社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（29）
2005－CSEC－28（29）
2005／3／22

結託耐性符号と非結託者識別符号の複合方式の提案と評価

後藤青竜[†]　若山公威[†]　岩田　彰[†]

デジタルコンテンツに電子透かしとして, 配布先 ID 情報を埋め込むフィンガープリンティングでは, 複数の不正者が互いのデータを比較し, 配布先情報を改変する結託攻撃への耐性と, 埋め込み符号長の大きさが問題となる．本稿では, 結託耐性符号に, 非結託者を識別する符号を組み合わせる手法と, 結託耐性符号を多段構成にすることで冗長性を減らす手法を提案し, 追跡精度の向上と符号長の削減について評価を行う.

Combination of Collusion-Secure Fingerprinting Code and Non-Colluder Detecting Code

Seiryu GOTO[†] ,Kimitake WAKAYAMA[†] and Akira IWATA[†]

Contents fingerprinting is a technology that embeds unique ID in content and identifies pirate users who distribute illegal copies. The fingerprinting must have a resilience against a collusion attack, in which several pirates compare their fingerprinted copies to find and alter the marks. Existing secure fingerprinting codes have a very huge code length. In this paper, we propose two methods and evaluate effectiveness of the tracing performance and the code length.In the first method we use collusion secure code and Non-Colluder detecting code. The other method is to compose the collusion secure code in multi-steps.

1. はじめに

フィンガープリンティングはデジタルデータに配布先の識別情報を埋め込み, 不正コピーが流出した際に配布元を特定する技術である．埋め込まれる識別情報はユーザごとにユニークなものであるため, 複数の著作権侵害者がデータを持ち寄り, 互いの差分を調べることで識別情報を推測, 改竄する結託攻撃（collusion attack）が問題となる．この結託攻撃に耐性を有する符号を結託耐性符号と呼ぶ.

Boneh ら [1] は c 人以下のどのような結託からでも少なくとも 1 人を誤追跡確率 ε で特定可能な c-secure code with error ε と呼ばれる結託耐性符号を示した．ここで誤追跡とは結託者に含まれないユーザを誤って結託者と特定することである．$\varepsilon = 0$ の場合を特に totally c-secure 符号と呼ぶが, 2 元符号では totaly c-secure 符号は存在しないことが示されている．Boneh らの方式を改良して 3 人以下の結託時には誤追跡率が小さく符号長の短い方式がいくつか提案されている [2)3)]．村谷 [4)5)] は,Boneh らが示した c-secure 符号の構成に中国人剰余定理を用い符号長を抑えた 2 元 c-secure CRT 符号を提案した．結託耐性符号は結託攻撃のみを考慮していたため, 吉岡ら [6)] は結託攻撃とランダム誤り付加の複合攻撃を想定し, 追跡アルゴリズムの改良を行い, 複合攻撃にも耐性を持たせた.

本稿では, 結託耐性符号の有する結託者の追跡性に, 非結託者の識別性を組み合わせることにより, 結託者候補から非結託者と判定されたユーザを除外する前処理を行うことで誤追跡率を小さくする方式を提案する．また, 結託耐性符号の冗長性に注目し, 結託耐性符号を多段構成にすることで, 符号長あたりの追跡精度を向上させ符号長を減少させる方式も提案する.

2. フィンガープリンティング符号と結託攻撃

ユーザ ID 情報を集合 $Q = \{0, 1, 2, \cdots q\}$ の元が L 個連結したものとして n 人に配布する. ユーザ i に配布する符号 F は以下のようになる.

$$F = \{\ w(i) = [w_0(i), w_1(i), \cdots, w_{L-1}(i)] | \\ w_j(i) \in Q, 0 \leq j < L, 0 \leq i < n\}$$

ここで $w_j(i) \in Q$ は, ユーザ i に配布される j 番目の符号アルファベット Q である．F は符号長 L, 符号数 n, 符号アルファベット Q の符号である. これを（L,n,q）符号 F と呼ぶ．以後本稿では 2 元符号

† 名古屋工業大学
Nagoya Institute of Technology

$Q=\{0,1\}$ として F を扱う. ID 情報は埋め込み位置 $pos_0, pos_1, \cdots pos_{L-1}$ に埋め込まれ, 抽出処理を行うことで取り出される. 埋め込み位置 $pos_0, pos_1, \cdots pos_{L-1}$ はすべてのユーザで共通し, 著作者以外は知り得ない情報であるとする. 抽出された符号に一致する w(i) を調べることで不正者の特定を行う.

ここで, 抽出された符号には結託攻撃による改変が加えられている可能性がある. 結託攻撃とは, 複数の購入者が互いのデータを持ち寄り比較することで ID 情報の位置を推測, 改変する攻撃である. 結託を構成するグループを C と呼ぶことにする. b 人が各符号語 $w_0(u), w_1(u), \cdots w_{L-1}(u)$ を持ち寄り, 結託しているとする. まず以下の U(C) を考える.

$$U(C)=\{i|w_i(u_0)=w_i(u_1)=\cdots=w_i(u_{b-1})\}$$

U(C) は結託 C のすべてのユーザの符号語において, 値が同じとなる埋め込み位置の集合であり,undetected digit と呼ぶ. 埋め込み位置情報を知る手段のない結託 C は U(C) がフィンガープリンティング w(i) の一部であると断定することはできず,U(C) に対して結託攻撃を行うことはできない. この仮定を marking assumption という. 一方, 結託 C のすべての符号語において 1 人以上が異なる値をとる埋め込み位置の集合 D(C) を detected digit と呼ぶ.

$$D(C)=\{i|w_i(u_x)\neq w_i(u_y), x,y\in n, x\neq y\}$$

結託攻撃の対象となる符号は detected digit であり, 2 元符号の場合 0 または 1 のどちらかの値に改変される. 結託 C による改変後の符号が取りうる部分集合を feasible set といい,Fes(C) として表す.

$$Fes(C)=\{w\in\{0,1\}^v : w|_{D(C)}=w(u_i)|_{D(C)} ,\forall\, w(u_i)\in F\} \quad (1)$$

例として, 次のような符号を持つユーザ A とユーザ B が結託攻撃を行った場合を考える.

$$UserA=00001100110$$
$$UserB=10001000011$$

この場合の feasible set Fes(C) は

$$Fes(C)=\sigma 0001\sigma 00\sigma 1\sigma$$

となる. ここで $\sigma=\{0,1\}$ である. 結託攻撃を受けることで, 該当する結託者が存在しなくなる可能性や結託 C に含まれていないユーザを誤って追跡してしまう可能性が生じる. よって, 結託攻撃に耐性のある符号を用いて ID 情報を作成しなければいけない.

3. 結託耐性符号

Fes(C) から結託者を割り出すことのできる符号を結託耐性符号と呼ぶ. Boneh らが示した, 総配布数ユーザ n 人のうち c 人以下の結託が生成するどのような ID 情報からも誤り率 ε で結託者を識別できる c-secure 符号 [1] を改良し, 村谷は中国人剰余定理を用いることで, 符号長を削減した 2 元 c-secureCRT 符号を提案した [4]. 本稿では, 村谷が提案した c-secureCRT 符号と, 非結託者識別符号の組み合わせにより誤追跡率の減少を実現する. まず,c-secureCRT 符号について構成と追跡アルゴリズムを説明する.

3.1 c-secureCRT 符号の構成

c-secureCRT 符号は総配布ユーザ n 人中,c 人までの結託に対して誤追跡率 ε で結託者を追跡可能な符号である. 従来の c-secure 符号は n の増加に伴い符号長が増大する問題があった. そこで, 村谷は中国人剰余定理を利用した符号を構成することで n の大きさに関わらず一定の符号長となる c-secureCRT 符号を提案した [4][5]. c-secureCRT 符号は以下の構成を持つ.

法の設定 k,m,l を $\lfloor 2m/c\rfloor=(k+l)$ を満たす正の整数とする. 互いに素な数列 $p_0, p_1, \cdots p_{m-1}$ を用意する. ここで各数列は $p_0<p_1<\cdots<p_{m-1}$ かつ, $p_0\times p_1\times,\cdots,\times p_{k-1}\geq n$ を満たす正の整数であり, 法と呼ぶ. 法の平均値として $\bar{p}=\sum_{i=0}^{m-1} p_i/m$ を定義する.

剰余 整数 $u(0\leq u_i\leq n)$ をユーザ u の ID とする. それぞれの法において剰余をとった結果を $r_i=u\ mod\ p_i, (0\leq i\leq m)$ とする. 中国人剰余定理により, 一定の個数 k 以上の剰余に対応するユーザは一意に特定される.

内符号 $\Gamma_0(p_i,t)$ を内符号として定義する.$\Gamma_0(p_i,t)$ の符号語 $w_i^{(j)}$ は以下のように構成される.

$$w_i^{(j)}=\underbrace{00\cdots\cdots0}_{t\times j}\underbrace{11\cdots\cdots1}_{t\times(p_i-j-1)} for\ j\in Z_{p_i} \quad (2)$$

内符号 $w_i^{(j)}$ は, ユーザ ID を法 p_i で割った剰余が j となるユーザに割り当てられる. $w_i^{(j)}$ を先頭から t ビットずつ区切ったものをブロックと呼び,1 つのブロック内の符号はすべて 0 または 1 をとる. 内符号は p_i-1 個の t ビットで構成されるブロックに分割でき, 先頭から $B_0, B_1, \cdots, B_{p_{i-2}}$ と表す.

外符号 c-secureCRT 符号を内符号の連結として定義し, $\Gamma(p_0,\cdots p_{m-1};n,t)$ と表す. 外符号 W^u がユーザ u に割り当てられる.

$$W^u=w_0^{r_0}||w_1^{r_1}||\cdots||w_{m-1}^{r_m-1} \quad (3)$$

ここで $r_i\equiv u\ mod\ p_i\ for\ i\in Z_k$ である. 外符号の符号長 L は以下の式で表される.

$$L=\sum_{i=0}^{m-1} p_i t=\bar{p}mt \quad (4)$$

3.2 c-secureCRT 符号の追跡アルゴリズム

C-secureCRT 符号による追跡は, 抽出した符号を内符号に分割し, 各内符号のハミング重みを調べることで行う. 吉岡らは, 追跡アルゴリズムを改良することで符号全体にランダム誤りを付加した状況において, 追跡精度を向上させる手法を示した [6]. 以下に吉岡らの追跡アルゴリズムを示す.

不正コピーデータから L ビットの埋め込み情報 x を抽出し, 以下のように x を m 個に分割する.

$$x = \underbrace{x_0}_{t(p_0-1)bit} \;||\; \underbrace{x_1}_{t(p_1-1)bit} \;||\cdots||\; \underbrace{x_{m-1}}_{t(p_{m-1}-1)bit} \quad (5)$$

各 x_i に以下の追跡アルゴリズム A_3 を適用する.

Algorithm A_3

1:input x_i;
2:for$(min_i = 0; min_i < p_i - 1; min_i++)$
3:if$((hw_{min}(x) > hw_F) \wedge (hw_{min+1}(x_i) > hw_F) \wedge \ldots \wedge (hw_{min+ad_{th}-1}(x_i) > hw_F))$ $break$;
4:for$(max_i = p_i - 1; max_i > min_i; max_i--)$
5:if$((hw_{max_i}(x_i) < t - hw_B) \wedge (hw_{max} < t - hw_B) \wedge \ldots \wedge (hw_{max-adth+2}(x_i) < t - hw_B))$ $break$;
6:output min_i and max_i;

"∧" は AND 論理演算子である.

ここで $hw_{min}(x_i)$ はブロック B_{min} のハミング重み, $hw_{max}(x_i)$ はブロック B_{max} のハミング重みを表す. A_3 の出力 min_i, max_i をそれぞれ $r_i^{(-)}$,$r_i^{(+)}$ と表記し, 内符号 $\Gamma_0(p_i, t)$ の剰余対と呼ぶ. ここで $r_i^{(-)} \leq r_i^{(+)}$ である. A_3 では, ランダム誤り率 e の強弱に応じて閾値 hw_F, hw_B を動的に変化させ誤り訂正を行っている. また,c-secureCRT 符号の内符号の構成を利用した誤り訂正も行っている. 各剰余対を用いて全てのユーザ u について以下の D(u) を求める.

$$D(u) = |\{i \in Z_m | (u \equiv r_i^{(-)} (mod\ p_i)) \vee (u \equiv r_i^{(+)} (mod\ p_i))\}|, 0 \leq D(u) \leq m \quad (6)$$

"∨" は OR 論理演算子である.

D(u) は,u が各法において剰余対群と幾つの合同式を満たすかカウントしたものである. Dth=k+l をしきい値と定義する.$D(u) \geq Dth$ となるユーザ u を結託者として出力する.

4. 提案方式：非結託者識別符号

c-secureCRT 符号の追跡可能人数と追跡率を向上させるためには, 内符号を増やすことが考えられるが, 各内符号は互いに素な数という条件を満たす必要がある. そのため, 内符号を追加するたびに以前よりも大きな符号長を用意しなくてはならない. しかし, 内符号は大きさに関わらず,1 個の内符号あたり一組の剰余対による追跡しか行うことができないため, 符号効率が悪くなると言える. そこで非結託者を識別する符号を用い, c-secureCRT 符号と組み合わせることで, 総配布ユーザの中から結託者候補を小さく絞りこむことを可能にし, 追跡精度の向上を実現する手法を提案する.

4.1 非結託者識別符号の構成

ユーザ ID として 0,1,2, ⋯ ,n-1 を n 人に割り当てる. 図 1 の手順で非結託者識別符号を作成し, 各ユーザを M 通りの異なる分類方法 C によって N グループに分類する. U_i に分類方法 C_j を行った結果, グループ k に分類されることを次のように表すものとする.

$$U_i \in \{C_j(U_i)_k | 0 \leq k < N, 0 \leq j < M\}$$

分類方法 C_j として, ハッシュ関数と mod 関数を用いる. ハッシュを j 回行った値の N の剰余をとり, 剰余の値 R_j によって k=R_j となるグループに分類する.

$$U_i \in \{(H_j(U_i) mod\ N)_k | 0 \leq k < N, 0 \leq j < M\}$$

この結果を用いて次の内符号 IN_j を作成する.

$$IN_j = Block(R_j) = I_0 || I_1 || I_2 || \cdots || I_{N-1}$$

ここで $I_0, I_1, \cdots I_{N-1}$ はブロック長 t で, 以下の条件を満たす符号とする.

$$I_{(H_j(U_i) mod\ N)} = \underbrace{11\cdots11}_{t}$$

$$I_p = \underbrace{00\cdots00}_{t}, p \neq (H_j(U_i) mod\ N)$$

最終的に各ユーザに埋め込む符号は IN_j を M 個連結した外符号 OUT_i となる

$$OUT_i = IN_0 || IN_1 || IN_2 || \cdots || IN_{M-1}$$

OUT_i を非結託者識別符号と呼ぶこととする.

4.2 非結託者識別符号による非結託者の判定

非結託者識別符号により, 総配布ユーザ n 人の中から非結託者と判定されたユーザを結託者追跡の対象から除外する. 結託攻撃後のデータから抽出した, 非結

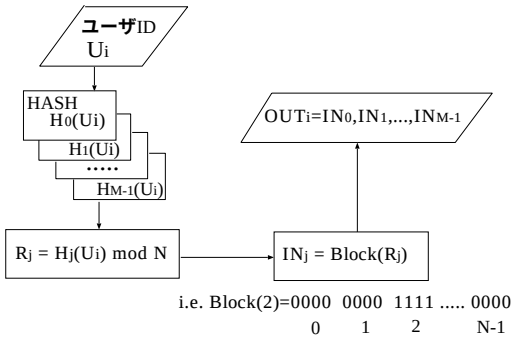

図 1 非結託者識別符号の作成手順

託者識別符号 OUT' を内符号に分割したものを IN'_j とする.

$$IN'_j = I'_0 \,|I'_1\,|I'_2\,|\cdots\,|I'_{N-1} \quad (7)$$

ここで, 各ブロック I'_k のハミング重み Hw を調べる. ハミング重みがしきい値 th 以上となるブロックを I_{mth}, しきい値 th 以下となるブロックを I_{lth} とする.

$$I_{mth} = \{I'_k | H_w(I'_k) > th\} \quad (8)$$

$$I_{lth} = \{I'_k | H_w(I'_k) < th\} \quad (9)$$

I_{mth} は結託攻撃による改変を受けているブロック, I_{lth} は結託攻撃による改変を受けていないブロックと判定される. I_{mth} を改変することが可能なユーザは, 結託攻撃に加わっている可能性がある. 一方, I_{lth} を改変することが可能なユーザは, 結託攻撃には加わっていないと言える. よって,I_{lth} に属するユーザは非結託者と判断し, 結託者候補から除外する. 結託者の人数を c としたとき, 一つの IN'_j から得られる I_{mth} の期待値を ϵ_{mth} とすると, ある 1 人の非結託者が I_{mth} に属する確率は ϵ_{mth} / N となる. 非結託者が除外されないのは,$0 \leq j \leq M$ のすべての IN'_j において,I_{mth} に属した場合であり, その確率は以下のようになる.

$$\epsilon_2 = (\epsilon_{mth}/N)^M \quad (10)$$

c-secureCRT 符号により誤り率 ϵ_1 で結託者と誤って判定され, かつ, 誤り率 ϵ_2 で非結託者として除外されなかった場合が誤追跡となる. その確率は,

$$\epsilon = \epsilon_1 \times \epsilon_2 \quad (11)$$

となり, c-secureCRT 符号のみを用いた場合よりも ϵ_2 分誤追跡率が抑えられる.

5. 提案方式：c-secureCRT 符号の多段化

c-secureCRT 符号は, 最大・最小剰余を検出することで結託者の追跡を行う. その際, 図 2 に示すように, 追跡に利用される情報は最大・最小剰余のみで, 中間は利用されない, 冗長な符号となる. ここで,c-secureCRT 符号の内符号で符号長が L, 結託者の人数を c とした場合に最少剰余 $r^{(-)}$ が定数 r_{min} 以下となる確率 $P(X \leq r_{min})$ と, 最大剰余 $r^{(+)}$ が定数 r_{max} 以上となる確率 $P(X \geq r_{max})$ は次の式で表される.

$$P(r^{(-)} \leq r_{min}) = 1 - ((L - r_{min})/L)^c \quad (12)$$

$$P(r^{(+)} \geq r_{max}) = 1 - (r_{max}/L)^c \quad (13)$$

結託者の人数 c が多いほど式 12, 式 13 の値は大きく

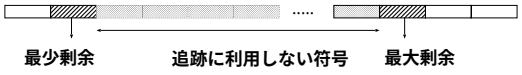

図 2 C-secureCRT 符号の単一構成の問題点

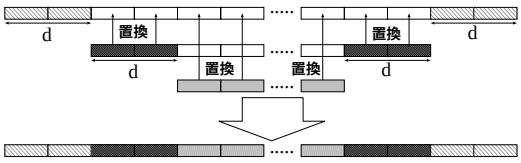

図 3 C-secureCRT 符号の多段構成

なり冗長な符号が多く発生することになる.

5.1 多段構成の符号構成

C-secureCRT 符号を多段構成にすることで, 図 3 に示すように冗長となる符号を追跡に再利用する手法を提案する. 最初に以下の語句を定義する.

- 最外内符号：最も外側の内符号
- 最内内符号：最も内側の内符号
- 第 i 内符号：最外内符号から i 番目の内符号
- d：多段構成にする際に確保するブロック数

m を内符号の数, 互いに素な数列を $p_0, p_1, \ldots, p_{m-1}$ とし, これらの整数を法と呼ぶ. p_0 を最も大きい法とし, p_{i+1}を $p_i - 2 \times d$ よりも小さい最大の法, または, $p_i - 2 \times d$ よりも小さい法が無い場合は,p_{i+1} 以前に使用されていない最大の法とする. 各法を用いて 3 章と同構成の内符号を作成し, 多段構成に置き換えた符号を連結して外符号を作成する.

5.2 追跡アルゴリズム

多段構成の c-secureCRT 符号の追跡アルゴリズムを説明する. 追跡アルゴリズム A_3 を多段構成に対応するように拡張したものであり, 追跡アルゴリズム A_{multi} と定義する. 以下の関数を用意する.

- decode(X):X を多段構成から単一構成に複合する
- chk_multi_stage(d,p_i, p_{i+1}):p_{i+1}が $p_i - 2 \times d$ よりも小さければ TRUE, 大きければ FALSE を返す.

追跡は以下のステップで行われる

ステップ 1) 入手した不正コピーから L ビットの埋め込み情報 X を抽出する.

ステップ 2) X から, 以下のように x_i を作成する.

$$decode(X) = \underbrace{x_0}_{t(p_0-1)bit} \;||\; \underbrace{x_1}_{t(p_1-1)bit} \;||\cdots||\; \underbrace{x_{m-1}}_{t(p_{m-1}-1)bit}$$

x_i は, 単一構成の形式に戻したものになっている. ただし, 最内内符号以外は単一構成に正しく複合できず, 両端から d 以外は不明な符号で構成されている.

ステップ 3) 各 $x_i (i = 0, 1, \ldots, m-1)$ について追跡アルゴリズム A_{multi} を適用する. 3,9 行目で最内内符号以外は, 両端からの距離 d よりも内側のブロックになった時点で追跡に失敗したものとしている.

Algorithm A_{multi}

1:input x_i;

2:for($min_i = 0; min_i < p_i - 1; min_i++$){
3: if(chk_multi_stage(d,p_i, p_{i+1})) $\wedge$ ($min_i \geq d$){
4: $min_i = -1$;
5: break;}
6: if(($hw_{min}(x) > hw_F$) $\wedge$ ($hw_{min+1}(x_i) > hw_F$) $\wedge \ldots \wedge$ ($hw_{min+ad_{th}-1}(x_i) > hw_F$))$break$;
7:}
8:for($max_i = p_i - 1; max_i > min_i; max_i--$){
9:if(chk_multi_stage(d,p_i, p_{i+1}))$\wedge$($max_i \leq p_i - d$){
10: $max_i = -1$;
11: break;}
12: if(($hw_{max_i}(x_i) < t - hw_B$)$\wedge$($hw_{max} < t - hw_B$) $\wedge \ldots \wedge$ ($hw_{max-adth+2}(x_i) < t - hw_B$))$break$;
13:}
14:output min_i *and* max_i;

“$\wedge$” は AND 論理演算子である.

A_{multi} の出力 min_i, max_i をそれぞれ $r_i^{(-)}$,$r_i^{(+)}$ とする．ここで min_i, max_i が -1 の値を取るときは, 最少・最大剰余の検出に失敗したことを意味する.

ステップ 4) ステップ 3 で得られた各剰余対を用いて, 全てのユーザについて以下に示す D(u) を求める.

$$D(u) = |\{i \in Z_m | (u \equiv r_i^{(-)} (mod\ p_i)) \vee (u \equiv r_i^{(+)} (mod\ p_i))\}|, 0 \leq D(u) \leq m \quad (14)$$

“$\vee$” は OR 論理演算子である.

$r_i^{(-)}$,$r_i^{(+)}$ が -1 の時は, 剰余が負となることはないため合同式を満たすことはなくカウントされない.

ステップ 5) しきい値 Dth=k+l に対して,$D(u) \geq Dth$ となるユーザ u を結託者として出力する.

6. 結託者追跡実験

従来方式を c-secureCRT 符号のみを用いた場合, 提案方式 1 を c-secureCRT 符号と非結託者識別符号の複合方式, 提案方式 2 を c-secureCRT 符号を多段構成にした方式とし, 表 1 のパラメータを用いて結託者追跡実験を行う． ここで c は想定最大結託人数,n は総配布ユーザ数,t はブロック長, m は c-secureCRT 符号の内符号の数,p_i は c-secureCRT 符号の各法であり, p_{min}, p_{max} は法の最小値, 最大値である．L は埋め込み符号長,Dth は c-secureCRT 符号の追跡の際のしきい値である．また,N は非結託者識別符号の法の値,M は非結託者識別符号の数であり, d は多段構成の際に確保する両端からのブロック数である．実験時の前提を以下に示す.

- 結託攻撃は marking assumption が成立する範囲で行われる

表 1 実験パラメータ

パラメータ	従来方式	提案方式 1	提案方式 2
c(人)	15	15	15
n(人)	10000	10000	10000
t	25	25	25
m	52	50	66
p_{min}	103	103	103
p_{max}	367	359	449
L(bit)	2.9×10^5	2.9×10^5	1.5×10^5
Dth	5,7	5,7	7
N	none	48	none
M	none	13	none
d	none	none	34
追跡アルゴリズム	A_3	A_3	A_{multi}

- 結託攻撃は, 違いが認められたビットをランダムに改変することを想定する.
- 結託攻撃を行った後にランダム誤りを付加し, ビットの反転を行う.

また, 全ユーザ ID のうち,0,1,$\cdots$,366 までを weakID として除いてシミュレーションを行った.ID として小さな値を持つユーザは内符号の追跡アルゴリズムに追跡される確率が高く, 偏った追跡結果となる可能性があるため, 法の最大値よりも小さな値を weakID として除くことで追跡精度の劣化を抑制している.[5] 各ユーザに割り振る ID は 367,368,...10367 とする．提案方式 1 では m を小さくして, 符号長が従来方式よりも大きくならないように非結託者識別符号を追加する.

6.1 結託耐性符号と非結託者識別符号の複合方式による追跡実験

以下の手順によって提案方式 1 の埋め込み, 抽出, 追跡のシミュレーションを行う.

手順 1）オリジナルデータを符号長が 6.0×10^5 で 0 または 1 のどちらかの値をランダムに取る PN 系列として作成する. オリジナルデータにおいて c-secureCRT 符号, 非結託者識別符号, 共通ビットの埋め込み位置を重複しないように設定する. ここで共通ビットとは, すべてのユーザで共通するビットである.

手順 2）367 から 10367 までの数字をランダムに c 個選び, 結託グループに設定する.

手順 3）各ユーザに対応する c-secureCRT 符号を作成し, オリジナルデータに埋め込む.

手順 4）各ユーザに対応する非結託者識別符号を作成し, オリジナルデータに埋め込む.

手順 5）c 人による結託攻撃を行う.

手順 6）手順 5) によって生成された改変データにさらにランダム誤り e を付加する.e は 1.0×10^{-1} から 4.0×10^{-1} までの範囲とする.

手順 7）攻撃後の改変データから埋め込み情報を抽出

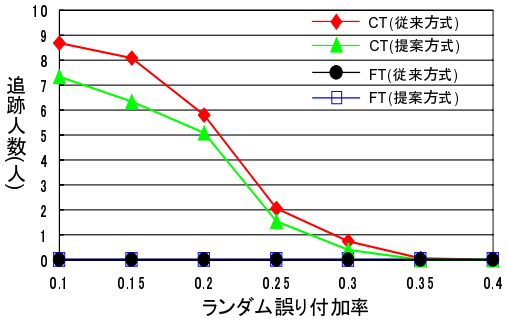

図 4 しきい値 Dth=7 の追跡精度比較

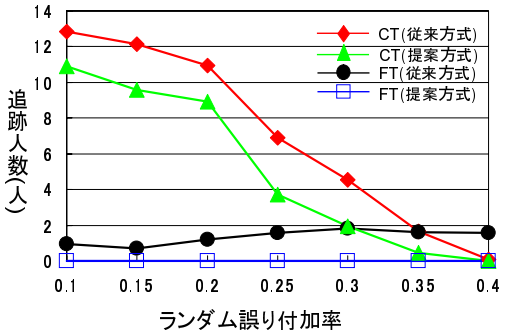

図 5 しきい値 Dth=5 の追跡精度比較

し, 非結託者識別符号を用いて結託者候補を絞りこんでから,A_3 による追跡アルゴリズムを行う.

結果を平均追跡成功人数 CT（人）, 平均誤追跡人数 FT（人）に関して, 従来方式との比較を行う.

図 4, 図 5 に従来方式と提案方式 1 のしきい値 Dth が 7 と 5 の場合の結託者追跡の結果を示す. 図は 20 回の試行の平均である. 横軸はランダム誤り付加率, 縦軸は追跡人数を表す. 図 4 ではどちらも誤追跡が発生していないが, 図 5 では従来方式において誤追跡が発生している. 一方, 提案方式では誤追跡は発生しておらず, より安全な追跡が行えていると言える.

6.2 多段構成 c-secureCRT 符号による追跡実験

c-secureCRT 符号を多段構成にした方式について, 従来方式との比較を行う. 実験手順は提案方式 1 において, 作成する符号を多段構成にし, 非結託者識別符号を使用しないようにしたものである. 追跡アルゴリズムには A_{multi} を用いる. 図 6 に c-secureCRT 符号の多段構成の結託者追跡結果を示す. 図は 20 回の試行の平均であり, 誤追跡は発生していない. 図 6 より, 従来方式よりも良い追跡精度が得られていることがわかる. さらに提案方式の符号長は 1.5×10^5 であり, 符号長を 51 %に削減することができた. 以上より,c-secureCRT 符号を多段構成にすることで符号長の削減と追跡精度の向上が可能であることを示した.

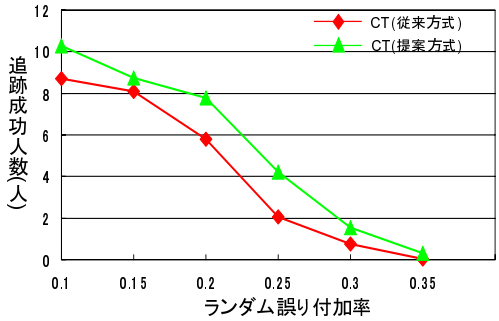

図 6 c-secureCRT 符号多段構成の追跡結果

7. ま と め

本研究では, コンテンツフィンガープリンティングにおける結託耐性符号の問題となる追跡精度と符号長の大きさについて,C-secureCRT 符号の結託耐性と非結託者識別性を組み合わせることによって誤追跡を抑える方式と, c-secureCRT 符号を多段構成にすることで, 符号長を削減し, 追跡精度を向上させる方式の提案を行った. 従来方式よりも誤追跡の起こりにくい結託者の追跡が可能となり, 符号長を約半分にすることに成功した. 本稿では結託攻撃として, 得られた feasible set に対しランダムに改変を行うことを仮定している. 今後の課題は, 様々な結託攻撃に耐性を持つようにすることである.

参 考 文 献

1) D.Boneh and J.Shaw: *"Collusion-secure fingerprinting for digital data"* IEEE Transactions on Information Theory 44 pp1897-1905(1998)
2) Francesc Sebe and Josep Domingo-Ferrer: *"Short 3-Secure Fingerprinting Codes for Copyright Protection"*Proceedings of ACISP'02, LNCS Vol.2384,pp316-327(2002)
3) Hans Georg Schaathun: *"The Boneh-Shaw Fingerprinting Scheme is Better than We Thought"* Technical Report 256,Department of Informatics,University of Bergen (2003)
4) 村谷博文: *"Random Error Resilience of c-secure CRT code"* CSS' 2000,pp73-78(2000)
5) 村谷博文: **"結託耐性符号のランダム誤り制御"**ISEC2000-83 pp29-36,(2000)
6) 吉岡克成, 松本勉: *"Random-Error Resilience of a Short Collusion-Secure Code"* IEICE TRANS. FUNDAMENTALS,Vol.E86-A,NO.5, pp1147-1155(2003)