Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 27-29, 2006 (pp40-45)

A Data-Hiding Scheme for Binary Images with Content-Based Hiding Rates

PHEN-LAN LIN[1], PO-WHEI HUANG[2]
[1]Department of Computer Science and Information Engineering
Providence University
Shalu, Taichung, TAIWAN

[2]Department of Computer Science
National Chung Hsing University
Taichung, TAIWAN

Abstract: A block-based information hiding scheme that hides more information into more complex blocks for binary images is presented. The block complexity is measured by entropy and DCT spectrum and a set of secret keys that categorizes block complexity prevents correct decoding from unauthorized users. The embedded bits are selected based on a CPT coding algorithm and a WL flippability score so that good balance between imperceptibility and hiding capacity can be achieved. Compared to other schemes, the distortion measure DRD of our scheme grows slower with hidden amount than that of either CPT or its enhance version CPT1. Such DRD advantage becomes very significant when compared to scheme WL.

Key-Words: Data hiding, Binary image, Image complexity, Entropy, Spectrum, Stego-image

1 Introduction

Information hiding embeds secret information into a media in such a way that degradation made to the cover- or the stego-media is kept imperceptible and only the authorized user can extract the secret information correctly. Hence, embedding capacity, visual imperceptibility, and security are major concerns when designing an information-hiding scheme.

Many data-hiding schemes for binary images hide each bit of information by enforcing odd-even relationship of object pixel count within a non-uniform block [1-3]. Such schemes hide one bit per 0.5 pixel change on an average. Thus, the more bits are hidden, the more pixels will be changed. And, the more visual artifacts the stego-image could possibly have. In [4], a different approach, named CPT scheme, that can hide up to $\lfloor(log_2(mn+1)\rfloor$ bits of information within each block of $m \times n$ pixels by flipping at most two pixels is presented. Instead of enforcing odd-even relationship of a given block, the scheme applies modulo arithmetic to a weighted sum of the block to encode/decode the hidden information. CPT scheme is later revised to trade one-bit hiding capacity per block for reducing visual artifacts by enforcing the embedded pixel adjacent to the pixel that has a value equals to the hidden bit [5]. Several algorithms are also proposed for reducing visual artifacts of hiding effect. In [3], WL score, which is computed according to the change in connectivity and smoothness of the pixel after bit-flipping, is presented.

Most block-based schemes hide a fixed number of bits into each non-uniform block in which not all pixels have same color. Although these schemes make hidden information easier to be decoded at extraction without rate information, they are not as secure as those having hiding rate varied from block to block. Obviously, it is easy to implement schemes with non-fixed hiding rate by randomly generating the rates using a secret key. However, the potential of causing severe visual artifacts to stego-images using random rates exists, because some non-uniform but rather smooth blocks may be assigned to hide the most bits. Although CPT method needs only flip at most two pixels within one block even hiding its maximum capacity of bits; however, the chance of finding an embedding-pixel that will not cause visual artifacts after flipping is very limited when hiding near maximum capacity of information into rather

This research is supported by National Science Council of ROC under Grant NSC-94-2213-E-126-004

smooth blocks. Thus, information hiding schemes with content-based rates can truly provide good balance between hiding capacity and visual imperceptibility.

In this paper, we present a block-based information hiding scheme for binary images with hiding rates based on block's entropy and DCT spectrum. DCT spectrum clearly signifies frequency variations within a block; however, one- or two-pixel changes due to data embedding could affect the spectrum enough for a wrong estimation of hiding rate at data extraction. Entropy measured by frequencies of object-pixel occurrence can also provide some insight of block complexity, though it cannot differentiate the case of two different looking blocks having same object-pixel counts. Thus, using both complexity measures together to assign the hiding rate of each block allows the scheme hide more information into more complex blocks. In addition, our scheme adopts CPT algorithm for encoding/decoding hidden information in each block once the hiding rate is determined and adopts WL score for selecting an embedding pixel. As a result, both imperceptibility and good hiding capacity can be achieved. Our scheme achieves security by using secret parameters to set the complexity category. The unauthorized users cannot correctly decode the hiding information with only the information of entropy or DCT spectrum that can be obtained directly from the stego-images.

The rest of this paper is organized as follows. In Section 2, we brief the algorithms and measures adopted by this proposed scheme. In Section 3, we present our proposed scheme in detail. The experiments and results, as wells as comparisons to the adopted schemes are presented in Section 4. Finally, the concluding remarks are in Section 5.

2 Backgrounds

2.1 Data Hiding Scheme CPT

Tseng, Chen, and Pan (CPT) proposed an algorithm that can hide as many as $\lfloor(log_2(mn+1)\rfloor$ bits of information into a block of size $m \times n$ [4]. In their scheme, a host image F is divided into blocks of size $m \times n$. A weight matrix W with its element w $\in\{1, 2, \ldots, 2^r-1\}$, $1 <= r <= \lfloor(log_2(mn+1)\rfloor$ and appears at least once in W and a randomly selected binary matrix of size $m \times n$ are served as secret keys for data extraction. To embed information $b_1\, b_2 \ldots b_r$ into a block F_i, the scheme modifies F_i into F_i' by flipping at most two bits in F_i such that SUM[$(F_i' \oplus K) \otimes W$] $\equiv b_1\, b_2 \ldots b_r$ (mod 2^r). The hidden data $b_1\, b_2 \ldots b_r$ can then be extracted easily by applying SUM[$(F_i' \oplus K) \otimes W$] (mod 2^r).

2.2 WL Score

Wu and Liu [3] proposed an algorithm for computing flippability scores of pixels in nondithered binary images measured by the change in connectivity and smoothness after pixel flipping. Fig.1 lists the scores for 72 possible 3 ×3 patterns calculated based on the algorithm. Patterns not shown are either the rotated or the inverted form The detail description of this algorithm can be found in [3].

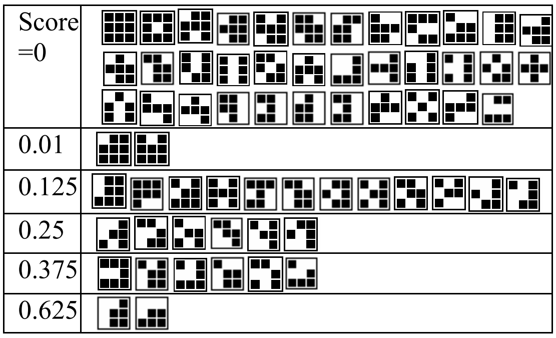


Fig. 1 WL scores for 72 possible 3 ×3 patterns

2.3 Distance Reciprocal Distortion Measurement (DRD)

Lu et al. [6] presented an objective distortion measure, named DRD, for binary document images based on the reciprocal of distance. They demonstrated that such measure matched well to subjective evaluation by human perception. The DRD can be calculated by the following equations.

$$DRD = \frac{\sum_{k=1}^{s} DRD_k}{NUBN} \quad (1)$$

$$DRD_k = \sum_{i,j} [D_k(i,j) \times W_{Nm}(i,j)] \quad (2)$$

$$D_k(i,j) = | B_k(i,j) - g[(x,y)_k] | \quad (3)$$

$$W_{Nm}(i,j) = \frac{W_m(i,j)}{\sum_{i=1}^{m} \sum_{j=1}^{m} W_m(i,j)} \quad (4)$$

$$W_m(i,j) = \begin{cases} 0, \text{for} \quad i = i_C \text{ and } j = j_C \\ \dfrac{1}{\sqrt{(i-i_C)^2 + (j-j_C)^2}}, \text{otherwise} \end{cases} \quad (5)$$

where DRD_k is the distortion measure for flipped pixel $g(x, y)_k$ in block B_k , $(W_{Nm}(i, j))/ W_m(i, j)$, $1<=i$, $j <=m$, is the (normalized) weight for pixel (i, j) within an m x m template, respectively, $B_k(i_c, j_c)= g(x, y)_k$, and $NUBN$ is the number of non-uniform (neither all white nor all black) blocks of size >= m x m in original image $f(x, y)$.

2.4 Entropy

The entropy of a binary image, denoted H, is the measure of the average information in bits in that image. It can be calculated by

$$H = -(p\log p + (1-p)\log(1-p)) \qquad (6)$$

where p is the probability of the occurrence of object or background pixel

3 Our proposed scheme-MIMC

The goal of our scheme, More Information in More Complex blocks (MIMC), is to achieve a good balance between hiding capacity and visual imperceptibility with moderate security. In follows, we describe our scheme MIMC in detail.

3.1 General description of scheme MIMC

Theoretically, the complexity of each block can be measured by its entropy or spectrum distribution. Entropy measured by Eq. (6) can provide some insight of block complexity, though it cannot differentiate two different looking blocks having same entropy. In fact, Eq. (6) reveals information about the occurrence frequency of object pixels in a binary image, as there are only two types of pixels in binary images. Since confining object-pixel count within a preset range during pixel manipulation for embedding is more deterministic than confining entropy, we use object-pixel count as the substitute measure of block entropy and use it as the first basis for complexity measurement. To differentiate two different looking blocks with same entropy, we introduce a second complexity measure-spectra category, which is defined as the frequency sub-band in that spectra energy is most concentrated. Fig.2 is one example of three frequency sub-bands P_L, P_M, P_H, where P_L= [1, 14], P_M= [15, 41], P_H= [42, 63].

For easier implementation, we divide entropy into several categories and further divide blocks within each entropy category into three spectra categories. Two blocks with same object-pixel count belong to the same entropy category and two blocks with their spectra energies concentrated in the same sub-band will be in the same spectra category.

DC	1	5	6	14	15	27	28
P_L:	Low	Freq.	Region	16	26	29	42
3	8	12	17	25	30	41	43
9	11	P_M:	Medium	Freq.	Region	44	53
10	19	23	32	39	45	52	54
20	22	33	38	P_H:	High	Freq.	Region
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Fig. 2 Frequency sub-bands: P_L, P_M, P_H, where P_L=[1,14], P_M=[15,41], P_H=[42,63]

3.2 MIMC Procedure:

1. Divide the host image into blocks of $m \times n$.
2. Check each block if it is embeddable.
3. Divide all embeddable blocks into N_H entropy categories with bounds [H_{Li}, H_{Ui}] for each category i, $1<=i<=N_H$.
4. Determine hiding rate of blocks within each entropy category C_{Hi}.
5. Determine complexity (C_H, C_S) of each embeddable block B.
6. For each embeddable block, (a) Obtain its hiding rate based on its (C_H, C_S), (b) Embed the hidden information.

Steps 2-5 and 6.b of the above procedure are further described in Algorithms 1-4 and Algorithm_CPTM, which is our improved version of CPT scheme, respectively.

Algorithm_1: Check if block B_i is embeddable
1. Count its entropy H_i, the object-pixel count.
2. Mark B_i as embeddable if H_i > threshold T_H.

Algorithm_2: Divide all embeddable blocks into N_H entropy categories with bounds [H_{Li}, H_{Ui}] for each category i, $1<=i<=N_H$.
1. Set the number of total entropy categories N_H, $0<N_H <= \lfloor(\log_2 (m \times n +1)\rfloor$
2. Randomly divide (H_{min}, H_{max}) into N_H categories with each category bounded by [H_{Li}, H_{Ui}], 1<=1<= N_H.

For example, if T_H=10 and N_H=5, {[H_L, H_U]} = {[10, 17], [19, 26], [28, 35], [37, 44], [46, 55]}. Note that we leave one pixel between bounds of each category so that we can force the embeddable block to not-embedding in case of no pixel with WL-score >0 can be found.

Algorithm_3: Determine hiding rate of blocks within each entropy category

1. Let $m=\lfloor(N_H+1)/2\rfloor$
2. Let $r_{max}= \lfloor(log_2(mn+1)\rfloor$
3. Assign rate($C_{H(m+i)}$) = (r_{max}-j-2, r_{max}-j-1, r_{max}-j), where i= -(m-1),…,0,…, (m-1), $j<=|i|$.

For example, the hiding rates for {[10, 17], [19, 26], [28, 35], [37, 44], [46, 55]} could be [2,3,4], [3,4,5], [4,5,6], [3,4,5], [2,3,4]. Note that the maximum entropy computed by Eq. (6) occurs at p=1/2. That is, blocks belong to the entropy category that contains approximately same number of object pixels and background pixels are supposed to be more complex than blocks in other entropy categories. Thus, we assign the maximum hiding rate for blocks in these entropy categories.

Algorithm_4: Determine (C_H, C_S) of block B_i

1. Assign B_i to entropy category C_{Hk} if $H_{Lk} <= H_i <= H_{Uk}$
2. Compute its DCT spectrum $S_i(u, v)= C_i^2(u, v)$.
3. Compute its total energy $E_i=\sum_{u,v}[S_i(u,v)]$
4. Compute its energy in all three frequency sub-bands, denoted E_{iL}, E_{iM}, E_{iH}, by $E_{ij} = \sum_{(u,v)\in Pj}[S_i(u,v)]$, $j=L, M, H$, where P_j = {Z_i| DCT coefficients, $jl<=i<=ju$}, $j=L, M, H$, is frequency sub-band j, as shown in Fig. 2.
5. Assign B_i to spectra category C_{Sj}, $j=L,M, H$, if $E_{ij} >= T_S \times E_i$.

For example, if block B_i has $H_i=11$, $E_i=100.3$, $E_{iL}=30$, $E_{iM}=51$, $E_{iH}=20$, and $T_S=0.5$, then complexity $(C_H, C_S)_i$ = (1, M).

Algorithm_CPTM: Hiding information $I_i=b_1…b_{ri}$ into block B_i

1. Prepare the weight matrix W_i for this block by assigning a repeated sequence of 1 to 2^{ri}-1 to $W_i(k, l)$, $1<= k <=m$, $1<= l <=n$. Note that we did not assign number 1 to 2^{ri}-1 randomly as scheme CPT did, because we hide various number of bits in each block. If we used W_i as a secret key, then we would need to store more than one weight matrix.
2. Compute the weighted sum of the block wv_i, using $wv_i=\sum W_i(k, l)*V_i(k, l) \bmod \mu_i$, where $V_i(k, l)$ is the value of pixel p at location (k, l) within block B_i, and $\mu_i=2^{ri}$.
3. If hiding information $I_i=b_1…b_{ri}= wv_i$, no pixel should be flipped.
4. If $I_i \neq wv_i$, compute $\Delta= I_i - wv_i$, if $I_i >= wv_i$ or $\Delta= I_i - wv_i + \mu_i$, if $I_i < wv_i$.
5. Start Flip-1.
6. If Flip-1 does not succeed, start Flip-2.
7. If Flip-2 fails, mark block as not embedding and stop.

Flip-1searches for and flips one particular pixel p within the block that satisfies the following conditions after flipping p: (a), $wv'_i=\sum W_i(k, l)*V'_i(k, l) \bmod \mu_i = I_i$, (b) $H_{Lj} <= H_i <= H_{Uj}$, (c) $C_S'=C_S$, and (d) p has the highest WL score >0 . The algorithm is detailed as follows.

Algorithm Flip_1:

1. Find all pixels P={p|($V_i(k, l)$=0, $W_i(k,l)=\Delta$) or ($V_i(k, l)$=1, $W_i(k, l)=\mu_i-\Delta$) if $H_{Lj} < H_i < H_{Uj}$, ($V_i(k, l)$=0, $W_i(k, l)=\Delta$) if $H_i = H_{Lj}$, ($V_i(k, l)$=1, $W_i(k, l)= \mu_i-\Delta$) if $H_i = H_{Uj}$, for all $1<=k<=m$, $1<=l<=n$}, where H_i is the number of pixels with $V_i(k, l)$=1.
2. If $P=\emptyset$, Flip-1 fails.
3. For all $p \in P$, keep only those satisfy $C_S'=C_S$ and name the new set P'.
4. For each $p \in P'$, obtain the WL score s from the lookup table shown in Fig.2.
5. Flip p_j that has the highest WL score>0, i.e, $p_j >= p_k$, $1<=k, j<= |P'|$ (the size of P'), $j\neq k$.

Algorithm_Flip 2:

1. Find all pixels P that after flipping (p_1, p_2), $wv'_i=\sum W_i(k, l)*V'_i(k, l) \bmod \mu_i = I_i$.
2. If $P=\emptyset$, return Flip-2 fail and stop
3. For all $p \in P$, keep only those satisfy $H_{Lj} <= H'_i <= H_{Uj}$, and $C_S'=C_S$, and name it P'.
4. For each $p \in P'$, obtain the WL score s from the lookup table shown in Fig.2.
5. Flip pixels p_l and p_j that have the highest two WL scores >0. That is, p_l, $p_j \in P'$, p_l, $p_j >= p_k$, $1<=k, l, j<= |P'|$ (the size of P'), $l\neq j\neq k$.

4 Experiments and results

4.1 Effect of image complexity

In this experiment, we test how image complexity affects both visual imperceptibility and hidden capacity. Four binary images of size 256 x256: "English", "Baboon", "Laugh", and "Mickey", as shown in Figs. 3(a)-(d), are used as host images. All images are hidden in 500 bits each the first time, then with 500-bit increment till their respective maximum capacity is reached. The secret key set used is listed in Table 1. Figs. 4(a)-(d) depict the stego-images with 1000 hidden bits and their respective DRD. Figs. 4(e)-(h) are the stego-images with DRD=0.4 and their respective hidden amount.

Observing Fig.4, we find that all stego-images maintain rather good visual quality. The DRDs with 1000 hidden bits for "English" and "Baboon" are around 1/3 of those for "Laugh" and "Mickey". For a DRD of 0.4, the hiding capacity of the former two images is about three times as much as that of the later twos. Since both images "English" and "Baboon" are visually more complex than the other two images, it is logical that both images have more blocks that can hide more bits without much degrading the quality of the host.

4.2 Comparison with CPT

We conduct this experiment to find out how the image-quality constraints and variable block rate of scheme MIMC affect image imperceptibility when compared to scheme CPT and its enhanced version CPT1. For better comparison, scheme MIMC is tested three times with its complexity measurement based on: (a) spectra-grouping only, (b) spectra- and entropy-grouping, and (c) none, respectively. Such three tests are named MIMC-1, MIMC-2, and MIMC-3 in follows. We repeatedly hide same amount of data into each image, as shown in Fig.3, and compute the DRD of each stego-image. The grouping bounds and rates used in MIMC-1 and MIMC-2 are listed in Table 2 and in Table 1, respectively, while the rate for MIMC-3 is 5.

The results, as shown in Fig. 5, demonstrate that our scheme, using either only spectra grouping as in MIMC-1, both spectra- and entropy-grouping as in MIMC-2, or no grouping but only fixed rate as in MIMC-3, produces stego-images with smaller DRD than both CPT and CPT1 do when hiding same amount of data in all four images.

4.3 Comparison with WL scheme

We first use scheme MIMC with block size of 8x8 to hide 49, 98, and 147 bits of information into the image shown in Fig. 6 (a). We then hide 49 and 98 bits of same information into the same image using scheme WL with same block size. The results, as shown in Figs. 6 (b)-(f), demonstrate that for hiding same amount of data, MIMC produced images with smaller DRD values because it only flips less than 1/2 as many pixels than scheme WL does. Furthermore, our scheme can produce stego-images with 50% more hidden bits and smaller DRD.

4.4 Security check

Four tests of using completely or partially right key for data extraction are conducted and the results are shown in Fig. 7.

Observing the extracted information, it is clear that one cannot extract the correct hidden information without using the exact secret keys. Any single incorrect parameter resulted in wrong extracted data from the current processed block and the blocks followed. If we apply encryption to the hidden information before it was hidden, the probability that any attacker can extract the correct hidden information becomes very slim.

5 Conclusions

We presented a block-based information hiding scheme-MIMC for binary images that can achieve good balance between hiding capacity and visual imperceptibility while maintaining moderate security. Unlike most block-based schemes that hide fixed number of bits per block, our scheme hides more bits into more complex blocks with their complexity measured by entropy and spectra-energy concentration. A set of secret keys that categorizes block complexity prevents correct decoding from unauthorized users. We demonstrated that scheme MIMC can hide good amount of information into various types of images while maintaining imperceptibility and extract correct hidden information only when using the exact key set. Compared to other schemes, the distortion measure DRD of stego-images by our scheme grows slower than that by either CPT or CPT1. Such DRD advantage becomes very significant when compared to scheme WL.

(a)English	(b) Baboon	(c)Laugh	(d)Micky

Fig.3. Four host images

1000 bit hidden				
DRD	(a) 0.139	(b) 0.127	(c) 0.381	(d) 0.486
DRD =0.4				
#bits	(e) 2941	(f) 2882	(g) 1047	(h) 822

Fig. 4.Effect of host images

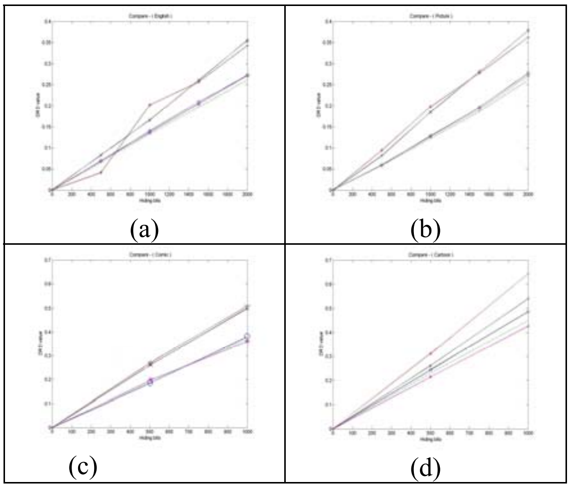


Fig.5. Comparison of DRD among MIMC (H+S, -○-), MIMC (S only, ---), MIMC (fixed, —●), CPT1 (-x-), CPT (-+-).

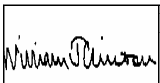
	MIMC -49	MIMC -98	MIMC -147	Wu-49	Wu-98
DRD	0.063	0.115	0.159	0.105	0.241
NFP	11	18	26	23	46
(a)	(b)	(c)	(d)	(e)	(f)

Fig.6 Comparison with scheme WL

Table 1 Secret key set for experiments 4.1, 4.3

Entropy category	Block rate (L/M/H)	Spectra category	T_S
5-9, 51-59	2/3/4/	P_L: 1- 9;	50%
11-19, 41-49	3/4/5	P_M:10-21	
21-39	4/5/6	P_H: 22-63	

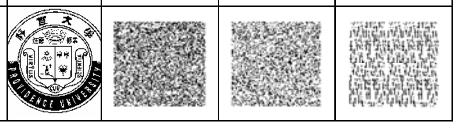
HC	○	×	○	○
SC	○	○	×	○
T_s	○	○	○	×
				

Fig.7. Extracted information for various key sets (○: Correct, ×: Incorrect).

Table 2 Block rate for various categories

	SG only	HG only	H+S	Fixed
Entropy category	L/M/H	rate L/M/H	rate L/M/H	rate L/M/H
5-9	4/5/6	3/3/3	3/4/5	4/4/4
11-49	4/5/6	5/5/5	4/5/6	4/4/4
51-59	4/5/6	3/3/3	3/4/5	4/4/4

References

[1] J. Chen, T. S. Chen, and M.W. Cheng, "A new data hiding method in binary image," in *Proc. Fifth Int. Sym. Multimedia Software Engineering*, 2003, Dec. 2003, pp. 88 – 93.

[2] T. H. Liu and L.W. Chang, "An adaptive data hiding technique for binary images, ", in *Proc. 17th Int. Conf. Pattern Recognition*, vol. 4, Aug. 2004, pp. 831 – 833.

[3] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no.4, Aug. 2004, pp. 528-538.

[4] Y. C. Tseng, Y. Y. Chen, and H. K. Pan, "A secure data hiding scheme for binary images," *IEEE Trans. Communications*, vol. 50, no.8, Aug. 2002, pp.1227-1231.

[5] Y. C. Tseng and H. K. Pan, "Secure and Invisible Data Hiding in 2-Color Images", in *Proc. IEEE INFOCOM*, 2001, pp.887-896.

[6] H. Lu, A.C. Kot, and Y.Q. Shi, "Distance reciprocal distortion measure for binary document images," *IEEE Signal Processing Letters*, vol.11, no.2, Feb. 2004, pp. 228-231.