M-97

電子透かし技術実装化におけるシステム構成とその応用

利根川聡子*1)、上條浩一*2)
日本アイ・ビー・エム 株式会社 ソフトウェア開発研究所*1)、東京基礎研究所*2)

1. はじめに[1]

ブロードバンド時代におけるデジタルコンテンツの急速な利用者数の増大に伴い、そのコンテンツの権利を証明する必要が高まっている。コンテンツの権利を主張する方法のひとつである「所有者証明」は、コンテンツが「所有者」のものであることを証明すると同時に「所有者」以外のものではないことを確定するものである。フォーマット変換が通常的に行われるデジタルコンテンツの「所有者証明」を行う手段としては、電子署名ではなく、電子透かし（不可視高耐性データハイディング技術[1]）が最適である。

本論文は、所有者証明を行うシステムの安全性を保障した当技術のシステム構築における課題の考察、及び、手軽さと正確さを有したコンテンツ所有者証明ツール（単独埋め込み器・検出器）の実装方法について報告する。

2. 電子透かし実装システムの課題

電子透かし技術が「所有者証明」を実現するためには、「所有者」のみがコンテンツ管理情報等の電子透かしをデジタルコンテンツへ埋め込むことができ、また、埋込コンテンツからは「所有者」以外の電子透かし検出は決して出ないという条件を満足させなければならない。そのためデータハイディング鍵（*Kdh*）の秘密性とコンテンツ管理情報の完全性の二項目について考慮する必要がある。

2.1 電子透かし鍵（*Kdh*）の秘密性

電子透かし技術は、埋め込み対象となるデジタルコンテンツ(*D*)を特定するための埋込データ(*ID*)を、電子透かし鍵(*Kdh*)を用いてスクランブルし、*D* の特性に合わせた電子透かし(*WM*)を作成する。次に *D* を表すバイナリデータを変更することにより *WM* を埋め込み、埋め込みコンテンツ(*D'*)を作成する。それらの関係式を次に示す。

$$WM=Scramble(ID,Kdh) \quad (1)$$

$$D'=DHembed(WM,D) \quad (2)$$

次に *D'*の所有者証明を実現するための検出では、*D'*から *WM* を抽出し、*Kdh* を用いて *WM* からスクランブルを解くことにより *ID* を検出する。

$$WM=DHdetect(D') \quad (3)$$

$$ID=Scramble^{-1}(WM,Kdh) \quad (4)$$

*D'*が埋め込みを行った所有者のものであることを証明する為には、他者による *D'*の偽装を防ぎ、なりすまし防止を行う必要がある。その為には、式(1), (4)からわかるように、*Kdh* は対称鍵であるため、*Kdh* の保護が必要となる。具体的には、*Kdh* が各所有者に対してユニークであり、かつ容易に類推できないことが必要となる。加えて、電子透かしの埋込器と検出器が別システムにある場合、*Kdh* の受け渡しについては、非対称鍵で *Kdh* を保護する方法を用いるなど、注意を払わなければならない。

2．2コンテンツ管理情報の完全性

通常、埋込データ(*ID*)は以下の式によりデータベースと連携する事によりコンテンツ管理情報を表現する。

$$ID=\{Info_1+Info_2...Info_n\} \quad (5)$$

検出プログラムにおいて *ID* を検出した場合、その内容として、コンテンツ管理情報{ $Info_1+Info_2...Info_n$ }を表示する。しかしその情報そのものが改変された場合、検出した *ID* が正しい場合でも不正情報となる。そのためコンテンツ管理情報と埋め込みデータの完全性の保護が必要となる。具体的にはコンテンツ管理情報のダイジェスト(*Hinfo*)をコンテンツ管理情報データベース内に保管し、管理情報を閲覧する場合、*Hinfo* とアクセスする管理情報から求められるダイジェスト値を比較することによって情報の完全性を検査し完全である情報に対してのみ閲覧を許可する。ここで *Hinfo* の算出には Hash 関数(6)が用いる。

$$Hinfo=Hash(\{ID, Info_1+Info_2...Info_n\},Kh) \quad (6)$$

正しいダイジェスト値（Hinfo）を算出できる権利を持つ者は、コンテンツ管理情報を所有する者と同等である。そのためここで使用する Hash 鍵 Kh は Kdh と同じでも良い。

3.電子透かし実装システムの構成

上記２で示した本実装システム構築で必要となる機能とその流れを以下に、図１にシステム構成図を示す。

3．1 埋込操作

1)「電子透かし鍵作成機能」で各所有者に対してユニークである鍵(*Kdh*)の生成を行い、電子透かし鍵データベースに保存する。

2)「コンテンツ管理情報作成機能」で管理情報(*Info*)とそれに対応する埋込データ(*ID*)のダイジェスト値(*Hinfo*)を鍵 *Kdh* を用いてを生成し、コンテンツ管理情報データベースに管理情報と *Hinfo* を保存する。

3)「コンテンツ管理情報検査機能」でコンテンツ管理情報データベース内の *Info* と *ID* から算出されるダイジェスト値とデータベース内の *Hinfo* を比較し、同じである *ID* を出力する。

4)「電子透かし埋込機能」は、データハイディグ埋込ライブラリを含み、1)の *Kdh*、3)の *ID*、外部入力である所有者証明を施したいデジタルコンテンツ(*D*)を入力とし、電子透かし付きコンテンツ(*D'*)を出力する。

3.2 検出操作

1)電子透かし検出ライブラリを含む「電子透かし検出機能」は、電子透かし付きコンテンツ(*D'*)を入力し、*Kdh* か

[1] Watermarking applied system using DataHiding technology
Satoko TONEGAWA, Koichi KAMIJO, Software Development Laboratory - Yamato (YSL) IBM Japan, Ltd., Tokyo Research Laboratory

ら *ID* を検出する。

2)「コンテンツ管理情報検査機能」は、1)の *ID* から導かれる *Info* を *Hinfo* を用いて検査した後、管理情報を出力する。

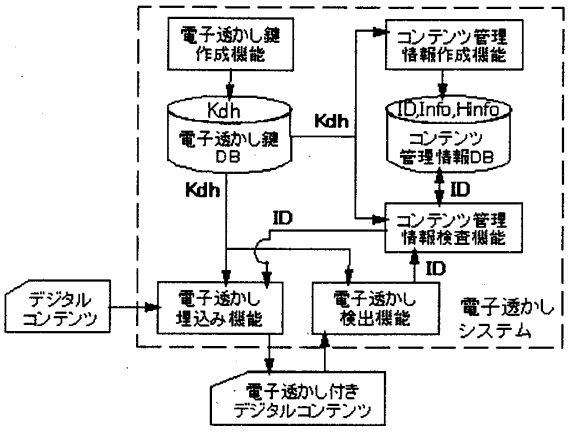

図１電子透かし実装システム構成図

4.単独埋込器の構成

上記３で示したシステムを所有し、所有者証明書を発行する登録証明機関が、コンテンツ所有者に証明書埋込装置を発行する場合、コンテンツ所有者個人の電子透かし鍵で埋め込みを実施する単独埋込器が必要となる。単独埋込器の構成は以下のようになる。

単独埋込器＝

[埋込アルゴリズム部]+[データ読込み部]+[データ部]

[データ部]には、コンテンツ所有者一人分の電子透かし鍵（*Kdh*）、埋込データ（*ID*）が含まれ、安全性を守るため次のように構成する。

[データ部]=

Encrypt[{Hash(<Kdh+ID>,Kh)+<Kdh+ID>}, Ke]

Hash はハッシュ関数であり、ハッシュ鍵 *Kh* で *<Kdh+ID>* のダイジェスト値を算出する。これにより、*Kdh* と *ID* の完全性が守られる。Encrypt は暗号化関数であり、暗号鍵 *Ke* で *Kdh*、*ID* と *<Kdh+ID>* のダイジェスト値を暗号化し、*Kdh*、*ID*、*<Kdh+ID>* のダイジェスト値の秘密性を守る。

[データ読込み部]では、[データ部]を復号化関数 Decrypt により *<Kdh+ID>* と *<Kdh+ID>* のダイジェスト値を復号する。

{Hash(<Kdh+ID>,Kh)+<Kdh+ID>}=

Decrypt([データ部],Ke)

次に *<Kdh+ID>* のダイジェスト値を算出し、復号化されたダイジェスト値と比べることによって、*<Kdh+ID>* の完全性を検査した後、式（1）、（2）で示した電子透かし埋込操作を行う。

暗号鍵 *Ke* とハッシュ鍵 *Kh* は登録証明機関から送付されるが、これらの鍵の受け渡しについては、非対称鍵等で保護する等注意を払わなければならない。

5.単独検出器の構成

上記３で示したシステムを所有し、所有者証明書を発行する登録証明機関が、コンテンツの価値を判断する所有者証明装置を第３者に発行する場合、コンテンツ所有者個人の電子透かし鍵で検出を実施する単独検出器が必要となる。単独検出器の構成を以下に示す。

単独検出器＝

[検出アルゴリズム部]+[データ読込み部]+[データ部]

ここで、コンテンツ管理情報と埋込データは複数存在するため、以下のように定義する。

$Data_1=\{Info_1+Info_2..Info_n\}_1+ID_1$

$Data_2=\{Info_1+Info_2..Info_n\}_2+ID_2$

：

$Data_m=\{Info_1+Info_2...Info_n\}_m+ID_m$

$Data=Data_1+Data_2+...Data_m$

[データ部]は、コンテンツ所有者一人分の電子透かし鍵（*Kdh*）と *Data* が含まれる。データの安全性とプライバシーを守るため以下のような構成になる。

[データ部]=

Encrypt[{Hash(<Kdh+Data>,Kh)+<Kdh+Data>}, Ke]

ハッシュ鍵 *Kh* で *<Kdh+Data>* のダイジェスト値を算出し、*Data* のプライバシーを守り、かつ、*Kdh*、*Data* と *<Kdh+Data>* のダイジェスト値の秘密性を守るため Encrypt を用いて暗号鍵 *Ke* で暗号化する。

[データ読込み部]では、まず[データ部]を復号化する。

{Hash(<Kdh+Data>,Kh)+<Kdh+Data>}

=Decrypt([データ部],Ke)

次に *<Kdh+Data>* のダイジェスト値を算出する事によって $Kdh, Data_1, Data_2...Data_m$ の完全性を検査した後、式（3）、（4）で示した電子透かし検出操作で検出された *ID* から求められるコンテンツ管理情報を表示する。

暗号鍵 *Ke* とハッシュ鍵 *Kh* は登録証明機関から送付されるが、これらの鍵の受け渡しについては、ワンタイムパスワード等を用い鍵の保護に注意を払わなければならない。また、単独検出器が登録証明機関から発行されたものであることの信憑性も確認する必要がある。[2]

6.まとめ

本論文では、不可視高耐性電子透かし技術が所有者証明を行うための課題を提起し、それらを考慮した実装システムは安全性を保障するものであることを示した。また実用化に不可欠な単独埋込器・検出器の概要を解説し、その構成方法を解明することにより、手軽さと正確さを有したコンテンツ所有者証明ツール作成の可能性を示すことができた。

電子透かし技術の更なる実用化のためには、「著作権件保護」「改ざん防止」「認証」「情報追跡・監視」「コピー制御」のための実装システム構築における考察が今後の課題である。

参考文献

[1]DataHiding
http://www.trl.ibm.com/projects/RightsManagement/datahiding/index.htm

[2]D.E.R.デニング：「暗号とデータセキュリティ」培風館