J_053

公開鍵暗号を用いたJPEG圧縮デジタル写真の改ざん位置特定可能な電子透かし法

Fragile Watermarking for Authentication of JPEG-Compressed Digital Pictures Using Public Key Cryptography

汐崎 陽 †
Akira Shiozaki

1. まえがき

写真のデジタル化が急激に進んでいる一方，デジタル写真は痕跡を残さず改変が容易なため，証拠写真として用いる場合，改ざんされていない正真性の保証をどうするかが問題となる．デジタル画像の正真性を保証する方法として，壊れやすい電子透かしを画像に埋め込む方法が提案されている [1]-[4]．この中，誰でも改ざん検知ができるように，公開鍵暗号を利用する方法が提案されている [3],[4]．本稿では，公開鍵暗号を用いて，誰でもデジタル写真の正真性を確かめることのできる電子透かし法を提案する．デジタル写真は一般にJPEG圧縮されて保存されるので，デジタルカメラに組み込むことを前提に，透かしをJPEG圧縮過程で埋め込む．画像自体の公開鍵暗号に基づく電子署名を透かし情報とし，誤り訂正符号化された透かし情報を埋め込む．誤り訂正は改ざん位置を特定するのに利用する．公開鍵署名を用いているので公開鍵により誰でも改ざんの有無を確認でき，かつ正真性証明の信頼性が高い．訂正能力の高い誤り訂正符号を用いることで，改ざん位置の特定精度を高めている．

2. 透かし埋め込みの原理

透かしはJPEG圧縮過程で埋め込む．基本的なJPEG圧縮ではまず，原画の表色系を YC_bC_r 表色系に変換する．次に，Y成分画像とダウンサンプリングされた C_b，C_r 成分画像が 8×8 画素のブロックに分割され，各ブロックに2次元DCT変換が施される．その後，DCT係数を量子化し，量子化DCT係数をランレングス符号化・ハフマン符号化してJPEG符号系列を得る．透かしは，Y成分の特定の量子化DCT係数のLSB（Least Significant Bit）に埋め込む．埋め込みの手順は以下の通りである．ここで，透かしが埋め込まれるY成分の各ブロックの量子化DCT係数を Y_w とする．

Step 1) Y_w のLSBを0とした全てのY成分の量子化DCT係数と全ての C_b, C_r 成分の量子化DCT係数を m として，ハッシュ関数 $H(\cdot)$ により長さ p のハッシュ値 $H(m)$ を求める．

Step 2) ハッシュ値 $H(m)$ を長さが r になるようにパディングし，パディングされたハッシュ値 $H'(m)$ を鍵長 r の公開鍵暗号 $C(\cdot)$ と秘密鍵 k_D で暗号化して電子署名 $C_{k_D}(H'(m))$ を求める．

Step 3) 長さ r の電子署名 $C_{k_D}(H'(m))$ を符号長 w の誤り訂正符号 $E(\cdot)$ で符号化して，符号語 $E(C_{k_D}(H'(m)))$ を求める．誤り訂正符号化関数 $E(\cdot)$ は，長さ u のビット系列を長さ w $(>u\geq r)$ のビット系列に符号化する．

Step 4) Y_w のLSBを $E(C_{k_D}(H'(m)))$ の各ビットと置き換えることにより透かしを埋め込む．

秘密鍵 k_D だけが秘密であり，他は全て公開である．

3. 認証/改ざん検出の原理

認証および改ざん検出の手順は以下の通りである．

Step 1) JPEG圧縮された画像をハフマン復号・ランレングス復号して，量子化されたDCT係数を求め，Y_w のLSBを取り出し，$E(C_{k_D}(H'(m)))$ を得る．

Step 2) 誤り訂正符号語 $E(C_{k_D}(H'(m)))$ を復号し，もし誤りが検出されなければStep 3へ行く．そうでなければStep 4へ行く．

Step 3) 電子署名 $C_{k_D}(H'(m))$ を公開鍵 k_E で復号し，$H'(m)$ のパディングを外してハッシュ値 $H(m)$ を求める．一方，Y_w のLSBを0とした全てのY成分の量子化DCT係数と全ての C_b, C_r 成分の量子化DCT係数を m として，ハッシュ値 $\tilde{H}(m)$ を求める．$H(m)$ と $\tilde{H}(m)$ が等しければ，改ざんが行われていないと認証できる．そうでなければ，改ざん位置の特定が不能な改ざんが行われているとする．

Step 4) 誤り訂正復号により，符号語 $E(C_{k_D}(H'(m)))$ の誤り位置を求める．求められた誤り位置は改ざんされた箇所を示す．訂正不能な誤りが検出されれば，改ざん位置の特定が不能な改ざんが行われているとする．

誤り訂正符号は改ざん箇所の特定に用いる．誤りが検出されれば改ざんが行われていることを示す．誤り位置が改ざん箇所に対応する．誤り訂正が不能な誤りが検出されれば，改ざん箇所の特定はできないものの，改ざんされていることが示される．誤りが検出されなくても，改ざんが見逃されている場合があるので，電子署名により認証を行う．なお，改ざん位置の特定は 8×8 ブロックごとに行われる．

4. 実験

実験に用いた画像は 480×640 画素，R,G,B各8ビットのBMP画像である．ハッシュ関数にはSHA-1を，パディングにはPKCS#1 ver.2.0を，公開鍵暗号には鍵長 $r=1200$ ビットのRSA暗号を用いた．誤り訂正符号には文献 [5] の符号を一部修正したものを用い，情報記号数 $u=2400$ ビット，符号長 $w=4800$ ビットとした．透かしは，8×8 ブロックの量子化DCT係数の $(1,1)$ 座標（$(0,0)$ 座標が直流成分）に埋め込んだ．すなわち，160ビットのハッシュ値を1200ビットにパディングして暗号

†大阪府立大学大学院工学研究科

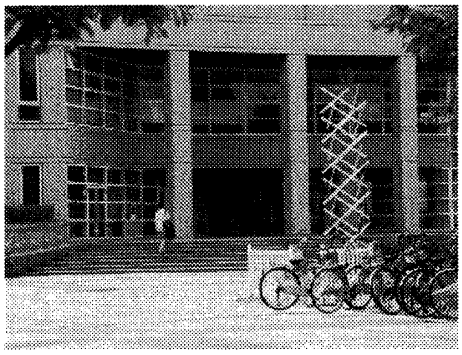

図 1: 透かし入り画像

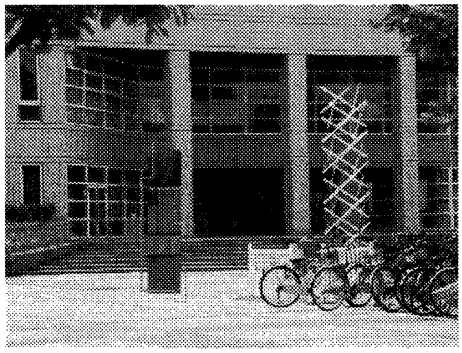

図 2: 改ざん検出結果

化し，1200 ビットの電子署名を 2 つ連結して長さ 2400 ビットにしたものを誤り訂正符号化して，長さ 4800 ビットの符号語を求めた．Y 成分の量子化 DCT 係数の 8×8 ブロックは 4800 個あるので、各ブロックに 1 ビットづつ透かしを埋め込んだ．

図 1 は透かし入り画像である．透かしを入れずに JPEG 圧縮した画像に対する透かしを入れて JPEG 圧縮した画像の PSNR は 52.7 dB であった．PSNR は，JPEG 圧縮された画像を BMP 画像に変換して計算した．図 2 は改ざん検出結果を示す．改ざん箇所が正しく特定されていることがわかる．

5. 考察

一般に，公開鍵暗号を用いた改ざん箇所検出のための電子透かし法では，暗号化データ（透かし）をある大きさのブロック毎に埋め込み，その暗号化データがあらかじめ決められた規則に合わなければ，そのブロック内で改ざんが行われたと判定する．公開鍵暗号を用いて正真性保証の信頼性を高めるためには，鍵長の長い暗号を用いる必要がある．しかし鍵長を長くすると，暗号化データを埋め込むブロックを大きくせざるを得なくなり，誤り箇所特定の精度が下がることになる．特に，JPEG 圧縮画像のような冗長性の低い画像に透かしを埋め込む場合には，この制約は厳しいものとなる．このように，一般に安全性と改ざん箇所特定精度の間にはトレードオフの関係がある．

本提案方式では，鍵長の長い暗号で暗号化されたデータを画像全体に埋め込むことにより正真性保証の信頼性を高め，しかも誤り訂正符号を用いることにより改ざん箇所の特定を行っている．これにより，安全性と改ざん箇所特定精度を両立させている．誤り訂正符号語は画像全体に埋め込まれるため，符号長が長く誤り訂正能力の高い符号を使うことができ，改ざん箇所の特定能力を高めることができる．実験によれば，画像全体の約 5% の改ざんに対して改ざん箇所を正しく特定することができ，それ以上の改ざんに対しては改ざん箇所の特定はできないものの改ざんを検出することができる．誤りが検出されなかった場合でも電子署名により認証を行うので，正真性の信頼性が高い．しかし，量子化 DCT 係数のどれか 1 ビットでも書き換えられると電子署名により改ざん検出が行われるので，JPEG 再圧縮を改ざんと見なす場合が起こり得る．

透かしは特定の量子化 DCT 係数の LSB に埋め込んでいるので，改ざん前と改ざん後でその LSB を同一にする改ざんが考えられるが，電子署名まで同じにするには秘密鍵がない限り不可能である．電子署名により正真性を検証しているので，同一画像の一部あるいは別の透かし入り画像の一部をコピーして貼り付けるような改ざんに対しても，同じ理由から改ざんを検出することができる．

不正者が，異なる秘密鍵を用いて改ざん画像の電子署名を生成し，それに基づく透かしを改ざん画像に埋め込み，対応する公開鍵を公開する場合，公開鍵の正当性が保証されないと改ざんは検出できない．そのため公開鍵証明書により公開鍵の正当性を保証する必要がある．

6. まとめ

画像を JPEG 圧縮する過程で透かしを埋め込み，その JPEG 画像の正真性を保証する電子透かし法を提案した．本手法の特長は以下の点にある．

1) 画像の電子署名を画像自身に透かしとして埋め込んでいるので，正真性保証の信頼性が高い．

2) 公開鍵暗号を利用しているので、だれでも正真性を確認できる．

3) 公開鍵暗号の安全性を高め，かつ改変場所の特定範囲を狭めるために，誤り訂正符号を利用している．

謝辞 本研究は，(財) 柏森情報科学振興財団の研究助成を受けて行われた．

参考文献

[1] E.T.Lin and E.J.Delp, "A review of fragile image watermarks," *Proc. of the Multimedia and Security Workshop (ACM Multimedia '99)*, Orlando, pp.25-29, 1999.

[2] M.Wu and B.Liu, "Watermarking for image authentication," *Proc. of the IEEE International Conference on Image Processing*, vol.2, pp.437-441, Chicago, Illinois, Oct. 1998.

[3] P.W.Wong and N.Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Trans. Image Processing*, vol.10, no.10, pp.1593-1601, 2001.

[4] 杉村友幸, 西垣正勝, 中村逸一, 曽我正和, 田窪昭夫, "公開鍵暗号を用いたアルゴリズム公開型電子透かしによる弱い透かし," 2003 年暗号と情報セキュリティシンポジウム予稿集, pp.971-976, 2003.

[5] A.Shiozaki and H.Fukuhara, "Error performance of codes to which belief propagation decoding algorithm is applicable," *IEICE Trans. Fundamentals*, vol.E85-A, no.5, pp.1183-1186, 2002.