6W-7

情報ハイディングのための組合せ符号構成法

山本 紘太郎 †　　岩切 宗利 †
防衛大学校 情報工学科

1. はじめに

近年のディジタルコンテンツの利用拡大により，コンテンツに別の情報を密かに隠す情報ハイディング技術の重要性が高まっている．この技術では，コンテンツに情報を埋め込むために，コンテンツの一部を書き換えるか，あるいは別の情報を挿入する処理を施す．

そのため，従来の方法 [1, 2] では，埋込み量を増大させるためにコンテンツに対する制御量を大きくしなければならなかった．すなわち，埋込み容量の増大に伴う符号量の増大や品質低下の問題があった．

本報告では，埋込み情報を表現するために複数の埋込み領域を用いた．符号パターンの組合わせ（Combination）によって情報を埋め込む手法を提案する．提案方式を用いると，コンテンツに対する制御量を抑制しつつ従来法よりも多くの情報を埋込むことができる．

2. 従来方式

2.1 情報表現法

既存の情報ハイディングでは，動画，音声，画像，電子文書などをカバーデータとして用いる．これらに対する情報ハイディング方式では，それぞれのファイル形式の特性に応じて埋込み領域および埋込み方法を決定している．たとえば画像や音声では，各画素値や波形データの下位ビットを埋込み情報で置換する下位ビット置換法や，圧縮に用いる各種変換に適応する方法などがある [1, 2]．ほかにも，XML[3] などの構造化文書の表記法に冗長性を見出す方法，自然言語処理を用い，言葉の置換えによって情報を表現する方法などがある [4]．

これらの方式には，埋込み情報と埋込み領域が一対一で対応しているという共通点がある．

2.2 埋込み制御量とその効率

情報を埋め込むことによるコンテンツへの情報系列の変化量を総制御量 C とし，そのときの埋込み情報量を P とする．このとき，総制御量に対する情報埋込みの効率は，

$$E = \frac{P}{C} \tag{1}$$

である．

1 つの情報を埋め込むために a の制御量が必要であるならば，従来手法では R の情報埋込みに $R \times a$ の総制御量が必要である．すなわち，埋込み情報量と総制御量が線形関係にあることを示している．このときの埋込み効率は

$$E = \frac{R}{a \times R} = \frac{1}{a} \tag{2}$$

により求まる．

A Construction Method of Combination Code for Information Hiding
† Kotaro Yamamoto, Munetoshi Iwakiri, Dept. of Computer Science, National Defense Academy

図 1　提案方式の概要

3. 提案方式

図 1 に情報ハイディング技術のための組合せ符号構成法を示す．本研究では情報埋込みに必要なコンテンツ総制御量を減少させることを目標とした．

3.1 組合せ符号の構成

情報埋込みに利用可能な領域数（以下，領域数と呼ぶ）を F とし，実際に制御する領域数（以下，制御数と呼ぶ）を r とすると，その制御パターンは ${}_F\mathrm{C}_r$ 通り存在する．提案方式では，これを組合せ符号として利用する．組合せ符号は $\lfloor \log_2 {}_F\mathrm{C}_r \rfloor$ ビットの情報を表現できる．すなわち，組合せそれぞれに情報を対応させれば，その種類数に応じた量の情報埋込みを実現できる．ただし，埋め込まれた情報を読み取るには，各パターンと情報の対応を定義した変換表が必要である．

本方式では，この表をあらかじめ key table（共通鍵）として共有しておく．**表 1** の Combination code（組合せ符号）“- - 1 1” は，4 つある領域のうち前 2 つは制御をせず，後半のみを制御することを示している．また，これに対応する Data（埋込み情報）は “00” である．

この組合せ符号は次のように用いる．

(1)　カバーデータから領域数 F を求め，それと制御数 r の関係から埋込み量

$$M = \lfloor log_2 {}_F\mathrm{C}_r \rfloor \quad [\mathrm{bit}] \tag{3}$$

を求める．

表 1 key table の一例

Field size	Control	Combination code ⇔ Data
2	1	1 - ⇔ 0
		- 1 ⇔ 1
4	2	- - 1 1 ⇔ 00
		- 1 - 1 ⇔ 01
		- 1 1 - ⇔ 10
		1 - - 1 ⇔ 11
		1 - 1 - ⇔ unused
		1 1 - - ⇔ unused
5	1	- - - - 1 ⇔ 00
		- - - 1 - ⇔ 01
		- - 1 - - ⇔ 10
		- 1 - - - ⇔ 11
		1 - - - - ⇔ unused

(2) 埋込み情報列（Data）から M ビット取出し，領域数 F（Feild size）と制御数 r（Control）の対応から key table を調べ，符号を決定する．

3.2 提案方式の性能

図 2 に，$F = 256$ における埋込み量と制御数との関係を示す．これによると，$r = F/2$ のときに組合せ数が最大になり，埋込み容量も最大となることが分かる．また，埋込み容量において提案方式が有利なのは $r \leq \lfloor log_{2F}\mathrm{C}_r \rfloor$ のときであり，これを超えると従来方式が有利となる．したがって，提案方式による埋込み容量を最大にしたい場合は，制御数 $r = F/2$ として用いればよい．

埋込み効率については，F が大きく r が小さいほど効率が良くなる．たとえば制御数 $r = 1$ として提案方式を用いる場合，$F = 256$ であれば 8 ビットの埋込みが可能だが，$F = 65536$ であれば同じ制御数でも 16 ビットの埋込みが可能である．このことから，カバーデータに含まれる F が大きいほど，少ない制御数で多量の情報を表現できることがわかる．

4. 情報ハイディングへの応用例

文献 [4] では複数のステガノグラフィ方式を提案している．本研究では，組合せ符号の実装に XML タグ中の空白文字を利用する方式を利用した．この方式は，XML のタグを閉じるブランケット “>” の前に空白を配置できるという標記上の特性を利用する方式である．すなわち，閉ブランケット直前のスペースの有無により埋込み情報を表現する．

まず，XML のタグ数を求め，組合せ符号を構成する．こうして準備した組合せ符号により定まる閉ブランケットの直前にスペースを挿入する．埋込み情報の抽出は，共有 key table に対応する値をステゴデータ内の組合せ符号に応じて取り出すことで実現できる．

実際に，**表 2** に示す 3 種類の実験用カバーデータ（SVG 形式の XML ファイル）に埋込みを施し，提案方式を評価した．実験結果として，埋込みビット数（**表 3**）とその埋込み効率（**表 4**）を示す．

表 3 からは，同じ制御数でもファイル中のタグ数が多いほど，つまり領域数が多いほど埋込み容量が増大することがわかる．表 4 の埋込み効率からは，3.2 節のとおりタグ数が多く，制御数が少ないほど埋込み効率が高くなることを確認できた．また，従来方式と比べると埋込み効率は向上しており，提案方式によって総制御量が抑制できていることがわかる．

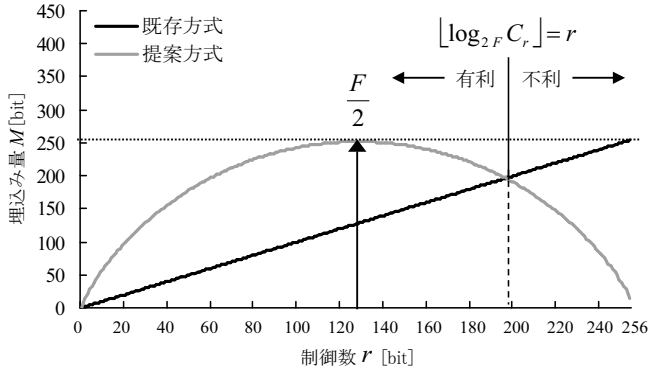

図 2 制御数と埋込み量（$F = 256$）

表 2 実験用 SVG データ

sample	orca	hawk	build
File size [byte]	15723	79948	484957
Tags	109	373	944

表 3 提案方式の埋込み結果 [bit]

r	proposal method			previous
	10	20	30	method
orca	45	71	88	109
hawk	63	109	146	373
build	76	136	188	944

表 4 提案方式の埋込み効率

r	proposal method			previous
	10	20	30	method
orca	0.56	0.44	0.37	0.13
hawk	0.79	0.68	0.61	0.13
build	0.95	0.85	0.78	0.13

5. おわりに

本報告では，情報ハイディングの埋込み効率を，埋込み容量とコンテンツ総制御量を用いて表し，この効率を高める組合せ符号の構成法について提案した．組合せ符号を採用することで，情報ハイディングの埋込み効率が向上し，従来よりも少ない総制御量で多量の情報埋込みを実現できることを確認した．

参考文献

[1] 松井甲子雄 ：電子透かしの基礎，森北出版 (1998).

[2] 情報処理振興事業協会 ：「インフォメーションハイディングの技術調査」報告書 (1998).

[3] JIS X 4159:2005 ：拡張可能なマーク付け言語 (XML) 1.0(2005).

[4] 井上信吾，村瀬一郎，滝澤修，松本勉，中川裕志 ：XML におけるステガノグラフィ手法の提案，2002 年暗号と情報セキュリティシンポジウム予稿集，pp.301–306(2002).