L-058

ネットワークモデル上の結託攻撃に対する電子指紋の安全性

○鈴木一実* 草苅良至** 能登谷淳一** 笠井雅夫**
*秋田県立大学システム科学技術研究科 **秋田県立大学システム科学技術学部

1 はじめに

近年、様々なマルチメディアコンテンツがデジタル化されて、インターネットなどのネットワーク上で配布されるようになってきた。これらのデジタルデータは容易に複製することができ、瞬く間に世界中に再配布することができる。このようなことからネットワークを通じて配布されるデジタル化されたマルチメディアコンテンツの著作権侵害が頻繁に起きるようになっている。

こうした問題を解決する技術として、電子指紋技術が挙げられる。電子指紋とは「コンテンツの特徴を損なわないように埋め込まれたコンテンツ自体とは別の情報」のことである。電子指紋はコンテンツの利用者には秘密に埋め込まれる利用者 ID として働き、コンテンツの配布者はネットワーク上の電子指紋を識別することですべての利用者を一意に識別することができる。もし利用者にコンテンツの複製を作成されてネットワーク上に再配布されたとしても、再配布されたコンテンツはすべて同じ電子指紋であることから、どの利用者再配布しているのかをつきとめることができる。このようにマルチメディアコンテンツの著作権保護技術として電子指紋技術が注目されている。

2 電子指紋技術

2.1 電子指紋モデル

本稿で扱うモデルでは、**配布者d**がn人の**利用者** $u_1, u_2, \dots, u_n$に電子指紋をあらかじめ埋め込んだコンテンツを配布するものとする。**電子指紋w**はビット長lの２進数列とする。

$$w \in W = \{0,1\}^l$$

ここで、Wを**電子指紋空間**と呼ぶ。電子指紋wのi番目のビットを$\langle w \rangle_i$と表す。各$i, (1 \le i \le n)$に対して配布者dは利用者u_iに電子指紋$w_i \in W$を割り振る。このように配布者dによって利用者$u_1, u_2, \dots, u_n$に割り振られた電子指紋を**正規の電子指紋**と呼ぶ。n人の利用者に割り振る正規の電子指紋の集合を**符号**と呼び、$\Gamma = \{w_1, w_2, \dots, w_n\}$と表す。

本稿では複数の利用者が結託して電子指紋を攻撃する結託攻撃に焦点をあてる。このような結託攻撃においては印仮定に基づいて議論されることが多い。[1]本稿でも以下の印仮定に従うものとする。

> 印仮定
> 単独の利用者ではコンテンツの内のどこに電子指紋が埋め込まれているのか特定することができない。２人以上の利用者が結託すればお互いのコンテンツを比較することで、ビットが異なっている部分の電子指紋部分は特定することができる。電子指紋部分は削除することができない。特定された電子指紋部分を任意のビット(0 or 1)に書き換えることができる。

2.2 結託攻撃

符号Γの空でない部分集合を**結託$C \subseteq \Gamma$**と呼ぶ。r個の電子指紋からなる結託は

$$C = \{w_{C_1}, w_{C_2}, \dots, w_{C_r}\} \subseteq \Gamma$$

と表される。$1 \le i \le r$に対して$1 \le C_i \le n$である。結託$C = \{w_{C_1}, w_{C_2}, \dots, w_{C_r}\}$中の電子指紋$w_{C_i}$を割り振られた利用者$u_{C_i}$の集合$\{u_{C_1}, u_{C_2}, \dots, u_{C_r}\}$も**結託**と呼ぶ。

結託したr人の利用者はお互いのコンテンツを比較することで、コンテンツのビットが異なっている部分から電子指紋部分を特定することができる。結託$C = \{w_{C_1}, w_{C_2}, \dots, w_{C_r}\}$に対して全ての電子指紋のi番目のビットが同じならば、結託Cによってもコンテンツに埋め込まれている電子指紋のi番目のビットの位置を特定することはできない。しかし、結託$C = \{w_{C_1}, w_{C_2}, \dots, w_{C_r}\}$にi番目のビットが異なっている電子指紋が含まれているならば、結託Cは埋め込まれている電子指紋のi番目のビットの位置を特定することができる。結託した利用者は電子指紋の特定されたi番目のビットを任意に書き換えることで、他の利用者に割り振られた電子指紋や正規の電子指紋ではない電子指紋を作り出すことができる。

結託により作り出される電子指紋の集合を結託Cによる**偽造電子指紋集合**といい、F(C)と表す。

$$F(C) = \{w \in \{0,1\}^n | \forall i \in [1,n], \exists w' \in C, \langle w \rangle_i = \langle w' \rangle_i\}$$

F(C)は集合であるが、以下に示すようにl個の記号の列で表現することができる。

$$\langle F(C) \rangle_i = \begin{cases} 0 & \langle w_{C_1} \rangle_i = \langle w_{C_2} \rangle_i = \cdots = \langle w_{C_r} \rangle_i = 0 \text{ のとき} \\ 1 & \langle w_{C_1} \rangle_i = \langle w_{C_2} \rangle_i = \cdots = \langle w_{C_r} \rangle_i = 1 \text{ のとき} \\ * & \text{その他} \end{cases}$$

ここで、＊ は任意項であり 0 あるいは 1 を表す。

ある結託$C \subseteq \Gamma$が存在して、結託Cによって偽造される電子指紋を**不正な電子指紋**と呼ぶ。

2.3 安全性

符号Γに対して電子指紋$w \in W$を偽造できる結託を**被疑結託**と呼ぶ。すなわち、$w \in F(C)$となるような結託Cが被疑結託である。符号Γと電子指紋$w \in W$に対して、wを偽造できる全ての被疑結託の集合を**被疑結託族**と呼ぶ。すなわち、被疑結託族$S(w;\Gamma)$は次式で定義される。

$$S(w;\Gamma) = \{C \subseteq \Gamma | w \in F(C)\}$$

被疑結託族Sに対して、全ての結託$C_i \in S$が共通部分を持てば、すなわち、$\bigcap_{C_i \in S} = \emptyset$であるならば結託族Sは**中心的**である。$\bigcap_{C_i \in S}$を結託族Sの中心と呼び、Core(S)と表す.

3 閾値モデル

符号Γに対して、形成することができる結託族は2^{2^n}通り考えられる。したがって、被疑結託族$S(w,\Gamma)$は2^{2^n}通りのいずれかである。このような膨大な種類の被疑結託族が中心的であるかを調べることは、計算機を用いたとしても多くの時間を必要とし困難である。このようなことから結託の形成に制限を加えて電子指紋の安全性を評価する研究が行われている。制限方法の代表的なものとして、結託に参加できる利用者数を制限する閾値モデルがある[1]。このモデルにおいては結託に参加できる利用者の数の上限を閾値とする。

符号Γに対して結託に含まれる電子指紋の個数が閾値c以

下と制限されている場合の被疑結託族を$S(w; c, \Gamma)$と表す。

$$S(w; c, \Gamma) = \{C \subseteq \Gamma | 1 \leq |C| \leq c, w \in F(C)\}$$

4 ネットワークモデル

4.1 ネットワークモデルでの結託の形成

ネットワークモデルでは結託を形成できる利用者は必ず知り合いであると仮定する。したがって、利用者間の知り合い関係は**利用者ネットワーク**と呼ばれるグラフ$G(\Gamma, E)$で表わされるとする。ここで、辺集合Eは

$$E = \{(w_i, w_j) | w_i, w_j \in \Gamma, w_i \text{を配布された利用者} u_i \text{と} w_j \text{を配布された利用者} u_j \text{は知り合い}\}$$

を意味する。このように結託の形成を利用者ネットワークにより制限しているモデルを**ネットワークモデル**と呼ぶ。ネットワークモデルでは利用者同士が利用者ネットワーク上で連結でなければ、その利用者同士は知り合いではないので結託することができない。連結であればその利用者間は知り合い同士なので結託することができる。

グラフ$G = (\Gamma, E)$において結託Cは点集合Γの部分集合であり、結託Cにより誘導される部分グラフを結託ネットワークと呼び$G[C]$と書く。ネットワークモデルでは結託ネットワーク$G[C]$が非連結ならば偽造できないという仮定を新たに加える。この仮定によりネットワーク$G = (\Gamma, E)$における不正電子指紋$w \in W$の被疑結託族$S(w; G)$を次のように定義する。

$$S(w; G) = \{C \subseteq \Gamma | G[C] \text{は連結}, w \in F(C)\}$$

また、ネットワークモデルにおいて閾値cを持つ被疑結託族$S(w; c, G)$を次のように定義する。

$$S(w; c, G) = \{C | C \in S(w; G), 1 \leq |C| \leq c\}$$
$$= \{C | G[C] \text{は連結}, w \in F(C), 1 \leq |C| \leq c\}$$

4.2 ネットワークモデルの安全指標

利用者ネットワーク$G = (\Gamma, E)$での被疑結託族$S(w; c, G)$が中心的であるならば、中心に含まれる正規の電子指紋w_{C_i}が割り振られている利用者u_{C_i}は電子指紋の偽造をした犯人だといえる。

一方、偽造電子指紋集合において次の性質が成り立つ。

$$C \subseteq C' \text{ならば } F(C) \subseteq F(C')$$

よって、各結託$C \subseteq \Gamma$での偽造電子指紋集合$F(C)$は符号Γ全体の偽造電子指紋集合$F(\Gamma)$に包含される。$F(\Gamma)$に含まれる多くの電子指紋$w \in F(\Gamma)$に対して、wに関する被疑結託族$S(w; \Gamma)$が中心的であることが望まれる。この考え方に基づいて安全指標を定義する。符号Γに対して被疑結託族$S(w; \Gamma)$が中心的となるような電子指紋$w \in F(\Gamma)$の集合を中心集合と呼び、$Core(\Gamma) \subseteq F(\Gamma)$と表す。このとき、

$$I_{Core}(\Gamma) = \frac{|Core(\Gamma)|}{|F(\Gamma)|}$$

を符号Γにおける中心率と呼ぶ。同様に利用者ネットワーク$G = (\Gamma, E)$と閾値cに対して被疑結託族$S(w; c, G)$に関する中心集合を$Core(c, G)$と表す。このとき

$$I_{Core}(c, G) = \frac{|Core(c, G)|}{|F(\Gamma)|}$$

を閾値ネットワークモデルでの中心率と呼ぶ。中心率は大きいほど安全性が高いと考えられる。また、中心率$I_{Core}(\Gamma)$が 1 の符号Γは中心的であり、中心率$I_{Core}(c, G)$が 1 の利用者ネットワーク$G = (\Gamma, E)$は閾値cで中心的である。本稿ではこの中心率をシミュレーションによって実験的に推定する。

5 安全指標の実験的検証

不正な電子指紋wを$F(\Gamma)$内でランダムに発見したとして、不正な電子指紋wの被疑結託族$S(w; c, \Gamma)$が中心的であるかを実験的に調べる。今回は利用者ネットワークに完全グラフと WS グラフを適用して実験を行う。WS グラフとは近隣に位置する点との繋がりは密であるが、遠くに離れた点との繋がりは疎であるようなグラフである[2]。WS グラフにおいて次数kが大きくなる程、密なグラフが得られる。

5.1 シミュレーション方法

① 符号Γをランダムに生成してn人の利用者$u_1, u_2, \ldots, u_n$に割り振る。また、利用者ネットワークを$G = (\Gamma, E)$、閾値をcとする。

② 偽造電子指紋集合$F(\Gamma)$から不正な電子指紋wを 1 つランダムに選択する。

③ 不正な電子指紋wに対する被疑結託族$S(w; c, G)$を求め、被疑結託族$S(w; c, G)$が中心的であるかどうかを判定する。

④ ①～③の手順を 100 回繰り返して符号Γの中心率を求める。

5.2 実験結果

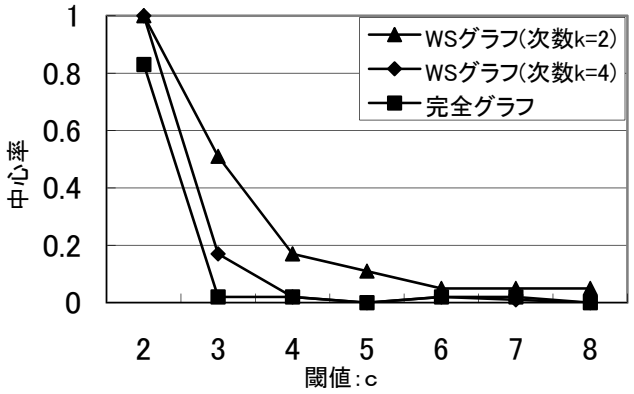

図１　利用者ネットワークごとの中心率の比較
（ビット長：$l = 15$、利用者数：$n = 15$）

6 まとめ

提案したネットワークモデルにおける電子指紋の中心率については、利用者ネットワークによる利用者同士の繋がりが密であるほど中心率は低くなり、疎になるほど中心率が高くなることがわかった。利用者同士の繋がりが密ならば形成できる結託の種類が増えるので、中心的となる電子指紋の割合が減少し、逆に疎であるならば結託の種類が減少するからだと考えられる。このようにネットワークモデルでは利用者ネットワークが結託の形成に大きな影響を与え、中心率が異なってくることがわかった。

7 参考文献

[1] Kozo BANNO, Shingo ORIHARA, Takaaki MIZUKI, Takao NISHIZEKI, “Best Security Index for Digital Fingerprinting” IEICE TRANS.FUNDAMENTALS, VOL.E89-A,NO.1 JANUARY 2006.

[2] 増田直紀　今野紀雄　“複雑ネットワークの科学” 産業図書