I-077

幾何学的改変と結託攻撃に耐性をもたせた電子透かし法

Digital watermarking method robust against geometrical distortion and collusion attack.

田中 香菜子† 汐崎 陽† 岩田 基† 荻原 昭夫†
Kanako Tanaka Akira Shiozaki Motoi Iwata Akio Ogihara

1. まえがき

近年, インターネットの普及とマルチメディアの発達により, 画像, 音声, 動画といったデジタルコンテンツを扱う機会が増加している. デジタルコンテンツは複製が容易であり, 複製しても品質が劣化しないため, 不正に流通する恐れがあり, その著作権侵害が問題となっている. この問題を解決するための方法の一つとして, 電子透かしという技術がある [1]. 電子透かしとは, デジタルコンテンツに人間が知覚できないように情報を埋め込む技術のことであり, 埋め込む情報を透かしと呼ぶ. 透かしとして, 購入者を識別できる情報を用いれば, 購入者が不正配布した場合に, 不正配布されたコンテンツから購入者の識別情報を抽出して, 不正者を特定できる.

画像への電子透かしには, 画像に対する拡大・縮小や一部切り出しなどの幾何学的改変や, 複数のユーザがコンテンツを比較することにより, 改ざん等を行う結託攻撃など, 透かしを消そうとする攻撃に対する耐性が求められる. 高精細画像を対象とした電子透かしを考案するとき, 透かしを埋め込んでも劣化が全く知覚されないことが要求される. すなわち, 高精細画像においては, 画質の劣化に対する要求が一般的な画像より厳しい.

そこで本稿では, 高精細画像を対象として, 幾何学的改変などに耐性を持つようにユーザ ID 情報を埋め込み, 同時に, 結託攻撃に耐性を持つように利用者識別情報を埋め込むことにより幾何学的改変と結託攻撃に耐性を持たせた電子透かしを提案する. 本手法では, 抽出の際に原画を必要とする. 一般的に, 抽出の際に原画像を必要とする電子透かしはコンテンツ管理が繁雑になるという欠点があるが, 本手法では攻撃に耐性を持たせることを重視する.

2. ユーザ ID の埋め込み法と抽出法

2.1 埋め込み法

64 ビットのユーザ ID 情報を CRC 符号化して 16 ビットの検査ビットを付加して計 80 ビットとし, BMP カラー画像の R,G,B 各成分に埋め込む. 画像サイズを $W \times H$ 画素とする. 画像を $W_B \times H_B$ 画素の K 個のブロックに分割し, 各ブロックをさらに $M \times N$ 画素 ($M = W_B/10, N = H_B/8$) のサブブロックに分割する. 各サブブロックにユーザ ID 情報を 1 ビット埋め込み, 1 つのブロックに 80 ビットを埋め込む. 図 1 に示すように, 各ブロック内の同じ位置のサブブロックには, 同じビットが埋め込まれる. 長さ $L = W/M \times H/N$, 周期 $P(< K < L)$ の, $\{-1, 1\}$ からなる 2 値 M 系列を準備し, M 系列の各要素と各サブブロックを, 各ブロック内の同じ位置にあるサブブロックから順に対応づける. サブブロックに ID 情報ビット"1"を埋め込むときは, 対応する M 系列の要素が 1 ならサブブロック内の画素値の平均を増やすように, 要素が -1 なら減らすように, サブブロックの画素値を変化させる. サブブロックに ID 情報ビット"0"を埋め込むときは, 対応する M 系列の要素に対する画素値の平均の増減を, "1"のときと逆にする. サブブロック内の画素値の平均値の増減は, $-B$ から $+A$ の一様乱数をサブブロック内の画素値に加算もしくは減算することによって行う. ここで, A, B は埋め込み強度であり, $0 < B < A$ を満たすものとする.

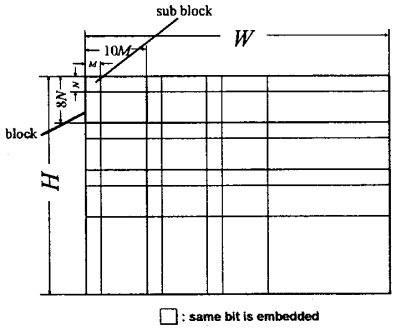

図 1 透かしビットの埋め込み

この埋め込み法では, 透かしを繰り返し埋め込むことにより幾何学的改変に耐性を持たせている. しかし, 結託攻撃に耐性をもたない. よって, $-B$ から $+A$ の一様乱数を任意に定められることをユーザ識別法に利用し, 結託攻撃に耐性を持たせる.

2.2 抽出法

検証の対象となる画像 I_s のサイズを $W_s \times H_s$ ($W_s \leq W, H_s \leq H$) 画素とする. 原画像 I と I_s を用いて, 画像が切り抜かれた場合に対処するために切り抜き位置を探索する. 原画像 I と同じサイズで, 切り抜かれた範囲の画素値は原画像と同じでそれ以外の画素値は 0 である画像 I_0 を作成する. また, 原画像 I と同じサイズで, 切り抜かれた範囲の画素値は I_s と同じでそれ以外の画素値は 0 である画像 I_{s0} を作成する. 次に, I_0 と I_{s0} を用いて, 微小な位置ずれに対処するために, I_{s0} に位置補正を施した画像 I_{s1} を作成する. 画像 I_{s1} と画像 I_0 をサブブロックに分割し, n 番目のサブブロック内の画素値の平均値をそれぞれ $p_n^{(1)}, p_n^{(0)}$ とし, 系列 $S_n = p_n^{(1)} - p_n^{(0)}$ を作成する. 系列 S_n と, 埋め込み時と同じ M 系列について, 周期 P ごとの内積値を求め, 内積値の正負によって"0", "1"の透かしビット候補を求める. 区間をずらして $(K - P + 1)$ 個の内積値を求め, また RGB 各成分の総計 $3(K - P + 1)$ 個の多数決により n 番目の透かしビット"0","1"を抽出する. 80 ビットの透かしを抽出し, CRC

† 大阪府立大学大学院工学研究科

符号で誤り検出を行い，誤りが検出されれば，画像 I_0 に対して位置補正をやり直した画像 I_{s1} を用いて再度抽出の処理を行い，透かしを抽出する．誤りが検出されなければ，透かしが正しく抽出されたとして終了する．位置補正の方法については，紙幅の関係で省略する．

3. 結託ユーザ識別法

3.1 ユーザ識別情報の埋め込み法

2.1 節で，ユーザ ID 情報を埋め込む際に，サブブロック内の平均値を増減させるために $-B$ から $+A$ の一様乱数を増減させる操作がある．ここで，この一様乱数は任意であり，ユーザ ID 抽出の際にこの一様乱数の知識は必要としない．そこで，一様乱数をユーザごとに異なる seed で発生させ，この一様乱数をユーザ識別情報とする．

3.2 結託画像からのユーザ識別情報の検出

結託画像 I_C は原画像 I と同じサイズとする．結託画像 I_C と原画像 I をそれぞれ埋め込み時と同様にブロック分割，サブブロック分割する．各サブブロックについて，I_C の各画素値から I の各画素値を引いた差の値を，平均 0 に正規化し，要素が正であれば $+1$，負であれば -1 とする系列を作成する．この操作を M 系列に対応させた順に行い，長さ WH の検出ユーザ識別情報 C を得る．

3.3 ユーザ識別情報の 2 値化

ユーザ数を n とし，ユーザ識別情報系列 R_n を求める．ユーザ i についての R_i は，以下のように求める．$-B$ から $+A$ の一様乱数で構成される長さ WH のユーザ識別情報を長さ MN の区間に区切って，区間ごとに平均 0 に正規化し，要素が正であれば $+1$，負であれば -1 とする系列を作成する．この操作を全ての区間に対して行い，長さ WH のユーザ識別情報系列 R_i を得る．$i = 1, 2, \ldots, n$ として，R_1〜R_n を得る．

3.4 識別法

3.2 節で求めた検出ユーザ識別情報 C と，3.3 節で求めた各ユーザの識別情報系列 R_i との内積を MN ごとにとり，それぞれの絶対値の総和を求める．この操作を R,G,B 各成分に行い，各成分から得られる値の総和をとり，内積値とする．内積値が他と比べて大きな値を示したユーザ識別情報 R_i に対応するユーザ i が結託者であると特定する．

4. 実験と考察

実験には，4288 × 2848 画素，RGB 各 256 階調の画像を用いた．パラメータは，$M = 4, N = 4, P = 127$ とした．ユーザ ID 情報を 0,1 の乱数列 64 ビットとして埋め込んだ．画質の客観評価には PSNR を用いた．

透かし入り画像の PSNR は 43.54[dB] となり，画質に劣化は見られなかった．

4.1 幾何学的改変に対する耐性

攻撃は，電子透かしの耐性検証ツールである StirMark4.0 を使用した．表 1 に，攻撃を加えた画像からユーザ ID を抽出できたときのパラメータを示す．なお，拡大縮小，回転の攻撃に対しては，画像サイズを元のサイズに変換した後，あるいは画像を逆回転した後に，透かしの抽出を行った．

表 1 攻撃に対する耐性

攻撃	抽出可能なパラメータ
JPEGcompresssion	15〜100
RemoveLine	10〜100
Cropping	15〜100
Rescale	50〜200
Rotation	-2〜2
RotationCrop	-2〜2
RotationScale	-0.25, 0.25

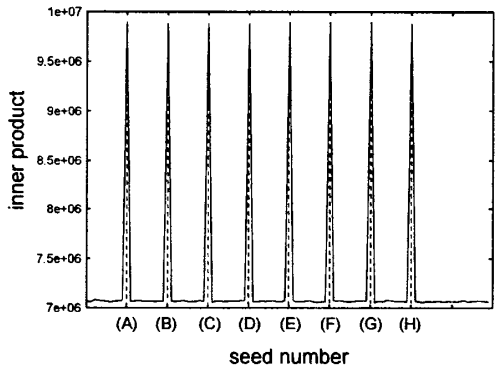

図 2 結託画像の内積値

JPEG 圧縮，切り取り，拡大縮小，微小回転の攻撃に，耐性を有することがわかる．

4.2 ユーザ識別法の有効性の確認

結託者を 8 人として，(A) から (H) の異なるユーザ識別情報を埋め込み，画像 [a] から [h] を作成した．結託攻撃は，異なる画像同士の各画素値を足して平均値をとる攻撃とし，画像 [a] から [h] を結託させた結託画像を作成した．結託画像から系列 C を作成し，(A) から (H) を含む 100 種類のユーザ識別情報系列 R との内積をとり，(A) から (H) のユーザとその他のユーザで，内積値に差が見られるか調べた．図 2 に結託画像から求めた系列の結果を示す．

図 2 で，結託画像の内積値が高い値を示しているのは，結託攻撃に用いられた画像のユーザ (A) から (H) の箇所である．この結果から，結託したユーザを特定可能であることがわかる．

5. むすび

本稿では，幾何学的改変と結託攻撃に耐性をもたせた電子透かし法を提案した．実験により，単一の幾何学的改変に耐性をもつこと，ユーザごとに識別情報を埋め込むことによって結託攻撃を受けた際に誰が結託したかを特定できることを示した．結託者を特定する際にユーザ識別情報系列の内積の計算量が膨大になること，ユーザ識別情報とユーザ ID 情報との対応の工夫が，今後の課題となる．

参考文献

[1] 松井甲子雄，“電子透かしの基礎，” 森北出版，1998.