5D-6

ハフマン符号長不変な不完全暗号系によるDRM方式

岩切 宗利 †　　タミンタイン †
防衛大学校 情報工学科

1. はじめに

無秩序なファイル交換ネットワークによるデジタルコンテンツの不正配布が多発し，無視できない社会問題となっている．この対策として，コンテンツの流通や再生に制限を加える DRM(Digital Rights Management) 技術 [1] が注目を集めている．

DRM 技術とは，暗号 [2] や電子透かし [3] などの技術を統括して，著作権の保護や管理を実現するためのしくみである．しかし，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].

その対策として，文献 [4] では，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．しかし，文献 [4] の方式では，著作権情報などをコンテンツに埋め込むと，コンテンツのサイズがわずかに変化する問題があった．

そこで本報告では，従来手法を改良して，コンテンツデータのサイズを変化させない手法を提案する．

2. 従来方式とその問題点

文献 [4] に示した従来方式の概要を示す．制作者はコンテンツ P の一部を暗号化した半開示状態の試用版コンテンツ C 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の購入手続きが完了すると，制作者は，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 K' を用いて利用者が C を復号すると，利用者識別情報が透かしとして埋め込まれたコンテンツ P' が生成される．文献 [4] の方式は，この埋め込み処理に不完全復号性を利用する点に特徴がある．

この方式では，利用者識別情報により，正規利用であるかどうかを個別に確認できる．しかし，JPEG を対象とした従来方式 [4] では，DCT 係数の一部を透かしに置き換えることにより，ハフマン符号長に違いが生じ，ファイルサイズが変化する．

表1 Huffman codes for AC coefficients

Rc \ S	0	1	2	...	10
0	1010(EOB)	00	01	···	1111111110000011
1	non	1100	11011	···	1111111110001000
2	non	11100	11111001	···	1111111110001110
...	non	···	···	···	···
15	11111111001(ZRL)	1111111111110101	1111111111110110	...	1111111111111110

表2 Additional bits

diff	S	Huffman code	Addition bits
-2047…-1024,1024…2047	11	111111110	00000000000…01111111111,10000000000…11111111111
-1023…-512,512…1024	10	11111110	0000000000…0111111111,1000000000…1111111111
-511…-256,256…511	9	1111110	000000000…011111111,100000000…111111111
-255…-128,128…255	8	111110	00000000…01111111,10000000…11111111
-127…-64,64…127	7	11110	0000000…0111111,1000000…1111111
-63…-32,32…63	6	1110	000000…011111,100000…111111
-31…-16,16…31	5	110	00000…01111,10000…11111
-15…-8,8…15	4	101	0000…0111,1000…1111
-7…-4,4…7	3	100	000…011,100,111
-3,-2,2,3	2	11	00,01,10,11
-1,1	1	10	0,1
0	0	00	non

Huffman Code Length Unchanging DRM Technique based on Incomplete Cryptography System.

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

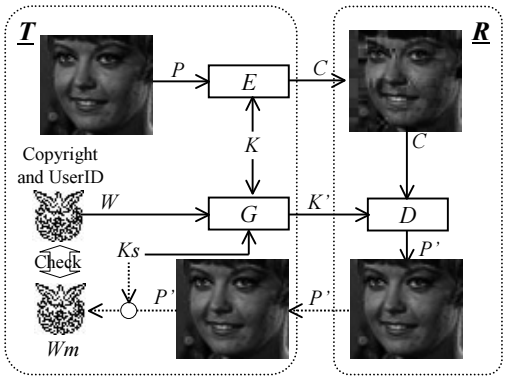

図 1 Systematic flow of proposal method.

3. JPEG 画像のハフマン符号 [5]

JPEG では，64 個の DCT 係数を DC 成分と AC 成分に分割してハフマン符号化する．ここでは AC 成分の符号化手順を示す．

Step 1. AC 成分をジグザグスキャンしながら，ゼロ値の連続数 Rc を求める．

Step 2. Step 1 の処理において出現した 0 でない成分のカテゴリ S を求める．

Step 3. **表 1** に示した Rc と S の組合せにより可変長符号を構成する．

Step 4. Step 3 により得た可変長符号と**表 2** により定まる付加ビットを連結し，符号語として出力する．

このように JPEG の DCT 係数は定まったハフマンテーブルを用いて符号化される．文献 [4] の手法では各符号長が変わることにより，画像データのサイズが変化していた．

4. 提案方式

表 2 に示したハフマン符号の特徴として，一つのカテゴリに属する要素の符号長は同じであることがあげられる．そこで本提案では，**図 1** のように従来方式 [4] を基本として，JPEG 画像のハフマン符号語長を変化させないように暗号化と復号の処理を工夫した．

まず，制作者 T は特定の鍵 K による暗号化関数 E を用いて，コンテンツ P を C に暗号化する．E は，表 2 の同一カテゴリに属する符号をランダムに選択する関数である．C を利用者 R へ配送する．R は C を試用した後，購入手続きおよび利用者登録を行なう．T は，鍵生成関数 G を用いて，鍵 K と著作権情報 W および秘密鍵 Ks から復号鍵 K' を作成し，R に送る．R は，復号関数 D と復号鍵 K' を用いて，C を P' に復号する．

このとき，$P' \neq P$ であるが，P' と P のサイズには変化がない状態となる．さらに，P' と P それぞれに含

まれる DCT 値が近い値になるような K' を準備することにより，P' と P の品質は同等になる．また，秘密鍵 K_s を用いて，P' の特定カテゴリを調べると透かし W_m を抽出できる．K_s は，情報埋め込み位置を定める鍵である．この方式では，コンテンツに対する正規使用を確認するために，秘密鍵 K_s を保持する者（コンテンツ管理者など）が P' から透かし情報 W_m を抽出し，W と比較する．

ここで，DCT 係数を提案方式により処理した一例を**図 2** に示す．まず，図 2(a) は P の DCT テーブルの一部である．これをジグザクスキャンすると {2，1，3，3，EOB} となる．次に，AC 成分 {1，3，3，EOB} をエントロピー符号化する手順を示す．

Step 1. 各値から (Rc，AC 成分値) の組を求める．
{(0，1)，(0，3)，(0，3)，EOB}

Step 2. AC 成分からカテゴリ S を定める．
{(0，1)，(0，2)，(0，2)，EOB}

Step 3. 表 1 により (Rc, S) の可変長符号を得る．
{00，01，01，1010} となる．

Step 4. Step 3 の結果と付加ビットを連結し，
{001，0111，0111，1010} を生成する．

Step 1 〜 4 により，AC 成分のハフマン符号語は，

{001 01<u>11</u> 0111 1010}

の 15 ビットになる．

一方，関数 E を用いて図 2(a) を暗号化した結果である図 2(b) をエントロピー符号に展開する．そのジグザクスキャン結果は {2，1，<u>-2</u>，3，EOB} となる．Step 1 〜 4 の手順と同様にハフマン符号化すると

{001 01<u>01</u> 0111 1010}

の 15 ビットが得られる．

さらに，図 2(b) を復号関数 D により，復号すると図 2(c) になる．復号関数 D は，図 2(b) での暗号化値-2 を，元の値 3 と同じカテゴリの近似値 2（図 2(c)）に復号する．図 2(c) のジグザグスキャン結果は {2，1，<u>2</u>，3，EOB} となる．これをハフマン符号化すると，

{001 01<u>10</u> 0111 1010}

の 15 ビットになる．

このように，{P, C, P'} の AC 成分のエントロピー符号長はいずれも 15 ビットである．よって，DCT 係数のハフマン符号長を変化することなく，情報の半開示または埋め込みをできることがわかる．

5. 提案方式の評価

本実験では，SIDBA（Standard Image Data BAse）の標準画像 GIRL を用いてシステムを評価した．画像の評価には PSNR[dB] を用いた．DCT 係数（Y,UV）の AC 成分カテゴリ $S = 4$ のみを処理した結果 E_4 および

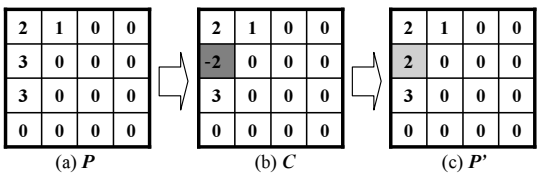

図 2 An example of DCT coefficients.

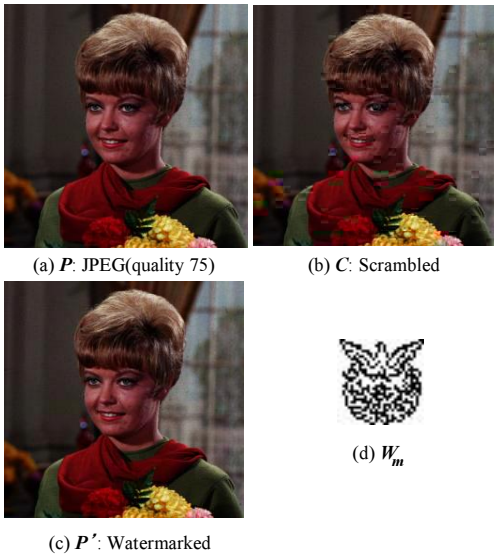

図 3 Experimental results $E_{3,4,5}$.

表 3 PSNR[dB]/size[bits] and Embedded bits

	P	C	P'	W[bit]
E_4	32.70/9947	28.91/9947	32.69/9947	757
$E_{3,4,5}$	32.70/9947	27.71/9947	32.69/9947	340

カテゴリの相関関係 $S = \{3, 4, 5\}$ を利用した結果 $E_{3,4,5}$ を**表 3** に示した．また，本実験の $E_{3,4,5}$ の画像出力例を**図 3** に示した．$E_{3,4,5}$ は符号の伸縮が相殺されるようにハフマン符号を操作する応用方式の一つである．表 3 および図 3 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，P，C および P' のサイズはいずれも 9947 ビットとなっている．本実験では，図 3(c) 復号画像 P' から図 3(d) の W_m(757 ビット) を正しく抽出できることも確認した．

これらの結果から，提案方式によれば，同一カテゴリまたは複数カテゴリのハフマン符号語を制御することにより，ファイルサイズを変えることなく，文献 [4] と同等のシステムを実現できることが分かった．

6. おわりに

本報告では，文献 [4] に示した方式の問題点を解消する一手法を示した．本研究では，エントロピー符号語長を変えることなく，従来手法と同等の性能を実現する方法について検討し，実験により，その性能を確かめた．

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] 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）.