推薦論文

暗号学的安全性モデルに基づく電子透かしアルゴリズムの評価と改良

金子 聡[†1] 吉浦 裕[†2]

従来の電子透かしの安全性は，埋め込みや検出などのアルゴリズムの非公開を前提としていたが，パブリックレビューや広い普及のためにはアルゴリズムを公開する必要がある．そこで，公開しても安全性を維持できるような電子透かしアルゴリズムを確立するために，暗号分析学を参考にした安全性の分析モデルを提案する．このモデルに基づいて，パッチワークアルゴリズムについて安全性を分析し，脆弱性を明らかにしたうえで，対策案を提案する．

Evaluation and Improvement of Digital Watermarking Algorithm Based on Cryptographic Security Models

Satoshi Kaneko[†1] and Hiroshi Yoshiura[†2]

Existing digital watermarking methods base their security on the assumption that their embedding and detection algorithms are kept secret. These methods are inconvenient, however, for public review and wide uses. A watermarking algorithm that can be open while maintaining its security is therefore needed. To establish the open secure algorithm, this paper proposes security analysis models for digital watermarking based on the analogy to cryptanalysis models. Using the proposed models, the Patchwork algorithm is analyzed to find its weakness and is improved.

1. はじめに

近年，デジタルコンテンツは私たちの生活に浸透しているが，複製や頒布が容易なため著作権侵害が懸念されている．その対策として電子透かし技術がある．電子透かしとはコンテンツに著作権情報や購入者 ID などの情報を埋め込み，必要なときに検出する技術であり，不正コピーを抑止する働きがある．

従来の電子透かしアルゴリズム[1),2)] は，透かしの埋め込みおよび検出手順といったアルゴリズムを非公開にすることを前提としている．しかし，これらのアルゴリズムは安全性をアルゴリズムの秘匿に依存しているので，第三者による評価を受けられない，ソフトウェアとして広く利用できないなどの問題をかかえている．よって，アルゴリズムを公開可能な電子透かしアルゴリズムが必要とされている．

今までも電子透かしアルゴリズムの安全性分析は行われていたが[3)–5)]，攻撃者の能力，目的についての前提が体系的にモデル化されていなかった．また，構想段階の論文が多く，具体的なアルゴリズムに対する安全性分析や改良案を示していなかった．また，透かし埋め込み者，検出者，コンテンツホルダ間のプロトコルを工夫して，透かし埋め込み位置などの秘密情報の秘匿を試みる電子透かし利用プロトコルはいくつか提案されていたが[6)–8)]，いずれも基礎となっている電子透かしアルゴリズムの安全性を前提としていた．

本論文では暗号分析学とのアナロジに基づいて電子透かしアルゴリズムの安全性を分析する枠組みを提案する．そして，従来の電子透かしアルゴリズムの代表例としてパッチワークアルゴリズム[1)] を取り上げ，アルゴリズムを知られることでどんな攻撃が可能かを明

†1 電気通信大学大学院電気通信学研究科
Graduate School of Electro-Communications, The University of Electro-Communications
†2 電気通信大学電気通信学部
Department of Electro-Communications, The University of Electro-Communications

本論文の内容は 2006 年 10 月のコンピュータセキュリティシンポジウム 2006 にて報告され，CSEC 研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

らかにし，対策案を提案する．

本論文は以下のように構成される．2 章で従来の電子透かしの安全性分析について述べる．3 章で前提となるパッチワークアルゴリズムについて述べる．4 章で電子透かしアルゴリズムの安全性分析方法を提案する．5 章で提案方法に基づいてパッチワークアルゴリズムの安全性評価を行う．6 章でアルゴリズムの改良案について述べる．7 章で本論文の内容をまとめる．

2. 従来研究

2.1 電子透かしアルゴリズムの安全性評価

従来も暗号を参考にした電子透かしの安全性分析が行われている．文献 3) は，電子透かしを通信システムと見なし，通信データの改ざんおよび除去への安全性を検討した．特に，透かし入り画像から原画像を推定し，両者の差分をとることで透かし平面を推定する攻撃，またそれを他の透かし入り画像に貼り替える攻撃の可能性を示した．その対策として，透かし平面を原画像に依存して作成する必要性を示した．さらに，攻撃者の能力として透かし埋め込み装置および検出装置の利用可否を考慮する必要性を示した．しかし，これらの分析では，攻撃者の能力，目的についての前提が体系的にモデル化されていなかったので，示された攻撃や対策の有効範囲が不明確であった．

文献 4) は，ステガノグラフィにおいて情報が埋め込まれているか否かの識別可能性を分析した．攻撃を，情報埋め込みコンテンツのみを利用した攻撃，情報埋め込みコンテンツと原コンテンツを利用した攻撃に分類し，後者の場合に，情報埋め込みコンテンツと原コンテンツの差分をとることにより，情報理論的安全性が成立しないことを示した．この脆弱性を解消する方法として，コンテンツ集合を用意し，情報を埋め込む際に原コンテンツをコンテンツ集合からランダムかつ秘密に選択する方法を示した．

文献 5) は，鍵によって原画像の特定位置を透かし情報に置き換える置換型電子透かし方式の安全性を分析した．攻撃者が透かし入り画像のみを利用できるときは，透かし入り画像がシャノンの Perfect Cover であれば透かし平面を特定できない．透かし入り画像と透かし平面を利用できるときは，安全性は透かし入り画像のデータ量に依存する．透かし入り画像と原画像を利用できるときは透かし平面を推定し，透かしを除去可能であることを示した．さらに，置換型だけでなくスペクトル拡散型電子透かしについても分析を行い，同様の結論を得た．

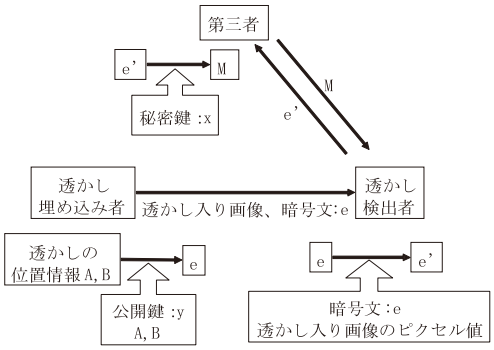

図 1 非対称電子透かしプロトコル
Fig. 1 Asymmetric digital watermarking protocol.

2.2 電子透かし利用プロトコル

従来の多くの電子透かしアルゴリズムでは透かしの埋め込みに使用される鍵と検出に使用される鍵が同じであったために，鍵によって検出者が透かしの位置を特定することができ，透かしを消去したり，任意の埋め込みを行ったりできることが問題であった．そこで，検出者に鍵を渡さないで検出を実行できるように，透かしの埋め込み者，検出者，コンテンツホルダなどの間のプロトコルを工夫する研究が行われている[6)–8)]．

1 つの研究を例にあげる[8)]．この研究は，パッチワークアルゴリズムを基礎として用いており，プロトコルが次のような性質を持つ（**図 1**）．

第三者は，秘密鍵 x のときの El Gamal 暗号の公開鍵 $y = g^x \bmod p$ を生成し，透かし埋め込み者に公開鍵 y を送る．

(1) 透かし埋め込み者は輝度増減を行うピクセル位置集合 A，B を選び（$A \wedge B = \phi$，$|A| = |B| = n$），透かし入り画像を生成し，配布，流通させる．そして，透かし埋め込み者は公開鍵 y およびピクセル位置 A，B から，暗号文 $e(y, A, B)$ を作成する．最後に透かし埋め込み者は，透かし検出者に暗号文 e を送る．

(2) 透かし検出者は透かし入り画像を入手し透かしを検出するときに，透かし入り画像と暗号文 e から暗号文 $e' = (Z, e(y, A, B))$ を生成する．ここで Z とは，透かし入り画像の各ピクセル値を表す．そして，e' を第三者に送る．

(3) 第三者は秘密鍵 x で e' から $M = g^V$ を計算し復号する．ただし，V とは透かしの評価値である．第三者は透かし検出者に M を送る．

(4) 透かし検出者は $M = g^V$ から V を求め，埋め込まれている情報 $\omega = 0$ or 1 を抽出する．なお，V の候補数が少なく，総当たりによって

V を算出できることが前提となっている．

このアルゴリズムは次のことを達成している．

(a) 透かし検出者と第三者に対して透かしの位置 A，B を秘密にする（透かし位置に基づく暗号値だけ送る）ことで，透かしの改ざん，消去を防止．

(b) 第三者に対して画像の中身を秘密にする．

このアルゴリズムは，パッチワークアルゴリズムをベースとしており，そのアルゴリズムが安全であることを暗黙の前提としている．もし，パッチワークアルゴリズムが安全でなければ，上記のプロトコルの安全性は成立しない．たとえば，

① 透かし入り画像を入手したときに，上述したステップ (3) の手順で第三者に依頼し，ステップ (4) により，埋め込まれた情報を知る．

② 一方，様々な A，B を仮定し，パッチワークアルゴリズムの検出手順に従って自分で検出を行い，① と同一の情報が出てきたとき A，B が推定される．

ここで，② が現実的な時間内で可能ならば，結局上記のプロトコルは (a) について安全ではない．

2.3 暗号の安全性モデル

暗号分析学では，分析者は暗号アルゴリズムを細部まで把握していると想定されており，以下の 3 つの観点から分析している[9)–11)]．

2.3.1 攻撃の目的

鍵を特定する，鍵の特定と等価のアルゴリズムを得る，暗号文から平文を推定する，暗号文に操作を加えることにより対応する平文に意図的な変更を加えるなどがある．

2.3.2 攻撃者の能力

暗号文および平文の利用可否といった攻撃者の能力によって分類される．具体的には，いくつかの暗号文のみを利用できる暗号文のみ攻撃，いくつかの暗号文と平文のペアを利用可能な既知平文攻撃，暗号化される平文が選べる選択平文攻撃，前に選んだ平文の暗号化結果を見てから適応的に次の平文の選択を変えることができる適応型選択平文攻撃，いくつかの暗号文を選んで復号してもらい，その復号された平文を入手できるという選択暗号文攻撃などがある．また，暗号化装置および復号装置をオラクルとして利用可能か，といった分類もある．

2.3.3 安全性の評価基準

計算量的安全性[12)]：暗号を解読するアルゴリズムの計算量によって評価される安全性である．多項式時間の計算量である場合は，安全でないと見なされる．多項式時間よりも大きい計算量，たとえば指数時間の計算量である場合は安全であると見なされる．

情報量的安全性[12)]：攻撃者の入手可能なデータ（たとえば暗号文）の情報から，平文に関してどれだけの情報が得られるか，によって評価される安全性である．解読には，無限の計算能力を用いてもよい．

情報量的安全性が成立するならば計算量的安全性は必ず成立するので，情報量的安全性は計算量的安全性よりも上位の安全性基準である．

3. 前提となる電子透かしアルゴリズム

3.1 パッチワークアルゴリズムの概要

本研究の例題として扱うパッチワークアルゴリズム[1)]の具体的な情報の埋め込みおよび検出手順について説明する．

＜情報の埋め込み＞

図 2 が示すように，透かしを埋め込む画像と同じサイズでピクセルの値がすべて 0 である画像を用意する．その画像において，埋め込み情報ビット（b）にピクセル値の変更を行う 2 つのピクセル集合（A，B）を対応付ける．その際，A，B は同数ずつ存在し，かつ重ならないものとする．そして，$b=1$ ならば A に $+1$，B に -1 を，$b=0$ ならば A に -1，B に $+1$ を割り当て，透かし平面を作成する．そして，その透かし平面に割り当てた値（± 1）を δ 倍する．このパラメータ δ を透かしの埋め込み強度と呼ぶ．上記の透かし平面と原画像を重ねて，割り当てた値（$\pm\delta$）に応じて原画像のピクセル値を $\pm\delta$ 加算することで透かし入り画像を作成する．

＜情報の検出＞

適切な正値 T をしきい値として，ビット情報に対応付けられたピクセル集合（A）と（B）のピクセル値の平均値の差分が T 以上であるときに $b=1$ を検出し，$-T$ 以下であるときに $b=0$ を検出する．

ここまで，1 ビットの情報を埋め込む手順を説明したが，これを n ビットに拡張するには，画像を n 分

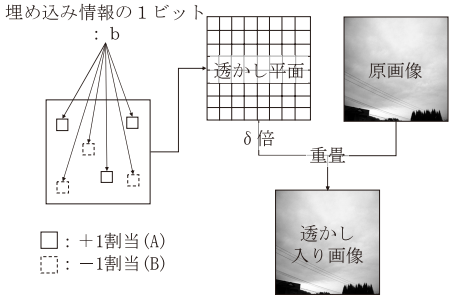

図 2 透かし入り画像の作成例
Fig. 2 Example of watermark embedding.

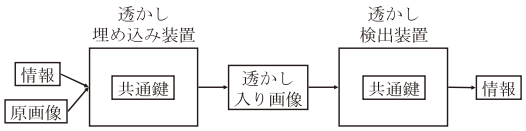

図 3 パッチワークアルゴリズムにおける鍵の利用
Fig. 3 Use of key in Patchwork algorithm.

割して，それぞれについて上述のアルゴリズムを適用すればよい．

3.2 パッチワークアルゴリズムのセキュリティ

パッチワークアルゴリズムのセキュリティを向上させる方策として，情報の埋め込みおよび検出に鍵を用いることが考えられてきた[6)–8)]．これは，暗号において暗号化と復号に共通の鍵を用いる共通鍵暗号モデルと類似したモデルであり，透かしの埋め込みと検出の際に共通の鍵を利用する．

具体的には，**図 3** が示すように，3.1 節の**＜情報の埋め込み＞**の際に，透かし埋め込み装置に内蔵されている共通鍵を用い，埋め込み情報ビットに対応するピクセルの位置を決定する．そして 3.1 節の**＜情報の検出＞**の際には，検出装置に内蔵されている共通鍵を用いて，埋め込みビット情報に対応付けられている透かし入り画像の内部のピクセル位置を特定する．

上記のようにして情報を埋め込む場合，埋め込み情報ビットに対応するピクセルの位置は鍵にのみ依存して決定されるため，原画像はピクセル値の増減を行うピクセル位置の決定に影響を与えない．

4. 分 析 方 法

暗号分析学とのアナロジに基づいて，電子透かしアルゴリズムの安全性の分析方法を提案する．

4.1 分析の前提

パッチワークアルゴリズムの原論文では，安全性に関するアルゴリズムの詳細が規定されていなかった．よって，分析の際に前提条件を定める必要がある．本論文の前提条件を以下に示す．

(1) 埋め込みおよび検出アルゴリズムは公開されている．
(2) 攻撃者は原画像を入手できない．
(3) 攻撃者は透かし入り画像を入手できる．
(4) 攻撃者は埋め込み情報を知っている．
(5) 攻撃者は透かし平面を利用可能な場合がある．

本研究の目的よりアルゴリズムは公開されていると定めた．電子透かしは著作権の保護を目的としているため，原画像は入手できないものとした．透かし入り画像は流通しているため，容易に手に入る．埋め込み情報がそのコンテンツの配布先や所有者の ID などのときは，埋め込み情報を知ることができる．通常知ることのできない暗号値のような情報が埋め込まれている場合も考えられるが，今回はより厳しい条件を仮定して，埋め込まれている情報は既知とした．通常，透かし入り画像において，透かし平面は原画像によって隠されているが，原画像あるいはその一部が平坦であったり連続的なグラデーションな場合，透かし入り画像から透かし平面を推測できる．

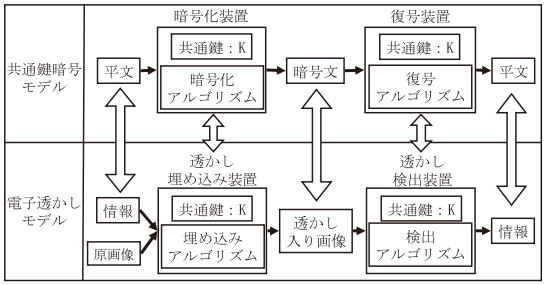

図 4 暗号と電子透かしの対応付け
Fig. 4 Mapping cryptography to digital watermarking.

表 1 暗号と電子透かしの対応関係
Table 1 Correspondence between cryptography and digital watermarking.

平文	暗号文	暗号化	復号化
埋め込み情報	透かし入り画像	透かし埋め込み	透かし検出

4.2 暗号と電子透かしとの対応付け

共通鍵暗号モデルと電子透かしを**図 4** のように，平文は埋め込み情報，暗号文は透かし入り画像，暗号化は透かしの埋め込み，復号は透かしの検出と対応付けた．

暗号と電子透かしの対応付けの結果を**表 1** に示す．ここでは，暗号の平文を電子透かしの埋め込み情報に対応付けたが，別の可能性として，電子透かしの原画像に対応付けることも考えられるので，この点について論じる．図 4 に示すように，ここでは，暗号の復号装置を電子透かしの検出装置に対応付けた．復号装置の出力は平文であり，検出装置の出力は埋め込み情報であるので，それらの部分に焦点を当てた場合には，平文を埋め込み情報に対応付けるのが自然となる．

また，埋め込み情報と原画像の一方を，暗号の平文と見なすと，他方は「暗号化のパラメータ」と見なされる．後述するように，本論文では，攻撃者の目的，能力に関して，**表 2** のように場合分けして分析する．たとえば，攻撃目的が，透かし入り画像の改ざんによる「意図した情報の埋め込み」，攻撃者の能力は「埋

め込み装置，検出装置ともに使用不可」の場合を考える．平文を埋め込み情報に対応付けると，電子透かしにおける「意図した情報の埋め込み」は，暗号における「意図した平文を復号させるような暗号文の作成」となる．一方，平文を原画像に対応付けると，暗号パラメータが埋め込み情報に対応することになるので，電子透かしにおける「意図した情報の埋め込み」は，暗号における「意図した暗号化パラメータを復号させるような暗号文の作成」となる．この2つのうち，平文を埋め込み情報に対応付けるほうが，より自然なアナロジとなる．

しかし，暗号化装置と透かし埋め込み装置の対応に着目すると，別の結論になる．すなわち，平文を埋め込み情報に対応付ける場合，原画像をパラメータとして，平文（埋め込み情報）から，暗号文（透かし入り画像）を作成することになる．一方，平文を原画像に対応付ける場合，埋め込み情報をパラメータとして，平文（原画像）から暗号文（透かし入り画像）を作成することになる．この2つのうち，平文を原画像に対応付ける方がより自然なアナロジとなる．このように，平文を埋め込み情報と原画像のいずれにするのが自然かは，分析の視点によるので一概にどちらが良いかは決められない．本論文では，1つの方向として平文を埋め込み情報としたが，平文を原画像とする分析も今後必要と考えられる．

4.3 攻撃の目的

暗号分析学とのアナロジに基づいて以下の2つを想定した．

(1) 鍵の特定および鍵の特定と等価のアルゴリズムの獲得．
(2) 透かし入り画像を改ざんし，異なる情報を埋め込む．

(2)はさらに2つに分類することができる．1つ目は，透かし入り画像を改ざんして，意図した情報を埋め込むというというもの．2つ目は，透かし入り画像を改ざんして，意図した情報でなくても，元とは異なる情報を埋め込めればよいというものである．これら以外に，埋め込み情報を検出できないようにする，という攻撃も考えられる．これは電子透かしにおいては重要な問題であるが，暗号学との対比にそぐわないため本論文では扱わず，今後の課題とする．以上より，下記(a)，(b)，(c)に攻撃の目的を分類し，検討を行う．

(a) 鍵を特定する．
(b) 透かし入り画像を改ざんし，意図した情報を埋め込む．
(c) 透かし入り画像を改ざんし，元とは異なる情報を埋め込む．

4.4 攻撃者の能力

4.1節より攻撃者は埋め込み情報および透かし入り画像を利用可能であり，場合に応じて透かし平面を利用可能である．

また暗号分析学との対比より，暗号の暗号化装置および復号装置に相当する透かし埋め込み装置および検出装置の使用可否も考慮する．

（ア）透かし埋め込み装置の使用可否

攻撃者が埋め込み装置を使用可能な状況としては，ASP（Application Service Provider）などがネットワーク経由で透かし埋め込みサービスを提供しており[13),14)]，外部の攻撃者がそのサービスを通じて埋め込み装置を利用する場合が考えられる．また，組織の著作権管理部門などが透かし埋め込みシステムを購入して埋め込みサービスを組織内に提供しており，組織内の攻撃者がその埋め込みサービスを利用する場合も考えられる．透かし埋め込み装置を使用可能な場合，任意の情報を埋め込んだ透かし入り画像を作成可能である．そこで，分析に都合の良い埋め込み情報と透かし入り画像の対を任意に入手することができる．

（イ）透かし検出装置の使用可否

攻撃者が検出装置を使用可能な状況としては，埋め込み装置の場合と同様のケースが考えられる[13)–15)]．検出装置を使用可能な場合，任意の透かし入り画像から埋め込み情報を検出可能である，そこで，分析に都合の良い透かし入り画像と埋め込み情報の対を任意に入手することができる．

攻撃者は透かし埋め込みおよび検出装置を外部から利用するだけであり，内蔵された鍵を取り出すことはできないものとする．また，埋め込み装置と検出装置の鍵は固定であるとする．

4.5 安全性の評価基準

暗号分析学からのアナロジにより，以下の2つの基準を設ける．

計算量的安全性：上述した電子透かしにおける攻撃者の能力を前提として，攻撃の目的達成のためのアルゴリズムの計算量によって評価される安全性である．多項式時間の計算量である場合は，安全でないと見なされる．多項式時間よりも大きい計算量，たとえば指数時間の計算量である場合は安全であると見なされる．

情報量的安全性：上述した電子透かしにおける攻撃者の能力を前提として，攻撃の目的がどれだけ達成できるか，によって評価される安全性である．攻撃には，無限の計算能力を用いてもよい．

これらの2つの基準に加えて，電子透かしに固有の

表 2 パッチワークアルゴリズムの安全性モデル
Table 2 Security model of Patchwork algorithm.

	目的／能力		(a) 鍵の特定	(b) 意図した情報を埋め込む	(c) 異なる情報を埋め込む
	埋	検			
1	×	×	埋め込み情報と透かし入り画像のペアを利用可能であり，暗号における既知平文攻撃に相当.	埋め込み情報と透かし入り画像のペアを利用可能であり，暗号における意図した平文に対応する暗号文を作成する攻撃に相当.	埋め込み情報と透かし入り画像のペアを利用可能であり，元とは異なる平文に対応する暗号文を作成する攻撃に相当する.
2	×	○	暗号における適応的選択暗号文攻撃に相当．また，(a) -1と同様に既知平文攻撃も可能.	暗号における，攻撃者が復号オラクルを利用可能で，意図した平文に対応する暗号文を作成する攻撃に相当.	暗号における，攻撃者が復号オラクルを利用可能で，元とは異なる平文に対応する暗号文を作成する攻撃に相当.
3	○	×	暗号における適応的選択平文攻撃に相当.	暗号における，暗号化オラクルを利用可能で，意図した平文に対応する暗号文を作成する攻撃に相当.	暗号における，暗号化オラクルを利用可能で，元とは異なる平文に対応する暗号文を作成する攻撃に相当.
4	○	○	暗号における適応的選択暗号文攻撃と適応的選択平文攻撃に相当.	暗号における，暗号化オラクルと復号オラクルを利用可能で，意図した平文に対応する暗号文を作成する攻撃に相当.	暗号における，暗号化オラクルと復号オラクルを利用可能で，元とは異なる平文に対応する暗号文を作成する攻撃に相当.

安全性評価基準として，以下を設ける．

上書き不能性：情報を埋め込んだ画像に後から別の情報を埋め込むことで，後に埋め込まれた情報だけが検出され，先に埋め込まれた情報は検出できないようにすることを上書き攻撃と呼ぶ．上述した攻撃者の能力を前提として，攻撃の目的達成のための上書き攻撃がどれだけ可能かにより評価される安全性である．

5. パッチワークアルゴリズムの安全性評価

5.1 安全性モデル

4 章の分析方法に基づいて，パッチワークアルゴリズムの安全性を分析した．分析の際に，(a) 鍵の特定，(b) 意図した情報を埋め込む，(c) 異なる情報を埋め込む，の 3 つの攻撃目的と，攻撃者の能力として，透かし埋め込み装置と検出装置の利用可否，計 4 通りとで場合分けを行った．以下に $3 \times 4 = 12$ 通りの分析結果を示す（表 2）．

＜(a)-1 攻撃者の目的：鍵の特定；攻撃者の能力：埋込装置，検出装置使用不可＞

平文に相当する埋め込み情報と暗号文に相当する透かし入り画像を利用して，暗号における既知平文攻撃に相当する攻撃が可能である．

＜(a)-2 目的：鍵の特定；能力：検出装置のみ使用可能＞

攻撃者は公開されたアルゴリズムに従って，任意の透かし入り画像（暗号文）を作成し，その画像に埋め込まれている情報（平文）を検出可能である．暗号では，任意の暗号文を復号可能である適応的選択暗号文攻撃に相当する．また，(a)-1 と同様に既知平文攻撃も可能である．

＜(a)-3 目的：鍵の特定；能力：埋込装置のみ使用可能＞

攻撃者は埋め込み装置を用いて，任意の埋め込み情報（平文）に対する透かし入り画像（暗号文）を作成可能である．暗号では，任意の平文に対する暗号文を入手可能である適応的選択平文攻撃に相当する．

＜(a)-4 目的：鍵の特定；能力：両装置使用可能＞

(a)-2，(a)-3 の両ケースの攻撃が可能であり，暗号では適応的選択暗号文攻撃と適応的選択平文攻撃に相当する．

＜(b)-1 目的：意図した情報を埋め込む；能力：両装置使用不可＞

攻撃者は埋め込み情報（平文）と透かし入り画像（暗号文）のペアを分析することで，意図した情報（平文）を検出させるような透かし入り画像の作成を試みる．暗号では意図した平文に対応する暗号文を作成する攻撃に相当する．

＜(b)-2 目的：意図した情報を埋め込む；能力：検出装置のみ使用可能＞

(b)-1 において，さらに検出装置を使用可能である．暗号では，復号オラクルを利用可能で，意図した平文に対応する暗号文を作成する攻撃に相当する．

＜(b)-3 目的：意図した情報を埋め込む；能力：埋込装置のみ使用可能＞

攻撃者は埋め込み装置を用いて任意の埋め込み情報（平文）に対する透かし入り画像（暗号文）を作成し，これを分析することで，意図した情報（平文）が検出されるような画像の作成を試みる．暗号では，暗号化オラクルを利用可能で，意図した平文に対応する暗号文を作成する攻撃に相当する．

＜(b)-4 目的：意図した情報を埋め込む；能力：両装置使用可能＞

攻撃者は埋め込み装置と検出装置を用いて意図した情報（平文）が検出されるような透かし入り画像（暗号文）の作成を試みる．暗号では，暗号化オラクルと復号オラクルを利用可能で，意図した平文に対応する暗号文を作成する攻撃に相当する．

＜(c)-1 目的：異なる情報を埋め込む；能力：両装置使用不可＞

攻撃者は埋め込み情報（平文）と透かし入り画像（暗号文）のペアを分析することで元とは異なる情報（平文）に対応する透かし入り画像（暗号文）の作成を試みる．暗号では，元とは異なる平文に対応する暗号文を作成する攻撃に相当する．

＜(c)-2 目的：異なる情報を埋め込む；能力：検出装置のみ使用可能＞

(c)-1 において，さらに検出装置を使用できる．暗号では復号オラクルを利用可能で，元とは異なる平文に対応する暗号文を作成する攻撃に相当する．

＜(c)-3 目的：異なる情報を埋め込む；能力：埋込装置のみ使用可能＞

攻撃者は埋め込み装置を用いて，任意の埋め込み情報（平文）に対する透かし入り画像（暗号文）を作成可能である．暗号では，暗号化オラクルを利用可能で，元とは異なる平文に対応する暗号文を作成する攻撃に相当する．

＜(c)-4 目的：異なる情報を埋め込む；能力：両装置使用可能＞

攻撃者は埋め込み装置と検出装置を用いて任意の埋め込み情報（平文）に対する透かし入り画像（暗号文）を作成可能である．暗号では，暗号化オラクルと復号オラクルを利用可能で，元とは異なる平文に対応する暗号文を作成する攻撃に相当する．

5.2 攻撃方法

5.1 節のモデルに基づいて，$3 \times 4 = 12$ 通りの場合におけるパッチワークアルゴリズムへの攻撃方法を示す．

＜(a)-1 攻撃者の目的：鍵の特定；攻撃者の能力：埋込装置，検出装置使用不可＞

攻撃者は透かし入り画像と埋め込み情報を入手可能であるため，それらを用いて以下の攻撃が可能である．

(1) 公開されたアルゴリズムをもとに，任意の鍵を内蔵した透かし検出装置を作成する．
(2) (1) で作成した透かし検出装置を用いて，入手した透かし入り画像から埋め込み情報を検出する．その結果検出された情報が，入手した埋め込み情報と同一であるとき，そのとき用いた鍵が真の鍵である．もし，同一でなかった場合は，(1) で使用する鍵を変えて (1)，(2) を実行する．この作業を真の鍵が判明するまで繰り返す．

この攻撃の必要とする計算量によって，計算量的安全性が評価される．また，この攻撃は鍵の総当たりを行えば必ず成功する．したがって，無限の計算能力があれば攻撃が成功するので，情報量的安全性は成立しない．

＜(a)-2 目的：鍵の特定；能力：検出装置のみ使用可能＞

(1) 公開されたアルゴリズムをもとに埋め込み装置を作成し，それを用いて透かし入り画像を作成する．
(2) 正規の検出装置を用いて，(1) で作成した透かし入り画像から情報を検出する．
(3) 公開されたアルゴリズムをもとに，任意の鍵を内蔵した検出装置を作成する．
(4) (3) で作成した検出装置を用いて，(1) で作成した透かし入り画像から情報を検出する．
(5) (2) で検出した情報と，(4) で検出した情報が同一であるとき，(4) で用いた鍵が真の鍵である．もし，同一でなかった場合は，(4) で検出した情報を参考にして，(1) で透かし入り画像を適応的に作成し，(2) 以降の作業を繰り返す．

このとき上記 (1) から (5) の処理が現実的な時間内で計算可能か否かで，計算量的安全性が評価される．

＜(a)-3 目的：鍵の特定；能力：埋込装置のみ使用可能＞

(1) 埋め込み装置を用いて，埋め込みビット情報の i 番目だけが異なる 2 つの透かし平面を作成する．
(2) (1) で作成した 2 つの透かし平面を比較することで，i 番目のビット情報に対応するピクセル値の増減部分（透かし埋め込み箇所）を特定する．
(3) (1)，(2) の作業を，全ビットに対して行うことで埋め込み情報と透かし平面の対応関係を特定可能である．

この攻撃は，埋め込みビット数に比例した時間で可能であり，容易に実行可能である．鍵の特定と等価のアルゴリズムを得ることができる．

＜(a)-4 目的：鍵の特定；能力：両装置使用可能＞

(a)-2，(a)-3 の攻撃が可能である．

＜(b)-1 目的：意図した情報を埋め込む；能力：両装置使用不可＞

攻撃者は，埋め込み情報と透かし平面のペアを複数所持しているとき，埋め込み情報と透かし平面の対応

関係を分析可能である．具体的には 2 つの場合がある．1 つ目は，埋め込みビット情報の i 番目だけが異なり，さらに，原画像が同一である 2 つの透かし入り画像を所持している場合．このとき，この 2 つの透かし入り画像を比較することで，i 番目のビット情報に対応するピクセル値の変更部分を特定できる．2 つ目は，4.1 節の (5) より，埋め込みビット情報の i 番目だけが異なる 2 つの透かし入り画像から各々の透かし平面を推定できる場合．このとき，2 つの透かし平面を比較することで，i 番目のビット情報に対応するピクセル値の変更部分を特定できる．この方法の場合は，原画像が異なっていてもよい．この 2 つの方法により透かし平面を分析可能である．

この攻撃は，意図した情報に対応する透かし平面を有意な確率で得ることができる．その透かし平面を任意の透かし入り画像に対して，2 倍の強度で埋め込むことで意図した情報を埋め込むことができる．また，複数ビット異なるペアを複数セット入手し，そこから意図した情報に対応する透かし平面を有意な確率で得るという攻撃に一般化できる可能性がある．

＜(b)-2 目的：意図した情報を埋め込む；能力：検出装置のみ使用可能＞

(b)-1 の方法に加えて以下の攻撃が可能となる．

(1) 公開されたアルゴリズムに従って，透かし平面を作成する．
(2) 検出装置を用いて，(1) で作成した透かし平面から情報を検出する．
(3) (1) で作成した透かし平面の一部を固定したまま，ほかの部分を変更した透かし平面を作成する．
(4) 検出装置を用いて，(3) で作成した透かし平面から情報を検出する．もし，(2) と (4) で検出した情報に同じ部分が存在する場合，その部分は (3) で固定した透かし平面の一部と対応していると考えられる．この作業を，(3) で固定する位置を変えながら繰り返すことで埋め込み情報と透かし平面の対応関係を特定可能である．

この攻撃は，透かし平面と埋め込み情報の対応関係を一部分ずつ推定可能なため，攻撃に必要な計算量は鍵の総当たり攻撃に比べて低下する．よって，計算量的安全性が成立しない可能性がある．

＜(b)-3 目的：意図した情報を埋め込む；能力：埋込装置のみ使用可能＞

(a)-3 の方法で鍵を求めて，意図した情報を埋め込む攻撃が可能である．また，埋め込み装置を用いて意図した情報を埋め込む攻撃も可能である．このとき，埋め込み装置の鍵が固定されており，ビットに対応するピクセル集合（A，B）が固定されているため，元々の埋め込み情報に対応した透かし平面が打ち消され，攻撃者が埋め込んだ意図した情報だけが検出されるようになるので，上書き不能性が成立しない．

＜(b)-4 目的：意図した情報を埋め込む；能力：両装置使用可能＞

(b)-3 と同じ攻撃が可能である．

＜(c)-1 目的：異なる情報を埋め込む；能力：両装置使用不可＞

(b)-1 の攻撃をより効率的に実行可能である．(b)-1 では，すべてのビットについてピクセル値の変更部分を求める必要があったが，(c)-1 では 1 ビットでも変更部分が分かれば，そのピクセル値の変更分を反転することで攻撃が可能なため，(b)-1 に比べて容易に実行可能である．それ以外に以下の 2 つの攻撃が可能である．4.1 節の (5) より，透かし平面を利用できるとき，攻撃者はその透かし平面を元とは異なる透かし入り画像に 2 倍の強度で貼り替えることにより，その透かし平面に対応した情報を埋め込むことができる．このとき，埋め込み装置の鍵が固定されており，ビットに対応するピクセル集合（A，B）が固定されているため，元々の埋め込み情報に対応した透かし平面が打ち消され，貼り替えた透かし平面だけが画像内に存在するようになる．その結果，元々の埋め込み情報は検出されず，貼り替えた透かし平面の情報だけが検出されるようになるので，上書き不能性が成立しない．さらに，元となる透かし入り画像に対しては，その透かし平面を反転したものを 2 倍の強度で上書きすることで，1 と 0 を反転した情報を埋め込むことができる．この攻撃は，元となる透かし入り画像に対する貼り替え攻撃であり，上記と同様に，鍵が固定されているため，上書き不能性が成立しない．

＜(c)-2 目的：異なる情報を埋め込む；能力：検出装置のみ使用可能＞

(1) 公開されたアルゴリズムをもとに，任意の鍵を内蔵した透かし埋め込み装置を作成する．
(2) (1) で作成した透かし埋め込み装置を用いて，透かし入り画像に対し元とは異なる情報を 2 倍の強度で埋め込み，新しい透かし入り画像を作成する．
(3) 検出装置を用いて，(2) で作成した透かし入り画像から情報を検出する．検出された情報が元とは異なる情報であるとき攻撃成功となる．もし異なる情報が検出されなかった場合は，(1) で使用する鍵を変えながら (1)，(2)，(3) の作業を繰り返す．

＜(c)-3 目的：異なる情報を埋め込む；能力：埋込装置のみ使用可能＞

(c)-2，(a)-3 および(b)-3 と同じ攻撃が可能である．

＜(c)-4 目的：異なる情報を埋め込む；能力：両装置使用可能＞

(c)-2，(a)-4 および(b)-3 と同じ攻撃が可能である．

5.3 パッチワークアルゴリズムの脆弱性

5.2 節の分析に基づいて脆弱性についてまとめる．まず，無限の計算能力が利用できるならば，5.2 節(a)-1 で述べた攻撃方法で鍵を総当たりすることにより，鍵の特定が可能である．特定した鍵を用いれば，意図した情報埋め込み，異なる情報埋め込みも可能である．したがって，表 2 のすべてのケースにおいて情報量的安全性は成立しない．

上記以外の脆弱性について，以下では**（a）鍵特定**，**（b）意図した情報埋め込み**，**（c）異なる情報埋め込み**に分けて議論する．なお，鍵の特定が可能であれば，それを用いて意図した情報埋め込み，異なる情報埋め込みも可能となり，意図した情報埋め込みが可能であれば，異なる情報埋め込みも可能である．また，埋め込み装置および検出装置の使用可否に関しては，使用不能なケースで攻撃が可能であれば，使用可能なケースでも同じ攻撃が可能である．記載を簡潔にするために，これらの点はデフォールトとし，以下の個別の分析では逐一言及しないものとする．

（a）鍵の特定

（ア）計算量的安全性が成立しないケース

5.2 節(a)-3 のケースが該当する．透かし埋め込み装置を使用することで，埋め込み情報と透かし平面の対応関係を求め，鍵特定と等価のアルゴリズムを得ることができる．

（イ）計算量的安全性が成立しない可能性があるケース

パッチワークアルゴリズムの安全性に関する部分が詳細に定義されていないため，(a)-1 および(a)-2 の攻撃の計算量が不明である．そこで，(a)-1 および(a)-2 では計算量的安全性が成立しない可能性がある．

（b）意図した情報埋め込み

（ア）計算量的安全性が成立しないケース

(b)-3，(b)-4 が該当する．(a)-3 の方法で鍵を特定し，その鍵を用いて攻撃が可能である．

（イ）計算量的安全性が成立しない可能性があるケース

(b)-1 の攻撃は，特定の関係にある埋め込み情報と透かし入り画像を攻撃者がたまたま入手する場合に可能であり，そのようなデータをいったん入手したら計算量的安全性は成立しない．そこで，(b)-1 では計算量的安全性が成立しない可能性がある．パッチワークアルゴリズムの安全性に関する部分が詳細に定義されていないため，5.2 節(b)-2 の攻撃の計算量が不明であり，(b)-2 で計算量的安全性が成立しない可能性がある．

（ウ）上書き不能性が成立しないケース

(b)-3，(b)-4 が該当する．埋め込み装置を用いた上書き攻撃が可能である．

（c）異なる情報埋め込み

（ア）計算量的安全性が成立しないケース

(c)-3，(c)-4 が該当する．(a)-3 の方法で鍵を特定し，その鍵を用いて攻撃が可能である．

（イ）計算量的安全性が成立しない可能性があるケース

パッチワークアルゴリズムの安全性に関する部分が詳細に定義されていないため，5.2 節(c)-2 の攻撃の計算量が不明であり，計算量的安全性が成立しない可能性がある．

（ウ）上書き不能性が成立しないケース

(c)-3，(c)-4 が該当する．(b)-3，(b)-4 と同じ上書き攻撃が可能である．

（エ）上書き不能性が成立しない可能性があるケース

5.2 節(c)-1 のうち貼り替え攻撃は，攻撃者がたまたま透かし平面を利用できる場合に可能となる．そこで，(c)-1 では上書き不能性が成立しない可能性がある．

6. 改 良 案

6.1 提案方式 1

6.1.1 構成と処理

以下の方針に従って，5.3 節で述べた脆弱性の一部を解消する．

(1) 安全性の維持を目的とする部分と，画像への情報埋め込みを目的とする部分を分離する．
(2) 埋め込み情報から透かし平面への変換は 1 対 1 変換とする．また，この変換は二進数から十進数のように形式を変換するだけであり，安全性の手段とはしない．
(3) 安全性維持の部分は，従来の暗号アルゴリズムを用いて構成する．
(4) 電子透かし全体の安全性を（3）で用いた暗号アルゴリズムの安全性に帰着させる．

これらの方針は，以下の単純な構成により実現できる．

提案方式 1 では，従来のパッチワークアルゴリズムに，埋め込み情報の暗号化プロセスを追加する（**図 5**）．

＜情報の埋め込み＞

鍵（K）を用いて，埋め込む情報を暗号化する．そして，暗号化された情報（C）を埋め込み情報と見な

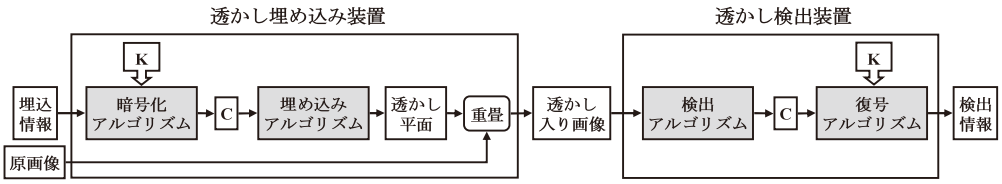

図 5 提案方式 1 の構成
Fig. 5 Structure of proposed method 1.

し，パッチワークアルゴリズムに従い透かし平面を作成し，原画像と重畳することで，透かし入り画像を作成する．このとき，C と透かし平面は 1 対 1 関係にある．

＜情報の検出＞

パッチワークアルゴリズムに従い，暗号化情報（C）を検出する．そして，埋め込みで用いたものと同じ鍵（K）を用いて，検出した情報を復号することで埋め込まれている情報を得る．

6.1.2 安 全 性

5.3 節の各ケースについて安全性を検証する．

(a) 鍵の特定

(ア) 計算量的安全性が成立しないケース

脆弱性の原因は 5.1 節の(a)-3，5.2 節の(a)-3 で述べたように，埋め込み情報を平文，透かし入り画像を暗号文とした適応的選択平文攻撃への脆弱性であった．ここで提案方式 1 の安全性について考えると，まず 3.2 節で述べたように，原画像は透かしの位置決定に影響を与えないため，透かし入り画像を暗号文とした適応的選択平文攻撃に対する安全性と，透かし平面を暗号文とした適応的選択平文攻撃に対する安全性は同等である．さらに，透かし平面と暗号化情報（C）は 1 対 1 関係なので，透かし平面を暗号文とした適応的選択平文攻撃に対する安全性と，暗号化情報（C）を暗号文とした適応的選択平文攻撃に対する安全性は同等である．埋め込み情報を平文，暗号化情報（C）を暗号文とした適応的選択平文攻撃に対する安全性は暗号アルゴリズムの安全性と同等であるため，このケースの安全性は暗号アルゴリズムの安全性に帰着する．

(イ) 計算量的安全性が成立しない可能性があるケース

(a)-1 の攻撃は，埋め込み情報を平文，透かし入り画像を暗号文とした既知平文攻撃であり，(a)-2 の攻撃は，埋め込み情報を平文，透かし入り画像を暗号文とした適応的選択暗号文攻撃に対応する．そこで，上記（a）（ア）で述べた対応関係により，(a)-1，(a)-2 における安全性は，既知平文攻撃および適応的選択暗号文攻撃に対する暗号アルゴリズムの安全性に帰着する．

(b) 意図した情報埋め込み

(ア) 計算量的安全性が成立しないケース

このケースにおける攻撃は，(a)-3 の攻撃（適応的選択平文攻撃による鍵特定）に基づくので，安全性は(a)-3 の攻撃への安全性に帰着する．すなわち，適応的選択平文攻撃に対する暗号アルゴリズムの安全性に帰着する．

(イ) 計算量的安全性が成立しない可能性があるケース

埋め込み情報を平文，透かし入り画像を暗号文として，(b)-1 では，意図した平文に対応する暗号文を作成する攻撃の可能性があった．また，(b)-2 では．復号オラクルを使用して，意図した平文に対応する暗号文を作成する攻撃が可能であった．これらは，上記（a）（ア）で述べた対応関係により，同じ攻撃に対する暗号アルゴリズムの安全性に帰着する．

(ウ) 上書き不能性が成立しないケース

(b)-3，(b)-4 では埋め込み装置を用いた上書き攻撃が可能であった．暗号は上書き攻撃を想定しておらず，対策もしていない．そのため，暗号を用いた提案方式 1 では，本ケースにおける脆弱性は解消されていない．

(c) 異なる情報埋め込み

(ア) 計算量的安全性が成立しないケース

上記（b）（ア）と同様に，適応的選択平文攻撃に対する暗号アルゴリズムの安全性に帰着する．

(イ) 計算量的安全性が成立しない可能性があるケース

(c)-2 の攻撃は，正規の鍵を知らない攻撃者が，透かし入り画像に対して，公開されたアルゴリズムと任意の鍵を用いて，別の情報を 2 倍の強度で埋め込むものであった．この攻撃を受けると，正規の透かし検出装置において，図 5 の検出アルゴリズムが元とは異なる暗号文 C' を検出する可能性がある．暗号では，任意の暗号文から平文が復号される．そのため，いったん C' が検出されると，復号アルゴリズムによって元とは異なる埋め込み情報が復号され，全体として元とは異なる情報の埋め込みに成功する可能性がある．この問題の原因は，暗号では任意の暗号文から平文が復号されることにある．

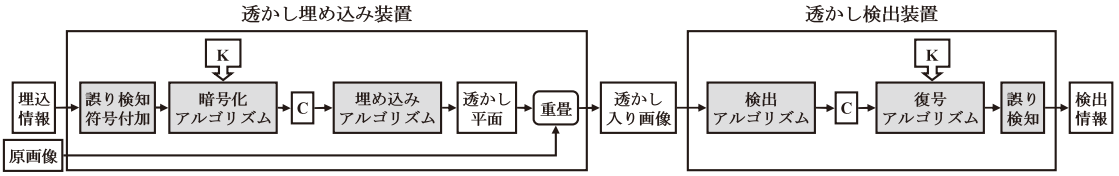

図 6 提案方式 2 の構成
Fig. 6 Structure of proposed method 2.

（ウ）上書き不能性が成立しないケース

上記（b）（ウ）と同じ理由により，(c)-3，(c)-4 における，埋め込み装置を通じた上書き攻撃への脆弱性は解消されていない．

（エ）上書き不能性が成立しない可能性があるケース

上記（b）（ウ）と同じ理由により，(c)-1 における貼り替えを通じた上書き攻撃の可能性は解消されていない．

以上より，提案方式 1 は (a) 鍵特定の全ケース，(b) 意図した情報埋め込みのうち（ア）（イ），(c) 異なる情報埋め込みのうち（ア）における脆弱性を解消している．しかし，(b) の（ウ），(c) の（イ），（ウ），（エ）の脆弱性は解消していない．

6.2 提案方式 2

6.2.1 構成と処理

誤り検知符号を用いることで，6.1.2 項で述べた**(c) 異なる情報埋め込み**の**（イ）計算量的安全性が成立しない可能性があるケース**における脆弱性について，解消を試みる．提案方式 2 の構成を**図 6** に示す．電子透かしアルゴリズムと同様に，誤り検知符号のアルゴリズムは公開されているものとする．

＜情報の埋め込み＞

埋め込み情報に誤り検知符号を付加する．そして，誤り検知符号を付加した埋め込み情報を，鍵 K を用いて暗号化し，暗号化情報 C を得る．以降は，提案方式 1 と同様に透かし入り画像を作成する．

＜情報の検出＞

提案方式 1 に従って暗号化情報 C を得る．埋め込みと同じ鍵 K を用いて暗号化情報 C を復号する．そして，復号した情報に含まれている誤り検知符号により埋め込み情報の改ざんを検知する．

6.2.2 安 全 性

6.1.2 項**(c)（イ）**の攻撃は，任意の鍵を用いた情報埋め込みによって元と異なる情報を検出させるものである．提案方式 2 に対して，この攻撃が成功するためには，正規の透かし検出装置における誤り検知を通過する必要がある．そのためには，正規の鍵 K で復号したときに，埋め込み情報とそれに対する誤り検知符号のペアが復号される必要がある．すなわち，任意の埋め込み情報を I，その誤り検知符号を $E(I)$ とすると，鍵 K によって $I|E(I)$ が復号されるような暗号文を，K を知らない攻撃者が作成できるときに攻撃成功となる．この攻撃に対する安全性は，暗号アルゴリズム，誤り検知アルゴリズム，および，誤り検知符号の符号長に依存する．安全性の厳密な評価は今後の課題となる．

6.3 貼り替えを通じた上書き攻撃への対策案

6.1.2 項の**(c)（エ）上書き不能性が成立しない可能性があるケース**の貼り替え攻撃への対策として，2.1 節の最初の従来研究[3] を参考にして，埋め込み情報に原画像の特徴値を含める方式を考えた．この方式は原画像のうち，透かしの埋め込みによっても変化しない部分の特徴値を埋め込み情報に含める．検出の際には，検出情報と透かし入り画像の整合性から貼り替えの有無を確認する．この方式の安全性については，今後さらに評価する必要がある．

7. おわりに

本論文では，暗号分析学とのアナロジに基づき，攻撃者の目的，攻撃者の能力，安全性のレベルを設定したうえでパッチワークアルゴリズムの安全性を分析し，脆弱性を明らかにした．その分析に基づき，電子透かしの安全性を暗号に帰着させる方式を提案した．この提案方式 1 の安全性をさらに分析し，(1) 任意の鍵を用いた情報埋め込みによって元と異なる情報を検出させる攻撃，(2) 貼り替えを通じた上書き攻撃，(3) 正規の透かし埋め込み装置を用いた上書き攻撃には依然として脆弱であることを示した．そして，誤り検知符号の利用および埋め込み情報に原画像の特徴値を含めることでこれらへの脆弱性を解消する可能性を示した．

今後の課題としては，まず，(1) の任意の鍵を用いた攻撃について，誤り検知符号を利用した提案方式 2 の安全性を評価することがあげられる．また，埋め込み情報に原画像の特徴値を含めるという改良方式を具体化し，(2) の貼り替えを通じた上書き攻撃について，安全性を評価する．さらに，(3) 正規の透かし埋め込

み装置を用いた上書き攻撃について，対策を検討する．最後に，本論文では鍵の推定および埋め込み情報の改ざんに対する安全性を分析したが，電子透かしのもう1つの重要な問題である消去攻撃に対する安全性の分析を行う．

参 考 文 献

1) Bender, W., Gruhl, D., Morimoto, N. and Lu, A.: Techniques for data hiding, *IBM Syst. J.*, Vol.35, No.3&4, pp.313–336 (1996).
2) 電子情報通信学会：情報セキュリティハンドブック，6章情報ハイディング，pp.255–267，オーム社，東京 (2004).
3) Kalker, T.: Considerations on watermarking security, *Proc. 4th IEEE Workshop on Multimedia Signal Processing*, pp.201–206 (2001).
4) Zollner, J., Federrath, H., Klimant, H., Pfitzmann, A., Piotraschke, R., Wextfeld, A., Wicke, G. and Wolf, G.: Modeling the security of steganographic systems, *Proc. Information Hiding 2nd International Workshop*, pp.344–354 (1998).
5) Cayre, F., Fontaine, C. and Furon, T.: Watermarking Security: Theory and Practice, *IEEE Trans. Signal Processing*, Vol.53, No.10, pp.3976–3987 (2005).
6) 岡田満雄，菊地浩明：非対称電子透かしにおける効率的な多ビット埋め込みに関する考察，情報処理学会研究報告，CSEC, Vol.2005, No.70, pp.415–421 (2005).
7) Furukawa, J.: Secure Detection of Watermarks, *IEICE Trans.*, Vol.E87-A, No.1, pp.212–220 (2004).
8) Okada, M. and Kikuchi, H.: Secure Detection of Asymmetric Digital Watermark, *DICOMO* (2005).
9) 電子情報通信学会：情報セキュリティハンドブック，2編10章共通鍵暗号の安全性評価，同11章公開鍵暗号の安全性評価，同12章ハイブリッド暗号の安全性，pp.145–175，オーム社，東京 (2004).
10) 岡本栄司：暗号理論入門，pp.201–210，共立出版，東京 (2002).
11) 岡本龍明，山本博資：現代暗号，産業図書，東京 (2000).
12) 電子情報通信学会：情報セキュリティハンドブック，2編1章暗号の基礎，pp.25–26，オーム社，東京 (2004).
13) NTT コミュニケーションズ：ディジタルコンテンツの不正コピーを抑止する「ライセンシー認証プラットフォーム」サービスの提供開始について (2001). http://www.ntt.com/release/2001NEWS/0012/1219.html
14) コンテンツ ID フォーラム：cIDf 仕様書，第2.0版，Rev. 1.1, pp.45–46 (2007).
15) ケータイ Watch：電子透かし技術を応用したカメラ付き携帯向けの広告サービス実験 (2004). http://k-tai.impress.co.jp/cda/article/news_toppage/17341.html

(平成19年 5 月2日受付)
(平成19年12月4日採録)

推 薦 文

電子透かしのアルゴリズム公開を前提に，その安全性を暗号と同等の立場から評価しており，今後の電子透かし研究の新しいあるべき方向性を示している．具体的には，埋込情報を平文，埋め込み後の画像を暗号文などとして，電子透かしと暗号をマッピングし，電子透かしの安全性評価モデルを提案している．このモデルを用いて，代表的な電子透かしアルゴリズムを評価し，改ざんや鍵推定に関する脆弱性の明確化と改良方式の提案を行っている．このような研究を奨励することにより，電子透かしの安全性評価をオープンに議論できる基礎となっていくと思い推薦する．

（コンピュータセキュリティ研究会主査 寺田真敏）

金子 聡（学生会員）

2006年電気通信大学電気通信学部人間コミュニケーション学科卒業．現在，同大学大学院博士前期課程在学中．電子透かしの研究に従事．

吉浦 裕（正会員）

1981年東京大学理学部情報科学科卒業．日立製作所を経て，2003年より電気通信大学電気通信学部人間コミュニケーション学科勤務．現在，同教授．自然言語処理，知識処理の研究を経て，現在，情報セキュリティ，著作権保護の研究に従事．理学博士．電子情報通信学会，システム制御情報学会，人工知能学会，IEEE 各会員．2000年日立製作所社長技術賞，1990年情報処理学会学術奨励賞，2004年度情報処理学会論文賞，2005年システム制御情報学会産業技術賞受賞．