近傍ピクセルの性質を用いたデータハイディング
-付加情報埋め込みと抽出-

1V－2

上條浩一、小林誠士、清水周一

日本アイ ビー エム 株式会社 東京基礎研究所

1. はじめに

動画や音声などのデジタル・コンテンツにのデータ部を微少に変更することにより，ＩＤやコメント，署名などの付加情報を，不可視および不可聴の状態で埋め込んで隠し、またそれを検出する技術をデータハイディングと呼び、デジタル情報のセキュリティー、知的所有権保護等に有用な方法として注目を浴びている。

本稿では、デジタル静止画像を例に、ピクセルの幾つかの組を１セットとして１ビット情報を表現し、幾つかのセットを用いて多ビット情報を表現する方法、また統計的性質を利用して信頼性を予測し、埋め込み強度を決定する方法について論ずる。

2. 統計的性質を利用したデータハイディング

本手法は、デジタル データから二組の特徴量 ({an}, {bn}) を N 個づつ擬似ランダムに選択し、その平均値の差:

$$d = (1/N)\Sigma n an - (1/N)\Sigma n bn \qquad (1)$$

の値により、(-∞, -T), [-T, T], (T, ∞) の 3 状態を分類し、ビット情報を表現するものである。ここでの考え方は以下のとおりである。サンプル数 N が大きくなれば、各特徴量の平均値はデジタルデータ全体での特徴量の平均値に近付き、従って、その差 d は 0 に近づくと期待できる。適当な閾値 T を設ければ、デジタル データから観測された特徴量の平均値差 d は確率的に[-T, T]の範囲内に分布すると考えられる。ここで、d の値が[-T, T]を越えるように、意図的に各特徴量の値 an, bn を変更すれば、出現確率の非常に小さい状態を作り出すことが出来る。これを利用して、以下に示すように、上記３状態をビット情報として解釈する。

(-∞, -T):	不可情報あり、ビット 0
[-T , T] :	不可情報なし
(T, ∞):	不可情報あり、ビット 1

DataHiding based on neighbor pixels statistics
-embedding and detection-
Koichi KAMIJO, Seiji KOBAYASHI, Shuichi SHIMIZU
IBM Japan Ltd., Tokyo Research Laboratory

[-T,T]の範囲を越えるように意図的に特徴量を変更することを、付加情報を埋め込む、と呼ぶことにする。以下では、静止画像を例に、特徴量としては画素の輝度値を用いて議論する。以上は 1 ビット埋め込み・検出の場合だが、K ビットを埋め込む場合には、互いに重複しない画素列{an}, {bn}を K 個選び、2NK 画素を使うことによって実現出来る。

意図的に埋め込む方法としては、画素列{an}に一定値 c (◇0) を加え、{bn}から一定値 c を引く方法[1]があるが、この方法の欠点は、点列の画素値に操作を加えなくても、適当な二つの画素点列を選び出す事だけで、両点列の画素値の差の平均をほぼ 2c と出来る、c や N の選定が難しい、画面に何の処理を施さなくても埋め込まれているのに埋め込まれていないと判断する false negative がゼロで無い等の欠点がある。そこで、本手法では以下で述べる統計的手法を用いる事によって、これらの問題を解決している。

3. 埋め込み強度と抽出の信頼性

式(1)を、

$$d = (1/N)\Sigma n(an - bn) \qquad (2)$$

と書き直し、d の確率分布を求めてみる。埋め込みが無い場合、画素のとる値が相関が無く、独立な正規分布を取るとすると、an-bn の標準偏差

$$\sigma = \sqrt{<(an - bn)>^2} \qquad (3)$$

を用いて、変数 d の確率密度関数は正規分布

$$P(d) = \sqrt{N/2\pi\sigma^2}\exp(-Nd^2/2\sigma^2) \qquad (4)$$

で与えられる。尚、ここで中央極限定理によれば、各々の差分が正規分布に従うとの仮定がなくとも画素数 N を十分大きくとることによって、(4)が成立する。この時、埋め込みがされていないのにも関わらず、埋め込まれていると誤判定する確率(false positive)を一定値 Pp に押さえるためには、定数 t を

$$Pp = 2/\sqrt{2\pi}\int_{T}^{\infty} \exp(-x^2/2)dx \qquad (5)$$

として、閾値を

$$|d| > d_t = t\sigma/\sqrt{N} \qquad (6)$$

に設定する必要がある。このように、判定の閾値が画像の統計量に基づいて定める事が出来、又、false positive を計算出来るのが、本方法の特徴であり、利点である。

前述した多ビット(K ビット)埋め込みの場合の false positive は、K ビット全てが誤検出した場合をこの場合の false positive と定義すると、

$$P_{pk} = Pp^K \qquad (7)$$

で表わされる。

False negative に関しては、前述したとおり、画像に何らかの処理が施されていない限りゼロである。

4. 埋め込み、検出における留意点

実際に静止画を用いて本方法で埋め込み、検出を行う事を考える場合、次の条件を満たす必要がある。

1. データの埋め込みに起因する画質の劣化は、利用者が検知出来ないレベルである。
2. 誤検出が少ない。
3. 第三者が改ざんをする事が非常に困難である。
4. 埋め込まれた情報は、一般的なコンテンツの編集や圧縮に対しても安定して抽出出来る。

1. に関しては、c の値を小さくすればよい訳だが、N の値が正規分布で近似出来るほど十大きいばあい、8 ビット(256 レベル)の画像に対し、微少なcにより false positive が十分小さい埋め込みは可能で、その際、画質の劣化を肉眼で確認するのは殆ど不可能である。
2. に関しては、式(6)より、誤りの確率を予測することができるので、希望の誤り率を達成するための埋め込みの強さを決定するできる。
3. に関しては、第三者による改ざん防止、画素列の一様分布の目的があるが、実際の方法としては、既知の擬似乱数発生装置に特定の鍵を与えて乱数を発生させる方法が考えられ、埋め込み者と検出者で秘密鍵を持ち合うか、公開暗号方式を併用した埋め込み方式[2]等が考えられる。
4. に関しては本稿では省略させていただく。

5. 埋め込み手順

今までの議論を土台に本方式を利用して実際に埋め込みを行う際の操作手順を説明する。

1. False positive 値の決定
先ず、どのくらいの誤検出迄許されるかを決定する。これは、使用者の都合に因って変化するものである。
2. 画素列の選定
これは、前述した通り、一様分布性、機密性が保たれるように選出する。また、画素の対に関しても、σが小さくなるように選出すると都合がよい。
3. 標準偏差の計算
2. の画素列を基に、式(3)の計算を行う。
4. 埋め込み量の計算
3. で求めたσ、1. で設定した Pp を元にして、|d|の値を決定する。
5. 画素値の操作
式(2)が満たされるように{an}, {bn}の値を変更する。

6. おわりに

データハイディング技術において、擬似ランダムに選ばれた二組の画素列の特徴量を利用し、統計的手法を用いて埋め込み、検出を行う方法を、アルゴリズム、統計的性質、埋め込み、検出における留意点、具体的埋め込み方法と順を追って説明した。統計的性質を使った本方式の長所としては、誤検出率を設定した上で埋め込み量を調節できる、埋め込みの自由度が大きい為埋め込みによる画質の痛みを小さく出来る、擬似乱数を使う事によって、第三者の改ざんが難しい事があげられる。本稿では言及しなかったが、(an, bn) の対の選びかたによる標準偏差の変化、画像に処理を施したさいの false positive/negative の変化等は重要な研究課題である。

謝辞

本研究は情報処理新興事業協会で実施された創造的ソフトウエア育成事業の一環として行っており、この機会をいただいたことを感謝する。

参考文献

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu: "Techniques for data hiding," *IBM Systems Journal*, Vol. 35, pp. 313-336, 1996.
[2] 沼尾他:"データハイディングによるデジタル署名技術," *In Proc. Of IPSJ 53rd annual conf.* 1996
[3] 清水周一、沼尾雅之、森本典繁、"ピクセルブロックによる静止画像データハイディング," *In Proc. Of IPSJ 53rd annual conf.* 1996
[4] 小出昭夫: "Data Hiding 技術とその応用", 精密工学会原稿, 1998