デジタルコンテンツの著作権保護のための符号化手法に関する研究

八　木　秀　樹　　電気通信大学先端領域教育研究センター特任助教

1 はじめに

情報技術の発展に伴い，大量のデジタルコンテンツがコンピュータによって処理されるようになり，デジタルコンテンツの著作権を保護することが重要な課題となっている．このためのひとつの手法として，デジタル指紋（digital fingerprinting）が多くの注目を集めている．デジタル指紋の技術では，ユーザ固有の ID 情報（fingerprint）が元のコンテンツに電子透かしの情報を用いて埋め込まれる．その透かし情報を含んだコンテンツが各ユーザに配布される．

デジタル指紋技術では，複数人が結託してそれぞれの配布コンテンツに対して不正行為を行う結託攻撃（collusion attacks）に対する耐性が求められる．結託攻撃としては，シンボル選択攻撃(interleaving attack) [1],[4],[8],[9]や平均化攻撃(averaging attack) [4][11][12][13]が著名である．特に平均化攻撃はマルチメディアに対するデジタル指紋に対する攻撃として有用なことが知られている．W. Trappe らは balanced incomplete ブロックデザイン(BIBD) の考えを用いて，結託攻撃に対して耐性を持つ**結託耐性符号**を提案した[11]．Trappe らによって提案された符号は，BIBD に基づく結託耐性符号(BIBD-based AC 符号)と呼ばれる．これに対し，本研究（平成 19 年度）において，Trappe ら[11]や Yang ら[14]によって提案された BIBD-based AC 符号に対して，有限幾何に基づいて符号長，結託耐性を同一に保ったまま，その符号化レートを増加させ手法を提案した．この符号は従来の符号と同様，平均化攻撃に対してロバストであることが示されている．特に，ある定数以下の結託であれば，すべての結託者を検出できるという特徴をもつ[12]．この定数は特に**結託耐性**と呼ばれる．

本論文では，平成 19 年度の研究をさらに進め，その符号構成の符号化レートの改良と性能解析を行う．特に，従来の符号と結託耐性と符号語数を同一に保ったまま，符号長を短くする（短縮化）方法を有限幾何の構造を利用して導出する．また，符号化比率をさらに大きくするため，結託耐性符号と誤り訂正符号を組合せた連接符号化法を提案する．その結果として，デジタル指紋システムの安全性を同一に保ち，コンテンツに与える劣みを軽減しながら，多くのユーザに対してサービスを提供できるシステムを実現できる．さらに，誤り訂正能力を持つ結託耐性符号の構成法も，連接符号化法に基づいて提案する．

2 システムモデル

2-1 デジタル指紋

利用者にデジタルコンテンツを配布する際，各ユーザに固有の符号語を電子透かしの技術により，オリジナルのコンテンツに埋め込む．この各ユーザに割り当てられた符号語をユーザの **fingerprint** (**デジタル指紋**) と呼ぶ．悪意をもったユーザは不正に使用したコンテンツから自分の fingerprint がばれないよう，結託して攻撃をすることが考えられる．この行動を**結託攻撃** (collusion attack) と呼ぶ．不正に利用されたコンテンツが発見された場合，結託者検出器はそのコンテンツから結託者たちの fingerprint を推定する．この推定が成功すると，結託者を摘発することが可能となる．

集合 $D=\{1,2,\ldots,|D|\}$をコンテンツが配信される利用者の集合とする．利用者 $j\in D$ に対する符号語を $\mathbf{b}_j = (b_{j1},b_{j2}, \ldots, b_{jN})^T \in \{0,1\}^N$ と表す．ここで，ベクトル $\mathbf{b}_j$ は列ベクトルであり，T はベクトルの転置を表す．Fingerprint の透かし情報 $\mathbf{w}_j$ は定数エネルギーをもつ N 本の直交基底$\{\mathbf{u}_i \in R^N \mid i=1,2,\ldots, N\}$と符号語 b_j から，次のように構成される．

$$w_j = \sum_{i=1}^{N} (2b_{ij} - 1)\mathbf{u}_i \tag{1}$$

次に，各利用者に配布されたコンテンツをホスト信号と見なし，得られた透かし情報をそこに埋め込む．ホスト信号のベクトルを $\mathbf{x}\in R^N$ と表す時, 利用者 $j\in D$ へ配信されるコンテンツは $\mathbf{y}_j = \mathbf{x} + \mathbf{w}_j$ により与えられる．

各 fingerprint は電子透かし技術を用いて埋め込まれるため，すべての利用者は自分の透かし済みコンテンツ $\mathbf{y}_j$ から，自分の fingerprint 透かし情報 $\mathbf{w}_j$ を取り出すことはできない．したがって，悪意をもった利用者は配布されたコンテンツをから不正な fingerprint を作成して，不正規のコンテンツを作る．

2-2 結託攻撃

サイズ h の結託者集合を考え，この集合を $S \subseteq D$ と表す．ここでは簡単のため，$S = \{1,2, ..., h\}$ と仮定する．結託者集合 S から攻撃を受けたホスト信号は次式のように表わされる．

$$\mathbf{y} = \frac{1}{h}\sum_{j=1}^{h} y_j = \mathbf{x} + \frac{1}{h}\sum_{j=1}^{h}\sum_{i=1}^{N}(2b_{ij} - 1)\mathbf{u}_i \tag{2}$$

この結託攻撃法は**平均化攻撃**と呼ばれる，マルチディアデータのデジタル指紋に対して有効な攻撃法である[4][11][12][13]．結託者の検出器は攻撃されたホスト信号 $\mathbf{y} \in R^N$ から結託者集合 S を推定する．

3 平均化攻撃に耐性を持つ AC 符号

3-1 一般的な AC 符号

Trappe らは BIBD-based AC 符号と呼ばれる平均化攻撃に耐性を持つ結託耐性符号を提案した[11]．また，本研究者らは Trappe らの符号クラスを拡張し，その中に優れた符号があることを示した[15]．ここで，AC 符号に関する定義を与える．ここで，集合 Q(S)を S に属するすべての符号語 $\mathbf{b}_1,\ldots,\mathbf{b}_h$ が等しく 0-成分を持つシンボル位置の集合と定義する．

[定義 1]

ホスト信号 **x** は検出器に既知であると仮定する．このとき，ある正定数 L>0 に対し，結託者集合 S のサイズが $|S| \leq L$ のとき，Q(S)が唯一に定まる符号を L-**resilient** AC **符号**と呼ぶ．また，パラメータ L を AC 符号の**結託耐性**と呼ぶ．

□

L-resilient AC **符号**を用いれば，Q(S)を不正なコンテンツ **y** から計算することで S に参加しているすべての結託者を誤りなく検出できることが分かる．

本研究者らは，AC 符号の結託耐性について，以下の補題を示した [15]．ここで，ある実数 v に対し，$\lceil v \rceil$ により v を下回らない最小の整数を表すものとする．

[補題 1]

ある 2 元行列が以下の 2 つの条件を満足すると仮定する : (1) 各列ベクトルの Hamming 重みは少なくとも k, (2) 任意の 2 つの列ベクトルは高々t 個の 1-成分を共通に持つ．このとき，この 2 元行列の列ベクトルから構成される AC 符号は $(\lceil k/t \rceil - 1)$- resilient AC 符号となる．

□

Trappe らの符号[11]は Hamming 重みが一定の k，t=1 とおいた特殊な場合となることが確かめられる．

3-2 有限幾何に基づく AC 符号

先に述べた AC 符号のサブクラスは有限幾何を用いて代数的に構成することができる．ここで，準備として 2 種類の有限幾何について簡単に説明する．

ある整数 p と 2 つの正整数 $m \geq 2$, $s \geq 1$ に対し，有限体 $GF(p^s)$ 上で定義される m-次元**ユークリッド幾何** $EG(m, p^s)$ は**点・線・超平面**から構成される．$EG(m, p^s)$ 内の任意の点は $GF(p^s)$ 上の p^{ms} 個の m-次元ベクトルで表現される． $0 \leq r \leq m$ となる r に対し，r-次元超平面 (一般に，r-**flat** と呼ばれる) は r-次元部分空間 V とそのコセットとなり，ひとつの r-flat はちょうど p^{rs} 個の点を含む．点と線はそれぞれ 0-flat と 1-flat に対応する．

与えられた次元 r<m に対し，$\mathbf{a}_0, \mathbf{a}_1, ..., \mathbf{a}_r$ を $EG(m,p^s)$ 内の r+1 個の線形独立な点とする．このとき，$GF(p^s)$ 上の r 個の点 $b_1, b_2, ..., b_r$ を用いると，$\mathbf{a}_0 + b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \ldots + b_r\mathbf{a}_r$ で表現される p^{rs} 個の点はある r-flat を成す．2 つの r-flat のペア(F_1, F_2)は，高々1 つの(r-1)-flat を共通に持つ．このことは， F_1 と F_2 は高々$p^{(r-1)s}$ 個の点を共通に持つことを意味する．ユークリッド幾何 $EG(m,p^s)$ 内には全部で

$$f_{\mathrm{EG}}(r) = p^{(m-r)s}\prod_{i=1}^{r}\frac{p^{(m-i+1)s}-1}{p^{(r-i+1)s}-1} \tag{3}$$

個の r-flat が含まれる．

有限体 $GF(p^s)$上の m**−次元射影幾何**を $PG(m,p^s)$で表すとき，$PG(m,p^s)$は$(p^{(m+1)s}-1)/(p^s-1)$個の点からなる．射影幾何 $PG(m,p^s)$内には全部で

$$f_{\mathrm{PG}}(r)=\prod_{i=0}^{r}\frac{p^{(m-i+1)s}-1}{p^{(r-i+1)s}-1} \tag{4}$$

個の r-flat が含まれる．2 つの r-flat (F_1, F_2)は高々1 つの(r-1)-flat を共通に持つ．このことは，F_1 と F_2 が高々$(p^{rs}-1)/(p^s-1)$個の点を共通に持つことを意味する．

以降特に区別が必要ない場合は， $FG(m,p^s)$という表記により，ユークリッド幾何 $EG(m,p^s)$もしくは，射影幾何 $PG(m,p^s)$を表すものとする．同様に，$f_{FG}(r)$という表記によって，$f_{EG}(r)$もしくは $f_{PG}(r)$を表す．

ここで， $N_0 = f_{FG}(0)$と定義し，2 元 $N_0\times f_{FG}(r)$行列 $B_r = [b_{ij}]$を考える．この行列の各列に対し $FG(m,p^s)$内の各点を，各行に対し各 r-flat を対応させる．任意の成分 b_{ij} はもし点 i が r-flat j に含まれていれば $b_{ij}=1$，そうでなければ $b_{ij}=0$ を取るものとする．この行列 B_r は $FG(m,p^s)$における r-flat の点に対する**接続行列** (incident matrix) と呼ばれる．

本研究者らは，r -flat (r 次元超平面)の点に対する接続行列 B_r の列ベクトルを AC 符号の符号語に割り当てた．ここで，以下の 2 つの性質を利用している： (1) $FG(m, p^s)$における任意の r-flat は p^{rs} 個の点を持つ，(2) 2 つの r-flat は高々$p^{(r-1)s}$ 個の点を共通に持つ．これらの性質から，$EG(m,p^s)$から構成される任意の AC 符号は(p^s-1)-resilient AC 符号となることが分かる．また，$PG(m,p^s)$を用いると，p^s-resilient AC 符号が構成できることも確認できる．ここで，Trappe らの符号構成は r=1 とおいた場合に相当する．

ここで， AC 符号 $\mathbf{B}_r$ のパラメータについて確認する．符号長は N_0 となり，これは $FG(m,p^s)$内の点の総数と一致する．また，符号語数 (サービスを提供できる利用者数)は $f_{FG}(r)$となり，これは $FG(m,p^s)$内の r-flat の総数と一致する．したがって，符号の効率性を表す符号化レート R_r は $R_r=\log_2 f_{FG}(r)/N_0$ となる．結託耐性と符号長を固定した元では，符号語数を増やすほど，安全性とコンテンツに対する歪みを同一に保ったままサービスを利用できる利用者を増やすことができる．

一般に，有限幾何の次元数 m が大きくなるほど，AC 符号の効率は大きくなる．一方，このとき符号長 N_0 も併せて指数的に大きくなるため，元のデジタルコンテンツに与えるひずみが大きくなる．したがって，符号長はできるだけ短くとどめておく必要がある．これが，誤り訂正符号などの通信路符号の構成と異なり，AC 符号を構成する際の大きな制約となる．

4 AC 符号に対する短縮化法

4-1 提案短縮化法の基本的アイディア

本節では，AC 符号の結託耐性，符号語数を同一に保ったまま，短縮化する方法を提案する．まず，基本的なアイディアを以下に示す．

いま，符号語行列が下のように与えられたとしよう（各列が一つの符号語に対応する）．

$$B=\begin{bmatrix}1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\\1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}$$

補題 1 より，上記の符号語行列は Hamming 重み k=3,t=1 を持つことより，2-resilient AC 符号となる．ここで，どれか任意の 1 行を選び，この行列から取り除いてみよう．たとえば，7 行目の行を除いてみても，依然としてこの行列は 2-resilient AC 符号となることが確かめられる(すなわち, |S|<3 となる任意の S について，Q(S)が唯一に定まる)．新しい符号語行列では，Hamming 重みが 3 の列ベクトルと 2 の列ベクトルが存在する．ここで，Hamming 重みが 2 の任意の 2 列ベクトルに注目すると，同じ行に 1-成分は持たない．この構造が，修正後の符号語行列が依然として 2-resilient AC 符号を与える．一方，さらにもう一行除いてしまうと，新しい行列は 2-resilient AC 符号を与えない．一般には，以下の結果を得る．

[命題 1]

符号語行列 B'は高々列重み k を持つとし，Hamming 重み k-d (d=0,1,…,t)の列ベクトルは，Hamming 重みが k-d 以下の列ベクトルと高々t-d 個の 1-成分を共通に持つとする．このとき，符号語行列 B'は$(\lceil k/t \rceil - 1)$- resilient AC 符号を与える．

□

Hamming 重み k，任意の 2 列ベクトルの共通の 1-成分数は高々t となる符号語行列 B から，t 行を取り除いたとき，得られる行列 B'は，命題 1 の条件を満足する．すなわち，新たに得られた行列 B'は B と同じ結託耐性を持ち，符号長は少なくとも t ビット分短くすることができる．

4-2 有限幾何に基づく AC 符号の短縮化法

ここで，3-2 節で説明した有限幾何に基づく AC 符号の短縮化法を具体的に示す．

まず，有限幾何 FG(m,p^s)における各 r-flat (r≥1) の点に対する接続行列 B_r を考えよう．ここで，この有限幾何においてある(r-1)-flat を選び，この(r-1)-flat に含まる点に対応する行を B_r から取り除く．この結果得られる行列を B_r'と表す．行列 B_r'を符号語行列とする符号を $\mathbf{B}_r$'と表す．

[定理 1]

任意のユークリッド幾何 EG(m,p^s)に対し，符号 $\mathbf{B}_r$'は以下のパラメータを持つ AC 符号となる：(i) 符号長 $n'=p^{ms}-p^{(r-1)s}$，(ii) 符号語数 $f_{EG}(r)$，(iii) 結託耐性 p^s-1．

□

定理 1 により，任意の r 次の EG-AC 符号 $\mathbf{B}_r$ に対し，符号語数や結託耐性を同一に保ったまま，符号長を $p^{(r-1)s}$ ビット分だけ短縮化できることがわかる．

射影幾何を用いた場合も，ユークリッド幾何に基づく AC 符号と同様の結果が得られる．

[定理 2]

任意の射影幾何 PG(m,p^s)に対し，符号 $\mathbf{B}_r$'は以下のパラメータを持つ AC 符号となる：(i) 符号長 $n'=(p^{(m+1)s}-p^{rs})/(p^s-1)$，(ii) 符号語数 $f_{PG}(r)$，(iii) 結託耐性 p^s．

□

[例 1]

ここで，元の EG-AC 符号と短縮化 EG-AC 符号の例を示す．表 1 は(γ, ρ) QC-LDPC 行列から得られる L-resilient EG-AC 符号(ここで，L=min{γ-1, p^s-1}である)の結果を表す．ここで，QC-LDPC 行列は文献[2]の方法に基づいて構成されるものとする．表において，n および n'はそれぞれ元の符号長と短縮化後の符号長を表す．また，$\log_2 \rho f_{EG}(r)$は r 次 EG-AC 符号の符号語数を表す．短縮化による効果はユークリッド幾何 EG(m,p^s)の次元数 m が大きくなるにつれて，大きくなることが分かる．

表 1.　(γ, ρ) QC-LDPC 行列に基づく EG-AC 符号の元の符号と短縮化符号の例

γ	ρ	(m, p^s)	r	n	n'	$\log_2 \rho f_{\mathrm{EG}}(r)$
3	26	$(3, 3^1)$	1	81	78	11.57
3	80	$(4, 3^1)$	2	243	234	16.51
3	242	$(5, 3^1)$	2	729	720	22.92
4	63	$(3, 2^2)$	1	256	252	14.37
4	255	$(4, 2^2)$	2	1024	1008	20.47
4	1023	$(5, 2^2)$	2	4096	4080	28.49
5	124	$(3, 5^1)$	1	625	620	16.55
5	624	$(4, 5^1)$	2	3125	3100	23.58

5 連接符号化法による AC 符号の符号化レートの改良

5-1 連接 AC 符号

本節では，連接符号化法により L-resilient AC 符号の符号化レートを向上させることを考える．ここで考え

る連接符号化法は，ガロア体 GF(q)上で定義される誤り訂正符号を外部符号として先に符号化し，2 元 L-resilient AC 符号を内部符号として，ガロア体の各シンボルに AC 符号の符号語を対応させる．先に提案した有限幾何に基づく短縮化法は，内部符号の効率化に用いることができる．

いま，$C^o \subseteq GF^N(q)$を q 元線形(N,K,D)符号とする．ここで，N は符号長，K は情報記号長，D は最小距離を表す. デジタル指紋の符号器はまず外部符号 C^o の符号語 $\mathbf{c}=(c_1,c_2,\ldots,c_N)$を生成する. 各シンボル c_i をさらに，2 元 L-resilient AC 符号 **B** の符号語 **b** に写像する．この写像はあらかじめ決めて固定しておく．ここで，1 対 1 写像のため $|\mathbf{B}| \geqq q$ が成り立つものと仮定する．

ここで，連接符号化による AC 符号の復号法（不正者の検出法）を説明する．まず，不正者集合 S から作成された不正なコンテンツ $\mathbf{y}=(\mathbf{y}^{(1)}, \mathbf{y}^{(2)},\ldots,\mathbf{y}^{(N)}) \in \{0,1\}^{Nn}$ を復号器の入力とする. ここで, $\mathbf{y}^{(i)} \in \{0,1\}^n$, i=1,2,…,N, は，2 元 L-resilient AC 符号の符号語が重なり，式(2)によって作成される系列とする．そこで，復号器では，まず各 $\mathbf{y}_i$ に対し，2 元 L-resilient AC 符号の復号を実行する．この過程は，$|S| \leqq L$ であれば，不正な符号語を見つけられることに注意したい．その後，外部符号の復号を実行する．この過程は，各 $\mathbf{y}^{(i)}$を与える内部符号に対応する外部符号の符号シンボル集合を $Y^{(i)}$としたとき，集合系列 $\mathbf{Y}=(Y^{(1)}, Y^{(2)},\ldots,Y^{(N)})$と外部符号の各符号語の Hamming 距離を測ることにより実行できる．最終的に，Hamming 距離が 0 となる $|S|$ 個の符号語を不正者として検出する（ここで系列と集合の Hamming 距離は，集合に系列の要素が含まれていれば 0，含まれていなければ 1 と定義される）．

5-2 結託耐性 L を保証するための外部符号の条件

ここで，連接 AC 符号の結託耐性が L となる外部符号の十分条件を示す．

[定理 3]

ある L-resilient AC 符号 B を連接符号の内部符号 C^i として利用するとき，もし D> N(1-1/L) を満たす q 元(N,K,D)線形符号を外部符号 C^o とするならば，連接符号 C は L-resilient AC 符号となる．

□

定理 3 より，与えられたパラメータ N,K に対し，最小距離 D が大きい誤り訂正符号を外部符号として用意する必要がある．よく知られた Singleton 限界から，線形符号の最小距離は D ≦ N-K+1 を満たす[5]．したがって，この式を等号で満たす Reed-Solomon 符号（最大距離分離(MDS)符号の一クラス）[5]を外部符号として利用することは，ひとつの合理的な方法であろう．

ここで，自明な MDS 符号として N=1, K=1,D=1 となる符号が考えられる．この q 元符号を外部符号として利用すると，前節で述べた通常の L-resilient AC 符号となる．したがって，連接符号 AC は Trappe らの AC 符号[11]や本研究者らの AC 符号[15]の拡張となっていることが分かる．

[例 2]

ここで，連接 AC 符号による符号化レートの例を示す．内部符号 C^i を 2 元 L-resilient EG-AC 符号，外部符号 C^o を MDS 符号とする．表 2 に各符号のパラメータを記載する．

表 2.　連接 EG-AC 符号を構成する符号パラメータ

EG-AC code $\mathcal{B}_\mu$		Concatenated EG-AC code $\mathcal{C}$			
		Inner Code $\mathcal{C}^i$		Outer Code $\mathcal{C}^o$	
(m,p^s)	n	(m,p^s)	n	(N,K,D)	q
$(4,3^1)$	81	$(2,3^1)$	9	$(9,5,5)$	10
$(5,3^1)$	243	$(3,3^1)$	27	$(9,5,5)$	10
$(6,3^1)$	729	$(3,3^1)$	27	$(27,14,14)$	28
$(4,2^2)$	256	$(2,2^2)$	16	$(16,6,11)$	17
$(5,2^2)$	1024	$(3,2^2)$	64	$(16,6,11)$	17
$(6,2^2)$	4096	$(3,2^2)$	64	$(64,22,43)$	65

これらのパラメータの内部符号・外部符号をもとに構成した L-resilient 連接 AC 符号の符号長 Nn と符号語数を表 3 に示す. ここで比較のため, Trappe らの EG-AC 符号 $\mathbf{B}_r$ の符号語数を $\log_2|\mathbf{B}_r|$ の列に示す. 列 $\log_2|\mathbf{C}|$ が構成した連接 AC 符号の符号語数を表す．表 3 から，結託耐性と符号長を同一にしたまま，その符号語数を大幅に増やすことができることが分かる．

表 3.　最良次数を持つ PG-AC 符号の例

Resilience L	Code length Nn	# of Information Symbols	
		$\log_2 \lvert\mathcal{B}_\mu\rvert$	$\log_2 \lvert\mathcal{C}\rvert$
2	81	10.19	16.61
2	243	15.00	20.07
2	729	19.80	69.30
3	256	12.48	24.52
3	1024	18.50	28.77
3	4096	24.52	134.81

5-3 誤り訂正能力を持つ連接 AC 符号

前節まで議論した連接 AC 符号は基本的に誤り訂正能力を持たない．すなわち，雑音などの影響で 1 ビットでも誤りが起こってしまうと，保証する結託耐性までの不正者を検出できない．さらには，誤検出を起こし，不正を犯していない正規のユーザを不正者として摘発する可能性すらある．一方，実際のデジタル指紋システムを考えると，通信中やマルチメディアの処理の影響で，誤りが入ることが想定される．そこで，本節では，誤り訂正能力を持つ AC 符号の構成について議論する．具体的には，N 回行う内部符号の復号において，高々s 回までの誤検出であれば，外部符号の復号において，訂正可能となる符号の構成法を示す．

ここで提案する符号を L-resilient s-誤り訂正 AC 符号と呼ぶ．基本的な構成法は前節までの L-resilient 連接 AC 符号と同様である．ここで，外部符号の線形誤り訂正符号に対し，s-誤り訂正能力を持つ条件を示す．

[定理 4]

ある L-resilient AC 符号 B を連接符号の内部符号として利用するとき，もし D> N(1-1/L) +2s/L を満たす q 元(N,K,D)線形符号 C^o を外部符号とするならば，連接符号 C は L-resilient s-誤り訂正 AC 符号となる．

□

定理 4 により，より大きい最小距離 D を持つ q 元線形符号を外部符号として用意すれば，誤り訂正能力を持つ符号を構成することができる．ここでも，前節の議論と同様に，MDS 符号が選択肢の一つとなる．

復号の過程は，L-resilient 連接 AC 符号の復号法と基本的には同様である．s-誤り訂正能力を持つ場合は，外部符号の復号において，系列と集合の Hamming 距離が s 以下となる全ての符号語を不正者の fingerprint として検出する．

6 まとめと今後との課題

本論文では，Trappeらや本研究者らによって提案されたAC符号のクラスに対して，符号語数や結託耐性を保ったまま，符号長を短くできる手法を提案した．また，有限幾何に基づいて代数的に短縮化を実行できることを示した．結果が得られたAC符号は有限幾何 $FG(m,p^s)$の次元mが大きくなるほど，従来のAC符号に対してその有効性は大きくなる．

続いて，外部符号にq元誤り訂正符号，内部符号に2元L-resilient AC符号を組み合わせた連接符号化法を提案した．連接AC符号が結託耐性Lを持つための誤り訂正符号のパラメータに対する条件を導いた．この条件から，与えられたパラメータq,N,Kに対し，できるだけ最小距離Dを大きくすることが求められる．これは従来の誤り訂正符号の構成の目的とも合致しており，様々な誤り訂正符号の構成法が利用できる．先のAC符号の短縮化法を単独で用いたときの有効性に比べ, 連接符号化法の内部符号に提案した短縮化AC符号を用いることにより,その有効性を大きくすることができる．

さらに，本研究では，誤り訂正符号を外部符号に用いることにより，雑音による誤りを訂正できることも併せて示している．ここでもやはり，最小距離の大きい誤り訂正符号を外部符号として用意することが求められる．

本論文では，マルチメディのデジタル指紋システムに有効である，平均化攻撃を想定してロバストな符号構成に関する研究を行った．一方，実際のシステムでは，他の攻撃が加わった場合や攻撃方法が時々刻々と変化する攻撃法などを検討する必要がある．これらの問題は，引き続き検討するべき未解決な問題である．

【参考文献】

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Trans. Inform. Theory, vol. 44, pp. 1897-1905, Sep. 1998.

[2] I. Djurdjevic, J. Xu, K. Abdel-Ghaffar, and S. Lin, "A class of low-density parity check codes constructed based on Reed-Solomon codes with two information symbols," IEEE Commun. Letters, vol. 7, no. 7, pp. 317-319, June 2003.

[3] H. Fujita and K. Sakaniwa, "An efficient encoding method for LDPC codes based on cyclic shift," Proc. of 2004 IEEE Int. Symp. on Inform. Theory (ISIT2004), p. 275, Chicago, USA, June-July 2004.

[4] S. He and M. Wu, "Joint coding and embedding techniques for multimedia fingerprinting," IEEE Trans. on Information Forensics and Security, vol. 1, pp. 231-247, June 2006.

[5] S. Lin and D. J. Costello Jr.,Error Control Coding: Fundamentals and Applications, 2nd ed., Upper Saddle River, NJ: Prentice-Hall, 2004.

[6] T. Mittelholzer, "Efficient encoding and minimum distance bounds of Reed-Solomon-type array codes," Proc. of 2002 IEEE Int. Symp. on Inform. Theory (ISIT2002), p. 282, Lausanne, Switzerland, June-July 2003.

[7] C. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," IEEE J. Select. Areas Commun., vol. 16, pp. 525-540, May 1998.

[8] R. Safavi-Naini and Y. Wang, "New results on frame-proof codes and traceability schemes," IEEE Trans. Inform. Theory, vol. 47, no. 7, pp. 3029-3033, Nov. 2001.

[9] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," IEEE Trans. Inform. Theory, vol. 47, no. 3, pp. 1042-1049, Mar. 2001.

[10] H. Tang, J. Xu, S. Lin, and K. A. S. Abdel-Ghaffar, "Codes on finite geometries" IEEE. Trans. Inform. Theory, vol. 51, pp. 572-596, Feb. 2005.

[11] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, " Anti-collusion fingerprinting for multimedia," IEEE Trans. Signal Processing, vol. 51, pp. 1069-1087, Apr. 2003.

[12] M. Wu, W. Trappe, Z. J. Wang, and K. J. R. Liu, "Collusion-resistant fingerprinting for multimedia," IEEE Signal Processing Magazine, vol. 21, pp. 15-27, Mar. 2004.

[13] H. Yagi, T. Matsushima, and S. Hirasawa, "New traceability codes against a generalized collusion attack for digital fingerprinting," Proc. of 2006 Int. Workshop on Information Security Applications (WISA2006), pp.569-584, Jeju Island, Korea, Aug. 2006.

[14] J. Yang, P. Liu, and G. Z. Tan, "The digital fingerprint coding based on LDPC," Proc. of 2004 7th Int. Conf. on Signal Processing (ICSP2004), pp. 2600-2603,Beijing, China, Aug.-Sept. 2004.

[15] H. Yagi, T. Matsuhima, and S. Hirasawa, " Improved collusion-secure codes for digital fingerprinting based on finite geometries," Proc. of 2007 IEEE Int. Conf. on System, Man, Cybernetics, Montreal, Canada, Oct. 2007.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
Fingerprinting codes for multimedia data against averaging attack	IEICE Transaction on Fundamentals, vol.E-92, no.1	2009 年 1 月