A-012

グラフ制約を持つ結託攻撃に対する電子透かしの安全指標
Safety measures for digital watermarking against collusion attacks under graph constraints

鈴木 一実† 草苅 良至‡ 能登谷 純一‡ 笠井 雅夫‡
Suzuki Kazumi Kusakari Yoshiyuki Notoya Junniti Kasai Masao

1. はじめに

近年、音楽、静止画像、動画像などのディジタルコンテンツが違法に複製されることが問題となっている。電子透かしは、このようなディジタルコンテンツの違法な複製を抑止する技術として利用できる。電子透かしをディジタルコンテンツに一対一に対応するように埋め込むことで、電子透かしによりディジタルコンテンツを判別することが可能となる。電子透かしの埋め込まれたディジタルコンテンツが複製された場合、電子透かしも複製される。よって、複製の元となるディジタルコンテンツを特定できると期待される。このことが、ディジタルコンテンツの違法な複製の抑止になると考えられる。しかし、電子透かしの埋め込まれた複数のディジタルコンテンツを比較することで電子透かし部分を特定し、改竄する結託攻撃と呼ばれる攻撃法がある。結託攻撃を受けると、最初に埋め込まれてあった電子透かしとは異なる電子透かしに改竄されるために、複製の元となるディジタルコンテンツを特定できなくなる。

本稿では、結託攻撃を行う際の結託の形成に、グラフによる制約を与えた場合の電子透かしの安全性を考える。また、グラフ制約を持つ結託攻撃に対するランダムな電子透かしの安全指標を提案する。

2. 電子透かしの安全性

2.1 電子透かし

2.1.1 電子透かしの形態

n 個のディジタルコンテンツにランダムな電子透かしを一対一に対応するように埋め込んで配布する場合を考える。電子透かし w は l ビットのビット列とし、電子透かしがとりえる空間は $W=\{0,1\}^l$ とする。すなわち、

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

である。電子透かし空間 W から n 個のディジタルコンテンツと一対一に対応するように埋め込むランダムな電子透かしの集合 $\{w_1, w_2, \ldots, w_n\} \subseteq W$ を符号 Γ とする。すなわち、

$$\Gamma = \{w_1, w_2, \ldots, w_n\} \subseteq W$$

である。

2.1.2 攻撃に対する仮定

本稿では、結託攻撃に対する電子透かしの安全性を考えることを主な目的とする。このことから、次の2つの仮定に従うものとする。

- ディジタルコンテンツに電子透かし w が埋め込まれる位置を、一つのディジタルコンテンツから特定することはできない。
- ディジタルコンテンツに電子透かし w は直接に埋め込まれており、ディジタルコンテンツと一体となっているので電子透かし自体を削除することはできない。

2.2 電子透かしに対する攻撃

2.2.1 結託攻撃

結託攻撃とは、2つ以上のディジタルコンテンツのビット列を相互に比較することで、ビットの異なっている部分から電子透かしが埋め込まれている位置を特定・改竄する攻撃方法である。結託攻撃を行う際に、符号 Γ の部分集合 $C \subseteq \Gamma$ とする結託を形成する必要がある。したがって、符号 Γ の r 個の電子透かしで形成される結託 C は次のように表される。

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

ここで、$1 \le i \le r$ に対して $1 \le C_i \le n$ であり、結託 C に含まれる電子透かし数を $r = |C|$ と表す。また、電子透かし w の i 番目のビットを $\langle w \rangle_i$ と表す。$\forall i \in \{1,2,\ldots l\}$ に対して、$\exists j \in \{1,2,\ldots r\}, \exists j' \in \{1,2,\ldots,r\}, j \neq j', \langle w_{C_j} \rangle_i \wedge \langle w_{C_{j'}} \rangle_i$ ならば、$\langle w_{C_j} \rangle_i$ が電子透かしの一部であるとわかる。また、$\exists j \in \{1,2,\ldots,r\}, \forall j' = \{1,2,\ldots,r\}, j = j', \langle w_{C_j} \rangle_i \wedge \langle w_{C_{j'}} \rangle_i$ ならば、$\langle w_{C_j} \rangle_i$ が電子透かしの一部であるかはわからない。特定した電子透かしの部分は任意の $\{0,1\}$ に書き換えることができる。

2.2.2 偽造電子透かし

結託 $C \subseteq \Gamma$ の結託攻撃により偽造される電子透かしの集合を偽造電子透かし集合と呼び、$F(C) \subseteq W$ と表す。すなわち、$F(C)$ は次式で定義される。

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

したがって、偽造電子透かし集合 $F(C)$ の $\langle F(C) \rangle_i$ は次のように表される。

$$\langle F(C) \rangle_i = \begin{cases} 0 & if \ \langle w_{C_1} \rangle_i = \langle w_{C_2} \rangle_i = \cdots = \langle w_{C_r} \rangle_i = 0 \\ 1 & if \ \langle w_{C_1} \rangle_i = \langle w_{C_2} \rangle_i = \cdots = \langle w_{C_r} \rangle_i = 1 \\ * & otherwise \end{cases}$$

ここで、$*$ は任意なビットで 0 または 1 を表す。

2.3 被疑結託族

電子透かし $w \in F(C)$ を偽造できるすべての結託 $C \subseteq \Gamma$ を被疑結託と呼ぶ。電子透かし $w \in F(C)$ に対する被疑結託 $C \subseteq \Gamma$ の集合を被疑結託族 $S(w;\Gamma)$ と呼び、次式で定義される。

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

被疑結託族 $S(w;\Gamma)$ の被疑結託 $C_i \in S(w;\Gamma)$ の共通部分 $\bigcap_{C_i \in S(w;\Gamma)} C_i$ に電子透かし w が存在するならば、それは電子透かし $w \in F(C)$ を偽造するために必要不可欠である。つまり、すべての被疑結託 $C_i \in S(w;\Gamma)$ の共通部分 $\bigcap_{C_i \in S(w;\Gamma)} C_i$ は電子透かし $w \in F(C)$ を偽造した電子透かしである。このような $\bigcap_{C_i \in S(w;\Gamma)} C_i$ を被疑結託族 $S(w;\Gamma)$ の中心と呼び、$Core(S)$ と表す。$\bigcap_{C_i \in S(w;\Gamma)} C_i \neq \varnothing$ な被疑結託族 $S(w;\Gamma)$ を中心的であると呼ぶことにする。

3. グラフ制約

3.1 グラフ制約があるときの結託可能性

結託攻撃では、結託 C は $2^{|\Gamma|}$ 個の種類がある。また、被疑結託族 $S(w;\Gamma)$ は $2^{2^{|\Gamma|}}$ 通りのいずれかである。したがって、符号数 $|\Gamma|$ が増えると結託 C の種類は指数関数的に増える。電子透かし $w \in \Gamma$ に対する被疑結託族が中心的かどうかを調べることは計算量の面で困難である。そこで、結託の形成にグラフ制約を持つモデルを考える。

3.2 グラフ制約を持つ被疑結託族

電子透かし $w \in \Gamma$ を頂点とするグラフ $G(\Gamma, E)$ が与えられるとする。ここで、辺集合 E によって結託可能な関係を表す。すなわち、辺集合 E を次式で定義する。

$$E = \{(w_i, w_{i'}) \mid w_i, w_{i'} \in \Gamma, w_i \text{と} w_{i'} \text{は結託可能}\}$$

電子透かし集合 $C \subseteq \Gamma$ から誘導されるグラフ $G(\Gamma, E)$ の誘導部分グラフを $G[C]$ と表す。誘導部分グラフ $G[C]$ が連結ならば集合 C は結託を形成することが出来、非連結ならば形成できないものとする。したがって、グラフ $G(\Gamma, E)$ に対する被疑結託族 $S(w;G)$ を次式で定義する。

$$S(w;G) = \{C \in \Gamma \mid G[C] \text{は連結グラフ}, w \in F(C)\}$$

4. 安全指標

4.1 ランダム符号の中心率

結託攻撃に対する安全な電子透かしは、電子透かし $w \in \Gamma$ に対する被疑結託族 $S(w;\Gamma)$ が中心的になることが望まれる。また、結託 C, C' による偽造電子透かし集合 $F(C), F(C')$ では、次の関係が成り立つ。

$$C \subseteq C', F(C) \subseteq F(C')$$

したがって、結託 $C \subseteq \Gamma$ に対して $F(C) \subseteq F(\Gamma)$ が成り立つ。このような性質から、電子透かし $w \in F(C)$ よりも、電子透かし $w \in F(\Gamma)$ に対する被疑結託族 $S(w;\Gamma)$ が中心的になることが望まれる。これらの考えに基づいて、結託攻撃に対するランダムな符号 Γ の安全指標として中心率 $I_{Core}(\Gamma)$ を考える。中心率 $I_{Core}(\Gamma)$ は偽造電子透かし集合 $F(\Gamma)$ における電子透かし $w \in F(\Gamma)$ に対する被疑結託族 $S(w;\Gamma)$ が中心的になる割合と定める。すなわち、中心率 $I_{Core}(\Gamma)$ を次式で定義する。

$$I_{Core}(\Gamma) = \frac{\sum_{w \in F(\Gamma)} |Core(S(w;\Gamma)) \neq \varnothing|}{|F(\Gamma)|}$$

4.2 グラフ制約を持つランダム符号の中心率

4.2.1 結託可能率

$|\Gamma| = n$ になる符号 Γ のグラフ $G(\Gamma, E)$ で、n 個の頂点から $|C| = r$ になる結託 C を選ぶ組み合わせの総数に対して誘導部分グラフ $G[C]$ が連結である割合を結託可能率 $K(G[C])$ と定める。すなわち、次式で定義する。

$$K(G[C]) = \frac{\sum_{C \subseteq \Gamma} |G[C] \text{が連結}|}{\binom{n}{r}}$$

4.2.2 中心的になる確率

$|C| = r$ 個のランダムな結託 $C \subseteq \Gamma \subseteq \{0,1\}^l$ による電子透かし $w \in F(C)$ に対して、被疑結託族 $S(w;\Gamma)$ が中心的になる確率を考える。$\forall i \in \{1,2,\ldots,l\}$ に対して、$\exists j \in \{1,2,\ldots,r\}, \forall j', j \neq j' \in \{1,2,\ldots,r\}, \langle w_{C_j} \rangle_i \wedge \langle w_{C_{j'}} \rangle_i$ または、$\langle w_{C_j} \rangle_i \wedge \langle w_{C_{j'}} \rangle_i$ ならば、電子透かし $w \in F(C)$ に対する被疑結託族 $S(w;\Gamma)$ に $Core(S(w;\Gamma))$ が生成される。したがって、ランダム符号の場合、電子透かし集合 $C \subseteq \Gamma \subseteq \{0,1\}^l$ による電子透かし $w \in F(C)$ の被疑結託族 $S(w;\Gamma)$ が中心的になる確率は $\{1-(1/2)^{|C|-1}\}^l$ である。

4.2.3 グラフ制約を持つ中心率

グラフ制約を持つ場合の中心率 $I_{Core}(G)$ は、グラフ $G(\Gamma, E)$ に対する誘導部分グラフ $G[C]$ が連結であるような $F(C)$ における電子透かし $w \in F(C)$ に対する被疑結託族 $S(w;G)$ が中心的になる割合である。したがって、グラフ $G(\Gamma, E)$ に対する連結な誘導部分グラフ $G[C]$ の割合である結託可能率 $K(G[C])$ と、電子透かし集合 $w \in F(C)$ に対する被疑結託族 $S(w;\Gamma)$ が中心的になる確率 $\{1-(1/2)^{|C|-1}\}^l$ の積から中心率 $I_{Core}(G)$ は求まる。すなわち、グラフ制約を持つ中心率 $I_{Core}(G)$ は次式を満たす。

$$I_{Core}(G) = K(G[C]) \cdot \{1-(1/2)^{|C|-1}\}^l$$

4.3 シミュレーション結果

符号数 $|\Gamma| = 10000$, 符号長 $l = 100$

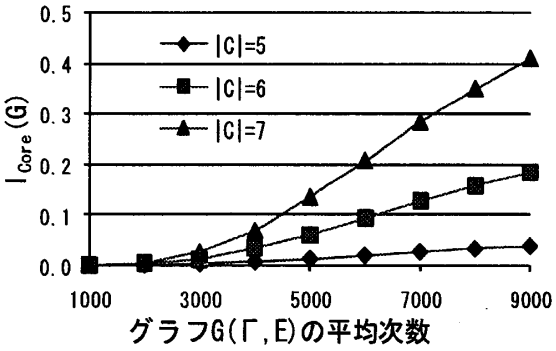

図1　グラフ $G(\Gamma, E)$ の次数変化による中心率の推移

5. まとめ

グラフ制約を持つ結託攻撃に対するランダムな電子透かしの安全指標として中心率 $I_{Core}(G)$ を定義した。中心率 $I_{Core}(G)$ は結託数 $|C|$ が増えるほど高くなる傾向にあることがわかった。また、グラフ $G(\Gamma, E)$ の平均次数が増えるほど中心率 $I_{Core}(G)$ が高くなる傾向にあることがわかった。

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 (2008).

[2]増田 直紀,今野 紀雄, "複雑ネットワークの科学", 産業図書

†秋田県立大学大学院

‡秋田県立大学