Communications and Network, 2009, 1-55
http://www.scirp.org/journal/cn

Provable Secure Digital Watermarking Scheme

Zheng YUAN
Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, Beijing100080, China
Center for Advanced Study, Tsinghua University, Beijing 100084, China

Abstract: A novel provable security watermarking scheme was presented by adopting the digital watermarking technology, cryptology and encode method, it comprises embedding watermarks scheme and detecting watermarks scheme. The participant ID, Hash of the digital work and watermarking keys are regarded as the watermarks in the scheme, so that the watermarks can be used to authenticate lawful user and judge the ownership. The scheme has rigorously security almost against all watermarks protocol attacks. Especially, it has correct ability, as so as higher efficiency.

Keywords: DRM, watermarking scheme, watermarking protocol attack, provable security, RO mode

1 引 言

隨著網路通信技術的發展，數位作品的網上傳輸和交易日益頻繁，由於具有易被拷貝、分發、盜用和篡改的特點，使數位作品的版權保護問題日趨嚴重。尤其是對等（peer-to-peer）網路技術的發展和應用，使數位作品的版權保護問題更加突出[1]。版權所有者最早使用密碼技術保護自己的作品，在發送之前加密內容，把密鑰給了那些購買了作品的合法用戶，這樣盜版者即使獲得了加密後的作品，也無法使用。但是密碼技術只能保護傳輸中的內容，而作品一旦被解密就不再有保護作用。因此迫切需要一種替代或補充技術，在解密後仍能夠保護作品。而浮水印技術[2]能把資訊隱藏在數位作品中，可以防止非法拷貝、還可以認證作品、鑒別所有者、跟蹤操作等，所以浮水印技術越來越受到學術研究和商業機構的重視。

設計浮水印方案應能滿足以下條件。

頑健性：指合法用戶正常使用嵌入浮水印的數位作品時，浮水印仍然存在，也就是說浮水印方案要有抵抗常規處理的特性，如抵抗剪切、濾波、加噪、有損壓縮、可接受保真度處理等。

安全性：指浮水印方案有抵抗蓄意篡改的能力，常見的蓄意攻擊有：未經授權的載入攻擊（或稱偽造攻擊）、未經授權的檢測攻擊（或稱被動攻擊）、未經授權的去除攻擊和系統攻擊等浮水印協定攻擊。這 4 種攻擊的具體內容是：未經授權的載入攻擊有完整的和不完整的 2 類，完整的未經授權的載入攻擊是敵手必須對原始資訊進行編輯和嵌入。不完整的未經授權的載入攻擊是敵手設法獲得預先編輯好的合法資訊（而不是自己編輯資訊），並且將此資訊非法地嵌入到作品中去，通常敵手不需要瞭解資訊的編碼方法。未經授權的檢測攻擊有 3 種：第一種是敵手完全解碼，可以解讀出浮水印的具體含義；第二種是敵手只需要知道浮水印是否存在，而不需要知道浮水印編碼的具體資訊；第三種是介於完全解碼和僅僅檢測浮水印是否存在兩者之間，敵手可以區分對不同浮水印資訊進行編碼的不同標誌（即使不知道資訊內容），也就是說給定 2 個已加入浮水印的作品，敵手可以確切說出這 2 個作品各自的標誌是對相同的資訊還是對不同的資訊進行編碼。未經授權的去除攻擊包括 2 種，一種是敵手成功去除了作品中的浮水印，另一種是敵手對浮水印資訊進行了掩蓋，浮水印依然存在，但只能被比正在使用的檢測器更完善的檢測器檢測出來。系統攻擊是利用浮水印使用過程中的弱點進行攻擊，而不是浮水印本身的弱點如拷貝攻擊、歧義攻擊等。

性能：主要指浮水印方案具有認證作品，簽別所有者，保持和驗證作品的完整性，同時還能保證作品受到衰減後仍然能認證作品，簽別所有者等性能。

目前關於抗浮水印協定攻擊的安全數位浮水印方案的文獻較少，現有的方案還有一些不足，如文獻[3]的方案簽名資訊沒有求散列，又用 2 個簽名作為浮水印，嵌入浮水印資訊多，方案的頑健性就會減弱；文獻[4]的方案不能抵抗共謀攻擊；文獻[5]的方案將浮水印資訊的圖像進行 Turbo 編碼嵌入圖像中，然後通過 Turbo 解碼密鑰恢復浮水印和載體圖像，該方案只適

用於圖像；文獻[6]研究了允許公開檢測條件下不被非法刪除或修改的數字浮水印方案，這些方案沒有考慮共謀攻擊和拷貝攻擊等問題；文獻[7]的方案不能抵抗共謀攻擊和未經授權的檢測攻擊。文獻[8]研究了抵抗共謀攻擊方法，但沒有考慮去除攻擊等問題；文獻[9]提出了抗可逆性攻擊浮水印方案，但沒有考慮共謀攻擊等問題；文獻[10]對文獻[9]的浮水印方案進行了改進，並用了可證明健忘選擇證明其改進方案的頑健性，但是該方案也沒有考慮共謀攻擊等問題。

本文綜合考慮了設計浮水印方案應滿足的條件，提出了一種可證安全的數字浮水印方案，方案中根據數位作品的類型和特點，選取適當的頑健性非對稱密鑰浮水印演算法，保證了方案的頑健性。方案中把作者、版權管理機構、載入驗證中心和購買者等有關實體的 ID、作品的雜湊值和浮水印密鑰作為浮水印資訊，結合了密碼學知識和編碼知識，保證了數位浮水印方案的安全，提高了方案的性能。本文用可證安全性理論[11]和隨機預言(RO)模型方法[12]證明了該浮水印方案的安全性，該浮水印方案可以抵抗目前所有的浮水印協議攻擊，尤其是方案具有很好的糾正恢復能力。

2 可證安全數位浮水印方案

為了描述方便，設定下列符號。

W/M: 數位作品 / 數位作品的版權資訊；$W_M/W_{M'}$: 有合法版權資訊的數位作品 / 有偽造版權資訊的數位作品；

ID_X: 身份標識，X 指某個通信實體或某個物件，如作者 A 的身份標識 ID_A、版權管理機構 R 的身份標識 ID_R、載入驗證中心 T 的身份標識 ID_T、購買者 B 身份標識 ID_B 等；另外用 ID_W 表示作品惟一標識號；

h: 任選的一個安全雜湊函數；

E/D: 一個安全的加密演算法 / 解密演算法；

p_X/q_X: 公鑰/私鑰對，X 指某個通信實體或某個對象，如作者 A 的公鑰/私鑰對 p_A/q_A；

$Sigq_X/Verp_X$: 某個通信實體或某個對象 X 進行簽名和驗證，其中簽名后信息長度為 n;

σ/σ^{-1}: 二進位安全編碼運算/解碼運算；

K_1/K_2: 嵌入數位浮水印的密鑰 / 提取數字浮水印的密鑰。

2.1 提取嵌入浮水印方案

不失一般性，假設作者 A 創作數位作品 W 後，在版權管理機構 R 註冊，由版權管理機構負責管理數位作品，由載入驗證浮水印中心 T 負責嵌入和驗證浮水印資訊。該數位浮水印方案的嵌入數位浮水印過程如下。

1) 作者 A 將作品作者資訊 $h(W\|ID_A)$ 簽名後，傳給載入驗證浮水印中心 T。

$$s_1 \leftarrow Sig_{q_A} h(W \| ID_A)$$

$$\mathrm{T} \leftarrow (h(W \| ID_A), s_1) \quad (1)$$

2)載入驗證浮水印中心 T 驗證 $h(W\|ID_A)$ 正確後，從數位浮水印候選演算法庫中選取一個有效的頑健性非對稱密鑰浮水印演算法(包括 Embed 演算法和 Detect 演算法)，選擇嵌入浮水印密鑰 K_1 及提取浮水印密鑰 K_2，並計算浮水印資料 M，然後將 M 加密成密文 C。

$$s \leftarrow Sig_{q_T}\left(ID \| h\left(ID \| K_1 \| K_2\right) \oplus h\left(W \| ID_A\right)\right)\right) \quad (2)$$

$$M \leftarrow \sigma\left(ID \| h\left(ID \| K_1 \| K_2\right) \oplus h\left(W \| ID_A\right)\right) \| s \quad (3)$$

$$C \leftarrow E_{p_T}(M) \quad (4)$$

其中:沒有購買者 B 時: $ID \leftarrow ID_W \| ID_A \| ID_T \| ID_R$；

有購買者 B 時：$ID \leftarrow ID_W \| ID_A \| ID_T \| ID_R \| ID_B$ 。

3) 載入驗證浮水印中心 T 在數位作品 W 中嵌入浮水印密文 C，即

$$W_M \leftarrow \mathrm{Embed}\ (W, C, K_1) \quad (5)$$

提取驗證浮水印方案包括驗證浮水印資訊 M、驗證數位簽名 s、驗證身份標識資訊 ID、驗證作品作者資訊 $h(W\|ID_A)$和嵌入提取驗證數字浮水印的密鑰 K_1/K_2 。

2.2 提取驗證浮水印方案

1) 載入驗證浮水印中心 T 用提取浮水印演算法 Detect 和密鑰 K_2 從作品 W_M 中提取出浮水印密文 C，解密得到浮水印資訊 M，然後與備份資料庫中保存值比較，若相同，就認為 M 正確。

$$C \leftarrow \mathrm{Detect}(\ W_M\ , K_2\ ) \quad (6)$$

$$\mathrm{M} \leftarrow D_{q_T}(C) \quad (7)$$

2) 令 M 的長度 $|M|=l$，$s \leftarrow Sig_{q_T}\left(ID \| h\left(ID \| K_1 \| K_2\right) \oplus h\left(W \| ID_A\right)\right)\right)$的長度$|s|=n$。載入驗證水印中心T取$M$的前$l-n$位$M_1^{l-n}$，解碼$M_1^{l-n}$ 。

$$ID\left\|\left(h\left(ID\right\|K_1\|K_2\right)\oplus h\left(W\right\|ID_A\right)\right)\leftarrow\sigma^{-1}\left(M_1^{l-n}\right) \quad \textbf{(8)}$$

3) 若載入驗證浮水印中心 T 驗證 s 正確，即：$Ver_{p_T}(s)=Ture$，則接受 $ID\|(h(ID\|K_1\|K_2)\oplus h(W\|ID_A))$，並認為 ID 正確，然後從備份資料庫中找出 $K_1,K_2,h(W\|ID_A)$，驗證並計算正確，該作品合法，結束。

4) 若載入驗證浮水印中心 T 驗證 s 不正確，即：$Ver_{p_T}(s)=False$，則比較簽名 s 和安全編碼 σ 中 2 個 $ID\,\|\,(h(ID\,\|\,K_1\,\|\,K_2)\,\oplus h(W\,\|\,ID_A))$ 的描述，先分別驗證其中包含的 $ID, h(W\|\,ID_A), K_1$ 和 K_2 是否相同。

例如在比較 ID 時，對 2 個描述中 ID 進行模糊比較，計算 2 個描述之間的相關性並將其一與某一閾值做比較，模糊匹配，就認為 ID 相同。同理，若 $h(W\|\,ID_A)$, K_1 和 K_2 都模糊匹配，重新計算 $ID\,\|\,(h(ID\,\|\,K_1\,\|\,K_2)\,\oplus h(W\,\|\,ID_A))$，這可能會與簽名 s 中的值不同，但證明簽名 s 有效，該作品合法，結束。

若 2 個 $ID\,\|\,(h(ID\,\|\,K_1\,\|\,K_2)\,\oplus h(W\,\|\,ID_A))$ 的描述中 $ID, h(W\,\|\,ID_A), K_1$ 和 K_2 至少有一對模糊不匹配，則簽名 s 無效，該作品是贋品，結束。

3 安全性分析

3.1 共謀攻擊的安全性[8]

不同的購買者有不同的身份標識，所以式(3)中的 ID 可以不同，也就是說該方案給同一作品 W 嵌入浮水印，可能產生不同的浮水印資訊，假設有 m 個包含不同浮水印資訊的數位作品 W_{M_1}, W_{M_2}, … , W_{M_m}，若敵手獲得這 m 個作品，或者擁有這 m 個作品的人實行共謀攻擊，獲取原始數位作品的精確近似，旳簡單的方法可能是計算這 m 個作品的平均，即

$$\overline{W}_M\leftarrow\frac{W_{M_1}+W_{M_1}+\cdots+W_{M_m}}{m} \quad \textbf{(9)}$$

由式(3)得：該浮水印方案中浮水印資訊 M 中包含共謀——安全碼 $\sigma\ (ID\ \|((\ \|\ K_1\ \|\ K_2)\ \oplus\ (\ \|\ ID_A\ ))$ [13]，使這 m 個作品中嵌入了一個獨特的安全碼字，$\overline{W}_M$ 也包含安全碼資訊，從中可以至少識別一個共謀者，所以該方案是抗共謀攻擊的。

3.2 未經授權檢測攻擊的安全性

根據 Kerckhoff 假設，任何人都可以知道浮水印嵌入演算法 Embed 和提取演算法 Detect，進行公開檢測。

若敵手公開檢測時得到了浮水印資訊的密文 C，由式(7)可知：敵手沒有載入驗證浮水印中心 T 的私鑰 q_T，不能得到浮水印資訊 M 及其包含的內容，所以該方案是抗未經授權的檢測攻擊的。

3.3 未經授權載入攻擊的安全性

定義 1 敵手 $\Re$ 用拷貝攻擊方法 CA[14]攻擊文中嵌入浮水印方案(WT)的優勢為：時間 $t_1(n)$內，$\Re$ 從有浮水印資料的數位作品 W_1 中成功拷貝了浮水印資料的密文 C，並嵌入到數位作品 W_2 中，使載入驗證浮水印中心 T 可以從數位作品 W_2 中正確提取出 C 的概率，即

$$Adv_{WT,\Re}^{CA}=\Pr\left[\begin{array}{c}W_1,W_2\in(1,0)^n\\ W_1'\leftarrow\mathrm{Embed}(W_1,C,K_1)\\ W_2'\leftarrow\Re(W_1',W_2,p_T,(p_X,q_X))\\ (C,W_2)\leftarrow T(W_2',K_2)\\ s\leftarrow T(C,p_T,q_T)\end{array}\right] \quad \textbf{(10)}$$

命題 1 存在敵手 $\Re$ 可以 $\left(t_1(n),Adv_{WT,\Re}^{CA}\right)$ 對本文的方案用拷貝攻擊獲得成功，則可以構造一個偽造者 Ψ 在 $(t_1'(n),Adv(n))$ 成功攻擊簽名方案 Sig_{q_X}，其中

$$t_1'(n)=t_{n_K}+2t_d+t_S+t_E+t_\omega+t_1(n)+o(n) \quad \textbf{(11)}$$

證明 令任意 (p_X, q_X) 為證明使用的密鑰對。

若 $\Re$ 可以 $\left(t_1(n),Adv_{WT,\Re}^{CA}\right)$ 用拷貝攻擊方法攻擊該方案，則可以構造簽名方案 Sig_{q_X} 的偽造者 Ψ，Ψ 身份標識 ID_Ψ，假設 Ψ 知道浮水印演算法和編碼運算 σ，則：

Ψ 運行系統參數，產生 n_K 長的嵌入浮水印密鑰 K_1 和提取浮水印密鑰 K_2，運行時間 t_{n_K}；Ψ 產生 2 個長度相同為 d 的不同資料作品 W_1 和 W_2，運行時間 2_{t_d}。

Ψ 任取 ID，用 (p_X, q_X) 進行隨機 RO 模型詢問後，得到 $h(W_1\,\|\,ID_\Psi)$ 和 $h(ID\|\,K_1\,\|\,K_2)$，再進行 RO 模型簽名詢問，運行時間 t_S。

Ψ 偽造載入驗證中心 T 對 $ID\ \|\ ((h(ID\ \|\ K_1\ \|\ K_2)\oplus h(W\,\|\,ID_\Psi)))$ 的簽名 s，運行時間忽略不計。

Ψ 計算浮水印資料 $M\leftarrow\sigma\,(ID\,\|\,(h(ID\|\,K_1\|\,K_2)\oplus h(W\,\|\,ID_\Psi)))\,\|\,s$，並用 T 的公鑰 p_T 加密 M 得密文 C，運行時間 t_E。

Ψ 由式(5)在 W_1 中嵌入密文 C 得 W_1'：$W_1'\leftarrow\mathrm{Embed}(W_1, C, K_1)$，運行時間 t_ω。$\Re$ 進行拷貝攻

擊: 從$W_1^{'}$中拷貝密文 C，嵌入到作品 W_2 中，得$W_2^{'}$：$W_2^{'} \leftarrow \Re\ (W_1^{'}, W_2, p_T, (p_X, q_X))$，$\Re$ 進行拷貝攻擊時間為 $t_1(n)$。

情況 1 $\Re$ 攻擊失敗, 載入驗證中心 T 不能從$W_2^{'}$中提取密文 C 或驗證簽名不正確，結束。

情況 2 $\Re$ 攻擊成功，載入驗證中心 T 用式(6)從$W_2^{'}$中提取得到浮水印資料密文 C，用式(7)解密得到浮水印資料 M，並驗證簽名 s 正確，旳後 T 正確輸出(W_2, s), 運行時間為 $o(n)$。因此, Ψ 可以用(p_X, q_X)在時間$t_1^{'}(n) = t_{n_K} + 2t_d + t_s + t_E + t_\omega + t_1(n) + o(n)$內成功偽造了 T 的簽名，偽造成功的優勢 $Adv(n)$ 就是$\Re$ 拷貝攻擊成功的優勢 $Adv_{WT,\Re}^{CA}$.

給定簽名方案 Sig_{qx}是不可偽造的, 所以該方案是抗拷貝攻擊的。除敵手外，作者、版權管理機構和合法購買者也不能將合法的浮水印資料嵌入到其他數位作品中拷貝攻擊。

3.4 系統攻擊的安全性

定義 2 敵手$\Re$ 用歧義方法 *ABMI*[15]攻擊本文的方案(WT)的優勢為：時間 $t_2(n)$內，$\Re$ 偽造浮水印資料 M' 並用 p_T計算其密文 C', 使載入驗證浮水印中心 T 從根本沒有嵌入浮水印密文 C'的數位作品 W 中, 提取出 C'並驗證正確的概率，即

$$Adv_{WT,\Re}^{CA} = \Pr\left[\begin{array}{c} W' \in (1,0)^n \\ W_1' \xleftarrow{No} \mathrm{Embed}(W, C', K_1) \\ W' \leftarrow (W, C', K_1) \leftarrow \Re(W, p_T, (p_X, q_X)) \\ (C', W) \leftarrow T(W', K_2) \\ s \leftarrow T(C', p_T, q_T) \end{array}\right] \quad \textbf{(12)}$$

命題 2 若存在敵手$\Re$ 可以$(t_2(n), Adv_{WT,\Re}^{AMBI})$ 用歧義方法成功攻擊本文的方案，則敵手 $\Re$ 可以$(t_2^{'}(n), Adv_2(n))$ 成功攻擊簽名方案 Sig_{qx}，其中

$$t_2^{'}(n) = t_{n_K} + t_S + t_E + t_2(n) + o(n) \quad \textbf{(13)}$$

證明 令任意(p_X, q_X)對為證明使用的密鑰，敵手 $\Re$ 身份標識 $ID_{\Re}$，假設 $\Re$ 知道水印算法和編碼運算 σ，$\Re$ 收到合法的數據作品 W 也知道其作者 F, 若$\Re$ 可以$(t_2(n), Adv_{WT,\Re}^{AMBI})$用歧義方法攻擊該方案, 則$\Re$ 可以偽造作品 W 的水印數據 M',也可以偽造簽名方案 Sig_{qx}，具體過程如下。

1) $\Re$ 運行系統參數，產生 n_K 長的浮水印密鑰 K_1 和 K_2，運行時間t_{n_K}。

2) $\Re$ 任取 ID 用(p_X, q_X) 進行隨機 RO 模型詢問後，得到 $h(W_1 \| ID_\Psi)$ 和 $h(ID \| K_1 \| K_2)$，再進行 RO 模型簽名詢問，運行時間 t_S。

3) $\Re$ 偽造載入驗證中心 T 對 $ID \| (h(ID \| K_1 \| K_2) \oplus h(W_1 \| ID_F))$的簽名 s，運行時間忽略不計。

4) $\Re$ 偽造水印數據 $M' \leftarrow \sigma(ID \| (h(ID \| K_1 \| K_2) \oplus h((W \| ID_F))) \| s$, 并用 p_T加密得 C'，運行時間 t_E。

5) $\Re$ 進行歧義攻擊，使載入驗證中心 T 從沒有嵌入 C' 的作品 W 中, 可以驗證出 C', 即: $W' \leftarrow (W, C', K_1) \leftarrow \Re\ (W, p_T, (p_X, q_X))$，歧義攻擊時間為 $t_2(n)$ 。

情況 1 $\Re$ 攻擊失敗，載入驗證中心 T 驗證 W' 中沒有正確 C'，結束。

情況 2 $\Re$ 攻擊成功，載入驗證中心 T 用式(6)和式(7)得到浮水印資料 M'，並驗證簽名 s 正確，旳後正確輸出(W, s)，運行時間為 $o(n)$。因此，$\Re$ 可以用(p_X, q_X)在時間$t_2^{'}(n) = t_{n_K} + t_S + t_E + t_2(n) + o(n)$內成功偽造了 T 的簽名, $\Re$ 偽造成功的優勢 $Adv(n)$就是$\Re$ 歧義攻擊成功的優勢 $Adv_{WT,\Re}^{AMBI}$。

給定簽名方案 Sig_{qx}是不可偽造的, 所以該方案是抗歧義攻擊的。

推論 根據命題 2，又由於浮水印資料 M 中的資訊需要計算散列值，而散列是不可逆的，所以本文的方案可以抵抗可逆性攻擊[9]。

3.5 未經授權去除攻擊的安全性

本文的方案選取了非對稱密鑰浮水印演算法，採用不同的嵌入數位浮水印密鑰 K_1 和提取數字浮水印密鑰 K_2。如同非對稱密鑰密碼演算法一樣，用非對稱密鑰浮水印演算法可以建立作品到其嵌入的浮水印資訊間多對一的映射，該映射產生嵌入同一浮水印資訊的所有作品的集合（即該浮水印資訊的檢測區域），這種集合還必須是產生頑健浮水印演算法的集合，即不同資訊的檢測區域必須具有頑健性，也就是說如果將映射為某一浮水印資訊的浮水印作品做輕微的改變，旳後得到的作品應該仍然映射為同一資訊。而浮水印作品做輕微的改變很難映射為同一資訊，所以敵手即使掌握了提取數位浮水印密鑰 K_2 也不能輕易刪除、修改或去除浮水印資訊。

從幾何角度分析，可以將這種非對稱密鑰浮水印演算法看作是對單個形狀（對於給定浮水印資訊的檢

測區域）建立兩個不同的描述，用嵌入數位浮水印密鑰 K_1 的描述使得在該形狀中找出一點（浮水印作品）非常容易，而這一點非常靠近形狀之外的一點（未加浮水印的原作）；用提取數字浮水印密鑰 K_2 的描述使得判定一點是否位於形狀之內非常容易，可是要找出形狀之外的鄰近點就非常困難，所以敵手即使掌握了提取數字浮水印密鑰 K_2 也不能輕易刪除、修改或去除浮水印資訊，否則檢測出錯。

4 其他性能分析

4.1 頑健性

本文的方案選取了頑健性浮水印演算法，可抵抗針對浮水印演算法的各種攻擊，根據文獻[2]可得，頑健性浮水印演算法可抵抗針對浮水印演算法的各種攻擊。

4.2 糾正恢復能力

在浮水印方案中，假如從嵌入浮水印到檢測浮水印之間受到衰減，浮水印資訊中包含的簽名內容必須是頑健的，否則即使有 1bit 發生改變，如式(2)中 ID，$h_1(W\| ID_A)$，K_1 和 K_2 中有 1bit 改變，散列值就會改變，最後使得驗證簽名 s 無效。

為此，本文的方案將簽名資訊 $ID\|(h(ID \| K_1 \| K_2) \oplus h(W\| ID_A))$ 進行了安全編碼，得到共謀安全碼 σ，在嵌入簽名 s 的同時還嵌入了 σ 碼，使得式(3)的浮水印資訊 M 中有 2 個 $ID\|(h(ID \| K_1 \| K_2) \oplus h(W\|ID_A))$ 的描述，其中 σ 碼中的描述更安全，作為精確描述，這樣電子作品信號尤其是電子簽名信號受到衰減，驗證簽名 s 無效時，用第 2.2 節 4)方法糾正，因此，該方案有很好的糾正恢復能力。

4.3 認證性和完整性

本文的方案由載入驗證浮水印中心 T 將浮水印資訊 M 簽名後加密，實現了 M 的認證性和保密性，也保證了 M 的正確性和完整性。

本文的方案將 $h(W\|ID_A)$作為水印信息的一部份，可以認證作品鑒別作者。

本文的方案將 ID 作為水印信息的一部份，可以鑒別數字作品所有者，跟蹤操作。

本文的方案將 K_1 和 K_2 作為水印信息的一部份，可以鑒別抵抗水印協議攻擊。

4.4 簽名安全性

本文的方案中將 $h(ID\|K1\| K2)$和 $h(W\|IDA)$的異或值作為浮水印資訊，而不是將二者鏈結，這樣既隱蔽了 $ID, h_1(W\| ID_A)$，K_1 和 K_2 的資訊，又提高了偽造簽名 Sig_{qx} 的計算複雜度。

令 ID 的長度$|ID|=f$，偽造者偽造 $s'\leftarrow Sig_{qx}(ID\|h(ID\|K_1\|K_2)\|h(W\|ID_A))$ 的計算複雜度約為 $2^{\frac{d}{2}f}$，而偽造 $s\leftarrow Sig_{q_T}(ID\|(h(ID\|K_1\|K_2)\oplus h(W \| ID_A)))$ 的計算複雜度約為 $2^{d\cdot f}$，提高了 1 倍。所以該方案中的數字簽名有較好的安全性，也增強了水印方案抵抗未經授權載入攻擊和系統攻擊的安全性。

4.5 不可知性

本文的方案中水印信息包含簽名信息是一個散列值，信息量比較小，不會增加信號的存儲空間和傳輸帶寬，具有很好的不可知性。

5 结 論

本文的數位浮水印方案用適當的頑健性浮水印演算法來抵抗各種浮水印演算法的攻擊，將加密、簽名、編碼技術結合起來並選取非對稱浮水印演算法來抵抗各種浮水印協定攻擊，文中還用可證安全性理論思想證明了該方案可以抵抗拷貝攻擊和歧義攻擊，也證明了該方案有較好的性能，尤其是採用了模糊匹配方法，對網路信號衰減進行了糾正恢復驗證。

由於目前還沒有真正找到導致敏感性攻擊等未經授權去除攻擊的基本安全性弱點，一些多對一的非對稱密鑰浮水印演算法[6]還不完善，還需要進一步研究其實現問題。

REFERENCES

[1] LIU Q, NAINI R S, SHEPPARD N P. Digital rights management for content distribution. Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003 (AISW2003). 2003. 49-58.

[2] LIN E T, ESKICIOGLU A M, LAGENDIJK R L, et al. Advances in digital video content protection. Proceedings of the IEEE, 2005, 93(1):171-183.

[3] KATZENBEISSER S, VEITH H. Securing symmetric watermarking schemes against protocol attacks. Proceedings of the SPIE vol. 4675, Security and Watermarking of Multimedia Contents IV. 2002. 260-268.

[4] LIU L G, CHEN X S, HU L. Digital copyright protection security schemes against protocol attacks. Acta of Sun-Yat-Sen University, 2004, 43(2):83-86.

[5] ZHANG Y, XIAO Y. Digital watermarking scheme based on Turbo code [EB/OL]. http://www.paper.edu.cn.

[6] TZENG J G, HWANG W L, CHERN I L. An asymmetric s ubspace watermarking method for copyright protection. IEEE

Transactions on Signal Processing, 2005, 53(2):784-792.

[7] ADELSBACH A, KATZENBEISSER S, VEITH H. Watermarking schemes provably secure against copy and ambiguity attacks. ACM Workshop on Digital Rights Management (DRM'03). Washington: ACM Press, 2003. 111-119.

[8] CELIK M U, SHARMA G, TEKALP A M. Collusion-resilient finger-printing by random pre-warping. IEEE Signal Processing Letters, 2004, 11(10)：837-865.

[9] YOO H, LEE H, LEE S, et al. Designated verification of non-invertible watermark. ISC'03. LNCS 2851, Berlin, Heidel-berg: Springer-Verlag, 2003. 338-351.

[10] SEKHAR M R, OKAMOTO T, OKAMOTO E. On designatedly verified (non-interactive) watermarking schemes [EB/OL]. http://eprint. iacr.org/, 2005.

[11] GOH E J, JARECKI S. A signature scheme as secure as the dif-fie-hellman problem. Proc of the Advances in Cryptology_EUROCRYPT 2003. LNCS 2656.Berlin, Heidelberg: Springer-Verlag, 2003. 401-415.

[12] BELLARE M, ROGAWAY P. Random oracles are practical: a para-digm for designing efficient protocols [EB/OL]. http://doi.acm.org/ 10.1145/168588.168596.

[13] MURATANI H. A Collusion-secure fingerprinting code reduced by Chinese remaindering and its random-error resilience. Proceedings of the 4th International Workshop on Information Hiding'01. Lon-don, UK: Springer-Verlag, 2001.303-315.

[14] KUTTER M, VOLOSHYNOVSKIY S, HERRIGEL A. The water-mark copy attack. Proceedings of SPIE. San Jose, California USA, 2000. 371-380.

[15] CRAVER S, MEMON N, YEO B L, et al Resolving rightful owner-ships with invisible watermarking techniques: limitations, attacks, and implications. IEEE Journal of Selected Areas in Communication 1998, 16(4): 573-586.

