差分方式を用いた不完全暗号系のための演算子の決定法

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 [1]．文献 [2] では，デジタルコンテンツの著作権を有効的に保護するために，差分方式による不完全暗号系 [3] を用いた DRM(Digital Rights Management) を提案した [2]．この方式は，コンテンツの不正流出のリスクを抑え，代価の確保を保証することを狙いとしている．特に，差分方式には，少ない鍵で効率よく不完全暗号化と不完全復号を実現できる特長がある．

ただし，単純な差分処理のみの従来方式には，符号値のみを用いた簡単な逆算で暗号が解けてしまう問題があった．その対策として，不完全復号に用いる演算子を制御する復号鍵をランダムなキーにすることが必要である [2]．

本報告では，暗号化演算子を制御するための鍵を設ける方法について示し，それを適用した実験結果により，秘匿性と復元画質をともに向上できることを示す．

2. 差分方式による不完全暗号系とその問題点

従来の差分方式 [2] では，2 つの暗号化鍵 $\{k_1, k_2\}$ を用いて，コンテンツの符号値を制御するものであった．k_1 は符号列の最初の係数を暗号化するための鍵である．一方，k_2 は暗号化と復号の過程で，演算子を制御する鍵として用いる．

まず，差分方式による不完全暗号系の一例を図 1 に示し，その問題点について明らかにする．

ここでは，説明をやさしくするために，鍵 k_2 による演算子をすべて減算とした（図 1）．このとき，k_2' による復号演算子は，図 1 のようにすべて加算となる．

図 1 (a) は，DCT 係数の一部を示したものである．これをジグザグスキャンすると $\{10,5,0,0,7,3,2,8,0,0,0,0,1,9\}$ となる．ここで，一つの鍵 k_1 を準備する．図 1 の例では，$k_1 = 3$ とした．末尾の非零 DCT 係数 9 と k_1 の差分値＋ 6 をもとの DCT 係数値 9 と置き換えることにより暗号化する．それ以外の非零 DCT 係数 {10,5,0,0,7,3,2,8,0,0,0,0,1} は，その直前の暗号値との差分を求めて処理し，情報半開示コンテンツ C を作成する．もし，演算結果が零になった場合は，暗号値に近い非零値を与える．この処理結果の一例は，図 1 (b) のとおりである．

復号の際は，不完全復号性を持たせるために，全ての非零 DCT 係数を復号しない．本実験では，復号鍵 k_1' のみを制御することにより，末尾の復号係数に透かしが残ることになる．

図 1 の下段に $k_1' = 2$ とした復号系列を示す．この結果，末尾の値 9 以外は DCT 係数は，直前の復号値との和なので完全復号される（図 1 (c)）．

したがって，従来の差分方式によれば，2 つの鍵 $\{k_1, k_2\}$ によって，符号値の差分を制御することでコンテンツの半開示状態を作成できる．また，復号鍵 $\{k_1', k_2'\}$ への細工により，不完全復号性を活用した DRM を実現できる．

本方式では，k_1' と k_2' の組み合わせにより，利用者個別に復号コンテンツを制御できる．よって，復号コンテンツのハッシュ値などを用いれば，容易に利用者を識別することができ，正規利用であることを確認できる．

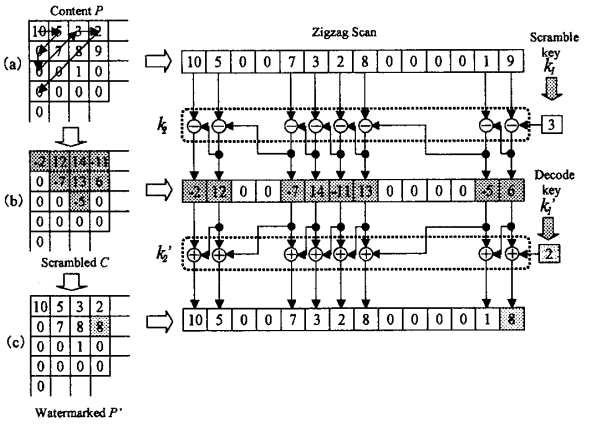

図 1 差分方式の処理例

しかし，k_2 と k_2' が単純な処理（すべて同じ演算）であった場合，暗号化係数のみからほとんどの DCT 係数を簡単な逆計算により復号できる問題がある [2]．したがって，実際は k_2 をランダムなキーにすることが望ましい．また，復号に用いる k_2' に細工を施すと，任意の DCT 係数（一部）を不完全復号できる．

3. 提案方式

暗号化と不完全復号処理の際に，k_2 はランダムなパターンであることが望ましい．しかし，完全に無作為に k_2 のパターンを定めると，画質を大きく劣化することになる．したがって，k_2 を適切に定める必要がある．

まず，コンテンツを暗号化処理する際には，無作為に暗号化鍵 k_2 を生成する．ここでは，k_2 を 2 進数とし，ビット“1”の演算子を加算，ビット“0”の演算子を減算とした．不完全復号には，その逆演算を用いる．特に本研究では，適切な k_2 をいかに生成するかを検討した．

3.1 高周波成分に着目した k_2 の決定法（方法 1）

DCT テーブルの高周波成分値がほとんど 0 に近い値である点と，人間の視覚特性に注目し，ジグザクスキャンの末尾に近い部分の演算子を制御すると画質の劣化を少なくできる．

本実験では，復号処理の際には n 個符号列の高周波成分から $\{n-1, n-2, n-3\}$ 番目の 3 つの係数の復号鍵を制御した．すなわち，これらに関しては，k_2' として正しい演算子を採用しないものとし，ランダムな復号用演算子を生成した．この方式を K2RAND とする．

3.2 差分選択による k_2 の決定法（方式 2）

復号可能な演算子を用いたすべての復号係数の差分値を調べ，最小差分値を選定することにより，特定位置を暗号化鍵と相殺しない演算子に置き換えると画質の劣化量を制御できる．この方式を K2DIFF とよぶ．この選択法のアルゴリズムは，次のようになる．

Step 1. 暗号化したコンテンツから情報系列

$$C = \{e_0, e_1, \cdots, e_n\} \quad (1)$$

を抽出する．

Decisive method of decoder operator pattern for the Incomplete Cryptographic System based on Selective Differential Codes.

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

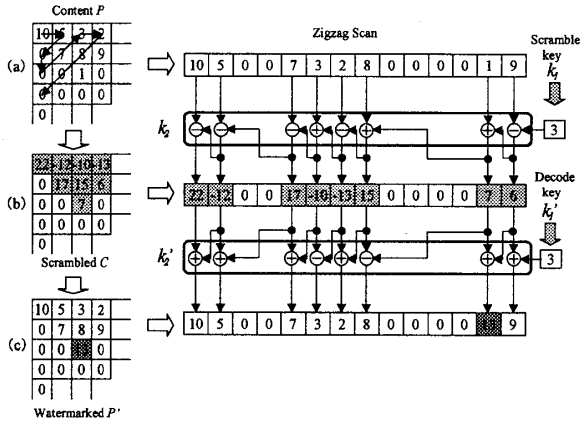

図 2　提案方式の処理例

表 1　PSNR[dB]（Girl）

Method	P	C	P'
K2RAND	32.7090	25.7631	32.7013
K2DIFF	32.7090	25.7631	32.7029

Step 2. C の n 番目以外の係数 $e_i (0 \leq i < n)$ に対して，加算による復号系列 add_i および減算による復号系列 sub_i を計算する．

$$\begin{aligned} add_i &= e_i + e_{i+1}, \\ sub_i &= e_i - e_{i+1}, \\ i &= 0, 1, 2, \cdots, n-1 \end{aligned} \tag{2}$$

Step 3. 加算と減算による復号の変化量を定めるために，add_i と sub_i の絶対差分値 $diff_i$ を，

$$\begin{aligned} diff_i &= |add_i - sub_i|, \\ i &= 0, 1, 2, \cdots, n-1 \end{aligned} \tag{3}$$

により取得する．

Step 4. Step 3 を繰り返し，最小差分値 $min(diff_i)$ を調べ，その位置 i_{min} を求める．

Step 5. k_2 のビット位置 i_{min} の値を調べ，それを k_2' のビット位置 i_{min} の値にする．

制作者は，この処理を繰り返し利用者識別情報付き鍵 k_2' を作成できる．

4.　実験結果と考察

本研究では，JPEG のアルゴリズム [4] を用いて，基本的なシミュレーション実験を行なった．ここでは，JPEG 画像の主要成分である DCT 係数を処理対象とした結果を示す．

提案方式の特性を評価するために SIDBA の標準画像 Girl を用いた．まず，画像を画質 75（最低 0 ↔ 100 最高）で JPEG 圧縮し，この圧縮データを実験画像とした．

画質の客観的評価法として，PSNR（Peak Signal to Noise Ratio）[5] を用いた．

提案方式による処理例を図 **2** に示す．まず，半開示処理の際に，暗号化鍵 $k_1 = 3$ と無作為な鍵 $k_2 = \{-,-,-,+,-,+,+,-\}$ を用いて，図 2 (a) の DCT テーブルを暗号化すると図 2 (b) を得られる．不完全復号を処理する際に，k_2 を本提案方式により決定する．

K2RAND により，k_2' の最末尾の 3 つ演算子をランダムに生成した．その実行結果を表 **1** に示した．この結果から，提案方式により不完全復号した状態の品質は，図 **3** のようにもとの画像とほぼ同等であることを確認した．

(a) P: JPEG(quality 75)　(b) C: Scrambled　(c) P': Watermarked

図 3　K2RAND による画像出力例

(a) P: JPEG(quality 75)　(b) C: Scrambled　(c) P': Watermarked

図 4　K2DIFF による画像出力例

また，K2DIFF により，k_2' を生成した．図 2 (b) の例では，末尾の係数以外に対して，その直前の DCT 係数との和 $add = \{10, 5, 7, -23, 2, 22, 13\}$ を求めた．次に，その直前の DCT 係数との差により，$sub = \{34, -29, 27, 3, -28, 8, 1\}$ が得られた．add と sub に対応する係数の絶対差分 $diff$ を求めると，$diff = \{24, 34, 20, 26, 30, 14, 12\}$ になった．これらから，最小差分値の位置を調べ，k_2' のその位置に対応する演算子と k_2 の演算子を相殺しない関係とすれば，不完全復号状態の品質の劣化を抑えることが可能である．

図 2 の例では，$diff$ の最小値は 12 であるので，その位置の演算子を "+" とした．このとき，k_2' の復号パターンは $k_2' = \{+,+,+,-,+,-,+,+\}$ である．この k_2' を用いて図 2 (b) を復号した結果，図 2 (c) を得た．

この実験結果を，表 1 および図 **4** に示す．図 4 (b) の結果から，無作為な鍵 k_1 を用いて暗号化することにより半開示状態を作成できることがわかる．k_2' により，図 4 (b) を復号すると高品質の図 4 (c) を得られた．よって，差分選択法により適切な不完全復号鍵 k_2' を生成できることもわかる．

5.　おわりに

本報告では，文献 [2] に示した差分方式簡単な逆算で暗号が解けてしまう問題点の解消法を示した．提案方式では，演算子を制御する復号鍵を設け，コンテンツの秘匿性を向上しながらその品質を改善した．本研究では，提案方式の実用性を簡単なシミュレーション実験により確かめた．

参考文献

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

[2] タミンタイン，岩切宗利：差分方式による不完全暗号系を用いた DRM，2007 年暗号と情報セキュリティシンポジウム予稿集，1D-1，pp.73–78（2007）．

[3] 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）．

[4] 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）．

[5] 松井甲子雄：電子透かしの基礎，森北出版（1998）．