2T-7

符号転置法による情報半開示と利用者識別

タミンタイン †　　岩切 宗利 †
防衛大学校 情報工学科

1. はじめに

デジタルコンテンツは品質を落とさずに複製でき，再配布も容易である．そのため，著作権者が関知しないところで著作物が流通する可能性がある．DRM(Digital Rights Management) 技術 [1] は，著作物に著作者の利益を保護するための仕掛けを施し，コンテンツの不正流出のリスクを抑え，代価の保証を確保することを狙いとしている．

例えば，コンテンツに対し，暗号化 [2] や電子透かし [3] などを施して不正コピーや流出を防ぎ，正規流通を促進させる著作権保護や管理システムが実現されている．ところが，現在の DRM 技術は暗号と電子透かしを個別に用いるため，コンテンツの原本情報がシステム内部に再現される問題がある [1].

文献 [4, 5, 6, 7] では，その対策として，不完全暗号系によるコンテンツ配信システムを提案した．これらの従来方式では，不完全暗号系の実現に，符号の値を暗号化する手法を用いていた．

本報告では，符号転置による不完全暗号系を用いた一実現法について示す．

2. 不完全暗号系

図 1 の不完全暗号系について示す．不完全暗号系では，平文 P を暗号化関数 E と暗号鍵 K によって，半開示情報 C に暗号化する（不完全秘匿性）．C は，復号関数 D と復号鍵 $K'(\neq K)$ を用いて，$P'(\neq P)$ に復号できる（不完全復号性）．

この不完全暗号系を用いることにより原本情報をシステム内に公開しない DRM を実現できる．

3. 提案方式

本提案方式の基本的な処理を**図 2** に示す．まず，制作者 T はコンテンツ $P = \{p_0, p_1, \cdots, p_i, \cdots, p_j, \cdots\}$ から符号要素 p_i と p_j をランダムに選択する．これらを**図 3** のように関数 $Swap(p_i, p_j)$ を用いて位置交換（転置）したコンテンツ C を生成する．

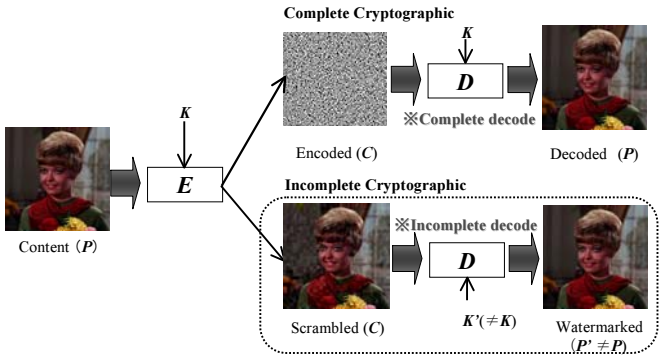


図 1　Complete and Incomplete Cryptographic System

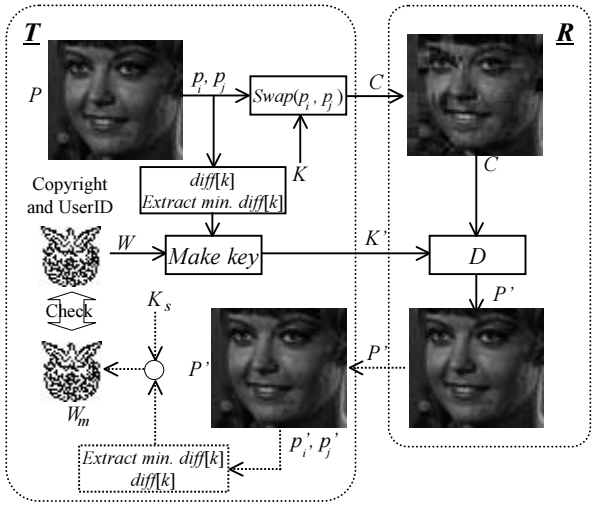


図 2　Systematic flow of proposal method.

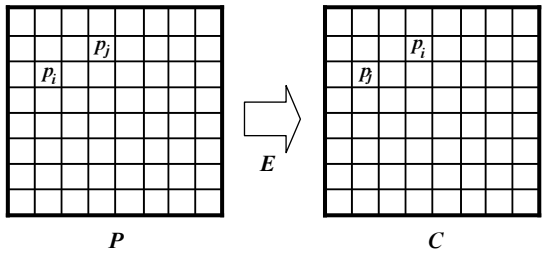


図 3　Transverse processing (Swap function).

$$C \leftarrow E(P, K)$$

この基本的な処理を示す．コンテンツから抽出した情報系列 $P = \{p_0, p_1, \cdots, \underline{p_i}, \cdots, \underline{p_j}, \cdots\}$ を暗号化関数 $Swap(P, i, j)$ を用いて，$C = \{p_0, p_1, \cdots, \underline{p_j}, \cdots, \underline{p_i}, \cdots\}$ のように暗号化する．本方式では，複数のパラメータを転置するために，秘密鍵 r を用いて，転置鍵 $K = \{(r_0, r_1), (r_2, r_3), \cdots, (r_{2n}, r_{2n+1})\}$, $n = 0, 1, 2, \cdots$ を生成する．K を用いて，ペアとなる各パラメータ (p_i, p_j) を定め，それらを転置する．すなわち，暗号化関数 E は，

$$E(P, K) = Swap(P, r_{2n}, r_{2n+1}), n = 0, 1, 2, \cdots$$

と表現できる．この処理により，半開示状態の試用版コンテンツ C が得られる．

これをネットワークなどを通じて広く配布する．C を試用して購入を決心した利用者 R の購入手続きが完了すると，T は，利用者識別情報付き鍵 K' を生成し，復号鍵として配送する．この鍵は，暗号化の際に転置した係数の「一部のみ」が元の位置に戻るように工夫する．

一方，R は K' を用いて C を復号する．

$$P' \leftarrow D(C, K')$$

Partial-scrambling and User Identification using Permutation Codes for JPEG Image.

† Ta Minh Thanh, Munetoshi Iwakiri, Dept. of Computer Science, National Defense Academy

K' を用いて復号した場合，転置されたままの情報系列が残ることになる．すなわち，転置の状態により利用者を識別できるコンテンツ P' が生成される．

提案方式は埋め込み処理に転置による復号を行なう点に特徴がある．この方式では，従来方式のように利用者識別により，正規使用であるかどうかを個別に確認できる．また，それを用いて不正配布の流出源追跡にも利用できる．

4. 適用例

4.1 JPEG 画像への応用

本研究では，JPEG のアルゴリズム [8] を用いて，基本的なシミュレーション実験を行なった．JPEG 画像の主要成分である DCT 係数を対象とした結果を示す．

まず，鍵 K により定まる DCT 係数列 P からランダムに選択した係数を入れ換えた半開示情報状態 C を生成する．

一方，C を復号するために復号鍵 K' が必要となる．K' を生成するために，最適な透かし埋め込み位置を差分選択法により決定する．その差分選択法のアルゴリズムを次に示す．

step 1. K により定まる DCT 係数の組を $p(r_i)$，$p(r_j)$ とし，その差分値の絶対値を求める．

$$diff[k] = |p(r_i) - p(r_j)|$$

step 2. step 1 をくり返し，最小差分値 $min(diff[k])$ を調べ，その位置 $(x_1, y_1), (x_2, y_2)$ を求める．

step 3. step 2 で選択した位置を復号するかどうかを定め，K' を作成する．

この差分選択法により選択した位置に透かしを埋め込むと画質の劣化を最小にできる．透かし情報の表現法として，組となる係数の大小関係を利用すればよい．たとえば，$p_1(x_1, y_1) > p_2(x_2, y_2)$ ときには，ビット値 “0” とし，それ以外を “1” として割り当てる．制作者は，この手法により利用者識別情報付きの鍵 K' を生成する．K' を購入した利用者は，K' を用いて C を P' に復号するだけでよい．

このとき，$P' \neq P$ であるが **step 1〜3** の工夫により P ’は P の品質に近い状態に復号できる．

4.2 実験システムの評価

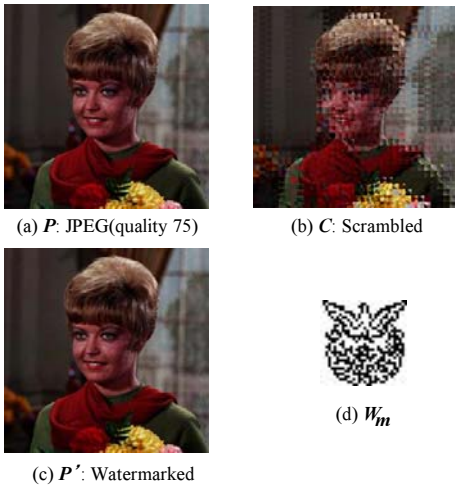
本実験では，SIDBA（Standard Image Data BAse）の標準画像（RGB 各 8bit，256×256 画素）を用いてシステムを評価した．また，各実験画像を画質設定 75（最低 $0 \leftrightarrow 100$ 最高）に JPEG 圧縮した画像および復号過程で埋め込むビット系列 W_m（32×32 画素の 2 値画像）を準備した．画像の評価には PSNR[dB][3] を用いた．

表 1 の結果から JPEG 画像 P を暗号化すると明らかに劣化を感じる品質 C まで劣化し，これを復号すると P と同等の品質 P' まで復元できることがわかる．また，この実験による画像の出力例を**図 4** に示す．

この実験では，コンテンツに対する正規使用を確認するため，情報の埋め込み位置を知る者のみが P' の DCT 係数 $p_1(x_1, y_1)$ と $p_2(x_2, y_2)$ を調べて，透かし W_m を抽出できる．本実験では，図 4(d) のように復号画像 P' から W_m を正しく抽出できることを確認した．

表 1 PSNR[dB] and Embedded bits.

	P	C	P'	Emb.[bit]
Airplane	30.20	19.25	29.64	751
Girl	32.70	22.23	32.40	602
Parrots	34.26	20.32	33.06	754
Couple	34.04	23.61	32.95	716



(a) P: JPEG(quality 75) (b) C: Scrambled

(c) P': Watermarked (d) W_m

図 4 An example of experimental result.

5. おわりに

本報告では，転置暗号を用いた不完全暗号系による方式を提案した．特に，差分値に基づく埋め込み位置選択法により，透かし情報の位置を定めることで，画質の劣化を抑えることができた．本実験では，JPEG 画像を用いた実装実験を行ない，提案方式の有用性を確かめた．

参考文献

[1] 画像電子学会：DRM 技術，Advanced Image Seminar 2003（2003）.

[2] Stinson,D.R.：CRYPTOGRAPHY – Theory and Practice, CRC Press (1995).

[3] 松井甲子雄：電子透かしの基礎，森北出版（1998）.

[4] 岩切宗利，タミンタイン： 不完全暗号系による電子透かし，2005 年暗号と情報セキュリティシンポジウム予稿集，3C1-2，pp.1039–1044（2005）.

[5] タミンタイン，岩切宗利，平野仁之： 不完全暗号系の応用に関する一検討，2005 年電子情報通信学会総合大会講演論文集，D-11-13，pp.13（2005）.

[6] 岩切宗利： 不完全暗号系による画像配信方式の提案と性能評価，2005 年画像メディア処理シンポジウム予稿集，I-1-04，pp.17–18（2005）.

[7] タミンタイン，岩切宗利：個人情報保護に配慮した不完全暗号系による画像配信方式，2006 年画像メディア処理シンポジウム予稿集，I-2-18，pp.47–48（2006）.

[8] 小野文考，渡辺裕： 国際標準画像符号化の基礎技術，コロナ社（1998）.