マルチメディア著作権保護のためのPGPを用いたシグネチャーマスキング法

4L－10

松尾由起子　若井良重　佐野智子　芝野耕司
東京国際大学商学部所属

1　はじめに

現在インターネットの爆発的な普及で、マルチメディアを手軽に扱える環境が整ってきており、多くのユーザーがホームページなどの画像データを手軽に入手できるようになってきた。しかし、ほとんどのユーザーがコンピュータの使用上の制約に無知なため、インターネット上などで他人の画像データを簡単に入手して、それを作者に無断でそのデータをコピーし、第三者に配るといった悪質な著作権違反が増加してきている。このようなユーザは自分のやっていることがそんなに大変なことは思っていない。こういった状況のなかで、いかにしてそのマルチメディア著作権を守るかが問題になってきている。

2　既存の方法

現在ある著作権保護に関する方法には、データ・ハイディングと呼ばれる画像処理技術の手法が二つある。それは、ロー・ビット・コーディングとテキスチャ・ブロック・コーディングである。データ・ハイディングとは、著作権などを示す文字データを密かに埋め込んでおく技術である。これは、一見しただけでは原画像と区別が付かないが、実はあらかじめ各画素のビット列を少しだけ書き換えて、肉眼ではまったく分からないように画像中に文字データを埋め込んでおくことができる。そしてそれに特定の復元処理を施すと、隠されている文字データがくっきりと浮かび上がるものである。そして、そこから画像データを不正にコピーした人に“動かぬ証拠”として突きつけることができる、というものである。

3　既存の方法の問題点

ロービットコーディングの問題点としては、画像のデータが２５６色で描かれている場合は、文字データを埋め込んだ際に、８桁の数字の中で 1、つまり色が１段階ずれるだけなのでそんなに目立たないが、もしほとんど同一色で描かれているような簡単な画像の場合、最下位ビットの書き換えを行うと、１段階のずれであってもそのずれが目立ってしまい元の画像に影響が出てしまう。つまり、この方法は写真のようにたくさんの色を使う画像データには適用できるが、白と黒の２値画像データには適用できないのである。　また、非常に多くの情報量を埋め込むことができるが、画像を編集されてしまうと、文字が復元できなくなってしまうという問題点も上げられる。

また、テキスチャブロックコーディングは、原画像のある部分を切り出し、同じ画像の中で色似ている部分に張り付けるという手法だが、これは、写真や絵のように複雑に色がからみあった画像データの場合では、似た色がなかなかないため、データをうまく隠すことができない。

これらの点を解決するためには、色を変える部分を最小限にする必要がある。しかしこの場合、色があまり変えられなければ多くの情報を入れるのは難しい。

また、根本的な問題ともいえる、出力された版権自体に法的効力をおけるのかということである。普段の生活のなかで使用している自筆サイン等に比べると、その判定にあやふやな部分が残ることは否めない。

4　新手法の考察

前述の問題点の一つである適用範囲の狭さを克服するために、シートという新しい概念を使用する。

これまでのデータハイディングで埋め込むデータは、どうしても出力する文字の形をそのまま引きずっているといえる。そのため、その形に合わない部分を変えるのだが、すべての場合にその場所が変化可能とは限らないため、適用不可能なデータが多くあった。

そこであらかじめ埋め込むデータの位置を指定したデータをもつシートを作っておく。これにより、もってくるデータの位置を指定できるため、無理やり元の画像データを変える必要もなく、真下のデータ以外ももってこれるため、出力される版権の形にとらわれることもなくなる。

また、埋め込んだデータを出力させたときに、そのデータ自体が法的効力を持たないという問題に対

Signature Masking method to use PGP based for Multimadia copy right protection

Yukiko Matuo, Yoshie Wakai, Tomoko Sano, Koji Shibano
Tokyo International University, the department of commercial science

処するために、PGPの電子署名を利用する。具体的には、PGPのメッセージ要約関数MD５でメッセージ処理をして、１２８ビットの数を生成させ、暗号化された署名をつくる。この１２８ビットの数字は、画像データの画素の最下位ビットと共通するため、画像データに埋め込みが可能となる。　このシート方式の方法として、まず画像データの各画素の最下位（８列目）のビットを利用して文字データを付加する。そして、電子署名を表わす１２８ビットの数を読み込むことができるシートを画像データに合わせて、指定されたデータだけを順番に取り出す。そして取り出されたデータを、自分の公開鍵で元の電子署名に直す。

この電子署名は、そのデータが正真正銘本物であることを数学的に検証することができるため、これを埋め込むことにより、版権自体に法的効力が発揮される。

この方法を、電子署名を隠すという意味から、シグネチャーマスキング法と名付ける。

5　これからのデータハイディングの満たすべき条件

次に、データハイディングを満たすべき条件を以下に示す。

（１）埋め込むデータ

電子署名のように著作権者がはっきりと識別できるようなデータでなければならない。

（２）画像の圧縮

圧縮処理される場合に、排除されないデータを埋め込まなければならない。

（３）画像の減色

データを色のデータに埋め込む場合、減色による色のデータの改変を考慮しなければならない。

（４）画像の拡大・縮小

拡大・縮小時に一目で露見するようなデータではならなず、また、埋め込んだデータがこうした変換でも保持されなければならない。

（５）画像のデータ形式変換

データ形式変換が多数存在するため、どの変換方法で処理されても、残るようなデータでなければならない。

（６）画像の検知可能性範囲

検知可能性範囲を設定しなければ、埋め込むデータの範囲が決定できないため、早急に決定しなければならない。

そのためには、処理過程でシグネチャーを埋め込むのではなく、原画像自体にシグネチャーを埋め込む必要がある。そうすれば、データ形式変換がどのように行われても、シグネチャーのうける影響は少ない。だが、シグネチャーの埋め込みによって、画像データのクオリティーを落としてはならない。データハイディングとは、埋め込んだ文字データがユーザーに認識されてはならないからだ。だが、復元処理を施したときには確実にデータが浮かびでてくる必要がある。

マルチメディア著作権を保護するためにこれからのデータハイディングに求められることは、できる限り多くの画像変換処理に耐えうる手法であること。埋め込んだデータによって著作者の判別がはっきりとできること。また、画像無断借用可能な範囲をはっきりさせ、それ以上の部分にはデータハイディングの手法を使用しつつも、原画像のクオリティを落とすことのないものであることなどが挙げられる。

6　おわりに

ここでは、マルチメディア著作権保護のためにデータハイディングの手法とその評価基準について述べてきた。現在の段階でもインターネット等のマルチメディアは成長過程にすぎない。これからもこの様な進歩に拍車がかかっていくだろう。そしてそれらの発展に伴い、著作権保護へのよりレベルの高い技術が求められていく。

ここで述べたシグネチャーマスキング法については、今後、ここで述べた評価基準を基にした検証および改良をおこなっていく予定である。

参考文献

画像深層暗号ー手法と応用ー
松井甲子雄　著　　森北出版株式会社

IBM system journal
-techniques for data hiding-