American Journal of Applied Sciences 10 (9): 1102-1108, 2013
ISSN: 1546-9239

doi:10.3844/ajassp.2013.1102.1108 Published Online 10 (9) 2013 (http://www.thescipub.com/ajas.toc)

Modules Over Rings of Small Characteristics and Maximality of Data Hiding ratio in CPTE Schemes

[1]Phan Trung Huy, [2]Cheonshik Kim and [3]Nguyen Hai Thanh

[1]Department of Applied Mathematics,
Hanoi University of Science and Technology, Hanoi, Vietnam
[2]Department in Digital Media Engineering,
Anyang University, Anyang-si, Gyeonggi-do, Republic of Korea
[3]Ministry of Education and Training, Hanoi, Vietnam

Received 2013-07-11, Revised 2013-08-16; Accepted 2013-08-21

ABSTRACT

Introduced CPT scheme as a block-based hiding scheme based on the ring of the integers modulo 2^r, which permits to embed $r = \lfloor \log_2(k+1) \rfloor$ secret bits in F by changing at most two entries, while the highest number of secret bits in any CPT-based schemes is $MSDR_2 = \lfloor \log_2(1+k\ (k+1)/2) \rfloor$, approximately 2r-1. This ratio can be reached approximately in our proposed CPTE1 scheme by using modules on the ring Z_2 of integers modulo 2, as an instance of application of modules over rings of small characteristics. As a consequence, a new modified scheme-CPTE2 is to control the quality of stego-images. The CPTE2 scheme gives 2r-2 embedded bits approximately, more than r-2 bits by Tseng-Pan's scheme, while the quality is the same.

Keywords: Maximality, Secret Data Ratio, Binary Image, Steganography, CPTE Scheme

1. INTRODUCTION

Binary data hiding (Cao and Kot, 2012; Gao and Su, 2010; Guo and Zhang, 2010; Lin, 2011; Yadav and Ojha, 2012) can be used for copyright, annotation and communication and can be achieved by altering some nonessential pixels in the cover image. For stego images, one of the most challenging problems is hiding the secret data into binary images with a high ratio of secret data and low image distortion.

In block-based approaches (Bierbrauer and Fridrich, 2008; Chang *et al*., 2008; Pan *et al*., 2000), each binary image is partitioned into binary blocks of the same size m×n. In a block F, WL scheme (Wu and Lee, 1998) can embed one bit by changing at most one bit of F. From CPT scheme proposed by (Pan *et al*., 2000), embedding rate are $r = \lfloor \log_2(q+1) \rfloor$ bits, $q = m \times n$, by changing at most two bits of F. The embedding performance largely depends on the choice of a key matrix. In order to solve the problem of CPT, modified scheme (MCPT scheme for short) was proposed. MCPT (Hirohisa, 2003) was derived from the CPT scheme, which was introduced by (Tseng and Pan, 2001) to control the high quality of embedded binary images.

In this study, we promote the use of modules over rings of characteristic 2 to data hiding area. It can be seen that this idea will be easily extended to others characteristics for different formats on multimedia environment. In this study, briefly describing CPT, CPTE1 and CPTE2 schemes and evaluate the performance of proposed schemes.

1.1. CPT Scheme

Given a binary image B which is partitioned into p blocks as binary matrices with the same size m×n. K is a binary key matrix, W is a weight matrix whose elements are integers chosen with the restriction Equation 1 below:

$$\left\{W_{ij}, 1 \le i \le m, 1 \le j \le n\right\} = \left\{1, 2, \ldots, 2^r - 1\right\} \quad (1)$$

In a block F, one can embed $r = \lfloor \log_2(m \times n+1) \rfloor$ secret bits. Each entry F_{ij} has a value 0 or 1. Changing (or inverting) F_{ij} in F means that F_{ij} is changed to F_{ij} ⊕

Corresponding Author: Cheonshik Kim, Department in Digital Media Engineering, Anyang University, Anyang-si, Gyeonggi-do, Republic of Korea

1, or equivalent, to 1-F_{ij}. F⊕K is the bitwise exclusive-OR on two equal-size binary matrices F and K, the operation ⊕ gives the sum, SUM[T⊕W] which is obtained by taking pair-wise multiplications on two equal-size integer matrices, that is T = F⊕K, SUM[T⊕W] = $\Sigma_{1\le i\le m}\Sigma_{1\le j\le n} T_{ij}\times W_{ij} \bmod 2^r$.

Given a block F. In CPT scheme, ones try to hide a bit stream of r bits b = $b_1b_2\ldots b_r$ into F by changing at most two pixels:

```
Embedding Algorithm (CPT)
Input: Block F of original image G, secret key K, secret weight matrix W, secret r-bit stream b = $b_1b_2...b_r$.
Output: Block F' of stego image G'.
Step 1: Compute $T = F \oplus K$
Step 2: Compute $S = SUM(T\oplus W) \bmod 2^r$,
where ⊗ is the bit-wise multiplication.
Step 3: Compute $d = b_1b_2\ldots b_r - S \bmod 2^r$.
 If d = 0, then F is not modified;
 Else {
 a) $h \in \{0, 1, ..., 2^r-1\}$, $S_{hd} \neq 0$ and $S_{-(h-1)d} \neq 0$.
 b) pick a $(j, k) \in S_{hd}$, complement $[F_i]_{j,k}$;
 c) pick a $(j, k) \in S_{-(h-1)d}$, complement $[F_i]_{j,k}$;
 }
```

Theorem 1

Given m×n binary matrices F, K and weight matrix W satisfied $\{W_{ij}, 1\le i\le m, 1\le j\le n\} = \{1, 2,\ldots, 2^r-1\}$, with $r = \lfloor \log_2(m\times n+1)\rfloor$. Let b = $b_1b_2\ldots b_r$ is a bit stream. We can invert at most two entries of F to get b = SUM [(F⊕K) ⊗W] mod 2^r.

2. MATERIALS AND METHODS

2.1. Modules over Rings of Small Characteristic and Maximal Embedded Data Ratio

We consider CPTE schemes that secret bits can be embedded in each matrix F by changing at most two entries. After by changing entries of F is called a configuration. Since |F| = q and each entry has k-1 ways to change, the number of configurations different from F after changing one entry is (k-1)q at most, if we change two entries in F, $(k-1)^2.q.(q-1)/2$ configurations can be obtained. Therefore, by changing at most two pixels in F, i.e., $1+(k-1).q+(k-1)^2.q.(q-1)/2$ configurations. Since the given scheme permits changing at most two pixels, each pixels has k-1 ways to change, then the number $1+(k-1)\times q+(k-1)^2\times q\times(q-1)/2$ of configurations gained by the method must be larger than or equal to 2^r, or r≤ Rmax where Rmax= $\lfloor\log_2(1+(k-1).q+(k-1)^2.q.(q-1)/2)\rfloor$.

This means that we can hide at most Rmax secret bits in F for any CPTE scheme. We denote Rmax by $MSDR_2$ and call it the Maximal Secret Data Ratio as the theoretic limit of all CPTE schemes (the index 2 means that at most two pixels can be changed in each block). Similarly, with the restriction: at most one bit can be changed in each block, we deduce $MSDR_1 = \lfloor\log_2(1+(k-1).q)\rfloor$ bits can be embedded in each block. Especially, for the case of binary image, k = 2, we deduce: $MSDR_1 = \lfloor\log_2(1+q)\rfloor$, $MSDR_2 = \lfloor\log_2(1+q+q.(q-1)/2)\rfloor = \lfloor\log_2(1+q.(q+1)/2)\rfloor$ secret bits can be embedded in F.

2.2. CPTE1 Scheme

Binary image can be considered as a two color images, so k = 2. The addition in Z_2 can be seen as the operation ⊕ (exclusive-OR) on bits and $M = Z_2 \times Z_2\times..\times Z_2$ is the n-fold Cartesian product of Z_2 which can be seen as a (right) Z_2-module. Then we have the unique 1-base U = M-{0}. Each element x = $(x_1,x_2,.., x_n)$ in M can be presented as an n-bit stream x = $x_1x_2..x_n$, with operations defined as follows:

- For any x = $x_1x_2..x_n$, y = $y_1..y_n$ in M, k in Z_2
- D1) x+y = $z_1z_2..z_n$ where z_i=x_i ⊕y_i, I = 1,..,n
- D2) x.k = $z_1z_2..z_n$ where z_i=x_i.k = x_i AND k

Given a binary image G, we set $C_G = Z_2 = \{0,1\}$ and Val is the identical function on Z_2, Val(c)=c for all c in Z_2. The mapping Next: $Z_2 \to Z_2$ by becomes the function satisfied Equation 2:

$$\text{Next}(c) = c+1, \text{for all c in } Z_2 \quad (2)$$

And changing or inverting a color c means that c is replaced by Next(c).

Example 1

The subset U = {0001,0010,0100,1000,1111} of 5 elements is a 2-base of the module $M = Z_2\times Z_2\times Z_2\times Z_2$. Therefore we use it to hide data. In any block S of 5 pixels, we can change at most two pixels to hide 4 bits. That is the $MSDR_2$ is obtained: $MSDR_2 = \lfloor\log_2(1+5(5+1)/2)\rfloor = 4 = \lfloor\log_2(|M|)\rfloor$. Hence U is an optimal 2-base of M. Let us remark that by CPT scheme we can hide only $\lfloor\log_2(1+5)\rfloor = 2$ bits in a block of 5 pixels.

We consider the general case that in each block F of a binary image G, two pixels can be changed to hide data in F. We consider F as one binary matrix F = (F_{ij}) of size m×n of G in which each entry F_{ij} of F presents the pixel (i,j) and its color $F_{ij} \in C_G = Z_2 = \{0,1\}$. Put p = mn+2 Equation 3 and 4:

$$\beta = t \text{ and } \alpha = t-1, \text{ if}(\lfloor \log p \rfloor = \lfloor \log(p/3) \rfloor + 1)$$
$$\beta = t-1 = \alpha, \text{ if}(\lfloor \log p \rfloor > \lfloor \log(p/3) \rfloor + 1) \quad (3)$$
$$\text{where } t = \lfloor \log p \rfloor$$

$$m(p) = \alpha + \beta \quad (4)$$

Now we consider the two phases of hiding and extracting secret bits by CPTE1 Scheme:

```
CPTE1: Embedding algorithm
Input: block F of image G, secret key K, secret-weight matrix W of same size m×n. Secret message b.
Output: Stego- block image F' (of the stego image G')

Step 1: Compute $T=F\oplus K$.
Step 2: Compute $S = [W.T]$, $x_1= S\wedge((2^\alpha -1)\times 2^\beta)$
 and $x_2 = S\wedge(2^\beta -1)$
Step 3: Compute $u = b\wedge((2^\alpha -1).2^\beta )$
 Compute $v = S\wedge(2^\beta -1)$, so that $b = u \oplus v$.
 a) $x_1=u$: intact;
 b) $x_1\neq u$: compute $y = u\oplus x_1 = W_{i,j}$,
 $F_{i,j}' = F_{i,j} + 1$
 c) $x_2=v$: intact;
 d) $x_2\neq v$: compute $y = v\oplus x_2 = W_{i,j}$,
 $F_{i,j}' = F_{i,j} + 1$
```

```
CPTE1: Extracting algorithm
Given F as the matrix which the secret bit stream d is embedded in.

Step 1: Compute $T= F\oplus K$;
Step 2: Compute $S= [W.T]$;
Step 3: Return S as the secret bit stream.
```

Example 2

Given 3×3 binary matrices F, K, a 3×3 weight matrix W and $d=d_4d_3d_2d_1$ 4bit stream ($p = 9+2 = 11 = 8+2+1$ has binary presentation as 1011, by ($\alpha = \beta = 2$, $m(p) = 4$). In details, $S_1=\{F_{11},F_{12},F_{13},F_{21},F_{22}\}$; $S_2=\{F_{23},F_{31},F_{32},F_{33}\}$, $M_1=\{0,12,8,4\}$, $M_2=\{0,3,2,1\}$ or in binary presentation, $M_1=\{0000,1100,1000,0100\}$, $M_2 = \{0000, 0011, 0010, 0001\}$. For example:

$$F = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} k = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} W = \begin{bmatrix} 8 & 12 & 4 \\ 4 & 8 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

$$T = F \oplus K = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$S = [W.T] = 8 \oplus 12 \oplus 4 \oplus 1 \oplus 2 = 1000 \oplus 1100 \oplus 0100 \oplus 0001 \oplus 0010 = 0011$:

- Write $S = x_1\oplus x_2$, $x_1= 0000$, $x_2 = 0011$
- with $d = 0011$, since $d = s$, F is not changed
- with $d = 0000$, we write $d = u\oplus v$, $u = 0000$, $v = 0000$. Since $u = x_1$, F is no change. By $v\neq x_2$, we need to change
- Putting $a = v\oplus x_2 = 0000 \oplus 0011 = 0011$, we need to choose $W_{33} = 0011$, or the corresponding F_{33} has to be changed to $F_{33}\oplus 1 = 0$

2.3. CPTE2 Scheme

To improve embedded binary image, in (Tseng and Pan, 2001) introduced a modified scheme (MCPT scheme for short) from CPT scheme (Pan *et al*., 2000; Hirohisa, 2003; Tseng and Pan, 2001) to control the high quality of embedded binary images. In this section we propose a new modified CPTE2 scheme based on our CPTE1 scheme, which is to improve the high quality of embedded binary images.

In this scheme, in the $m(p) = \alpha+\beta$ secret bit stream, say $d_{m(p)}d_{m(p)-1}..d_{m(p)-\alpha+1}$ $d_\beta d_{\beta-1}..d_2d_1$, α real secret bit stream $d_{m(p)}d_{m(p)-1}..d_{m(p)-\alpha+1}$ is hidden in S_1 by changing at most one pixel as before, in S_2 we hide β bit stream $d_\beta d_{\beta-1}..d_2d_1$ but only β-1 bit stream $d_\beta d_{\beta-1}..d_2$ is used as real secret data, the rest d_1 is used as a control bit for the hiding process and the β bit stream will be hidden in S_1. Putting $d_1 = 1$ means that the β bit stream is odd' which informs that the hiding process in F is failure and we need to hide these secret bits in next blocks F' of the image G and so on.

2.3.1. Modification for Quality Control

We calculate a binary control matrix d(F) with the same size m×n which is defined by: $d(F)_{ij} = 1$ in case $\min_{x,y} \{(i-x)^2 + (j-y)^2 \mid F_{xy}=1-F_{ij}\}\leq 2$ and $d(F)_{ij} = 0$ otherwise. The condition $d(F)_{ij} = 1$ means that there is a neighboring entry F_{xy} closed to F_{ij} (in at most 8 directions) in F such that $F_{xy}=1-F_{ij}$ as the completion value of F_{ij}. This matrix is used to check whether a pixel F_{ij} can be inverted (i.e., $d(F_{ij}) = 1$) or not. In cases of color images, the control matrix need to be defined more delicately and this is a subject of future works. For example, a binary block F and its d(F) are given by:

$$F = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} d(F) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

We need to set d = $d_{m(p)}d_{m(p)-1}..d_1$ =[W.(F'⊕K)], with d_1 = 0 if F is success changed to F', or d_1=1 otherwise.

Extra conditions put on W.

Condition 1

(odd condition): As in Tseng-Pan's scheme MCPT, each sub-matrix of size 2×2 in W having at least one odd element.

Condition 2

(skip condition) it should be Equation 5 and 6:

$$[W.K] \bmod 2 = 1 \tag{5}$$

$$[W. \sim K] \bmod 2 = 1 \tag{6}$$

where, ~K denotes the completion matrix of K (taking completion on each entry).

Remark 4

It should be satisfied the skip condition since that if F is mono-value, that is F having only 1, or 0 values, before-or after inversion, without this condition ones need to check whether F is mono-value or not since this leads to verify F is fail or success to hide secret data.

2.3.2 Embedding Algorithm for Quality Control

We assume that the conditions 1, 2:

Step 1:If F is mono-value, keep F intact and exit,

Step 2: u = [W.T].

Step 3: Set d'=d AND 11..10, where 11..10 is an m(p) bit stream and the AND is treated as bitwise AND on m(p) bit streams. We obtain the m(p) bit stream d'= $d_{m(p)}d_{m(p)-1..}d_2 0$. We try to embed d' into F as in CPTE1 scheme by at most one pixel is changed in S_1 and at most another in S_2 by using the control matrix d(F) in case we can. Otherwise, go to the next step.

Step 4: Try to mark F as failure. Present u as m(p) bit stream u= $u_{m(p)}u_{m(p)-1..}u_2u_1$.

One of two following cases can be happen:

+) u_1 =1: F is kept without changed and exit.

+) u_1 =0: invert at most one entry of S_2.

Set H={F_{ij} | W_{ij} is odd, a_{ij} =1}.

- if F is mono-value, then H = ∅, therefore S is odd by the skip condition 2, this is a contradiction. Hence F is not mono-value, H is not empty by the condition 1 (see Lemma 1 below) and we can randomly changing an arbitrary F_{ij} in H, after that u is changed to the odd value u' = u⊕W_{ij}, as we need: F is marked as failure, go to the next step.

Step 5: End.

2.3.3 Algorithm for Extracting Secret Data

```
Step 1: Compute T = F ⊕ K.
Step 2: Compute u = [W. T],
        - if u is odd: conclude F is fail and exit.
        - if u is even: u = $u_{m(p)}u_{m(p)-1..}u_2 0$, go to next step 3.
Step 3: Return $u_{m(p)}u_{m(p)-1..}u_2$ as the secret m(p)-1 bit.
```

3. RESULTS AND DISCUSSION

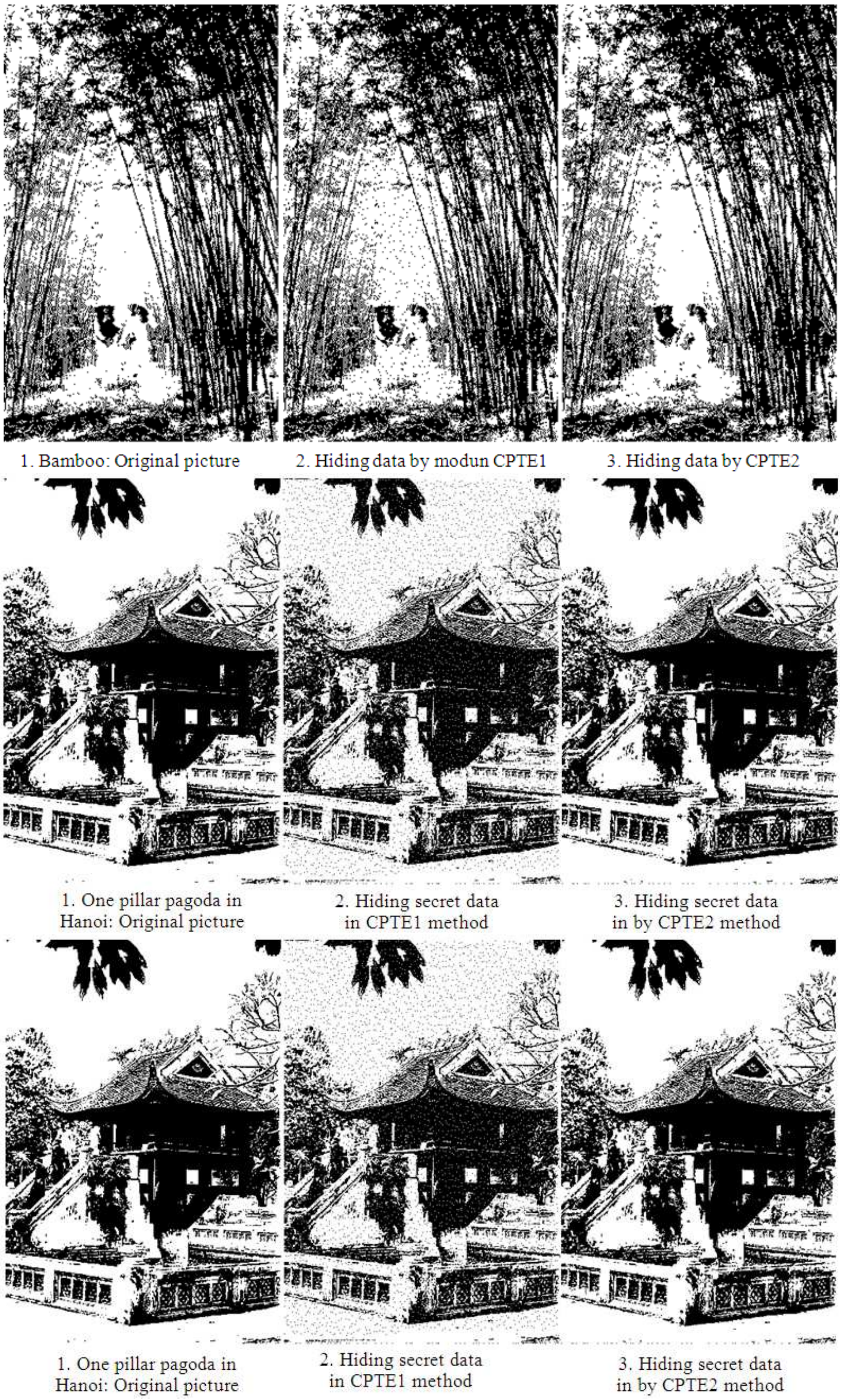
Table 1 show the comparison number of secret bits can be embedded in F with each scheme CPT, CPTE1, MCPT and CPTE2. **Table 2** gives comparisons for three binary images "Bamboo, One Pilot Pagoda in Hanoi, A little singer". Peak signal-to-noise ratio, often abbreviated PSNR, is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. The value PSNR is computed by Equation 7 and 8:

$$PSNR = 10 \bullet \log_{10}\left(\frac{255^2}{MSE}\right) \tag{7}$$

$$\frac{1}{m \times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I_{i,j} - K_{i,j}]^2 \tag{8}$$

Here m and n are the cover image's width and height, $I_{i,j}$ stands for the pixel value of the original m×n binary image at (i,j) and $K_{i,j}$ represents the pixel value after modifications at (i,j) in the m×n stego-image. In **Fig. 1**, we only present three sequences of the binary images by applying CPTE1, CPTE2 schemes, each F has the same size 8×8, since by applying CPT and MCPT schemes or by CPTE1 and CPTE2 respectively, with the same PSNRs, the result images look the same.

In **Table 2**, CPTE1 scheme shows a higher capacity than any of the other schemes. The CPTE2 scheme has very good image quality and a reasonable capacity. **Figure 1** show the comparison between original ("Bamboo", "One Pillar Pagoda" and "A Little Singer") and stego images with CPTE1 and CPTE2 schemes.



1. Bamboo: Original picture

2. Hiding data by modun CPTE1

3. Hiding data by CPTE2

1. One pillar pagoda in Hanoi: Original picture

2. Hiding secret data in CPTE1 method

3. Hiding secret data in by CPTE2 method

1. One pillar pagoda in Hanoi: Original picture

2. Hiding secret data in CPTE1 method

3. Hiding secret data in by CPTE2 method

Fig. 1. Experiment results based on CPTE1 and CPTE2 schemes

Table 1. Comparison of MSDR2 with other schemes

	Hidden bits				
F (size)	MSDR	CPT	CPTE1	MCPT	CPTE2
5	4	2	3	1	2
12	6	3	6	2	4
30	8	4	8	3	7
63	10	6	10	5	9
64	11	6	10	5	9

Table 2. Comparison of capacity and quality (dB) among CPT, MCPT, CPTE1 and CPTE2 schemes

	CPT		MCPT		CPTE1		CPTE2	
Name	PSNR	Bytes	PSNR	Bytes	PSNR	Bytes	PSNR	Bytes
Bamboo (250´400)	63.3	1139	73	95	63.3	1937	73	295
One Pilot Pagoda in Hanoi (350´514)	63.3	2063	73	100	63.3	3440	73	515
A little singer (274´330)	63.3	1044	73	92	63.3	1742	73	265

4. CONCLUSION

In this study, we proposed novel data hiding methods, namely, the CPTE1 and CPTE2 schemes. The CPTE1 and CPTE2 schemes have larger embedding rates than the CPT scheme and is approximate to that of MSDR. Our proposed scheme show the good quality in aspect of CPTE2. The results of our experiment showed that our schemes prove good scheme for binary data hiding.

5. ACKNOWLEDGEMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) by the Ministry of Education, Science and Technology (20120192).

6. REFERENCES

Bierbrauer, J. and J. Fridrich, 2008. Constructing good covering codes for applications in steganography. Trans. Data Hid. Multimedia Sec., Sci., 4920: 1-22. DOI: 10.1007/978-3-540-69019-1_1

Cao, H. and A.C. Kot, 2012. EAG: Edge adaptive grid data hiding for binary image authentication. Proceedings of the Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, Dec. 3-6, IEEE Xplore Press, Hollywood, CA., pp: 1-6. Gao, T. and M. Su, 2010. Topology based fragile watermark for binary image. Proceedings of the 6th International Conference on Digital Content, Multimedia Technology and its Applications, Aug. 16-18, IEEE Xploer Press, Seoul, pp: 290-295.

Chang, C.C., T.D. Kieu and Y.C. Chou, 2008. A high payload steganographic scheme based on (7, 4) hamming code for digital images. Proceedings of the International Symposium on Electronic Commerce and Security, Aug. 3-5, IEEE Xplore Press, Guangzhou City, pp: 16-21. DOI: 10.1109/ISECS.2008.222

Guo, M. and H. Zhang, 2010. High capacity data hiding for binary image authentication. Proceedings of the 20th International Conference on Pattern Recognition, Aug. 23-26, IEEE Xplore Press, Istanbul, pp: 1441-1444. DOI: 10.1109/ICPR.2010.356

Hirohisa, H., 2003. A modified CPT scheme for embedding data into binary images. Kyoto University.

Lin, K.T., 2011. Data encrypting in a binary image base on modified data hiding method. Proceedings of the 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Oct. 14-16, IEEE Xplore Press, Dalian, pp: 69-72. DOI: 10.1109/IIHMSP.2011.78

Pan, H.K., Y.Y. Chen and Y.C. Tseng, 2000. A secure data hiding scheme for two-color images. Proceedings of the 5th IEEE Symposium on Computers and Communications, Jul. 3-6, IEEE Xplore Press, Antibes-Juan les Pins, pp: 750-755. DOI: 10.1109/ISCC.2000.860731

Tseng, Y.C. and H.K. Pan, 2001. Secure and invisible data hiding in 2-color images. Proceedings of the IEEE 20th Annual Joint Conference of the IEEE Computer and Communications Societies, Apr. 22-26, IEEE Xplore Press, Anchorage, AK., pp: 887-896. DOI: 10.1109/INFCOM.2001.916280

Wu, M.Y. and J.H. Lee, 1998. A novel data embedding method for two-color facsimile images. Proceedings of the International Symposium on Multimedia Information Processing, (MIP' 98), CiteSeerX.

Yadav, G.S. and A. Ojha, 2012. A fast and efficient data hiding scheme in binary images. Proceedings of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Jul. 18-20, IEEE Xplore Press, Piraeus, pp: 79-84. DOI: 10.1109/IIH-MSP.2012.25