エレクトロニックコマース・セキュリティ特集

UDC ［681.324：343.45］：［343.98：681.325.3］

改ざん検出可能な電子透かし

Digital Watermark Technology for Image Alteration

須藤正之　Masayuki Sutou
三井靖博　Yasuhiro Mitsui

要　旨

昨今のインターネットビジネスの発展に伴い，マルティメディアコンテンツの著作権を保護する仕組みとして「電子透かし」が注目を集めている。本稿では，金融システムや電子政府システムなどにおいて，重要なイメージデータを不正改ざんから保護し，真正性を保証するための電子透かし技術を紹介する。

1．まえがき

デジタル化とネットワーク化が急速に進展している。デジタルデータは劣化せず編集も容易であり，しかもインターネット等を介して簡単に配信が可能である。その一方，デジタルデータは複製や改ざんも容易であるため，各種セキュリティ問題が深刻になりつつある。

デジタルデータを保護する仕組みの１つとして，データの中に情報を埋め込み利用する電子透かし（digital watermark）技術がある。最近，さまざまなマルチメディア・コンテンツの著作権を保護する仕組みとして注目を集め，研究開発が行なわれている[1)]。

一方，電子透かしは，重要な画像データなどに情報を密かに埋め込むことによって改ざんを検出し，不正を抑止する機能も併せ持つ。

本稿では，電子透かしの概要と当社および英国Signum Technology Ltdにおいて共同開発した改ざん検出可能な電子透かし技術について述べる。

須藤正之

システムソリューションカンパニー　情報技術開発センタ　技術開発第二部　セキュリティチーム　チームリーダ

三井靖博

システムソリューションカンパニー　情報技術開発センタ　技術開発第二部　セキュリティチーム

2．電子透かし技術の概要

電子透かし技術とは，いわゆるマルチメディアコンテンツなどのデジタルデータの冗長部分に人間には知覚できない，または知覚し難い変更を加えることにより情報を埋め込み，必要時に情報を抽出し，情報の有無や内容を，著作権情報やデータ変更の有無の確認などに利用する技術である。

デジタルデータを盗聴，改ざん等の不正から守るものとして暗号技術がある。暗号化によってデータ内容の秘密保持が可能であり，電子署名（およびメッセージダイジェスト）によって認証（及び改ざん検証）が可能である。しかし，暗号技術を利用した場合，暗号化したデータは安全であるが，そのままでは利用することができないので復号する必要がある。復号と同時にセキュリティのかかっていないオリジナルとまったく同じデータが再生され，不正者の攻撃にまったく無防備であり安全ではなくなる。また暗号化したデータは，明らかに暗号化されていることがわかり，重要なデータと認識され狙われやすい。

一方，電子透かし技術を利用した場合，透かしを埋め込んだ状態の画像データは通常の画像データとして利用することが可能であり，暗号技術を用いた場合には必要であった利用前の復号処理という追加処理の必

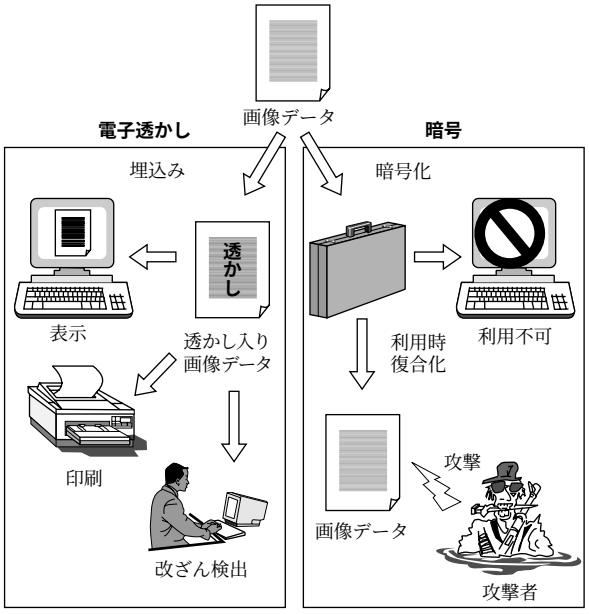

図１　電子透かし*v.s*暗号
Fig. 1　Digital watermark *v.s* cryptography

要がない。つまり，一度電子透かしを埋め込んだ画像は，そのままの状態で表示，印刷および種々の画像処理が可能であり，電子透かしを取除いた画像データを再生する必要がない。これは，イメージデータの利用容易性を損なわずにイメージデータのセキュリティを保つことができることを意味する(図１参照)。

電子透かし技術はさまざまなマルチメディアコンテンツへの適用方法が研究されている。DVDでは不正コピーを防止するために，電子透かしを用いて世代情報を埋め込み世代管理を行なう仕様を業界団体CPTWG (Copyright Protection Technical Working Group) のDHSG (Data Hiding Sub Group) で審議している。また，音楽配信向けの電子透かしでは，国際的な標準化団体 SDMI (Secure Digital Music Initiative) においてポータブルデバイスでのデジタル化された音楽コンテンツの著作権保護のために暫定的な仕様 (Phase１) が昨年策定され，「Phase２」と呼ぶ本格的な不正コピー防止技術の策定に向けて作業が開始された。

静止画像に対する電子透かしは，比較的古くから研究が行なわれている[2)]。特に著作権保護を目的とした電子透かしに関しては，さまざまな方式が提案されている。それらの特徴は電子透かしの存在を見破られ難く，切抜き・座標変換等の画像編集や，JPEG・MPEG圧縮等の圧縮で消去され難いことであり，耐性(電子透かしの消去され難さ)を向上させることを主目標に研究されている。

３．電子透かしによる画像改ざん検出技術

従来，画像データに対する電子透かし利用の目的としては著作権保護が一般的であったが，我々は，金融市場や電子政府など重要書類をデジタルデータ化して取り扱う機会の多い市場を睨み，改ざん検出のための電子透かし確立を目標として研究開発を進めてきた。

今回開発した電子透かしは，文書画像(２値画像)を含む静止画像用の電子透かしであり，改ざんを検出する基本アルゴリズムの改良を行なうとともに適用範囲を拡大すべく周辺機能を拡充している。

本電子透かしを用いると，電子透かし埋込み画像データと電子透かし鍵のみを用いて，画像データが改ざんされているかどうかを検証し，かつ，改ざんされている場合には，埋込み時に指定可能な小矩形である「ブロック」の単位で改ざん位置を特定することができる。検出可能な改ざんの最小サイズは１画素であり，確実に改ざんを検出することができる。

また，通常の著作権保護目的の電子透かしは画像データ全体に一律に埋め込まれるが，本電子透かしでは，埋込み領域サイズを自由に設定でき，かつ画像上の指定した複数領域に埋め込むことが可能である。また異なる鍵を用いて埋め込みを行なうことも可能である。このため帳票などの複数領域からなる画像を扱い，処理が複数の場所で連続的に行なわれるイメージワークフローシステムに適している。さらに，領域内の画質を考慮して埋込みパラメータを変えることが可能であり，対象画像に最適な埋め込みを行なうことができる。

表１に，改ざん検出のための本電子透かし，一般的な著作権保護のための電子透かしおよび電子署名の比較を示す。

鍵方式としては，埋め込む際と検証時に同じ電子透かし鍵を用いる共通鍵方式を用い，検証時に埋込み時に使用した鍵がなければ，検証を行なうことができない。

従来の電子透かしと同様にデータを埋め込むことも可能である。埋込み可能なデータのサイズは，画像形式，領域サイズとブロックサイズに依存する。120×

表１　技術比較
Table 1　Comparison of technologies

	電子透かし		電子署名
	本電子透かし	著作権保護	
機能	認証, 同一証明	著作権保護	認証, 同一証明
対象	静止画像 (文書画像等)	マルチメディア コンテンツ	デジタル データ
特徴	知覚困難	知覚困難	別データ
	分離不可	分離不可	分離可能
	改ざん検出 可能	改ざん検出 不可	改ざん検出 可能
	改ざん場所 特定可能	改ざん場所 特定不可	改ざん場所 特定不可
	データ量 変化なし	データ量 変化なし	データ量 増加

120画素の領域当たり，24ビット フルカラー画像であれば15×15画素のブロックサイズを用いて数千バイト，8bit インデックスカラー画像や4ビット画像であれば40×40画素のブロックサイズで数バイトのデータを埋め込むことが可能である。

図２は8ビットグレースケールの画像(サイズ；404×155画素) を対象に，電子透かし埋め込み・改ざん・改ざん検出を行なった例である。１番目の画像は全体に本電子透かしを埋め込んだ画像であり，電子透かし埋め込みによる画質変化は微少なため，印刷では見い出すことはできない。２番目の画像は，１番目の画像に汎用の画像操作ツールを用いて数字部分のカット&ペーストを行い，左の数字「1,336」を「3,336」に，右の数字「500」を「600」に改ざんした画像である。３番目の画像は２番目の画像に対して改ざん検出を行なった結果の画像である。２ヵ所の数字部分の改ざんが検出でき，改ざん位置がブロックサイズ単位で表示されている。この画像で使用したブロックサイズは15×15画素であり，３番目の画像に現れている改ざん検出表示では１つの四角を１ブロックとして表示している。

データ処理速度は画像形式および埋込みパラメータに依存する。詳細については現在評価調整中である。

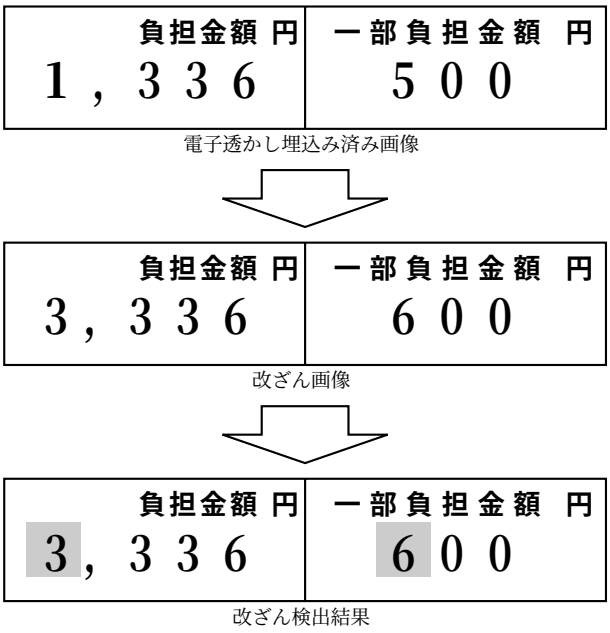

図２　改ざん検出例
Fig. 2　Example of detection for alteration

表２　本電子透かしの主な仕様
Table 2　Specifications of Oki's watermark

項目		仕様
画像形式	形式	BMP, JPEG
		JBIG2開発中
	画素サイズ	1, 4, 8, 24ビット
鍵方式	秘密鍵方式	埋込み・検証時同一鍵
埋込み	領域	サイズ可変
		複数領域可能
		ブロックサイズ可変
	メッセージ	サイズは領域サイズに依存
		文字, バイナリデータ
改ざん検　出	位置検出	ブロック単位
	検出数	すべての改ざんブロック
	最小改ざん	1画素

表２に，本電子透かしの主な仕様を示す。

４．適　　用　　例

銀行や保険・証券業界における業務処理のデジタル化や電子政府構想の進展に伴い，各種システム内での処理媒体は，これまでの「紙」から「電子データ」へ変遷しつつある。つまり，お金や物の売買に関する書類や，証明書類の画像など，改ざんによって価値が変化したり，誰かが不利益を被る画像データを扱う機会が増加している。

従来それらの書類は「紙」という「物」として原本性や真正性が保証されてきたが，いったんデジタルデータに変換されると原本保証が非常に難しくなり，コピーや改ざん等の不正を防止するシステムの構築が急務となっている。

そのようなシステムにおいて，改ざん検出可能な電子透かし技術を利用することにより，従来のイメージ処理システムを大幅に変更することなく，画像データに対する改ざんなどの不正を検出したり，防止することができる。つまり電子透かしを埋め込んだ画像データは，これまで通り画像データとして転送，閲覧，蓄積が可能であり，かつ必要時には画像データの電子透かし検証を行ない，改ざんの有無を調べることができる。また，画像データの改ざん検出だけでなく，電子透かし鍵と埋め込まれたメッセージを管理することによって，画像データや電子透かし鍵のすりかえを防ぐこともできる。

さらに，電子透かしを複数領域に分割して順次，独立して埋め込めむことが可能なため，ワークフローを利用した承認システム等の構築も可能である。

５．あ　と　が　き

改ざん検出可能な電子透かしを紹介した。現在，これをアプリケーションから簡単に利用できるようにするための各種ライブラリを開発中である。また，最新の国際標準フォーマットを扱うライブラリや高速処理が可能なボードの開発も予定している。

開発と同時に，今後，標準化の動向を見極め，積極的に標準化活動にも参加していく予定である。

６．参　考　文　献

1）高橋史忠：「電子透かし」がマルチメディア時代を守る, 日経エレクトロニクス, No.683, pp.99～124, 1997
2）松井甲子雄：電子透かしの基礎－マルチメディアのニュープロテクト技術－, 森北出版, 1998