データハイディングによるデジタル署名技術

1M－13

沼尾雅之　清水周一　森本典繁
日本アイ・ビー・エム株式会社 東京基礎研究所

1．はじめに

画像などのデジタルコンテンツ中に異なる情報を目立たないように埋め込む技術はデータハイディングと呼ばれ，デジタル情報の知的所有権保護などに有効な方法として注目を集めている．デジタルコンテンツは基本的に，ビット単位に簡単にコピーができてしまうために，いかに通信路上で暗号化しておいても，エンドユーザが復号化した時点でコピーすることは防げない．

しかし，こうしたコピーを検出できるような枠組み(システム)を作ることによって，不法コピーを抑制し，著作権を保護することは可能である．データハイディングでは，配布するデジタルコンテンツ中に所有者名や配布先ユーザ名などの情報を埋め込むことによって，所有権の主張や不法コピーの流通経路の特定に利用することができる．

また，ユーザ側から見た場合，受けとったデジタルコンテンツが本当に正規の所有者または供給者から来たものか，さらに，流通経路で改ざんされていないことの保証が欲しいことがある．これを実現するのがデジタル署名を応用した認証システムである．

図1は，デジタルコンテンツの流通経路上でのセキュリティ・システムの利用方法について示している．本稿では，こうしたセキュリティにデータハイディングを応用するためには，どんな条件が必要かを考察し，その上で，デジタル署名が可能なハイディング技術を紹介する．

2．セキュリティからみたハイディング技術

いうまでもなく，データハイディングによるシステムは，メッセージの埋め込みシステムとメッセージの抽出システムという２つのコンポーネントから構成されるが，この２つの関係をセキュリティの観点からみると，以下のような２つのレベルに分類される．

(1) 対象型：メッセージの埋め込みと抽出を同一アルゴリズムで行なうもの．これは，アルゴリズムを秘密にすることが必要であるため，システムの管理が大切であり，また，埋め込みはもちろんであるが，抽出が安全な場所でしかできないという制限がある．

(2) 非対象型：メッセージの埋め込みと抽出が異なるアルゴリズム，または，同一アルゴリズムでも異なるパラメータ(鍵)を使うもの．特に，公開鍵方式のように，後者のアルゴリズムまたは鍵から，前者のアルゴリズムまたは鍵が類推不可能な場合には，後者を公開することができる．

次に，メッセージとそれが埋め込まれる母体メディアとの分離不可能性(一体性)からは，以下の４つのレベルに分けることができる．

(1) メディア・メッセージ独立型: これは，埋め込み，抽出アルゴリズムがメディアおよびメッセージの内容にかかわらずに固定されている方法である．アルゴリズムは簡単になるが，攻撃に対して弱い．つまり，ある特定のハイディングメッセージの抽出がモニタされてしまうと，すべてのハイディングが破られてしまう．

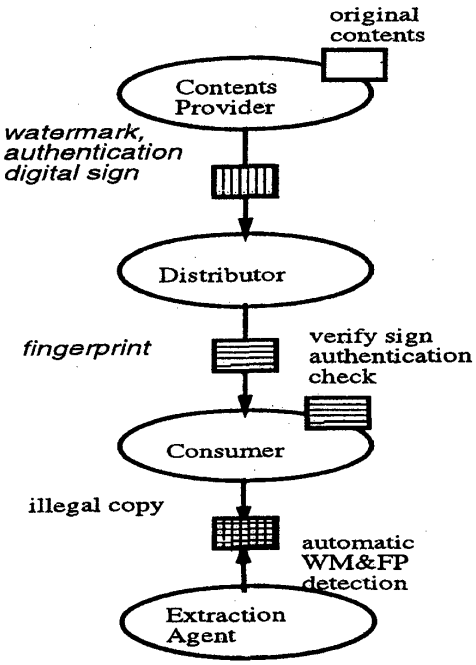

図 1: デジタルコンテンツの流通モデル

Digital Signature by Data Hiding.
Masayuki NUMAO, Shuichi SHIMIZU, Norishige MORIMOTO.
IBM Research, Tokyo Research Laboratory

(2) メディア依存・メッセージ独立型: これは，埋め込み，抽出アルゴリズムがメディアに依存して変化するものをいう．これもあるメディア上のメッセージ抽出がモニタされると，そのメディアに異なるメッセージを入れられてしまうという弱点を持っている．

(3) メディア独立・メッセージ依存型: これは，埋め込み，抽出アルゴリズムをメッセージに依存させたものであるが，上記と同様に，あるメッセージを異なるメディア上に入れられてしまう攻撃に弱い．

(4) メディア・メッセージ依存型: これは，もっともメディアとメッセージの間の一体性の高い方法であり，特定メディア上の特定メッセージの抽出方法がモニタされても，それを異なるメディアやメッセージに対しては利用できない．

3．データハイディングによるデジタル署名

3．1 公開鍵方式でのデジタル署名

公開鍵方式を利用したデジタル署名は，いろいろなバリエーションがあるが，もっとも簡単なものは以下のようになっている．

(1) まず，署名者 A は自分の秘密鍵 SK_A を保持し，公開鍵 PK_A を公開する．

(2) 署名者はメッセージ M を自分の秘密鍵で暗号化(署名) し，平文 M とともに検証者に送付する．

(3) 検証者 B は，署名されたメッセージを署名者の公開鍵で復号化し，それが平文 M と一致すれば，確かに署名者から送られたものと認定される．

3．2 列生成型データハイディング

上記のようなデジタル署名をデータハイディングに適用するには，2 節における非対象型アルゴリズムが必要であり，抽出アルゴリズムまたは鍵を公開しなければならない．その結果，特定メディア上の特定メッセージの抽出方法は常に明らかになってしまうので，偽の署名を防ぐためにはメディア・メッセージ依存型のハイディング法が必要であることが導かれる．

さて，このような条件を実現するものとしては列生成型ハイディング法がある．これは，まずメディア上の位置の系列を生成し，その位置にメッセージの系列を順番にハイディングしていくというものであり，

・列生成アルゴリズム

・メディア上の局所的ハイディング処理

の 2 つの要素に分けて考えられる．本稿では前者によるセキュリティ技術を議論する，参考文献 [1] では，後者の，目立たなく，かつ，JPEG などのコーディングや画像処理等に頑健なハイディング手法について議論している．

3．3 列生成アルゴリズム

さて，列生成アルゴリズムは以下の 2 点を満たすように構成すればよい．

(1) メッセージおよびメディア依存型列生成

(2) メッセージ埋め込み時の系列と抽出時の系列を異ならせること

(1) は例えば次のようにする．ここで，M は画像などのメディアの配列，m はメッセージの配列を示し，I, J をそれぞれ配列の大きさをとする．また，S_i を番目の状態変数，P_i を番目の位置変数とする．

$$P_i = S_i mod I$$

$$S_i = F_s(S_{i-1} \oplus m[i-1] \oplus M[P_{i-1}])$$

ここで F_s は状態推移関数,$\oplus$ は排他的論理和である．これによってメッセージとメディアの両方に依存した系列ができる．

次に，(2) は抽出時の系列を埋め込み時の逆順にすることを考える．まず，状態 i の時の埋め込みメッセージを以下のようにする．

$$m[i-1] \oplus M[P_{i-1}]$$

こうしておくと，状態 S_i から 1 つ前の状態 S_{i-1} は以下のように求められる．

$$S_{i-1} = F_p(S_i) \oplus X(P_i)$$

ここで，F_p は F_s の逆関数，また，$X(P_i)$ は状態 i での抽出メッセージ $(m[i-1] \oplus M[p_{i-1}])$ である．抽出メッセージから，実際に読み出すメッセージは次のようにすれば求められる．

$$m[i] = X_{i+1} \oplus M[i]$$

つまり，ある状態での抽出メッセージと次の状態でのメディア値との排他的論理和がメッセージの値になる．最後に得られたメッセージ列を逆順にすると本当のメッセージが得られる．

さて，F_p を公開鍵による暗号化関数，F_s を秘密鍵による復号化関数とすれば，前者を公開しても後者の安全は保たれる．さらに，状態変数の初期値を以下のように決めることによって逆方向のメッセージ埋め込みを防止する．

$$S_0 = H(m[i], 0 \leq i < J)$$

ここで，H は一方向ハッシュ関数とする．これによって，データハイディングによるデジタル署名ができる．

参考文献

[1] 清水他，“ピクセルブロックによる静止画像データハイディング” 情報処理学会第 53 回全国大会 1N-11, 1996.