication Technology, 2006. ICACT 2006, pp. 1723-1728, Feb 20-22, 2006.

[2] S. O. Hwang, K. S. Yoon, K. P. Jun, K. H. Lee, "Modeling and Implementation of Digital Rights", Journal of Systems and Software Vol. 73, Issue 3, pp. 533-549, 2004.

[3] W. Kanjanarin, T. Amornraksa, "Scrambling and Key Distribution Scheme for Digital Television", ICON, Proceedings of the 9th IEEE International Conference on Networks, pp. 140-145, 2001.

[4] N. Memon, P. W. Wong, "A Buyer Seller Watermarking Protocol", IEEE Transactions on image Processing, Vol. 10, No. 4, pp. 643-649, 2001.

[5] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC-Press, pp. 610-612, 1996.

[6] H. Muratani, "Optimization and Evaluation of Randomized c-Secure CRT Code Defined on Polynomial Ring", Information Hiding 6th International Workshop, IH 2004, Canada, pp. 282-292, May 23-25, 2004.

[7] A. Sachan, S. Emmanuel, A. Das, M. Kankanhalli, "Privacy Preserving Multiparty Multilevel DRM Architecture", Workshop on Digital Rights Management, 6th Annual IEEE Consumer Communications and Networking Conference, CCNC 2009, Jan.10-13, 2009.