電子透かしの現状と課題

高嶋洋一
ＮＴＴサイバーソリューション研究所

あらまし：インターネットの普及によりコンテンツ流通の発展が検討されているが、コンテンツの著作権保護を達成することが重要である。この一つの方法として考案されている電子透かし技術であるが、現状ではまだまだ解決しなければならない問題も多い。本稿では、現時点での達成度と残された課題を示す。

Watermarking Technology and Current Issues

Youichi Takashima
NTT Cyber Solutions Labs.

Abstract: Copyrights protection is one of the most important for content commerce over the network. Though watermarking technology is applied for a part of protection one, it has still remain some problems. This paper points out those problems and discuss about them.

1. はじめに

ネットワークの普及に伴い、デジタル化が進んでいる。デジタル化によって、オリジナルと同一のコピーを作ることが簡単になり、非常に便利になったが、一方、不正に複製することも容易になっているので製作者サイドの権利を保護する必要性が叫ばれている。ネットワークによる通信も蓄積メディアによる保存も一種の複製を作る行為であるので、これが正当であるかどうかを保証できるような機構が必要ということになる。

このような正当性を示すシステムが著作権保護システムであり、代表的な要素技術に暗号（署名を含む）技術と電子透かし技術がある。電子透かしとは、画像、映像、音声といったコンテンツに人間に知覚されないように、別の情報（透かし情報）を埋め込む技術である（図１参照）。コンテンツそのものに情報を埋め込むところに特徴があり、例えばヘッダに情報に埋め込む方法に比べ、フォーマット変換（AD->DA 変換も含む）されても透かし情報が残るところに特徴がある。そのため、暗号技術で通信路情報を保護した後、正当な（資格をもつ）利用者が不正に横流ししたような場合でも検出できるわけである。

透かし情報として、そのコンテンツの著作者情報や著作物使用条件などまたはその情報へのポインタ（リンク）を入れることもできる。また、利用者側の情報を埋め込むことにより、利用者を制限したり不正に利用されることを抑止したりする効果をもつ。

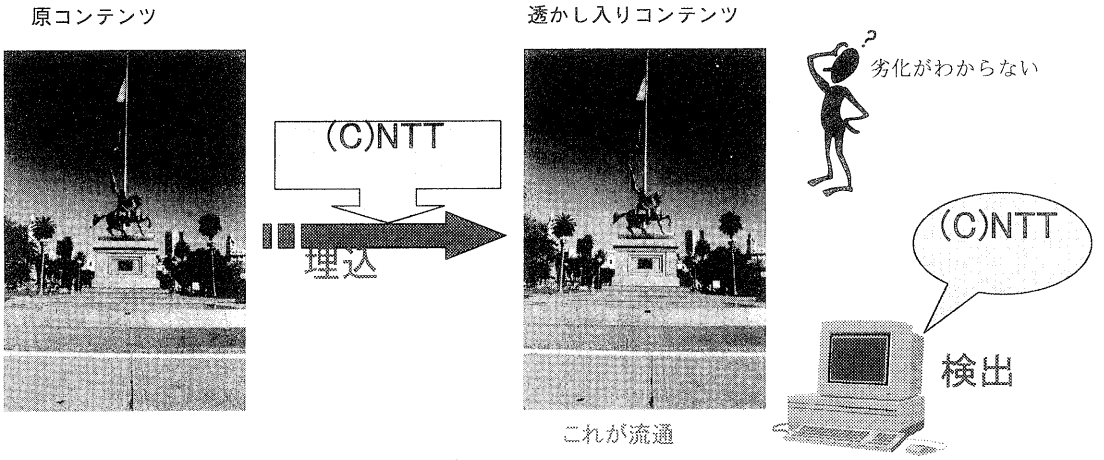

図1　電子透かしとは

本稿では、このようないろいろな特長を持つ電子透かし技術を中心に、現状の問題点を指摘し、将来の動向について述べてみることにする。
なお、著作権問題としては、制度的な問題や法律的な問題、運用の問題など種々雑多な問題が未解決であるが、それらに関してはここでは論じない。また、電子透かしの応用としては、著作権保護システムだけではなく、将来的に普及しそうなサービスの可能性を含めたアプリケーションも考えられる。それらの可能性についても触れてみる。

2.　電子透かしへの要求条件
一般に電子透かしに要求される条件は以下のとおりである。

2.1 コンテンツ品質
コンテンツのデータを書き換えるわけであるから、電子透かしを埋め込むことによってコンテンツの品質に必ず劣化が生じる。この劣化が利用者(人間)に検知されてしまうとコンテンツの商品としての価値がなくなってしまう。従ってこの劣化は人間に検知されない程、小さなものである必要がある。この検知限界を数値で表すことは難しく、もっぱら主観評価されている。

2.2 透かし情報量
埋め込む情報のビット数のことであるが、CPTWG(Copy Protection Technical Working Group)で定められたコピーフラグのように２ビットのものから、(埋め込まれるコンテンツの量にも依るが)数Kバイトの情報を埋め込むことも可能である。もちろん、埋め込まれるコンテンツのビット数より多くの情報を埋め込むことは不可能である。透かし情報量は多ければ多いほど良いが、他の要求条件とのトレードオフの関係にあるため、数十ビット程度としていることが多い。

2.3 計算量（処理速度）
透かしを埋め込む処理と透かしを検出する処理の２つがあるがあるが、高速であればあるほど優れている。ビデオや音楽といった時間軸にも制約の有るコンテンツの場合、実時間処理でできるかどうかは、ライブ放送に使えるかどうかの判断基準となる。

2.4 編集耐性
コンテンツ製作において編集作業が容易な点がデジタル化のメリットである。編集作業を行っても電子透かしが残ることが性能として望ましい。例えば画像を例に取ると以下のような耐性が望まれる。
（A）幾何学変換耐性
(1)　切り取り
(2)　回転
(3)　拡大縮小
(4)　射影変換
（B）非幾何学変換耐性
(1)　ノイズ付加
(2)　フィルタリング
(3)　圧縮

2.5 攻撃耐性
電子透かしを読み取れなくするとか、取り除いてしま

う、書き換えてしまうことを目的に透かし入りコンテンツを変換することを電子透かしに対する攻撃と定義すると、それに対する耐性も必要である。
(1) StirMark, Unzign
(2) リバースエンジニアリング
(3) 結託攻撃

2.6 相互接続性、更新可能性
暗号技術と似ているが、共通の電子透かしアルゴリズムを利用すれば、どの利用者（エンティティ）もその電子透かしを利用することができるのでどの利用者に対しても同じ透かしで済むため、インストールのコストを低く押さえられるメリットがある。反面、その透かしアルゴリズムが破られれば（透かしを無効にするアルゴリズムが発表されれば）、利用しているシステム全てが無意味（利用不可）となってしまう危険性も持っている。また、電子透かしアルゴリズムも対象コンテンツによって得手不得手があるので、利用者が利用するコンテンツによって電子透かしアルゴリズムを使い分けたほうが良いという意見もあり、いくつかの電子透かし方式を共存させながら、相互に利用できる方策が検討されている。
共通アルゴリズムであれば、それだけインストールすればよいのでコストがかからない。
さらに、透かし技術も年月その他によって陳腐化していくので、将来透かし装置を新しいものに置き換えていけるような余地を残しておくことも重要である。

3. 電子透かしの現状と問題
電子透かしは著作権保護システム実現への鍵を握っているが、それだけで何でも解決してしまう万能選手ではない。ここではいくつか指摘されている問題点を列挙する。

3.1 冗長度の無いデータへの電子透かし
不正コピー防止を目的として、例えば名簿データのようなものが流出した際、どこが流出元かを限定するために電子透かしを利用できないかといった依頼を受けることがあるが、コンテンツに相当する名簿データにそもそも冗長度が無ければ電子透かしを適用することは不可能である。

3.2 不正複製防止について
電子透かしを施しておけば、不正コピー防止が実現できるわけではない。不正コピーそのものを防ぐためには、コピーする手段に手を加えて、どの利用者もその制限付きのコピー手段を利用しなければならない状況に持っていく必要がある。電子透かしで実現できるのは、電子透かしをチェックすることにより、そのチェックしたコンテンツが不正に使われているかどうかを知ることができる（登録されている情報が正しいという糧が必要であるが）ということだけである。このことを事前に通知して、不正コピーの抑止を図ることはできる。

3.3 結託攻撃について
同じオリジナルのコンテンツに、異なる透かしを入れる場合、透かし入りコンテンツを何種類も集めてきて平均を求めることにより、オリジナルに近いコンテンツを得ることができる。これが結託攻撃である。同じコンテンツに利用者のＩＤを透かしとして埋め込むようなコンテンツ配信サービスでは、利用者が結託して、オリジナル（に近いもの）を得ることができるわけである。これを防ぐには、透かしを入れたことを示す（透かし情報によらない）共通の透かしパターンを透かしとして適用すればよい。

3.4 編集耐性について
ディジタルコンテンツの特性の一つに編集の容易性がある。従って、編集行為を行っても透かしが残っている必要がある。例えば、画像の場合、画面の一部を切り取って利用することは良く行われている。（人物の全体写真から、顔部分のみ切り出すなど） このような変換を施しても透かしが残っている必要があるが、例えば1ドットの画像に透かしが入る余地など無いわけだから、限界があることは明らかである。部分画像をどの程度まで意味があるとするかは非常に難しい問題である。人物写真のような場合、顔や目、鼻といったからだの一部分だけでなくつけているアクセサリに意味がある場合だってある。衛星写真などでは、ごく一部の地域のみ必要な場合だってあるだろう。
この意味を持つ部分画像というのは、明らかにそのコンテンツの利用者によって異なるわけであり、全てに満足するような透かし技術を作ることは無理なことである。実際には、透かし技術の切り取り耐性はそれほど優れておらず、まだ十分意味があると思われる画像ですら透かしが残らないことが多い。

3.5 圧縮耐性について
圧縮してコンテンツを伝送することも一般的に行われている。圧縮すれば、コンテンツの冗長度は一部取り除かれるわけであるから、電子透かしも取り除かれやすい。圧縮しても意味を持つコンテンツというのは、これもまた利用者によってさまざまなレベルがあるので、全ての利用者を満足させる電子透かしは不可能であろう。

3.6 攻撃耐性について
Stirmark, Unzign といったツールは電子透かし無効化ツールとして有名であるが、これらは現状の電子透かしの編集耐性に未熟な部分があるため、効率的に機能するのであるが、将来編集耐性が理想的な電子透かしができれば、この点は考慮しなくて済むようになるかもしれない。しかし、それまでは、攻撃ツールと電子透かしアルゴリズムとのいたちごっこが続くものと思われる。

3.7 公開性について
現状の電子透かしアルゴリズムの大半が非公開の物となっている。これは、暗号アルゴリズムが公開されて解読研究するのと対照的な事実である。実際、安全性を高めるためにアルゴリズムを公開し、強力な解読研究家の試練に耐えてこそ真の安全なアルゴリズムといえるのであるが、電子透かしの場合、暗号アルゴリズムに比べて、解読に要する計算量が小さく、まだまだ真の意味で安全ということが難しい。そのため、実用的なものは全てアルゴリズムそのものも非公開とし、企業秘密としている。

3.8 処理速度について
電子透かしの埋め込み処理と検出処理の２つに分けて考える。単純なモデルでは埋め込み処理より検出処理のほうが高速にできる。なぜなら、埋め込み処理側で検出処理を（ある意味）シミュレートして透かしを埋め込むからである。
しかし、編集耐性などの耐性が加わってくると検出処理もだんだん重くなってくる。すなわち編集されたコンテンツにどのような編集が加わっているかを検出し（全数探索を含む）、その後透かし情報を検出する処理となるからである。
つまり、高性能な電子透かしアルゴリズムを作ろうとすれば一般に計算量が多くなり処理速度は低下する。ライブ放送などの実時間処理が必要なサービスとコンテンツ品質、不正利用への安全性の確保のバランスが重要なのである。

3.9 改竄検出について
電子透かしを用いてコンテンツの改竄を検出するという話がある。電子透かし技術は編集耐性を高めて利用するというのを逆に編集耐性の弱い電子透かし技術とすれば、改竄されたときそれが検出できなくなるので改竄を検出できるわけである。
しかし、一般には改竄検出にはデジタル署名技術を用いることが望ましい。デジタル署名技術ならば、１ビットでも改竄すればそれを検出することができるが、電子透かしであれば、改竄されても電子透かしを検出できる場合もあるため、必ずしも機能しない。
圧縮された場合などを改竄とするかそうでないかという利用者の立場によっても異なるが、一般に電子透かしを改竄検出に用いることはセキュリティホールを作ることにもなる。

4. 標準化動向
電子透かしに関していろいろな標準化機関が検討している最中である。
(1) CPTWG (Copy Protection Technical Working Group)
DVD forum の下部組織で、透かしによるコピー制御（コピーフラグ）を最初に制定したところである。現在も、Galaxy グループ等が検討を進めている。
(2) JPEG[2]
ISO IEC/JTC1/SC29/WG1 のことで元々静止画圧縮技術による静止画フォーマットの標準化が中心である。ここの JPEG2000 では、電子透かしを組み込んだフォーマットも検討中。
(3) MPEG[3]
ISO IEC/JTC1/SC29/WG11 のことで、映像圧縮技術による動画（音声、ＣＧなど含む）フォーマットの標準化が中心である。電子透かしは、MPEG の検討項目ではないとされていたが、2000 年 10 月に、著作権保護技術でない電子透かしの標準化も検討することになった。
(4) SDMI (Secure Digital Music Initiative)[3]
音楽配信のための技術標準を策定している機関である。フェーズＩの透かしとして、ベランス社のものを用いることを決めているが、この度フェーズＩＩの透かしアルゴリズムを決めようとしている。この提案されている技術は、解読可能だとする意見があり、SDMI 側は解読コンテンストを行ったが、このコンテストでは、まだ破られていない透かし技術が残ったと SDMI 側は主張している。
しかし、コンテンストの評価自体も非公開で実際に安全なのかどうかはまだわからないというのが現状のようである。
このように、透かしの安全性に関する記事にはいろいろと憶測が多く現時点でどちらの主張が正しいかは不明である。

5. 電子透かしの応用
さて、ここでは著作権保護システムに限らない電子透かしの応用について紹介する。
デジマーク社[4]が一つの例を示しているが、雑誌に透かし入り画像（広告）を掲載し、それをカメラで取り込むことにより、透かし情報（URL）がとりだせ、簡単に Web ページへアクセスできるというものである。このように、実際の紙やモノとデジタル情報を結びつける技術として、電子透かし技術がある。今後、このような応用に関してさまざまなサービスが出てくるものと思われるが、ここでは割愛する。
また、透かし技術自体を共存させるため、cIDf（コンテンツＩＤフォーラム）[5]ではメタ透かし技術というのもある。これは透かし情報として、どの透かし技術を利用しているかの情報（透かし技術ＩＤ）を埋め込み、実際の透かし情報そのものは適用されている透かし技術により検出するというものである。これにより、透かし読み取りサービスなど、汎用的な透かしの利用方法が実現できる。

6. 電子透かしの今後
電子透かしの著作権保護としての利用には限界がある。電子透かしだけで実現することは困難で、他の技術との組み合わせが不可欠である。

また、公開鍵透かしというのも提案されている[6][7]。透かしを埋め込むことは、ある秘密情報を知っている者だけが可能であるが、透かしの検出は誰でもできるというものである。もちろん、アルゴリズムは公開でしかも偽造や改竄が困難なものである必要がある。

しかし、残念ながら実用的なものというレベルでは完成されたものはなく、今後の開発が期待される。

さらに、著作権保護に限らず適用する電子透かしのアプリケーションというもの出始めている。今後このようなサービスがいくつも提案されると予想でき、電子透かしの研究分野としては中心が徐々に移っていくように思われる。

参考文献

[1] http://www.jpeg.org
[2] http://www.cselt.it/mpeg
[3] http://www.sdmi.org
[4] http://www.digimarc.com
[5] http://www.cidf.org
[6]岩村、山口、今井："公開抽出情報を用いる電子透かし手法の提案"、コンピュータセキュリティシンポジウム CSS'98,pp.33-38(1998)
[7]山口、岩村、今井："誤り訂正符号を用いたアルゴリズム公開型電子透かし"、暗号と情報セキュリティシンポジウム SCIS99, No.T4-2.2, pp.713-718(1999)