データハイディングの諸技術とその機能

工学部　栗林 稔

1. データハイディング技術とは

インターネットに代表されるネットワーク通信技術の発達に伴い，情報のやりとりがネットワークを介して頻繁に行われるようになっている．遠く離れた二者間においてネットワーク通信は大変便利なものであるが，悪意のある第三者により二者間の通信が傍受されたり改ざんを加えられたりする恐れがあることも事実である．このような安全性が保証されない通信路を介して安全な通信を行うために，暗号技術が必要不可欠となっている．暗号通信を行えば，二者間で行っている通信内容を第三者から守ることができるため，ネットワークを使った取引などでは重要な役割を果たす．しかしながら，想定する通信環境や条件によっては，暗号技術が必ずしも安全性を保証してくれるとは限らない．例えば，二者間で暗号通信を行う場合，通信内容は秘匿にできるが，何らかの通信が行われていることを第三者に知られてしまう．また，知的著作物を取り扱う場合，暗号技術では第三者による盗聴は防ぐことはできるが，通信相手による複製物の不正配布までは取締ることができない．このような脅威に対する対策として，データハイディング技術が注目を浴びている．

データハイディング (Data Hiding) は，インフォメーションハイディング (Information Hiding) とも呼ばれ，直訳すれば “情報を隠す” という意味であり，秘密の情報を密かに忍ばせることや，通信自体を隠すことを意味する．特に，ディジタルコンテンツを取り扱ったデータハイディングの技術は，広く研究されている．ディジタル画像や映像，音声などのマルチメディアコンテンツには冗長となる成分が多く含まれるため，微小に変化させたとしてもその品質が著しく劣化することはない．この冗長成分を活用することでマルチメディアコンテンツに別の情報を密かに埋め込むことが可能である．図 1 に，データハイディング技術を用いた情報の埋め込みを示す．秘密情報を埋め込む操作は，必ず秘密鍵が用いられる．暗号通信と同様に，この秘密鍵によって埋め込まれた情報の秘匿性を保証している．

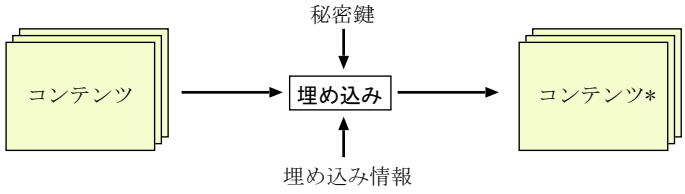

図 1: データハイディングの概略図

データハイディング技術は，その目的や用途によって二種類に分類される．例えば，埋め込む情報が重要でありかつその存在が知られないことが求められる場合には，ステガノグラフィ (Steganography) と呼ばれる．一方，秘密の情報が埋め込まれたコンテンツ自体

が重要な場合には，電子透かし (Digital Watermark) と呼ばれる．

2. ステガノグラフィ

ある二者間の通信において，その通信データが意味不明な記号列ならば，その通信を盗聴した第三者はそれが暗号文であることに気付き，解読を試みるかもしれない．しかし，通信データが意味のある記号列ならば，それが通信内容そのものであると確信するであろう．ここで，表面上は意味のある記号列の体裁をなすが，実はその陰に本当に重要な情報が隠されていれば，盗聴者に気付かれることなく安全な通信が行える．このような通信技術がステガノグラフィである．

ステガノグラフィでは，マルチメディアコンテンツを媒体として，秘密情報が密かに送信され，第三者からは音楽や画像，映像などの送受信が行われているように振る舞う．つまり，ダミーデータの送受信の間に重要なデータの送受信が秘密裏に行われるわけである．以下に，ステガノグラフィに求められる条件を挙げる．

- 秘密情報の埋め込みが知覚されない
- 埋め込み可能な情報量は多い方が望ましい
- 埋め込み位置はどこでもよい
- 攻撃に対する耐性は考慮しなくてよい

秘密情報の埋め込みにおいて，マルチメディアコンテンツの品質をあまり劣化させず，不自然さを生じさせずにできる限り多くの情報を埋め込むことのできる方式が優れたステガノグラフィの技術である．なぜならば，埋め込み可能な情報が多いほど，ダミーデータの送受信が少なくなるため，重要なデータのやりとりが効率良く行われるからである．図 2 に，ステガノグラフィを使った秘密情報の送信モデルを示す．このモデル図では，Alice

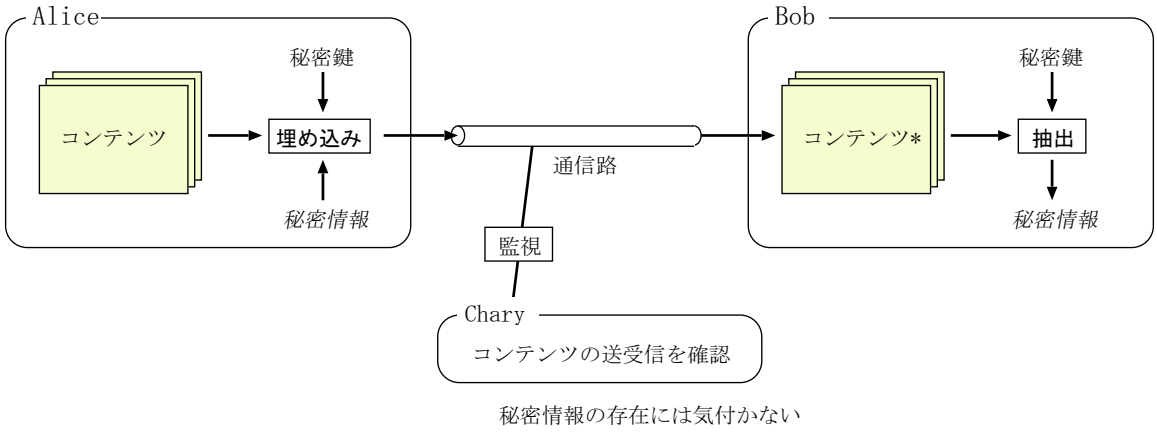

図 2: ステガノグラフィを用いた秘密情報の送信

と Bob がネットワークの監視をしている Chary に知られることなく秘密情報を共有している．実用例として，Alice が Web 上に秘密情報の埋め込まれたコンテンツを公開することが考えられる．この場合，第三者からすれば Bob は Web ページを閲覧しているユーザ

としか認識されない．しかし，実際には秘密情報が Alice から Bob に送られている．

3. 電子透かし

電子透かしは，知的財産であるマルチメディアコンテンツを保護するために識別情報などを埋め込む技術である．透かし情報として著作権情報を用いれば，不正コピーから埋め込まれた情報を取り出すことにより著作権を主張できる．また，購入者を示す情報を埋め込んだ場合には，不正コピーからその流出先を特定できるため，電子指紋としての働きをする．図 3 に，電子透かしを用いた不正者追跡システムの例を示す．ステガノグラフィと

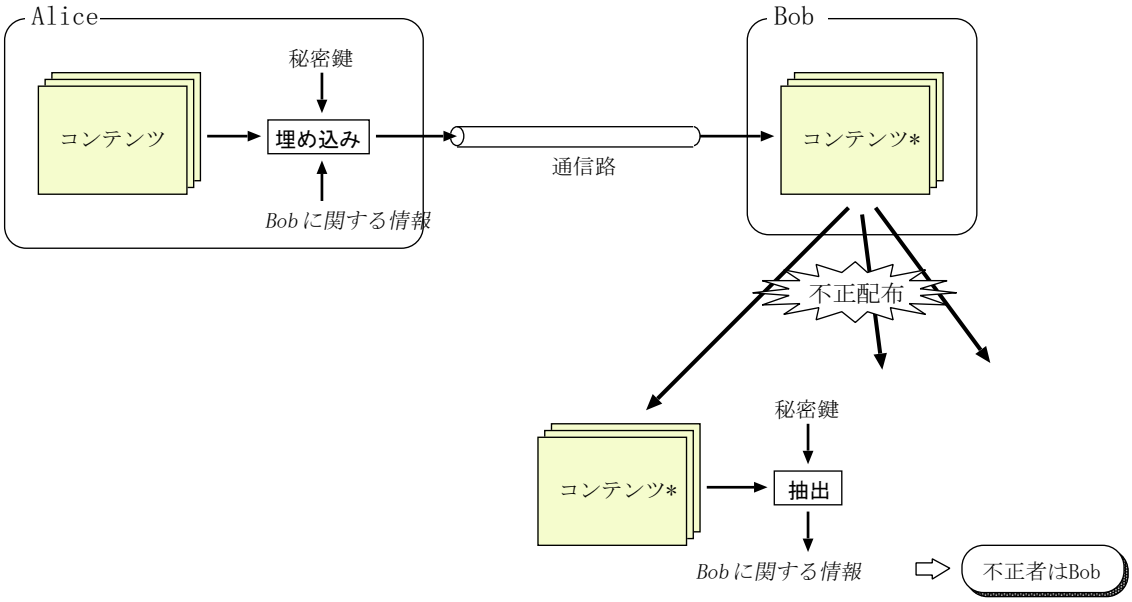

図 3: 電子透かしを用いた不正者追跡システム

の大きな違いは，第三者による攻撃を防ぐのではなく，マルチメディアコンテンツを受信する人が不正な行動をすることを取り締まることを目的としている．

電子透かしでは，マルチメディアコンテンツの中に秘密情報が埋め込まれてあることは公表した上で，送受信が行われる．そのため，透かし情報が埋め込まれていることが知られても秘密鍵がなければ，埋め込まれている情報を取り除いたり，改ざんが困難であることが必須条件となる．以下に，電子透かしに求められる条件を挙げる．

- 秘密情報の埋め込みは知覚されない
- 埋め込む情報量はあまり多くない
- 透かし情報はコンテンツ全体に埋め込む
- 攻撃に対する耐性が高い

秘密情報の埋め込みにおいて，マルチメディアコンテンツの品質をあまり劣化させることなく攻撃に対して耐性の高い方式が優れた方式である．ここで，攻撃とは許容範囲内の品質劣化を伴った埋め込み情報の改ざんや除去操作を意味する．ディジタル画像では，非可逆圧縮や高周波除去フィルタ，微小な拡大縮小，切抜き操作などが行われたとしても，埋め込まれた情報が正しく抽出できることが重要である．埋め込む情報は，“著作者が誰であるか” もしくは “購入者が誰であるか” を識別する情報であるため，識別番号のようなコンパクトな符号を利用すれば埋め込む情報量を抑えることができる．

電子透かしでは，透かし情報の埋め込み処理がされていることを公表し，マルチメディアコンテンツに著作権保護処理が施されていることを購入者に示すことで，著作権侵害となる行為自体を抑制する効果も期待できる．

4. トレードオフ

データハイディング技術では，マルチメディアコンテンツに別の情報を埋め込むために必ず品質劣化が生じる．埋め込む情報量を少なくすれば必然的に品質劣化は抑えられ，反対に多くの情報を埋め込めば品質劣化が激しくなる．

トレードオフの関係を分かりやすく説明するために，マルチメディアコンテンツを主信号として埋め込む情報を雑音と考える．もし，主信号の持つ信号エネルギー E_s に対して雑音の信号エネルギー E_n が小さければ，SN 比が高く品質の高い通信であるとみなせる．反対に，E_n が大きければ，SN 比が低く品質の低い通信となる．E_n をできる限り細かく分割して主信号に加える方式がステガノグラフィであり，適度な大きさの信号エネルギー e_w を持つように E_n を分割した信号を加える方式が電子透かしである．ステガノグラフィの場合，更なる雑音 e_n が分割された成分に加わると元の雑音信号がかき消されてしまう．一方電子透かしでは，$e_w > e_n$ の範囲内であれば元の雑音信号が抽出可能であり，e_n が増加すれば耐性は向上する．しかしながら，雑音信号を細かく分割できないので埋め込める信号の情報量は e_n の増加に伴って減少する．

以上のように，ステガノグラフィと電子透かしではトレードオフの関係が異なる．ステガノグラフィではマルチメディアコンテンツの品質と埋め込み可能な情報量がトレードオフの関係にあるが，電子透かしでは更に攻撃に対する耐性と埋め込み可能な情報量にトレードオフの関係がある．これらの関係より，電子透かしではマルチメディアコンテンツの品質と攻撃に対する耐性の間にもトレードオフの関係があることが導かれる．図 4 にこれらトレードオフの関係を示す．

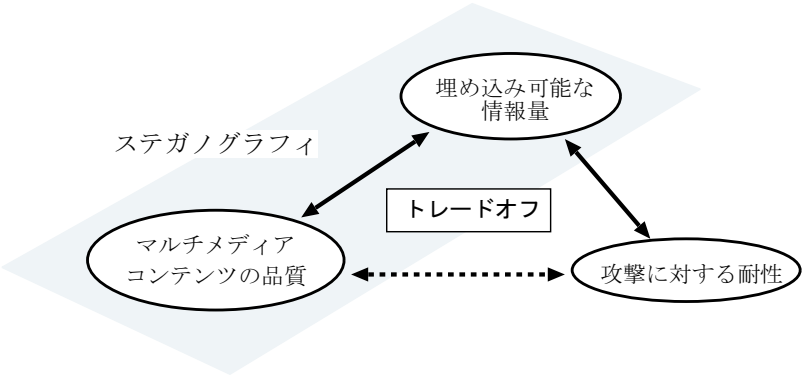

図 4: トレードオフの関係図

データハイディング技術を用いたアプリケーションでは，バランス良くトレードオフの関係を扱うことが重要である．

5. 電子指紋 (Fingerprinting) と不正者追跡

電子指紋は，データハイディング技術と暗号技術を組み合わせて著作権侵害を行った不正者を追跡可能とするための技術である．ネットワーク上での売買において，購入者を示

す情報をコンテンツに埋め込んでおけば，もし，不正コピーが流出したとしても，埋め込まれた電子指紋を検出することで不正者を特定することができる．

電子指紋技術では，販売者と購入者との間で行われる暗号プロトコルが重要となる．もし，販売者が独自に購入者を示す情報 (電子指紋) をコンテンツに埋め込み，それを購入者に送るシステムでは，不正者を法的に訴えることはできない．なぜならば，販売者が電子指紋の埋め込まれたコンテンツを持っているため，販売者がコピーを自ら流出させて購入者を陥れることができるからである．そのため，プロトコル終了後に購入者だけが電子指紋の埋め込まれたコンテンツを得ることができるシステムを暗号技術を用いて実現させる必要がある．

公開鍵暗号方式の中には，準同型写像の性質を有する方式があり，この性質を利用して電子指紋のプロトコルが構築される．準同型写像とは，二つの暗号文を乗算すると別の暗号文となり，そのメッセージが元の暗号文の二つのメッセージにある演算を施したものとなる性質のことである．ここで，ある演算とは，加算，乗算，排他的論理和である．メッセージ m の暗号文を $E(m)$ とすると，準同型写像の性質を有するならば，次の等式を満足する．

$$E(m_1) \cdot E(m_2) = E(g(m_1, m_2)), \tag{1}$$

ただし，$g(\cdot)$ は加算，乗算，排他的論理和の演算であり，用いる暗号方式により異なる．この特徴を利用することで電子指紋を販売者に公開することなく，購入者だけが電子指紋の埋め込まれたコンテンツを得られる．もし，コンテンツを m_1，電子指紋を m_2 とすれば，暗号化された情報を暗号化されたコンテンツに埋め込むことができる．ここで，$g(\cdot)$ の演算を適切に利用すれば，データハイディング技術による情報の埋め込みが実現できる．ここで，暗号化処理には公開鍵暗号方式が用いられているため，埋め込み処理を施された暗号文を復号できるのは復号鍵を所有する購入者だけである．ゆえに，不正コピーが発見された場合，不正者追跡のために電子指紋を検出すれば，不正者がこの購入者であることを販売者は立証できる．図 5 に電子指紋のプロトコルの流れを示す．

電子指紋技術では，暗号プロトコルを効率良く行うために，計算量や通信量を抑えた方式が優れた方式である．また，埋め込まれた電子指紋を改ざんしたり，消去したりする攻撃に対して耐性のある電子透かし技術が重要となる．特に，暗号化されたコンテンツに暗

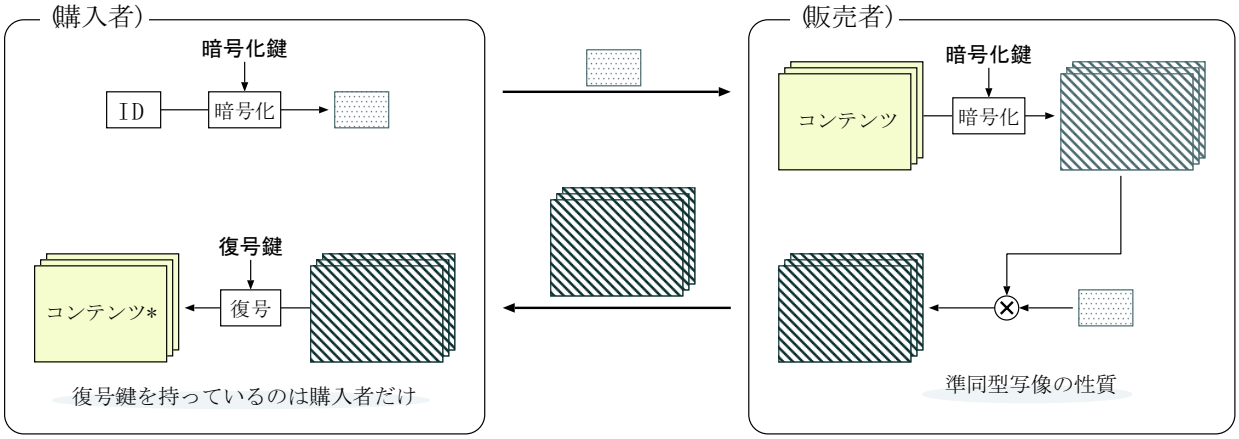

図 5: 電子指紋のプロトコル

号化された情報を埋め込むための工夫が求められている．

6．まとめ

データハイディング技術は，マルチメディアコンテンツを用いて二者間における通信自体を秘匿にさせるステガノグラフィや著作権侵害問題を解決する一つの手法である電子透かしとして発展している．これらの技術は，マルチメディアコンテンツに秘密情報を埋め込む手法という点では同じであるが，使用目的や注目する角度が異なるとその特性が違った技術へと分類される．データハイディング技術は，単純に情報を隠すという枠にとらわれず，今後，新しい特性を兼ね備えた技術が考案されることを期待したい．