

防衛大学校

情報工学教室

松井研究室

デジタル技術やネットワーク技術の急速な発展にしたがって、データがあまりにも簡単にコピーできるようになり、著作権が大きな問題となっている。法制度の整備も進んでいるが、技術的な仕組みも急速に進歩しつつある。それが、電子透かしの技術だ。松井教授は、この研究を始めて13年になり、現在の電子透かし技術の基礎を作った人である。



URL <http://www.nda.ac.jp/>

防衛大学校プロフィール
所在地
神奈川県横須賀市
走水1丁目10番20号

沿革
昭和27年、保安庁の付属機関として防衛大学校の前身となる保安大学校が設置された。昭和29年に、防衛大学校と名称を改めた。昭和59年の防衛庁設置法の改正によって、防衛庁管轄下の施設等機関になる。陸上、海上、航空各自衛隊の幹部自衛官となる人材を教育し、訓練するための機関として位置づけられている。

学生の身分は国家公務員で、宿舎での全寮生活をしながらの学生生活になる。

ネットワーク環境
学内ネットワークは100MのFDDIネットワークが設置されている。各建物内は各階ごとに10Mのイーサネットが結ばれている。学外接続は、64Kの専用線でWIDEの藤沢NOCにPPP接続している。現在、校外接続線が回線容量が不足しているため、現在容量増加に向けて準備中。



情報工学教室のホームページ
URL <http://cs.nda.ac.jp/>

電子透かしという研究を始めたきっかけを教えてください

今から13年くらい前に行った学会で、絵の中に文字を入れて暗号にするという研究が発表されていました。

しかし、その研究は文字を埋め込んだ絵を送り、同じ絵を持った人が、送られてきた絵と持っている絵の差分を取ると文字が浮き出てくるというものだったのです。

しかし、この方法は、送る情報の何倍もの情報を暗号化に費やしており、暗号化のシステムとしてよい方法と言えません。

そこで、それを改良した絵の中に文字を入れるという「見えない暗号」を作り出すと思ったのです。

見えない暗号とはどのようなものですか

見える暗号の場合、暗号文を電波で送るとすると、電波を傍受して解析すれば暗号部分を取り出して、それがどんな記号の羅列であれ見ることができます。見ることができれば、解読しようとする人が出てきます。その結果、暗号自体を公開鍵暗号のように

非常に複雑で堅牢にする必要性が出てくるのです。

これに対して見えない暗号は、電話で暗号文を送るとするならば、電話回線の空き帯域の中に暗号信号を入れるのではなく、電話の会話の中に暗号を埋め込むというものです。電話では普通にしゃべっているんだけど、その音声の中に別の意味を持った暗号を埋め込むのです。

「ああ、今日はいい天気だね」という普通の会話の中に、実は別の意味の言葉が埋め込まれている。これが見えない暗号なのです。

どういった仕組みになっているかという、人間の音声にしても、画像にしても“冗長度”という余分な部分を含んでいます。この冗長度の中に情報を埋め込むのです(図1参照)。

例えば、ファックスの中に別のファックスが入られるわけです。ファックスは、全体の文書をテレビの走査線のようにスキャンしたデータを、黒の部分と白の部分に分けて送ります。その白の部分のほんのわずかな量を、同じように黒の部分のほんのわずかな量を書き換えて情報を埋め込みます。受信したファックスは一見すると普通のファックスですが、その文字のぎざぎざの中に情報



暗号学はライフワークという松井甲子雄教授。



研究室には画像処理用の機材がずらり。ちょっと手狭だ。

が入っているのです。ファックスの場合、1つの点が0.12ミリですから、人間には埋め込まれた別の情報を見ることができません。専用の機具を使うことで初めて読むことができます。

と、13年前からこのような研究をしていました。これは「画像深層暗号」と呼ばれた研究です。日本ではあまり受け入れられていなかったのですが、MITの研究者が興味を持って、この画像深層暗号をインターネットの著作権保護に利用しようと考えたらしいのです。

そこで、私がアメリカに呼ばれて93年3月に講演を行ってから、この画像深層暗号が注目を集め、電子透かし技術が発展しました。当時は、外国にこういった論文はほとんどありませんでした。現在の電子透かしには、画像深層暗号のコンセプトがそのまま使われているのです。



電子透かしとはどんなものですか？

ここに2枚の同じ画像があります。どちらの画像もなんの変哲もない肖像画です。この2枚の画像を重ねるとある文字が浮かび上がります(写真あ)。これが画像の電子透かしです。このように、あるデータに見えない署名を入れておき、違法にコピーがされた場合に著作権者が、その署名を浮かび上がらせて著作権を主張できるようにするものです。

今は、2枚のフィルムを重ね合わせましたが、コンピュータのデータ上では、ある画像に鍵データを入れることで電子透かしが浮かび上がるような仕組みになっています。



どのようにデータの中に透かしを埋め込むのですか？

基本的には先ほどのファックスに埋め込んだ文字の仕組みと変わりません。例えば、画像ならばRGBの3つのデータがあります。



写真あ：これらの同じ画像の片方には見えないように情報が埋め込まれている。

図1：外側の文字を読んでも、内側の文字を読んでも、山という文字は読める。この文字の幅が冗長性だ。ここに情報を埋め込むことで、見えない暗号ができる。

この中の赤だけを取り出します。赤の中でもいくつかの階調に分かれて画像は構成されています。この中の一部分の階調のデータを拝借して、その中に文字データを埋め込むというわけです。拝借するといっても、ほんの一部分ですから画像の冗長性の範囲内です。画像の見目はまったく変わりません。

そして、埋め込んだデータがある方法で変換することで、どこに埋め込まれたのがまったく分からなくなります。そして、この変換の時にある乱数をかけます。これが、透かしデータを浮かび上がらせる鍵となるのです。これは一例ですが、現在さまざまなデータの埋め込み方式が研究されています。



電子透かしと公開鍵暗号には、どんな違いがあるのでしょうか？

電子透かし技術は、公開鍵暗号などの暗号技術と違うのは、破られる可能性が低いということです。公開鍵暗号などの暗号技術は、数学的な問題によってその堅牢さが保証されているものですし、そこに暗号があるという“見える”暗号なのです。それでは、破ろうとする人が多く現れるうえ、処理速度の速いコンピュータを使うことで破られる可能性が高くなります。

それに対して、電子透かしの技術は破るべき暗号を隠してしまう“見えない”暗号です。それによって、データに違った価値を埋め込むという目的のものです。

ここでは、埋め込まれた暗号を破って中の情報を取り出すというのは非常に困難です。しかし、もし新しい透かしを埋め込まれてしまうと、どちらが本物の透かしが分

からなくなってしまうという問題点があります。

そのためにもオリジナルデータの管理は必須ということになります。これはアナログな世界とまったく同じですね。



こういった電子透かしは、どのような目的で使われていくのでしょうか

大きく分けて4つあると思います。

1つは、著作権の保護です。これはすでに実用化されていますが、画像や音声の中に著作権者の署名を埋め込み、そのオリジナリティを保証するというものです。

ここからはまだ実用化の域に達してはいませんが、第2に購入者情報を埋め込むことが考えられます。ソフトの販売元などが販売先の情報を埋め込むということにも使えましょう。使用するソフトウェアに、いわゆるシリアルナンバーと販売先の情報を埋め込めば、誰がそのソフトウェアを使用しているのかが分かります。それによって違法なコピーを防ぐことができるのです。

3番目は、利用者情報を埋め込んで情報の履歴を管理するという目的です。例えば、ダウンロードしたファイルにダウンロード先のIPアドレスを埋め込むことによって、誰がいつファイルをダウンロードされたかを把握することができます。

4番目は、利用制限情報を埋め込むことです。もし、ある画像をコピーしたとします。コピーをしたとたんに、埋め込まれていたコピー禁止のマークが表示されてその画像は見ることができなくなるものです。このような形での違法コピーの禁止の手段になるはず



[インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

株式会社インプレスR&D

All-in-One INTERNET magazine 編集部

im-info@impress.co.jp