LJ-005

MPEG 画像の真正性を証明する電子透かしの方法
A Watermarking Scheme for MPEG Video Authentication

伊藤 浩† 卜部 辰一‡ 福岡 隆律‡ 木村 智広† 鈴木 光義†
Hiroshi Ito Shinichi Urabe Takanori Fukuoka Tomohiro Kimura Mitsuyoshi Suzuki

1. はじめに

デジタルデータは編集が容易であるために，監視や電子商取引などの産業分野においては，そのデータが改ざんされていないことを証明するための技術的対策が必要とされ，電子透かしはこれを与える一つの手段として注目されている [1].

電子透かしを用いてこのような画像の認証を行う方法には二つのアプローチがある．一つは，電子透かしを埋めこんで画像を配布し，受信側で透かしの残存を確認することによって，画像の改ざんを検知する方法である [1, 2]．これらの方法の多くは，画像データの（視覚的に重要とされる）一部の情報の変化に基づいて認証を行うため，改ざんの検出は確率的にしか行うことができない．

これに対して，Fridrich らは量子化された DCT 係数のハッシュ値を電子透かしとして埋め込むことにより，JPEG で符号化された画像の改ざんを検知する方法を示した [3]．また，ハッシュ値の計算に予測誤差の DCT 係数を用いることによって，これを MPEG に適用している [4]．この方法は，量子化インデックスが 1 ビットでも変化すれば確実にそれを検知することができる．しかし，符号化されたストリームが復号された後に電子透かしが残存する必要性は考慮されていない．

監視画像などでは，撮影された動画像の一部の画像が重要である場合がある．このようなとき，特定のフレームだけをストリームから抽出し，1 枚の静止画像としてその真正性を証明できることは有用であろう．

本文では，ハッシュ値を予測誤差からでなく，もとの画像の画素値から計算して電子透かしを埋め込み，その値が変化しないように MPEG の符号化を行うことによって，ストリームを復号した後にも残存する認証用電子透かしの方法を提案する．

2. MPEG 符号化と電子透かしの埋め込み

図 1(a) は電子透かしの埋め込みを含む MPEG 符号化器のブロック図である．フレームメモリ (FM) に蓄積された参照画像を動き補償して入力信号から減算し，その DCT 係数を量子化して伝送する部分は一般の MPEG 符号化器の動作と同じである．予測誤差の演算は時間領域でなく DCT 係数の領域で行われているが，これは，後述するように，復号器で電子透かしが失われないようにするためである．

入力信号の DCT 係数は，符号化とは別の系統で量子化マトリクス Q_w により量子化し，電子透かしが埋め込まれる．ここで，電子透かしの方法は，M 個のブロックに含まれる全ての量子化インデックスを入力として N ビットのハッシュ値を計算し（$N \leq M$），それを暗号化したものを，N 個のブロックに 1 ビットずつ埋め込むものとする [5]．具体的には，各ブロックのジグザグスキャンの最後の有意係数を，埋め込むビットに応じて ±1 に変更することによって情報を埋め込む．この透かしが埋め込まれた DCT 係数のインデックスを

$$\hat{y}_w = Q_w T x \tag{1}$$

と表す．ただし，Q_w と T はそれぞれ量子化と DCT の演算子，x は入力信号のベクトルである．

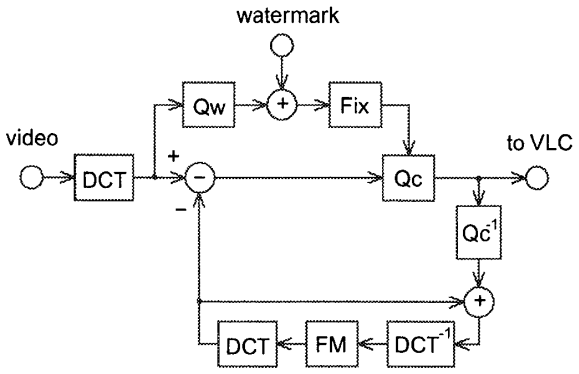
符号化器ではこの $\hat{y}_w$ が保存されるように予測誤差の量子化を行う．予測誤差の量子化インデックスを $\hat{e}_c$ とするとき，このような $\hat{e}_c$ は，

$$Q_w\{Q_c^{-1}\hat{e}_c + Tx'\} = \hat{y}_w \tag{2}$$

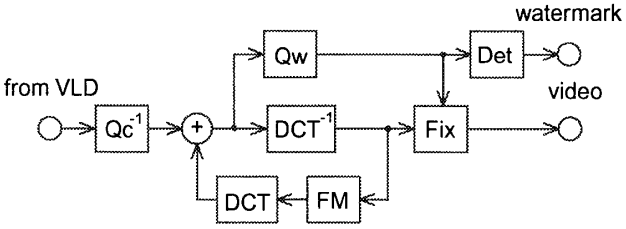
の条件の下で

$$d = |Q_c^{-1}\hat{e}_c - (Tx - Tx')| \tag{3}$$

を最小化するものとして求めることができる．ただし，Q_c は符号化のための量子化の演算子，Q_c^{-1} はその逆の演算子，x' は動き補償された参照ベクトルであり，$|\cdot|$ はベクトルのノルムを表す．



(a) Encoder



(b) Decoder

図 1: MPEG encoder and decoder with watermarking functions

†三菱電機（株）, Mitsubishi Electric Corporation
‡（株）プロシード, Proceed Co., Ltd.

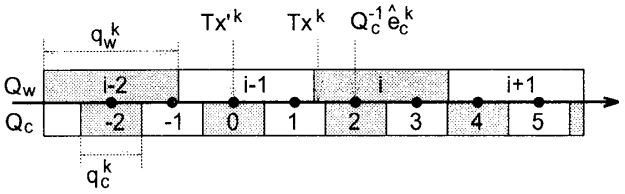


図 2: Quantization of prediction errors preserving a watermark

図 2 に量子化の例を示した．図は k 番目の DCT 係数を量子化する例を示している．上側に Q_w，下側に Q_c の量子化特性を，量子化インデックスとその量子化範囲で示した．中央の数直線上の点 $(\cdot)$ は Q_c の量子化代表値である．また，ベクトルの右肩の添え字 k は，それがベクトルの k 番目の成分であることを表す．q_c^k と q_w^k はこの DCT 係数に対する Q_c と Q_w の量子化幅であり，$q_c^k \leq q_w^k$ となるように設定されている．図から，入力信号 Tx^k を q_w^k で量子化するとその量子化インデックスは i である．一方，予測誤差 $Tx^k - Tx'^k$ を q_c^k で量子化するとその量子化インデックスは $\hat{e}_c^k = 1$ である．しかし，その量子化代表値は Q_w の i 番目の量子化範囲に入っていない．すなわち，$\hat{e}_c^k = 1$ は式 (2) の条件を満たさない．代表値が Q_w の i 番目の量子化範囲に属する Tx^k に最も近い量子化インデックスは $\hat{e}_c^k = 2$ であるので，これが符号化の量子化インデックスとして出力される．

3. 量子化に関する制約

前節の $\hat{e}_c$ が常に存在するためには，Q_w の全ての量子化範囲に，Q_c の量子化代表値が少なくとも一つ存在しなければならない．図 2 のように，Q_c が一様な量子化の場合は，全ての係数 k について，$q_w^k \geq q_c^k$（以下，$Q_w \geq Q_c$ と記す.）が成り立てばよい．ところが MPEG 符号化では 0 付近が粗い不均一な量子化特性が用いられる．この場合には，Q_c の量子化代表値の最も粗い部分の間隔を $T_{\max}$ とするとき，$Q_w \geq T_{\max}$ が成り立つことが，$\hat{e}_c$ が存在する十分条件である．

例えば，H.263[7] の量子化器に対して，Q_w は次のように設定される．H.263 の逆量子化演算は，$Q(Q = 1, \cdots, 31)$ を符号量を制御する量子化パラメータとするとき，Q が奇数ならば，

$$e_c^k = \{2\hat{e}_c^k + \mathrm{sign}(\hat{e}_c^k)\} \cdot Q \tag{4}$$

Q が偶数ならば，

$$e_c^k = \{2\hat{e}_c^k + \mathrm{sign}(\hat{e}_c^k)\} \cdot Q - \mathrm{sign}(\hat{e}_c^k) \tag{5}$$

で規定される．ただし，e_c^k は復元される量子化代表値，$\mathrm{sign}(x)$ は $x < 0$ のとき -1，$x = 0$ のとき 0，$x > 0$ のとき 1 となる関数である．この量子化器では，$T_{\max} = 3Q$ (Q:奇数) または，$T_{\max} = 3Q - 1$(Q:偶数) となる．一方，復号に伴う整数化の後に電子透かしが残存するためには，$q_w^k \geq 8$ でなければならない [5]．これらのことを考慮して，Q_w は以下の値に設定すればよい．

$$q_w^k = \begin{cases} \max(8, 3Q) & \text{for odd } Q \\ \max(8, 3Q - 1) & \text{for even } Q \end{cases} \tag{6}$$

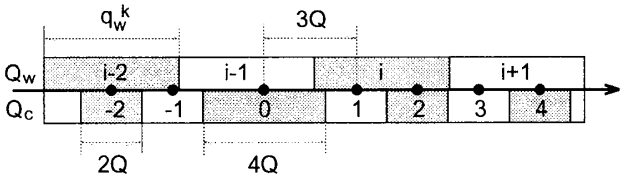


図 3: Non-uniform quantization used in MPEG

図 3 は，Q が奇数の場合の H.263 の量子化特性と Q_w の関係を示す．H.263 の量子化器は MPEG-4 のシンプルプロファイルでも用いられている．

4. MPEG 復号と電子透かしの残存

図 1(a) の符号化器に対応する MPEG の復号器の構成を図 1(b) に示した．図において，予測誤差の復号については，符号化器のローカルデコーダの処理がそのまま繰り返されている．したがって，復号器は符号化器と全く同じ演算を行い，ドリフトを生じることなく，画像信号を復号することができる．一方，参照ベクトルを加算した DCT 係数を Q_w で量子化すれば，その量子化インデックスには電子透かしが含まれているので，これを検算することにより復号された画像の真正性を確認することができる．

復号後に透かしが残存するためには，復号側で式 (2) が完全に再現されなければならない．図 1 の構成によれば，復号器は Tx' を再現することができ，$\hat{e}_c$ は伝送される．したがって，符号化器と復号器で Tx' の同じ値が再現されれば，式 (2) の左辺は正確に計算することができる．このためには，DCT の演算精度について，次の条件が成り立てばよい．

$$Ta = Tb \text{ for all } \{(a, b)|a = b\} \tag{7}$$

すなわち，同じ値を変換した結果が必ず同じ値であればよい．これは，DCT 演算の精度を適切に設定することにより実現できる条件である．式 (2) は，電子透かしが変換領域で埋め込まれていることに対応して，予測誤差を DCT 係数の領域で一定の値の範囲にするための条件となっている．このように，予測符号化を DCT 係数の領域で行うことによって，DCT の演算誤差による電子透かしの消失を防ぐことができる．

復号後の電子透かしの消失は，上記以外に，復号ベクトルの整数化やクリッピングなどによって生じる．3. で述べた $q_w^k \geq 8$ の条件は整数化に対する一つの対策であるが，これだけでは十分でない．特に，クリッピングは復号信号を 0 から 255 などの有限の整数値の範囲（ダイナミックレンジ）で表現するために行われるものであり，信号値が大きく変化するので対策が必要である．

このために，図 1 では，符号化器と復号器において，それぞれ Fix と記した処理回路が追加されている．符号化器側の Fix 回路は，電子透かしを埋め込んだブロックがダイナミックレンジを大きく超えないように，量子化インデックスの値を修正する．また，復号器側の Fix 回路は，復号されたベクトルが電子透かしを失わないようにその値を修正する．図 4 は，このような修正が，凸射

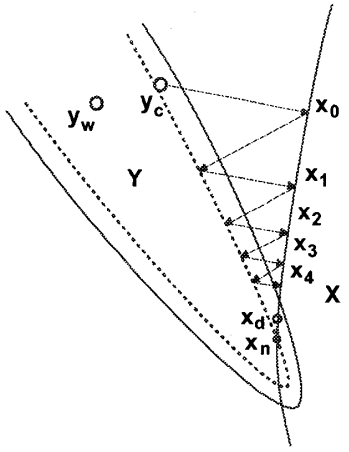


図 4: DCT decoding based on convex projections

影法の原理を利用して可能であることを示す [6]. 図において，X はその成分が全てダイナミックレンジの範囲に含まれるベクトルの集合，Y は電子透かしが保存されるベクトルの集合である．y_w は $\hat{y}_w$ の量子化代表値，y_c は $\hat{e}_c$ を Q_c によって復号し，参照ベクトルを加算したベクトルである．$y_c \in Y$ は保証されるが，$y_c \in X$ は一般に保証されない．このとき，集合 X と集合 Y はともに凸集合であることを利用して，それぞれの集合の間で図のような直交射影を繰り返すと唯一のベクトル $x_n \in X \cap Y$ に収束することが知られている [8]．ここで，x_n を整数化して得られるベクトル x_d が集合 $X \cap Y$ に属すれば，x_n は電子透かしを保存する復号ベクトルである．図 4 では，整数化によって x_d が $X \cap Y$ の外に復号されるのを防ぐため，点線で表される集合 Y の部分集合を用いて凸射影を繰り返す場合を示した．符号化側の Fix 回路で $X \cap Y$ が十分大きくなるように $\hat{y}_w$ を修正しておけば，高い確率で電子透かしを保存する復号ベクトルが得られることが確認されている [6].

なお，6. の計算機シミュレーションでは，この凸射影による復号は用いていない．6. では，符号化器の Fix 回路で $y_w \in X$ となるように $\hat{y}_w$ を修正し，復号側の Fix 回路で y_c を $y_c \in X \cap Y$ となるまで y_w に近づける手法を用いた．この手法は，$y_w \in X$ の条件が厳しいため，一部の画像で劣化が生じるが，電子透かしの消滅は確実に回避できる．

5. 適応処理

2. で述べたように，電子透かしは M 個の中の N 個のブロックに埋め込んでいるので，$N < M$ の場合は，埋め込むブロックを適切に選択することによって，電子透かしによる視覚的な妨害を軽減できる．ただし，電子透かしが埋め込まれたブロックは検出時に一意に求められなければならない．そのような方法はいくつか考えられるが，ここでは，量子化した後の非零の DCT 係数（有意係数）の数によって，ブロックのアクティビティを求め，このアクティビティが高い順に電子透かしを埋め込むことにする．平坦な部分では，有意係数の数が少ないので，電子透かしが埋め込まれる確率は低くなる．また，電子透かしの埋め込みによって有意係数の数は 1 だけ増加するので，各ブロックのアクティビティの順位は変わらない．したがって，検出において，電子透かしが埋め込まれたブロックを特定することができる．以下に，適応処理の手順を示す.

[埋め込み手順]

1. DCT 係数を Q_w で量子化して，有意係数の数を数える.
2. 有意係数の数が閾値より小さいブロックは除外する.
3. 残りのブロックから有意係数の数が多い順に N 個のブロックを選択する．同数の場合はランダムに選ぶ.
4. 選択されたブロックに電子透かしを埋め込む.

[検出手順]

1. 復号された DCT 係数を Q_w で量子化して，ブロック毎に有意係数の数を数える.
2. 有意係数の数が多い順に N 個のブロックを選択する.
3. 選択されたブロックから電子透かしを検出する.

埋め込み手順の 2 のために，全体的に平坦な画像では，埋め込みビットが不足することが考えられるが，このような場合は，画像そのものの価値が低いとみなして，その認証能力は低くてもよいとする.

6. 計算機シミュレーション

6.1 実験条件

MPEG と ITE の標準動画像から，“フラワーガーデン” や “和室” など，16 種の画像を選んで，提案方式の動作を確認した．これらの動画像はそれぞれ最初の 120 フレームを実験に用い，フレームのサイズは，原画の 720×480（画素）から 384×256（画素）に縮小して使用した.

実験の条件は以下の通りである．符号化については，1)15 フレームを一つの GOP (Group of Picture) として，2) 予測フレームは全て P ピクチャとし，3) 量子化は H.263 のものを用い，4) 量子化パラメータ (Q) の値は，1，8，15，31 の中から一つを選択する．H.263 を用いたのは，MPEG-4 のシンプルプロファイルを想定したからである．電子透かしについては，1) ハッシュ値は MD5 による $N = 128$ ビットのバイナリ系列とし，2) 量子化幅は，式 (6) で与えられる値を用いる．なお，DCT の演算は実数の精度で行い，その結果を四捨五入によって整数化した.

6.2 電子透かしの残存

まず，上記の条件で，電子透かしの埋め込みと MPEG の符号化を行い，復号器で得られる予測復号された DCT 係数を Q_w で量子化して，透かしを埋め込んだときの信号が再現されることを確認する．ここで，電子透かしは，128 個の DCT ブロックが含まれる 128×64 画素の領域にフレームを分割し，この領域単位に $M = 128 (= N)$

図 5: Decoded 14th frame of "flower garden" preserving a watermark

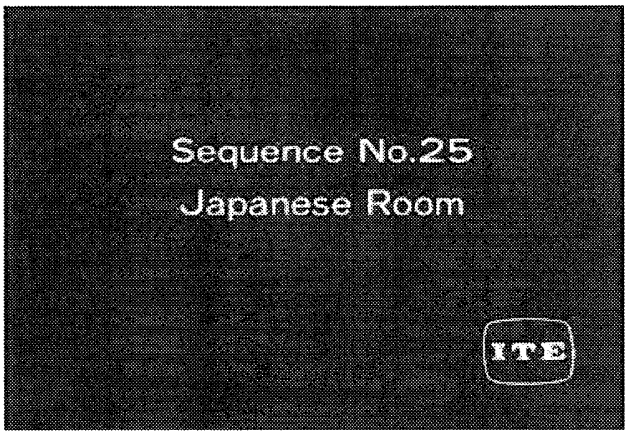


図 6: Decoded 1st frame of "Japanese room" with large Q and low density adaptive watermarking

として埋め込んだ．これにより全ての DCT ブロックに 1 ビットの情報が埋め込まれる．真正性の証明は，この領域単位に行うことができる．

実験の結果，$Q = 1, 8, 15, 31$ のそれぞれの値について，I ピクチャと P ピクチャの全てのフレームに電子透かしが残存することを確認した．これにより，本方式の基本的な動作が確認されたことになる．図 5 は $Q = 1$ で量子化された "フラワーガーデン" の第 14 フレームの復号画像である．この画像には電子透かしが埋め込まれている．

6.3 適応処理の効果

Q の値を大きくするにしたがって，平坦な部分での電子透かしの劣化が目立つようになる．"フラワーガーデン" の空の部分には，$Q = 8$ 程度から低周波パターンの妨害が現れた．このように平坦な部分の多い画像では，量子化が粗い場合に，あまり多くの電子透かしを埋め込むことは，画質上の問題がある．そこで，$M = 1536$ として，フレーム全体を一つの領域とし，ここに 128 ビットの情報を埋め込む実験を行った．埋め込むブロックの選択は 5. で述べた適応処理を用いる．図 6 は，"和室" のタイトルフレームに，この方法で電子透かしを埋め込んで符号化した場合の復号画像である．ただし，$Q = 31$ とした．平坦部の画質劣化はほとんど認められない．これは，埋め込み量を減らしたことと，平坦部を避けて適応的な埋め込みを行ったことの効果である．文字の周囲に見られる劣化は主に符号化によるものであり，電子透かしによるものは知覚できない程度である．

7. まとめ

復号後に残存する MPEG 画像の認証用電子透かしの方法を提案した．この方法は，入力画像の DCT 係数を量子化した値に基づいて電子透かしを埋め込み，この量子化値が変化しないように予測誤差を符号化するものである．電子透かしが消滅しないための量子化の条件を与えた．また，電子透かしの埋め込みによる画質劣化を軽減するための適応処理の方法を与えた．実験により，全ての I および P ピクチャに電子透かしが残存することと，埋め込み量を適切に設定すれば，電子透かしによる画質劣化は小さいことを確認した．

本手法は，B ピクチャに対しても同様に適用できると考える．また，適応処理を改良すれば，複雑な画像では電子透かしを多く埋め込んで認証の単位を細かくし，平坦な画像ではそれを粗くするなどの制御が容易に実現できる．

本手法により，MPEG ストリームから一部の画像を取り出した場合でも，その画像の真正性を証明することが可能になる．取り出された画像はビットマップとして保存できる．また，電子透かしを失うことなく JPEG に符号化することも可能である．このようなフォーマットの変換が容易に行えることは電子透かしの重要な利点の一つであると考える．

参考文献

[1] F. Bartonini, et. al., "Image Authentication Techniques for Surveillance Applications", Proc. IEEE, Oct. 2001.

[2] D. Kundur et. al., "Digital Watermarking for Telltale Tamper Proofing and Authentication," Proc. IEEE, July 1999.

[3] J. Fridrich et. al., "Invertible Authentication Watermark for JPEG Images," ITTC, April 2001.

[4] R. Du et. al., "Lossless Authentication of MPEG-2 Video," Proc. ICIP, Sept. 2002.

[5] 伊藤他,「JPEG 画像の真正性を証明する電子透かしの方法」, 信学総合大会, March, 2003.

[6] 伊藤他,「電子透かしを保存する凸射影法を用いた JPEG 復号方法」, 情処全国大会, March, 2004.

[7] Video Coding for Low Bitrate Communication, ITU-T Draft Recommendation H.263, May 1996.

[8] 西他,「超解像に見る多次元信号処理と逆問題」, 計測と制御, Setp. 1992.