

二値画像を埋め込むデータハイディング

2K-5

上條浩一⁽¹⁾、利根川聡子⁽²⁾日本アイ・ビー・エム株式会社 東京基礎研究所⁽¹⁾、インベディットシステムズ⁽²⁾

1. はじめに

画像や音声等のデジタル・コンテンツのデータ値を微妙に変化させ、IDやコメント、署名等の付加情報を不可視又は不可聴の状態で埋め込んで隠し、又それを抽出する技術をデータハイディング技術と呼ぶ。

本稿では、静止画像に対して、知覚できないように二値画像データを埋め込むデータハイディング技術の手法を示す。又、本方式で埋め込まれた二値画像データを抽出するには鍵を必要とするが、抽出される二値画像が任意の人為的な形状を含むように抽出鍵を偽造することは、非常に困難であることを示し、人為的形状を取り出せる鍵を持つことが、すなわち、所有者の証明になることを示す。

2. 二値画像の埋め込み

本手法では、ロゴ等の人工的二値画像 ($M \times N$ pixel, 以下画像 A) の埋め込みを対象となる静止画像 ($W \times H$ pixel, 以下画像 I , $M < W$, $N < H/2$) の隣接ピクセルの特徴量の大小を変化させる事によって行う。ここで、特徴量とは、輝度成分や色成分の大きさを指す。以下埋め込み手法を順を追って説明する。

(Step 1) $W \times H/2$ pixel の領域に A をタイル状に敷き詰め、二値画像 E_A を作る。

(Step 2) $P \times Q$ bit の鍵 K を E_A と同じサイズの領域にタイル状に敷き詰め、二値画像 T_K を作り、 T_K と E_A とで pixel 単位で xor を取ることにより新たな二値画像 E'_A を作る。ここで、 K は埋め込み者と抽出者のみが知り得

る鍵であり、 A は K に対し、

$$LCM(M, P) > W, LCM(N, Q) > H \quad \dots (1)$$

を満たす様に選ばれている必要がある。(LCM は最小公倍数)

(Step 3) I の各々のピクセルの特徴量 $I(x, y)$ を以下の手順で変化させ、 I' を作る。

```
if((E'A(x,y)==1 && p<m) ||
    (E'A(x,y)==0 && p>m))
    {I'(x,2y) =m; I'(x,2y+1)=p;}
else {I'(x,2y) =p; I'(x,2y+1)=m;}
... (2)
```

where $p = I(x, 2y)$, $m = I(x, 2y+1)$

ここで、 I' の画質劣化を防ぐ手段として、 $|p-m|$ がある値以上 (例えば I の特徴量の標準偏差の定数倍以上) の時や、 E_A の bit 値が '1' である領域から離れている部分のピクセルに関しては (2) の操作をスキップする方法がある。

3. 二値画像の抽出

抽出は、 I' と K より A を抽出する動作であり、以下の順で行われる。

(Step 4) Step 2 と同じ方法で T_K を作る。

(Step 5) 以下の方法で E_A と同じ画像サイズの抽出二値画像 $D_{i,j}$ を ($M \times N$) 個作る。

```
for(j=0; j<N; j++)
  for(i=0; i<M; i++)
    for(y=0; y<H/2; y++)
      for(x=0; x<W; x++)
        if(T_K(x-i,y-j)==1 && p>m)
          Di,j(x,y)=1;
        else if(T_K(x-i,y-j)==0 && p<m)
          Di,j(x,y)=0;
        else Di,j(x,y)=don't care;
      }}}
... (3)
```

where $p = I'(x, 2y)$, $m = I'(x, 2y+1)$

(Step 6) Step 5 で生成された ($M \times N$) 個の

$D_{i,j}$ の中に期待する埋出パターンがあるかどうかを抽出する。この作業は $D_{i,j}$ が人工的なパターンの繰り返しパターンからなっているか否かの検証であり、切り取りを施した後の画像に対しても適応出来る。以下にエントロピーを利用して検証する方法を説明する。

$D_{i,j}$ の中に人工的なパターンが含まれていない場合、縦、横、又は L 字のパターン等の中に連続して同じ bit 値が現れる確率は非常に小さい。しかし、含まれている場合は、その確率は非常に大きくなり、エントロピーはランダムなパターンよりはるかに小さくなる。そこで、 $D_{i,j}$ 全体に対し、あるマスクパターン P (例えば 3 pixel からなる L 字パターン) を当てた時、その中の bit 値が全て同じである個数を $Ss_{i,j}$ 、 P の当て得る個数を Cnt 、 $Sd_{i,j} = Cnt - Ss_{i,j}$ として、以下の様にエントロピー $H_{i,j}$ とその最小値 H_{min} を計算する。

$$H_{i,j} = - Ss_{i,j} / Cnt \cdot \log(Ss_{i,j} / Cnt) - Sd_{i,j} / Cnt \cdot \log(Sd_{i,j} / Cnt) \dots (4)$$

$$H_{min} = \min_{i,j} (H_{i,j}) \dots (5)$$

抽出パターンは H_{min} を与える $D_{i,j}$ を $M \times N$ block に分割したものを重ねあわせた物であり、それが明らかに人工的なパターンであれば、 I は埋め込みが施された画像という事が解る。

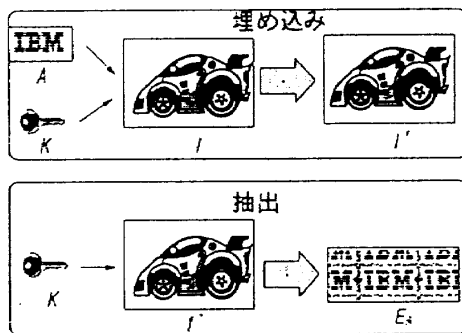


図1 埋め込み、抽出手順

4. セキュリティー

二値画像が埋められた画像 I' に対し、悪意の有る者 S が埋め込み者に成りすます事を考える。 S は M と N の値を何らかの方法で知ったとする。 S が偽りの鍵 K_s を作り出す

為には、以下条件を満たす K_s, B を作り出さなくては行けない。

$$E'_A(x, y) = (K_s(p, q) + E_B(m, n)) \bmod 2$$

$$(0 \leq x < W, 0 \leq y < H/2) \dots (6)$$

where $p = x \bmod P, \quad q = y \bmod Q,$
 $m = x \bmod M, \quad n = y \bmod N,$

ここで、 B は S が埋めたい二値画像、 E_B は B を E'_A の大きさにタイル状に敷き詰めた物である。(1)が満たされる場合、(6)は $(W \cdot H/2)$ 個の連立方程式からなる。しかし、変数の数は $PQ+MN$ 個あり、 $P, M \ll W$ と $Q, N \ll H/2$ より $W \cdot H/2 \gg PQ+MN$ が成立し、(6)を解く事は不可能であり、 S が偽りの K_s, B を作り出す事が不可能である事が解る。

5. まとめ

二値画像の静止画像への埋め込みとそれを抽出するアルゴリズム、及び、抽出するための鍵を人為的に偽造することは非常に困難であることを順を追って説明した。本アルゴリズムの長所としては、エントロピー等を使って人工的なパターンを検索するため、埋め込み画像がどのように切り取られた場合でも、埋め込んだ二値画像の抽出をすることができること、又、鍵の偽造がほぼ不可能であるため所有者の証明を容易に行うことができることがある。最後に本稿では言及しなかったが、埋め込み画像が切り取られるばかりでなく拡大または縮小された場合においても、二値画像が正確に抽出できるようにすることは大きな研究課題である。

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ェ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] 上條、小林、清水 " 近傍ピクセルの性質を用いたデータハイディング"
In Proc. Of IPSJ 56th annual conf. 1998

[2] 清水、沼尾、森本 " 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