

DRM 技法のためのデータ埋め込み技術 An Data Embedding Technique for DRM

加藤 幸親[†]
Yukichika Kato

姜 錫[†]
Seok Kang

青木 由直[†]
Yosinao Aoki

1. まえがき

近年、インターネットを利用した映像や音楽などのデジタルコンテンツの配信に対する需要は、通信のブロードバンド化などに伴い、急速に高まっている。しかしその反面、デジタルコンテンツの不正流出や不正コピーなどの問題は無視できない程に深刻化した。そうした中で、これらに問題に対抗するためにコンテンツの流通・再生に制限を設ける DRM 技術が注目を集めている。本稿では、画像に対し周波数変換を施し、その係数特徴に関する情報を符号化したものと正規ユーザ認識の ID を、低周波数成分に透かし情報として埋め込む方法を提案する。この透かしは画質を劣化させるノイズとも言え、提案法では、正しい ID で認証された時のみ、埋め込まれた透かしの完全に検出し、透かし埋め込み前の劣化の無い状態に復元する事が可能となる。

2. データ埋め込みによる DRM 技法

2.1 埋め込みデータの作成

埋め込みデータには、画像の特徴を示す情報とユーザ ID から成るビット列を用いる。以下にその方法を示す。

2.1.1 画像特徴量の抽出

原画像を $N_x \times N_y$ 画素とする。この画素を 8×8 画素のブロックに分割し、それぞれのブロックに対して 2 次元 DCT 変換を行う。次に量子化テーブルを用い量子化パラメータ q で量子化を行う。得られる量子化 DCT 係数をジグザグスキャンにより 1 次元配列へと変換する。ここで n ($n = 0, 1, 2, \dots, (N_x \times N_y)/64$) 番目のブロックの量子化 DCT 係数の 1 次元配列を $x_n[i]$ ($i = 0, 1, 2, \dots, 63$) とする。

次に、画像の特徴量であるこの $x_n[i]$ を埋め込みデータとする為に次の操作を行う。

$x_n[i]$ ($i = 0, 1, 2, \dots, 15$) に対して、隣り合った係数の組を考える。組の中から、要素間の値が異なる組を先頭から 4 つ選び、($j = 0, 1, 2, 3$ $k = 0, 1, 2, \dots, 8$) に対して

$$u_n[j] = \begin{cases} 0 & (x_n[2k] > x_n[2k+1]) \\ 1 & (x_n[2k] < x_n[2k+1]) \end{cases} \quad (1)$$

とおき、 U_n を

$$U_n = u_n[0] \cdot 2^3 + u_n[1] \cdot 2^2 + u_n[2] \cdot 2 + u_n[3] \quad (2)$$

とする。ただし、要素間の値の異なる組が 4 つに満たない場合、 $U_n = 0$ と考える。

最後に、 $\{U_0, U_1, U_2, \dots, U_{1024}\}$ を符号化し、データ量を圧縮する。これにより得られた符号化ビット列を $C(U)$ とする。本稿では BSTW 符号化を用いた。BSTW 符号化は、入力値 U_i がどれだけ前に処理されているか、その距離を符号化するものである。

2.1.2 ユーザ ID 挿入

前項で述べた符号化ビット列 $C(U)$ にユーザ ID を挿入する。挿入位置はユーザ ID の ASCII 文字コードより算出する。本稿では、ID 文字列の最初の文字下位 4 ビットを取り出し、その 10 進値 key を埋め込み位置とした。これにより得られるビット列を $C'(U)$ とする。

2.2 透かしの埋め込み

前項で述べた原画像の周波数成分である $x_n[i]$ ($i = 0, 1, 2, \dots, 63$) に、長さが $W_l = (N_x \times N_y)/16$ のビット列 $W[i]$ ($i = 0, 1, 2, \dots, W_l - 1$) を透かしデータとして埋め込む。 W には、 $C'(U)$ を繰り返し配置し、長さを W_l に調整したビット列を用いる。

ここで、 $x_n[i]$ ($i = 0, 1, 2, 3$) に対して

$$x'_n[i] = \begin{cases} 0 & (x_n[i] < 0) \\ 1 & (x_n[i] \geq 0) \end{cases} \quad (3)$$

とおき、 $x'_n[i]$ と $W[i + n \times 4]$ から

$$p_n[i] = (x'_n[i] \oplus W[i + n \times 4]) \oplus key_2[i] \quad (4)$$

を求める。ただし、 $key_2[i]$ は、 key_2 を key の 2 進表現とすると

$$key_2 = (key_2[0], key_2[1], key_2[2], key_2[3])$$

である。これより

$$P_n = p_n[0] \cdot 2^3 + p_n[1] \cdot 2^2 + p_n[2] \cdot 2 + p_n[3] + 1$$

を計算し、透かしの埋め込む位置 P_n を得る。また、埋め込む強度を V_n とすると、

$$V_n = (F(q) + M) \quad (5)$$

$F(q)$ は、量子化パラメータ q の関数であり、 $M = \max_{1 \leq i \leq 16} |x_n[i]|$ である。この P_n と V_n から

$$x_n[P_n] = \begin{cases} x_n[P_n] - V_n & (x_n[P_n] < 0) \\ x_n[P_n] + V_n & (x_n[P_n] \geq 0) \end{cases} \quad (6)$$

とすることにより、透かしの埋め込むことが出来る。この透かしの埋め込んだ量子化 DCT 係数列を x''_n とする。

2.3 透かしの抽出

前節で述べた、透かしの埋め込んだ量子化 DCT 係数列 x''_n ($n = 0, 1, 2, \dots, (N_x \times N_y - 1)$) に対し、以下の操作を行うことにより、 x''_n は透かしを入れる前のノイズの無い状態に復元される。

2.3.1 透かしの検出

$|x''_n[i]|$ ($i = 0, 1, 2, \dots, 16$) を求め、値の大きい順に M'_{1n}, M'_{2n}, \dots とする。この時の M'_{1n} の位置を P'_n とおく。この P'_n と key より

$$Y_n = key \oplus (P'_n - 1) \quad (7)$$

を計算し、この Y_n を二進表示した

$$Y_n = (Y_{n2}[0], Y_{n2}[1], Y_{n2}[2], Y_{n2}[3]) \quad (8)$$

を求める。ここで、埋め込み時と同様に $x''_n[i]$ ($i = 0, 1, 2, 3$) に対して

[†]北海道大学大学院情報科学研究科, 札幌市

$$y_n[i] = \begin{cases} 0 & (x_n''[i] < 0) \\ 1 & (x_n''[i] \geq 0) \end{cases} \quad (9)$$

とおき、最後に

$$W[i+4n] = y_n[i] \oplus Y_{n2}[i] \quad (i = 0, 1, 2, 3) \quad (10)$$

を計算することにより、透かしデータ $W[i] (i = 0, 1, 2, \dots, W_l - 1)$ 求めることができる。

2.3.2 画像の復元

透かしデータを除去し画像を劣化の無い状態に戻すには、前項で求めた P'_n, M'_{1n}, M'_{2n} および埋め込みの強度パラメータである $F(q)$ を用い、

・ $M'_{1n} > 2M'_{2n} + F(q)$ のとき、

$$x_n[Q_n] = \frac{x_n''[P'_n]}{|x_n''[P'_n]|} \cdot \frac{M'_{1n} - F(q)}{2}$$

・ $M'_{1n} \leq 2M'_{2n} + F(q)$ のとき、

$$x_n[Q_n] = \frac{x_n''[P'_n]}{|x_n''[P'_n]|} \cdot (M'_{1n} - M'_{2n} - F(q)) \quad (11)$$

を計算することにより、透かしを埋め込む前の量子化 DCT 係数列 x_n を復元することができる。

2.4 ID の認証

ユーザにより入力された ID を元に認証を行う。正規 ID が入力された場合は、2.3 で述べた方法により画像は正しくデコードされるが、不正な ID が入力された場合には、下に述べる方法でデコードが行われ、画質は劣化したままの状態が表示される。

入力 ID の 1 文字目の ASCII コード下位 4 ビットの値が正規 ID のものと違う場合

この 4 ビットの 10 進値を key2 とする。この key2 を key と見立て、2.3 で述べた方法によりデコードする。この操作により画像に新たなノイズが生じて、画質が劣化した状態が表示される。

ASCII コード下位 4 ビットの値は同じでも、入力 ID が正規 ID と一致しない場合

2.3 で述べた方法で正しくデコードすることが可能となるが、この場合、透かしを埋め込んだままデコードする。画質は劣化したままの状態が表示されることになる。

3. 実験と結果

本手法を用いて、Jpeg 画像の任意の量子化パラメータ $Quality$ に対する PSNR を、ID 認証の可否によって各々測定比較した。その結果を表 1 に示す。また、埋め込みの強度を表す $F(q)$ には以下の値を用いた。

$$F(q) = 0.04 * \exp(0.08 * Quality) \quad (12)$$

表 1 を見ると、入力 ID が正しいか不正であるかにより PSNR 値の差が十分に大きいことが分かる。これより本手法が、DRM 技法としての有効性を持っていると言える。また図 2 より、ノイズとも言える透かし情報は、特定の周波数成分に偏ることなく埋め込まれていることがわかる。これは、どのような画像に対しても期待する効果が得られる事を示している。

Quality	100	90	80	70	60
PSNR(Fig.1)	54.02	43.83	39.59	35.44	34.70
PSNR(Fig.2)	20.09	17.34	17.07	18.78	20.25

表 1: PSNR の比較



図 1: 正しい ID が入力された場合



図 2: 不正な ID が入力された場合

4. むすび

本稿では、データ埋め込みによる DRM 技法を提案し、実験結果からその妥当性を示した。今後の課題として、視覚的により見栄えの良い埋め込み法についての検討、他のコンテンツへの適用についての検討が挙げられる。

参考文献

- [1] 松井甲子雄, 電子透かしの基礎 - マルチメディアのニュープロテクト技術, 森北出版, 1998 年
- [2] 松本康祐, 青木直史, 青木由直, ロスレス型電子透かしを用いたユーザ認証の検討, 第 17 回 デジタル信号処理シンポジウム 2002 年
- [3] 内山文博, 宮崎明雄, 電子透かしによる画像の認証と保護について, 第 16 回 デジタル信号処理シンポジウム 2001 年
- [4] K.R.Rao, R.Yip, 安田浩, 藤原洋, 画像符号化技術 - DCT とその国際標準 -, オーム社, 1992 年