様式 C-19

科学研究費補助金研究成果報告書

平成２２年　４月１３日現在

研究種目：基盤研究(C)
研究期間：2007 年度～2009 年度
課題番号：19560397
研究課題名（和文）　アルゴリズム公開型電子透かしに関する研究

研究課題名（英文）　A Research on Public Algorithm Digital Watermark

研究代表者
岩村 恵市（IWAMURA KEIICHI）
東京理科大学・工学部電気工学科・教授
研究者番号：10434028

研究成果の概要（和文）：電子透かしの安全性に関する基準を構築し、アルゴリズム公開可能な電子透かし方式を実現するために種々の検討を行った。まず、電子透かしの安全性に関する一つの基準として、電子透かしの評価ツールを開発し、効率的で統一的な評価を可能にした。また、電子透かしのアルゴリズム公開可能性については、まず電子透かしをその応用形態に応じて分類し、いくつかの種類の電子透かしに関してアルゴリズム公開の可能性を示した。その結果、印刷物保護用電子透かしと、改竄位置検出用電子透かし、可視電子透かし、可逆電子透かしに関し、アルゴリズム公開や標準化の議論の第一歩となる成果を得ることができた。

研究成果の概要（英文）：We constructed a criteria on security of digital watermark, and researched digital watermarking schemes which can open the algorithm up to the public. The first result is having developed an evaluation tool of digital watermarking to use as a criteria on security of digital watermark. This tool can perform efficient and unific evaluation. The second result is a classification of digital watermarking according to applications and some digital watermarking schemes which can open the algorithm up to the public such as paper document watermarking, visible watermarking and reversible watermarking. These results can be used as the first step of the discussion on algorithm standardization or public presentation for digital watermarking.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	2,4000,000	720,000	3,120,000
２００８年度	600,000	180,000	780,000
２００９年度	600,000	180,000	780,000
年度			
年度			
総　計	3,600,000	1,080,000	4,680,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：著作権保護・コンテンツ保護、アルゴリズム、電子透かし、暗号・認証

様式 C-19

科学研究費補助金研究成果報告書

１．研究開始当初の背景

電子透かし技術はデジタルコンテンツ保護に必須と言われながら、その安全性に根拠をもたないため、アルゴリズムの公開ができず、技術の標準化などが困難である。また、電子透かしに対する攻撃手法や安全性評価手法も統一されておらず、評価の共通基準となるものがない。さらに、電子透かしは著作権保護や、原本性保証など種々の応用形態があるが、アルゴリズム公開型電子透かしという観点から、それらは体系的に研究されていない。

２．研究の目的

本研究は電子透かしの安全性評価の共通基準となる評価ツールを作成することを第１の目的とする。これによって、アルゴリズムが公開されていなくても、その安全性（強度）や画質に関しては、統一的な評価が可能になる。さらに、従来の評価ツールに不足しており、かつ電子透かしにとっては最も強力な攻撃と言える、複数のユーザが結託して各々の電子透かし画像を比較し、それらの差分から電子透かしの改変を行う結託攻撃などの攻撃を加えたツールとし、種々の攻撃手法に対する耐性を評価できるようにする。

さらに、種々の応用形態に対してアルゴリズム公開型電子透かしに関する研究を体系的に行い、標準化などの議論が可能となる基盤を構築することを最終目的とする。ただし、応募時の書類にも明記しているように、本研究の研究期間では全ての応用形態について研究を行い、統一的な観点からアルゴリズム公開型電子透かしを体系化することは時間的に困難であるため、本研究期間ではいくつかの応用形態についてアルゴリズム公開型電子透かしの可能性を検討し、今後の議論の基盤となる結果を導くことを第２の目的とする。

３．研究の方法

今回の研究期間内において、まず第１の目的を実現するために応募書類に示したように、以下の(1)を実施する。次に、第２の目的であるいくつかの応用形態についてアルゴリズム公開型電子透かしの可能性を検討に対しても同様に、以下の(2)(3)の研究を行う。

(1) 電子透かしに対する評価ツールとして、電子透かしに対して攻撃を行い、その耐性を評価できるツールを２種類開発する。１つは、アルゴリズムの解析･再現を可能にするツールを開発する。もう１つは、複数の異なる電子透かし画像を比較し、それらの差分から電子透かしの改変を行ういわゆる結託攻撃を行えるツールを開発する。

(2)アルゴリズム公開型電子透かしに関する研究と攻撃を体系化する。特に、著作権主張や原本性確認などの電子透かしの応用形態毎に従来の研究と攻撃を分類し、その応用形態で想定すべき複数の攻撃からなる攻撃群を明らかにする。さらに、その攻撃群の種類とその対応のしやすさによって、各応用形態の優先順位付けを行い、安全性と実用性が両立しやすい応用形態の順番を明らかにする。

(3)(2)で最も実現しやすいとされた応用形態を完全にカバーできるアルゴリズム公開型電子透かし手法を提案する。これは、少なくとも１つの応用形態においてアルゴリズムが公開され、かつその応用形態で想定すべき全ての攻撃に対して安全性の根拠を持つ電子透かし手法が実現できることを意味する。

４．研究成果

研究の方法に示した項目ごとに研究成果を示す。

(1) ２種類の攻撃ツールの機能を１つにまとめた攻撃ツールを開発した（最終頁にその外観を示す)。

このツールは、従来の画像処理を中心とした攻撃機能に加え、従来ツールに不足している結託攻撃を強化した攻撃機能を併せ持つ。すなわち、メニューバーのファイルから目的の画像を入力画像１または入力画像２に表示させ、従来の画像処理攻撃を行うときはメニューバーの単一画像攻撃から所定の攻撃を選択し実行する。また、結託攻撃を行うときは、複数画像攻撃から所定の攻撃を選択し実行する。ここで、単一画像攻撃に含まれる攻撃には従来の攻撃ツール（特に、Stirmark と JEWELS）に含まれる全ての攻撃が選択可能である。また、複数画像攻撃には結託のさせ方に応じて２種類の結託攻撃と平均値攻撃、差分攻撃が選択可能である（各攻撃に関する詳細説明は省略)。

また、従来の攻撃ツールがコマンドラインベースの使い勝手の良くないツールであったのに対し、図からわかるように攻撃結果に応じて次の攻撃を効率的に選択できるよう、GUI を生かして画像を見ながらの攻撃が可能である。すなわち、元画像は左の入力画像１、攻撃結果の画像は右の出力画像に表示されるため、その結果に応じて連続的に攻撃をメニューバーから選択可能である。よって、従来ツールに比べて強力かつ多彩な攻撃能力を持ち、さらに操作性や使い勝手は数段によい。

さらに、アルゴリズムの解析･再現を可能

とできるよう、任意の電子透かしや誤り訂正方式を追加できる機能を加え、さらに従来の攻撃にない新たな解析ができるよう各種画像処理の基本処理も行えるよう拡張した。すなわち、メニューバーの電子透かしや入力/ECC から追加した種々の電子透かし方式や誤り訂正方式が選択可能である。透かしとして埋め込む情報は左下の透かし入力に入れ、抽出結果は左の透かし出力に表示される。また、メニューバーの画像解析にはいくつかの画像フィルタが実装されており、電子透かしアルゴリズムの解析に用いることができる。

以上によって、今までなかった電子透かし評価に対する基盤ツールが構築でき、今後の評価基準とできるようになった。

この成果として雑誌論文 1 件[3]が採録され、国際会議 1 件[5]、国内発表 1 件[10]が行われた。

(2)電子透かしを強耐性電子透かしと弱耐性電子透かしに分類し、さらに強耐性電子透かしを応用形態に応じてデジタルコンテンツ保護用電子透かしと印刷物保護用電子透かしに分類した。また、弱耐性電子透かしに関しても、応用形態毎に改竄位置検出用電子透かし、可視電子透かし、可逆電子透かしなどに分類した。また、応用形態毎にアルゴリズム公開の可能性を検討し、攻撃をまとめた。

その結果、弱耐性電子透かしは透かし情報の破壊を防止するものではないため、暗号技術と組み合わせることにより、その暗号技術を安全性の根拠とできる場合が多いが、強耐性電子透かしは透かしの破壊自体を防止するもののため、暗号技術と組み合わせても有効でなく、安全性の根拠を持たせることは難しい場合が多いことがわかった。ただし、印刷物はデジタルコンテンツに比べて、人間が知覚できないような攻撃・改編が困難である。すなわち、デジタルコンテンツは素人でも画像エディタを用いれば人間に知覚できないような改編は容易に行え、それら全てに対応できる電子透かしの実現は現時点では困難であるが、印刷物は物質であるため、人間に知覚できないような自然な改編を容易に行うことは困難である、よって、対処すべき攻撃が限られ、印刷物保護用電子透かしはアルゴリズムを公開の可能性がある。ただし、印刷物保護用電子透かしは紙幣の偽造などと同様に莫大な費用をかければ、人間に知覚できないような改編が可能である。そのため、今回は素人が可能と思われる範囲の攻撃を想定した。

この成果は、(3)のアルゴリズム公開型電子透かし手法の各提案とともに論文にまとめた。よって、具体的な成果は(3)参照。

(3) 強耐性電子透かしのうち、デジタルコンテンツ保護用電子透かしのアルゴリズム公開は最も困難と思われるが、上記のように印刷物保護用の電子透かしはアルゴリズム公開の可能性がある。また、情報漏洩の経路として印刷物によるものが､2007 年度で 40.4%、2008 年度では全体の 55.9%にも上るという報告もあり、印刷物の保護技術は重要性が高い。よって、強耐性電子透かしでは印刷物保護用電子透かしに関して重点的に研究を行い、2 件の査読論文[1][2]と、2 件の国際会議発表[4][7]と、4 件の国内発表[11][12][13][16]を行った。ただし、この印刷物保護用電子透かしの研究は従来研究自体が少なく、かつまだ研究途中であり、アルゴリズムを公開しても完全に安全な手法は完成していない。よって、この技術を完成させるためには今後も研究を継続していく必要がある。

一方、弱耐性電子透かしは、暗号技術と組み合わせることにより、安全性の根拠をもたせることができるため、アルゴリズム公開可能なものが多い。特に、改竄位置検出用電子透かしは公開鍵暗号と組み合わせアルゴリズム公開を可能にしたものに関し 1 件の国際会議[6]と、2 件の国内発表[8][9]を行った。これによって、原本性保証のための改竄位置検出用電子透かしに関しては、アルゴリズムを公開しても想定される全ての攻撃に対して安全な電子透かし手法が実現できることが言える。

また、可視透かしも共通鍵暗号と組み合わせることによってアルゴリズム公開を可能にしたものに関し 1 件の国内発表[15]を行った。さらに、可逆電子透かしに関しては、アルゴリズム公開については未検討であるが、埋め込み容量について従来法を上回る手法について 1 件の国内発表[14]を行った。可視透かしや可逆透かしについては今後、国際会議や査読論文として発表していく予定である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 3 件）

1. 金田北洋，平野謙二，藤井雄騎，岩村惠市，半谷精一郎，“難視性パターンを用いた印刷文書に対する情報付加手法の提案”，情処学論，Vol.50, No.9, pp.1997-2007, Sep. 2009.
2. 金田北洋，藤井雄騎，鬼頭祐太，岩村惠市，半谷精一郎，“難視性パターンを用いた情報付加手法における攻撃耐性の改善”, 信学論, Vol.J93-A, No.2, pp.1-11, Feb. 2010.

3. K. Kamiya, K. Naoe, T. Mori, K. Iwamura：“Development and Evaluation of a Benchmark Tool for Digital Watermarking,” International Journal of Innovative Computing, Information and Control, Vol.6, No.3, pp.1305-1312, Mar.2010

〔国際会議発表〕（計４件）

4. K.Kaneda, F.Nagai, K.Iwamura, and S.Hangai: ”Information Hiding Technique using Simple Dot Pattern of High Density for Printed Document,” 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP-2008-IS05-008, Harbin, 2008-8.
5. K.Kamiya, T.Mori, and K.Iwamura: ”Development of Benchmark Tool for Digital Watermarking,” 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP-2008-IS05-009, Harbin, 2008-8.
6. H.Kubota and K.Iwamura: “A New Fragile Watermarking Scheme and its Security Evaluation,” 6th IEEE International Workshop on Digital Rights Management, Las Vegas, 2010-1.
7. K.Kaneda, Y.Fujii, K.Iwamura, S.Hangai : “An Improvement of Robustness against Physical Attacks and Equipment Independence in Information Hiding based on the Artificial Fiber Pattern,” Fourth International Workshop on Advances in Information Security, Krakow, 2010-2.

〔学会発表〕（計９件）

8. 岩村惠市：“公開鍵暗号を用いた改竄位置検出用電子透かしに関する考察と提案”，コンピュータセキュリティシンポジウム 2007 予稿集，１A-1，Oct.2007.
9. 岩村惠市：“アルゴリズム公開型改竄位置検出用電子透かし”，第 2 回マルチメディア情報ハイディング研究会資料，pp.1-6，Nov.2007.
10. 神谷光佑，森拓真，岩村惠市：“電子透かしに対する攻撃ツールの実装”，第 39 回コンピュータセキュリティ研究会．Dec.2007.
11. 金田北洋，永井文也，岩村惠市，半谷精一郎：“単一ドットパターンを用いた印刷文書用電子透かしに関する一提案”，第 4 回マルチメディア情報ハイディング研究会，pp.11-16，Jul.2008.
12. 松原 徳久，矢部 裕久，金田 北洋，岩村惠市：“印刷文書用電子透かしに適した誤り訂正符号”，コンピュータセキュリティシンポジウム 2008，pp.893-898，Oct.2008.
13. 小野 要，李 柱昊，金田 北洋，岩村 惠市:"単一ドットを用いた情報付加手法の文字印刷耐性に関する研究",第 45 回コンピュータセキュリティ研究会，No.16，May 2009
14. 矢部 裕久，岩村 惠市：“可逆電子透かしの埋め込み容量に関する一考察”，コンピュータセキュリティシンポジウム 2009，C1-1，Oct.2009.
15. 片岡 謙一朗，岩村 惠市：“可視型電子透かしに関する提案とその安全性の評価”，コンピュータセキュリティシンポジウム 2009，C1-2，Oct.2009.
16. 松原 徳久，萩原 学，岩村 惠市：”単一ドットを用いた情報付加手法に適した LDPC符号に関する検討”， 暗号と情報セキュリティシンポジウム 2010，3F2-2，Jan.2010.

〔その他〕
ホームページ等
http://www.sec.ee.kagu.tus.ac.jp/iwamura-lab/research/

６．研究組織
(1)研究代表者
岩村惠市（IWAMURA KEIICHI）
東京理科大学・工学部電気工学科・教授
研究者番号：10434028

(2)研究分担者
なし


電子透かし攻撃ツール
ファイル
入力/ECC
電子透かし
単一画像攻撃
複数画像攻撃
画像解析
入力画像1
入力画像2/出力画像
透かし入力
input
透かし出力
output