2007－CSEC－39（13）
2007／12／14

# 電子透かしに対する攻撃ツールの実装

神谷光佑　　森拓真　　岩村惠市
東京理科大学
〒102-0073　東京都千代田区九段北 1-14-1
E-mail：　iwamura@ee.kagu.tus.ac.jp

**あらまし**
近年，ディジタルコンテンツの不正コピーや改ざんを防止する為に，電子透かし技術が用いられている．電子透かしの強度を量る為には電子透かしに対する攻撃ツール（ベンチマークツール）が必要であり，Stirmark や JEWELS といった攻撃ツールが既に開発されている．しかし，既存の攻撃ツールは結託攻撃や平均化攻撃などの複数画像を用いた攻撃を効率的に行えない事や，コマンドラインベースのプログラムであるので扱っている画像ファイルを検証しながら作業できない事等から，機能が不十分であると考えられる．そこで本研究では，既存の攻撃ツールに対して上記問題点のない攻撃ツールを開発する事を目的とする．
**キーワード**　電子透かし，電子透かしに対する攻撃，ベンチマークツール

# Development of attack tool for the digital watermark.

Kosuke KAMIYA　　Takuma MORI　　Keiichi IWAMURA
Tokyo University of Science
1-14-1 Kudan-Kita, Chiyoda-Ku, Tokyo 102-0073, Japan
E-mail：　iwamura@ee.kagu.tus.ac.jp

**Outlone**
Technology of the digital watermark is used to prevent illegal copying and falsification of digital contents. The attack tool for the digital watermark (benchmark tool) is necessary to measure strength of the digital watermark. For example, Stirmark and JEWELS are already developed as the attack tool. But we thought that functions of existing attack tools are not enough. Therefore, this research is aimed at developing of attack tool for the digital watermark that has more excellent functions, which are supporting attacks using plural images and have graphical user interface and so on, than an existing attack tool.
**Keyword**　Digital watermark , Attack to digital watermark, benchmark tool

## 1．はじめに

近年，コンピュータ関連技術やネットワークインフラの発達に伴い，従来は紙やＣＤ等の媒体に記録した状態で取引されていた画像や音楽等がコンテンツ配信サービス等を通じてディジタルデータだけの姿で取引される事が増えている．このようなディジタルコンテンツはコピーや改ざんが簡単に行えるので，コンテンツの購入者が不正コピーして再配信するような事が起こりやすい．　そのような行為から著作者の正当な利益を保護する為に，不正コピーの防止や，不正コピーの証拠となる為の技術である電子透かし[1]が用いられている．

電子透かしとはディジタルコンテンツのデータを一部変更する事で著作権情報や改ざん検出情報等，元のコンテンツとは別の情報を埋め込む技術である．　電子透かしは静止画，動画，音声等，様々な種類のコンテンツに埋め込む事ができるが，本稿では静止画像のみを対象として考える．

コンテンツの不正利用や改ざんを防止する手段として電子透かしを使う場合，電子透かしが攻撃に対してどの程度の強度を持つかが問題とな

る．　電子透かしの強度を評価する為には実際に攻撃を行って電子透かしが壊れないかどうかを見る方法が一般的であり，その為に Stirmark[2] や JEWELS[3]といった攻撃ツールが開発されている．しかし，それら従来の攻撃ツールはコマンドラインベースなので画像ビューワと連携していない事や，単一画像による攻撃の機能に重点を置いている事など，機能が不十分であると考えられる．

そこで本研究では上記のような問題を解決した攻撃ツールを開発・実装することを目的とする．このツールは単一画像攻撃と複数画像攻撃の両方の機能を持ち，扱っている画像を画面に表示しながら連続的に攻撃を実行してゆく事ができる．

本稿では２章で電子透かしに対する攻撃と従来の攻撃ツールを，３章で本研究における攻撃ツールの開発方針を，４章でその実装を説明し，５章においてその評価結果の例をいくつか示す．

## ２．電子透かしに対する攻撃と従来の攻撃ツール

### ２．１　電子透かしに対する攻撃

電子透かしが埋め込まれたコンテンツに対して何らかの操作をして透かし情報を読み出せなくする事を「電子透かしへの攻撃」と呼ぶ．　ここで言う攻撃とは，透かし情報を読み出せなくしようという意図で行われる各種の操作の他に，JPEG 等による圧縮や，画像の一部分を切り取る（トリミング）等の一般的な画像処理も含まれる．

### ２．２　電子透かしに対する攻撃の種類

静止画像に埋め込まれた電子透かしへの攻撃は，大きく分けて単一画像を用いた攻撃（以後，単一画像攻撃）と複数の画像を用いた攻撃（以後，複数画像攻撃）の２種類がある．

単一画像攻撃とは 1 枚の透かし入り画像を用いる攻撃を指し，具体的には JPEG 等による圧縮，トリミング，拡大，縮小等の画像処理がある．

複数画像攻撃とは，２枚以上の透かし入り画像や，原画像と透かし入り画像の組み合わせ等の複数の画像を用いて行う攻撃を指し，具体的には各画像の画素値の平均を出力画像の画素値とする平均化攻撃[1]や，各画像の比較をして透かしの埋め込み位置を探る結託攻撃[4]などがある．

### ２．３　電子透かしに対する攻撃ツール

電子透かしの強度を評価するツールとして Stirmark と JEWELS の２つが有名である．

**（１）Stirmark**

Stirmark は 1998 年に Cambridge 大学で開発されたソフトで，2007 年 10 月現在，第４版が最新版である．　Stirmark はノイズ付加や回転などの画像処理を行うソフトで，パラメータを細かく設定できるのが特徴である．　これらは全て単一画像攻撃であり，複数画像攻撃の機能は無い．また，Stirmark はコマンドラインベースのプログラムであり，攻撃の出力画像を見る為には別に画像エディタを開く必要がある．

ここではページ数の関係で詳細は省略するが，詳細を知りたい場合は[2]を参照して頂きたい．

**（２）JEWELS**

JEWELS は 2000 年に電子情報技術産業協会で開発されたソフトであり，Stirmark 同様に画像に対して各種の攻撃的画像処理を行う．

JEWELS も Stirmark と同様，主に単一画像攻撃を行うツールであり，複数画像攻撃の機能は「重ね合わせ」１つだけである．また，Stirmark 同様コマンドラインベースのプログラムである．

詳細を知りたい場合は[3]を参照して頂きたい．

## ３．攻撃ツールの開発方針

この章では，本研究で開発・実装する電子透かし攻撃ツールの開発方針について述べる．

**（１）単一画像攻撃の機能は従来のツールの機能を利用する**

２章で述べた Stirmark や JEWELS は単一画像攻撃については多種多様の機能を持っており，攻撃のパラメータ（例えば JPEG 圧縮なら圧縮

率, ノイズ付加ならノイズの濃さ) も設定できる.

本攻撃ツールでは, その攻撃の多様性を生かし, また既存ツールとの互換性を持たせる為に単一画像攻撃の機能は Stirmark や JEWELS の機能を利用する. すなわち, 本攻撃ツールから Stirmark や JEWELS の機能を直接呼べるように攻撃ツールを構成する.

**(2) 従来の攻撃ツールに不足している複数画像攻撃の機能を充実させる**

複数画像攻撃の機能は Stirmark には無く, JEWELS には1つだけである事から, これらはどちらも単一画像攻撃に重きを置いたツールであると言える.

しかし, 電子透かしへの攻撃者が複数画像攻撃をしない保障は無いので, 電子透かしは複数画像攻撃への耐性も持っていなければならない. よって, 電子透かしの強度を評価するための攻撃ツールにも, より充実した複数画像攻撃の機能が必要だと考える. そこで本攻撃ツールには, 平均化攻撃と差分攻撃を実装する.

**(3) 視覚的なユーザインターフェースの実装**

Stirmark, JEWELS どちらのソフトウェアもコマンドラインベースのユーザインターフェース(CUI)である. 視覚的ユーザインターフェース(GUI)に比べて CUI はグラフィックにリソースを割かずに済むのでプログラミングがしやすく, 動作速度も速いという利点がある. しかし GUI 開発環境の普及やコンピュータの高性能・低価格化が進んだ昨今の状況を考えると操作方法が直感的になる事や画像を表示しながら作業できる利点を持つ GUI の方が良いと考える.

また, 電子透かし攻撃ツールは画像処理を行うプログラムであるから, 攻撃を次々と実行する過程で画像がどのように変化して行くのか確認しながら作業できるようにする事は大変有意義である. よって本攻撃ツールでは2つの画像表示スペースを用意して入出力画像を表示できるようにする. また攻撃の出力画像を入力側に戻して次の攻撃処理を行い, その出力を再び入力側に戻し……といった事を繰り返して, 連続的に攻撃を行えるようにする.

**(4) その他**

現在は未実装部分が多いが, 今後は以下の機能を充実させていく予定である.

**(a) 電子透かし**: 今回はパッチワーク法[6]で符号化なしの透かしを埋め込む機能のみ実装済みだが, 今後は種々の電子透かし手法をその強度調査のために実装していく.

**(b) 入力/ECC**: 現在は未実装だが, 入力データを種々の誤り訂正符号で符号化した電子透かしを埋め込む機能を実装予定である.

**(c) 画像処理**: 電子透かし解析に有効と思われる種々の画像処理機能も追加予定であり, 現在はフーリエ変換のみ実装済みである.

## 4. 攻撃ツールの実装

### 4.1 開発環境

開発環境は「Microsoft Visual Basic 6.0」と「Microsoft Visual C++ 6.0」を併用している.

原則として, GUI やファイル入出力に関するプログラムは GUI の実装が簡単な Visual Basic で書き, 画像処理そのものはプログラムの動作速度が速い事や Stirmark と JEWELS が C/C++で書かれている事から C/C++で書く事にした.

### 4.2 GUI の実装

図1に開発した攻撃ツールの外観を示す. ウィンドウの中央に PictureBox (画像表示スペース) を2つ配置しており, 入出力画像はここに表示される. ファイルを開く, 攻撃を行う等の操作は画面上部のメニューバーから目的の項目を選んで行う. 各メニューの詳細を以下で説明する.

### 4.3 ファイル

このメニューには各 PictureBox の画像ファイルを開く, 閉じる, 画像を移動する, プログラム

の終了といったサブメニューがある．　入力画像のファイル形式はBMPとJPEGに対応している．ここへの入力画像は（別ソフトで）電子透かしを埋め込んだ画像でも良いし，下記電子透かし機能により透かしを埋め込む予定の画像でも良い．基本的に左側が入力画像，右側が出力画像だが，複数画像攻撃の場合は 4.7 に後述するように特殊な入出力となる．

攻撃を行うと右の PictureBox に出力画像が表示されるが，画像移動のサブメニューによりこの画像を入力側に移動させる事ができる．　この機能により連続攻撃が可能になる．

### 4．4　入力/ECC

現在は未実装．

### 4．5　電子透かし

このメニューでは，現在実装済みのパッチワーク法の電子透かしの埋め込み・読み出しの機能を呼び出す．

透かし埋め込みの際は，画面左下のテキストボックスに埋め込みたい文字列を入力して，メニューから「埋め込み」を選ぶ．　すると透かしを埋め込んだ画像が右側に表示される．

透かし読み出しの際は，メニューから「読み出し」を選ぶ．　すると右下のテキストボックスに読み出された文字列が表示される．

### 4．6　単一画像攻撃

３章で述べた通り，単一画像攻撃の機能は Stirmark と JEWELS の機能を組み込んだ．　その中の各種攻撃はサブメニューから選択できる．

### 4．7　複数画像攻撃の実装

複数画像攻撃では，右と左の２枚の画像を入力画像とし，出力画像は右側に表示する．　その機能としては，平均化攻撃と差分攻撃を実装した．

平均化攻撃では入力画像の各画素の輝度の平

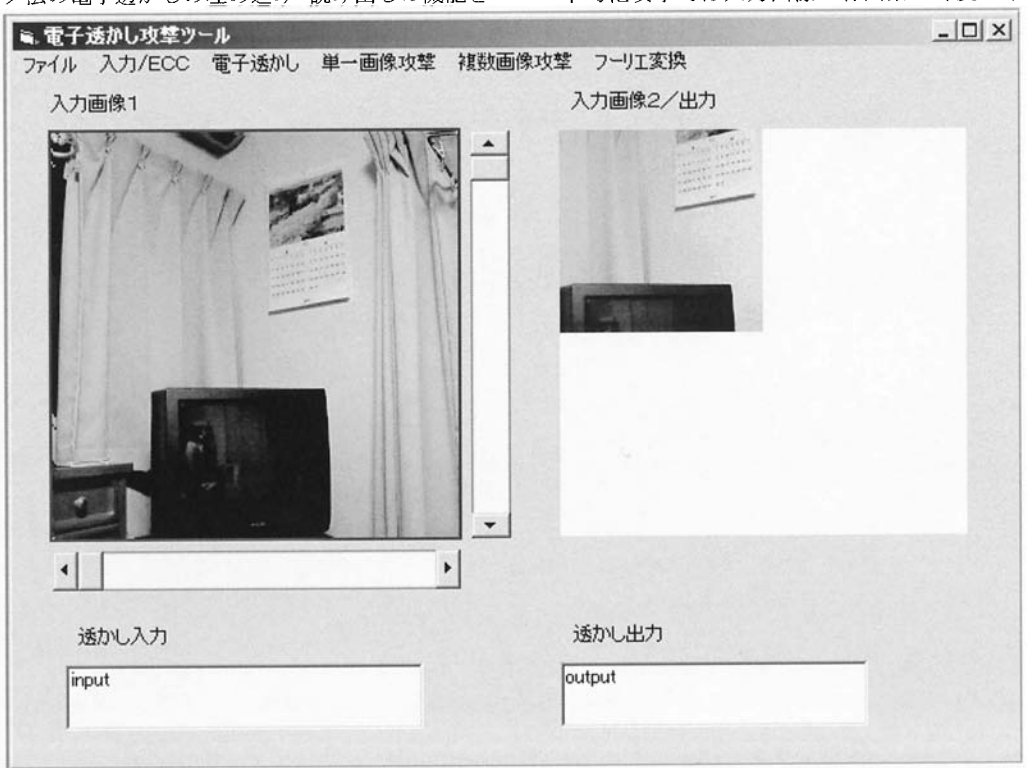


図１．攻撃ツールの外観

均を求め，それを出力画像の各画素の値とする．

差分攻撃では入力画像の各画素の輝度の差の絶対値を 255 から引いた値を求め，これを出力画像の各画素の輝度値とする．

## 5．評価結果の例

この章では，開発した攻撃ツールを用いて電子透かし入りの画像に対して攻撃を行った結果について述べる．

### 5．1　攻撃対象

図２の画像に対して下記（1）（2）の方法で電子透かしを埋め込み，これを攻撃対象とする．

画像サイズは 256×256 画素，ファイル形式は BMP である．

図２．透かし埋め込み前の画像

**（1）パッチワーク法**

4.5 で触れたパッチワーク法による電子透かしを埋め込んだ画像 2 枚（2 枚には別の情報を埋め込んだ）．　埋め込みの強度（[6]における δ）　は 10 とした．

**（2）デジマーク社の技術による電子透かし**

Adobe Photoshop にはデジマーク社の技術による電子透かし埋め込み機能が付いている．

この機能で透かしを埋め込んだ画像 2 枚（2 枚には別の情報を埋め込んだ）．「耐久度」のパラメータは 2 とした．

### 5．2　攻撃方法

単一画像攻撃の例として，Stirmark の Addnoise，Rotation，これらの連続攻撃，JEWELS のインデックスカラーを行い，出力画像から電子透かしが読み出せるかどうかを見る．

複数画像攻撃の例として 2 枚の画像に対する平均化攻撃と差分攻撃を行い，平均化攻撃の出力画像からは電子透かしが読み出せるかどうか，差分攻撃の出力画像からは電子透かしの埋め込み位置が判断できるかどうかを見る．

### 5．3　結果

**（1）単一画像攻撃，平均化攻撃**

表１に，上で示した攻撃のうち差分攻撃以外の攻撃を行った結果を示す．

**（2）差分攻撃**

図３および図４に差分攻撃の結果を示す．　ただし見やすくする為，4.7 で述べた差分攻撃の出力画像に対して輝度が 255 でない画素の輝度をにする処理をした．　この画像において黒い画素は対応する画素の輝度が 2 枚の入力画像で異なる事を示す．　2 枚の入力画像には異なる透かし情報を埋め込んであるので，黒い部分が一部に集まっていたとすれば，その箇所に集中的に透かし情報を埋め込んでいる事を意味する．

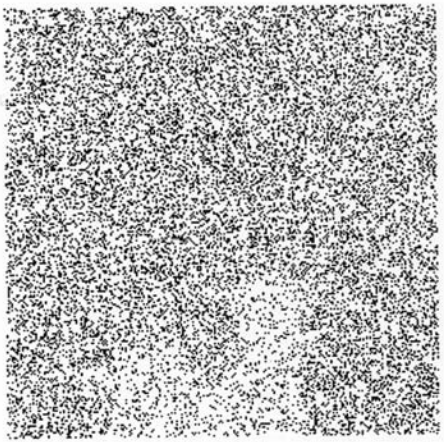

図３．差分攻撃（パッチワーク）

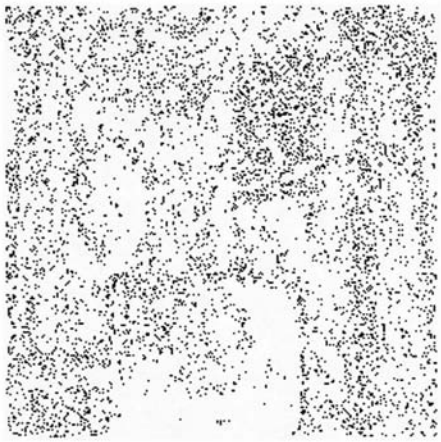

図４．差分攻撃（デジマーク）

図３，図４共に黒い画素が画像全体に散らばっているので，いずれの入力画像も特定の位置に集中的に透かし情報を埋め込んだ物ではない事が言える．

## ６．まとめ

本研究においては，単一画像攻撃と複数画像攻撃の両方の機能やGUIを持つ電子透かし攻撃ツールを開発・実装した．

今後は，現状では２種類しかない複数画像攻撃の機能の充実や，結託攻撃の結果などを勘や直感に頼らず定量的に分析する方法の確立などが課題である．

## 謝辞

本研究の一部は日本学術振興会科学研究費基盤(C) 一般(No.19560397) の援助による．

## 参考文献

[1]小野束，”電子透かしとコンテンツ保護”，
オーム社，2001
[2] ”Stirmark benchmark”
http://www.petitcolas.net/fabien/watermarking/Stirmark/
[3]”電子透かし技術に関する調査報告書”
http://it.jeita.or.jp/eltech/report/2001/01-jou-04.html
[4]画像電子学会，”電子透かし技術”，
東京電機大学出版局，pp.170，2004
[5]ﾁｬｯｸﾘｯﾄ，外山，山口，“JAVAを用いた電子透かしの評価ツール”，CSEC，Vol.1999 No.24.
[6]特許庁標準技術集，画素置換法
http://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/denshi_sukashi/1_a_2_1.htm

表１．攻撃の評価結果

| | パッチワーク法による透かし | デジマーク社の技術による透かし |
|---|---|---|
| Addnoise | パラメータ（ノイズ濃度）7 から文字化けが始まり，パラメータ 14 で全く読めなくなる． | パラメータ 4 以下では読み出せるが，5 以上では透かしが入っていないと表示され，全く読み出せない． |
| Rotation | 少しでも回転させると全く読み出せない． | 回転の角度によらず，情報を読み出す事ができる． |
| Addnoise と Rotation の連続攻撃 | 全く読み出せない． | パラメータ 3 のノイズを付加した後，0.25 度以上の回転を与えると透かしが読めなくなる．（ノイズ，回転共に単独なら充分読み出せる程度の攻撃である．） |
| インデックスカラー | 全く読み出せない． | 問題なく読み出せる． |
| 平均化攻撃 | 文字化けして全く読めない． | 「透かしを利用していますが，読み出せません」と表示される． |