■1 群（信号・システム）- 3 編（暗号理論）

13 章 情報ハイディング

（執筆者：渡辺　創）［2009 年 1 月 受領］

■概要■

情報ハイディング（情報隠蔽（ぺい）, information hiding）とは, あるものに本来とは異なる別の情報を秘密裏に埋め込むことをいい, またその際に用いられる技術は情報ハイディング技術と呼ぶ. 埋め込まれる対象データは紙などの媒体であってもよいが, ここではその埋め込まれる対象を, ディジタルデータに限定して主に議論する. FAX 通信や印刷された紙など, 汚れやノイズが入る可能性がある媒体であってもディジタルデータを埋め込めるステガノグラフィ, 電子透かし技術についても研究されている.

情報ハイディング技術はその利用目的, 応用形態により, ステガノグラフィと電子透かしの二つに分類できる.

- ステガノグラフィ（通信秘匿，steganography）

  通信の事実すら秘密にしつつ情報を伝達する技術である.

  多くの場合，別の媒体に情報を秘密裏に埋め込むことにより実現される.

  暗号を用いた通信を表す「秘匿通信」と違うことに注意しなければならない. これは「伝達される情報を秘匿して通信を行うこと」を意味している. 対して「通信秘匿」は「通信の事実, 及び伝達される情報を秘匿して通信を行うこと」を意味している.

- 電子透かし（digital watermarking）

  別の媒体に情報を埋め込むことにより，著作権主張や情報の改ざん検知などの様々な機能を実現する技術である.

  多くの場合, ある情報が伝達されていること自体は知られても構わない. ある場合においては, 電子透かしとして埋め込まれた情報が存在している, ということを明確に宣言することによって, 目的とする機能を高い次元で実現できることもある.

【本章の構成】

本章ではまずステガノグラフィ（13-1 節）について述べ, 次に電子透かし（13-2 節）を説明し, 最後にそれらの関係や近年の動向（13-3 節）についてまとめる.

■1 群 - 3 編 - 13 章

13-1 ステガノグラフィ

（執筆者：渡辺　創）[2009 年 1 月 受領]

ステガノグラフィ（通信秘匿，steganography）とは，ある伝達したい情報があったときに，別のデータを媒体とし，それを都合良く改変し，当事者以外に当該データを送信したこと自体を知られることなく，その内容を伝達する方法である．暗号との大きな違いは「送信の事実すら隠す」というところである．

ここで，実際に伝達したい情報は媒体となるデータに埋め込まれる．その理由によりこの情報は「埋め込み情報（embedded object, embedded information）」と呼ばれる．伝えたい情報の媒体とされるデータは「カバーデータ（cover-object, cover media, cover data あるいは単に cover）」と呼ばれる．また「カバーデータ」に「埋め込み情報」を埋め込んだ結果得られるデータは「ステゴデータ（stego-object, stego media, stego data）」と呼ばれる．ここで述べた英語による用語は First International Workshop on Information Hiding で合意されたもの[7]である．ステガノグラフィを用いた通信において，主に伝達したい情報は「埋め込み情報」であり，カバーデータ自体は特に伝達すべき情報である必要はない．

ステガノグラフィ通信で，毎回同じアルゴリズムで処理が行われると，第三者に通信を検知される危険性が増したり，別の相手とも通信する場合，同じ処理を用いると当該通信相手以外にも通信を検知されたり通信内容を得られる，といった危険性が増す．それを避けるため，暗号通信で用いられるような鍵（stego-key，以降ステゴ鍵と呼ぶ）と呼ばれるパラメータが処理において用いられる．

13-1-1 ステガノグラフィが満たすべき性質と情報秘匿技術

ステガノグラフィ技術で用いられる埋め込み処理や，そこで必要な情報，カバーデータの候補となるデータ集合には，通信の検知が困難であること，カバーデータの自然さ，という二つの性質が必要となる．

ステガノグラフィにおいて，埋め込み情報は，物理信号を変化，パケットヘッダの変更，メッセージのデータ部分の変更によって埋め込まれる．データ部分の変更では，カバーデータの冗長性を利用して，見かけ上同等に見えるようにステゴデータが作成される．カバーデータとして用いられるものとしては，テキスト，画像，音声，動画，プログラムなどがある．

13-1-2 ステゴ解析技術

ステガノグラフィにおいてはその目的から，別情報を通信しているという事実すら検出されてはならない．ステガノグラフィによる通信を検知する技術はステゴ解析（ステガナリシス，steganalysis）と呼ばれ，近年研究が始められつつある．通信検出を行う行為を「攻撃（attack）」と呼ぶ．ステゴ解析技術の研究事例はそれほど多くない．例えば，画像の LSB（least significant bit）に情報を埋め込むタイプのステガノグラフィに対するステゴ解析法などが提案されている．この方式は適用できる埋め込み方法が非常に単純なため，実際に用いられる（電子透かしで用いられるような複雑な）埋め込み方法と比較すると，解析の困難さに大きなギャップがある．

■1 群 - 3 編 - 13 章

13-2 電子透かし

（執筆者：渡辺　創）[2009 年 1 月 受領]

電子透かし（ディジタル透かしとも呼ばれる，（digital）watermarking）とは，ディジタルデータに対して別の情報を不可分に埋め込む処理，及び読み出す処理を合わせたものをいう．また電子透かしを利用して様々な目的を達成しているシステムを電子透かしシステム（（digital）watermarking system）と呼ぶ．

埋め込まれる情報は「電子透かし情報（（電子）透かし，透かし情報，（digital）watermark）」と呼ばれる．「電子透かし情報」が埋め込まれるデータは，ステガノグラフィと同様に「カバーデータ（cover-object, cover media, cover data あるいは単に cover）」と呼ばれる．また「カバーデータ」に「電子透かし情報」を埋め込んだ結果得られるデータは「電子透かし入りデータ（ステガノグラフィと同様，ステゴデータと呼ばれることもある，watermarked data）」と呼ばれる．電子透かし埋め込み，読み出し処理においては，鍵（key）と呼ばれるパラメータが用いられることも多い．ステガノグラフィで述べた理由と同様，不正行為をより困難にするためである．ここではステガノグラフィのときと同様ステゴ鍵（stego-key）と呼ぶことにする．

電子透かしシステムで用いられる fingerprint とは，同じ情報を表現した複数のディジタルデータ（例えばある映画のムービーデータ）を区別する必要があるとき，それを実現するために用いられる情報である．埋め込まれる情報として，例えば製造番号が考えられるであろう． fingerprinting とはこの目的のために電子透かし情報を埋め込む処理，及び読み出す処理をあわせたものをいう．

電子透かしには，知覚可能（可視）型電子透かし（perceptible（visible）watermarking）と呼ばれるものと，そうでないもの，すなわち紙幣の透かしに似て，計算機にすら知覚が困難な，知覚困難型電子透かし（imperceptible watermarking）がある．本節では以下，後者について述べる．

13-2-1 電子透かしの利用目的と満たすべき性質

電子透かしの利用目的としては，著作権者の識別，著作権保持の証拠不正コピー抑止，コピー行為の制御，改ざんの検知などが考えられている．

電子透かしシステムでは，別の情報が埋め込まれていることは既知であるため，それが改変（攻撃）される危険性がある．したがって電子透かしでは，電子透かしの知覚困難性（inperceptibility），攻撃への耐性（robustness）が求められる．この二つの性質の間にはトレードオフの関係が成立する傾向がある．

13-2-2 電子透かし技術

カバーデータとして用いられるものとしては，テキスト，画像，音声，動画，プログラムなどがある．電子透かしでは電子透かし入りデータを改変（攻撃）される危険を考えなければならない．そのような攻撃に対処するため，様々な方式が提案されている．そこで用いられている埋め込み方法は，大きく分けて次の二つがある．

- 空間領域におけるデータ操作：カバーデータの値を微小量変更することにより，電子透かし情報を埋め込む．
- 周波数領域におけるデータ操作：カバーデータに周波数変換（離散コサイン変換，ウエーブレット変換など）を施し，その変換されたデータに対して，電子透かし情報の埋め込みを行う．

13-2-3 電子透かしの実現例

ここでは埋め込み方法の例として，スペクトル拡散法を利用した一方式を簡単に説明する [1]．静止画像に対し，電子透かし情報は以下のように埋め込まれる．

STEP 1: 元の画像 D を DCT（離散コサイン変換）により周波数領域 F に展開する．

STEP 2: F の交流成分係数の高いものから，1000 個の値を選び，ベクトル $V = \{v_0, v_1, \ldots, v_{999}\}$ を構成する．

STEP 3: 正規分布 $N(0,1)$ に従って，埋め込まれる電子透かし情報 $X = \{x_0, x_1, \ldots, x_{999}\}$ を生成する．

STEP 4: V，X からベクトル $V' = \{v'_0, v'_1, \ldots, v'_{999} | v'_i = v_i(1 + \alpha x_i), 0 \leq i \leq 999\}$ を計算し，F における v_i を v'_i の値に置き換え F' を作成する．

STEP 5: F' を逆 DCT により静止画像データ D' に戻す．

得られたデータ D' は D とほとんど変わらない画像となる．ちなみに提案時には，$\alpha = 0.1$ として評価が行われている．電子透かし情報が埋め込まれた画像 D^* からの，電子透かし情報の検出処理は以下のようになる．

STEP 1: 画像 D^* を DCT により周波数領域 $F*$ に展開する．

STEP 2: F^* の，埋め込む際に使われた V に対応する位置の値から，V^* を作成する．

STEP 3: 埋め込み方式より，D^* に埋め込まれていた電子透かし情報 X^* は $V^* = V(I + \alpha X^*)$ すなわち $X^* = (V^* - V)/\alpha V$ となる． ここで， $I = \{1, 1, \ldots, 1 |$ 個数は 1000$\}$.

元の電子透かし情報を G^* より読み出した X^* から特定するには，各電子透かし情報 X に対し，$(X^* \cdot X_n)/\sqrt{(X^* \cdot X^*)}$ なる式を用いて類似度を計算し，一番近い X を元の情報として特定する．ここで X_n はユーザ n の購入者情報，$\cdot$ は内積を表す．

13-2-4 電子透かしに対する攻撃技術

電子透かしに対する攻撃としては，例えば信号の強調など（画像のシャープネス調整など），ノイズの付加（ガウスノイズなど），フィルタリング（線形，非線形），非可逆圧縮（JPEG，MPEG など），変形（回転，拡大縮小，切り取りなど），データの合成などがある．これまでに StirMark[6] など，攻撃による電子透かし評価ツールも提案されてきた．そこでは複数の幾何的変換，補正，圧縮などを組み合わせて電子透かし入りデータが改変される．これまで StirMark によって，多くの方式は安全でないことが示されている．

13-2-5 攻撃への対処技術

データの補正変換，幾何的変換や圧縮などに対処する技術として，新たな埋め込み方法が提案されてきている．多くの研究では，このように攻撃に十分な耐性をもつことができるよう埋め込み方法を設計し，実験的な評価をしたうえで提案されている．

不正コピー抑止などを目的とする場合など，fingerprinting が用いられたシステムにおいては，複数のユーザが結託し，電子透かしが埋め込まれたデータ（埋め込まれたデータはユーザにより異なる）を持ち寄り比較することにより，電子透かしが埋め込まれている位置を特定することができる．これは結託攻撃（collusion attack）と呼ばれる．結託攻撃に対処する別のアプローチとして，結託耐性符号（collusion-secure fingerprinting code）と呼ばれる電子透かし情報符号化法（及び復号，すなわち読み出し法）がある．これは結託攻撃に対処できるように，電子透かし情報を効率良く符号化する方式であり，近年盛んに研究が行われている．

■1 群 - 3 編 - 13 章

13-3 そのほか，まとめ

（執筆者：渡辺　創）[2009 年 1 月 受領]

最後にステガノグラフィと電子透かしの違い，規格化や標準化の現状について述べる．

13-3-1 ステガノグラフィと電子透かしの違い

これまで述べたステガノグラフィと電子透かしの違いをまとめると表 13･1 で表される．ステガノグラフィでは，埋め込み情報が実際に伝達したい情報であるのに対し，電子透かしシステムにおいては，カバーデータの情報を保護したり，補強あるいは補足したりする付加情報として用いられる．ステガノグラフィにおいて，カバーデータは特に伝えるべき情報である必要はない．

表 13･1　データの重要度

	ステガノグラフィ	電子透かし
埋め込み情報	◎	○
カバーデータ	△	◎

ステガノグラフィで用いる埋め込み方法は，その必要とされる性質（カバーデータの品質の保持）が共通であることから，電子透かしで用いられる埋め込み方法が有用である．

13-3-2 規格化，標準化の動向

ステガノグラフィではその目的から，規格化，標準化の動きは特に見られない．対して電子透かしシステムにおいては，コピー行為制御，など業界団体による電子透かし技術の規格化が必要となる応用形態も存在する．そのため様々な規格化，標準化の動きが見られる．業界団体による活動は近年始められ，一部は終了している．関連する団体や活動には，CPTWG（Copy Protection Technical Working Group）WaRP（Watermark Review Panel），DVD CCA（Copy Control Association），DAVIC（Digital Audio Visual Council, DAVIC specification は ISO/IEC 16500 として規格化），SDMI（Secure Digital Music Initiative），MUSE プロジェクト，JASRAC（社団法人日本音楽著作権協会），ISO/IEC JTC1/SC29/WG11 などがある．

■参考文献

1) Cox, I.J., Kilian, J., Leighton, T., Shamoon, T., “A Secure, Robust Watarmarking for Multimedia,” Proc. of Information Hiding ’96, LNCS1174, Springer-Verlag, pp.185-206, 1996.
2) Johnson, N.F., Duric, Z., Jajodia, S., “Information Hiding, Steganography and Watermarking-Attacks and Countermeasures,” Kluwer Academic Publishers, 2001.
3) Katzenbeisser, S., Petitcolas, F.A.P. eds., “Information Hiding Techniques for Steganography and Digital Watermarking,” Artech House, 2000.
4) 松井甲子雄, “電子透かしの基礎 –マルチメディアのニュープロテクト技術–,” 森北出版, 1998.
5) 小野　束, “電子透かしとコンテンツ保護,” オーム社，2003.
6) Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., “Attacks on copyright marking systems,” Proc. of Information Hiding ’98, LNCS1525, Springer-Verlag, pp.218-238, 1998.
7) Pfitzmann, B., “Information hiding terminology,” Proc. of Information Hiding ’96, LNCS1174, Springer-Verlag, pp.347-350, 1996.