Journal of Digital Contents Society Vol. 17 No. 6 Dec. 2016(pp. 461-469)
https://doi.org/10.9728/dcs.2016.17.6.461

Ternary Bose - Chaudhuri - Hocquenghem (BCH) with t = 2 code for steganography

Vasily Sachnev*, Yong Soo Choi**

Abstract

A novel steganography based on ternary BCH code with t = 2 is presented in this paper. Proposed method utilizes powerful BCH code with t = 2 for data hiding to the DCT coefficients from JPEG images. The presented data hiding technique uses a proposed look up table approach for searching multiple solutions for ternary BCH code with t = 2. The proposed look up table approach enables fast and efficient search for locations of DCT coefficients, which are necessary to modify for hiding data. Presented data hiding technique is the first steganography technique based on ternary BCH code. Experimental results clearly indicate advantages of using ternary BCH compared to binary BCH.

Keywords : BCH Code, Steganography, Compression Domain, Coefficients

3진 BCH (Bose - Chaudhuri - Hocquenghem) 코드를 이용하는 스테가노그라피 기법

Vasily Sachnev*, 최용수**

요 약

본 논문에서는 t = 2인 3진 BCH 코드를 기반으로 하는 새로운 스테가노그라피 방법을 제시한다. 제안 된 방법에서는 JPEG 영상으로부터 추출된 DCT 계수들에 데이터 은닉을 하기 위해 t = 2인 강력한 BCH 코드를 사용하였다. 제안하는 데이터 은닉 기술은 삼진 BCH 코드(t=2인 경우)에서 다양한 해결책을 찾기 위한 접근으로 제안된 룩업테이블을 사용하였다. 고안된 룩업 테이블 접근법은 데이터 은닉을 위해 수정이 필요한 DCT 계수들의 위치를 빠르고 효율적으로 연산 가능하게 하였다. 제시된 데이터 은닉 기술은 삼진 BCH 코드를 이용하는 최초의 스테가노그라피 기술이다. 실험 결과를 통해 이진 BCH 코드에 비해 삼진 BCH 코드를 사용하는 것이 우수함을 명확하게 증명하였다.

키워드 : BCH 코드, 스테가노그라피, 압축 도메인, 계수

1. Introduction

Recent advantages in multimedia, communication, internet and etc. create various threats and malicious activities. Traditional security based on cryptography techniques achieve high level of security and widely used nowadays. However, modern security techniques does not hide existence of using security and encrypted information is always visible. Hackers may always identify encrypted data easily. The steganography resolves this issue. Steganography may keep high level of security and hide the existence of using

※ Corresponding Author : Yong Soo Choi
Received : December 03, 2016
Revised : December 27, 2016
Accepted : Decembe 30, 2016
* School of Information, Communication and Electronics Engineering, Catholic University
email: bassvasys@hotmail.com
** Division of Liberal Arts & Teaching, Sungkyul University
Tel: +82-31-467-8374
email: ciechoi@sungkyul.ac.kr

cryptography, such that encrypted data becomes invisible. Steganography hides a secret message into a cover signal, such as image, audio, video, text, etc. Modified cover signal is stego signal, which contains hidden secret massage. Steganography modifies cover signal such that modifications become statistically undetectable compared to original unmodified cover. Hackers may see a lot of outgoing data (mostly images), which may contain secret messages or may not. Thus, stego images must be first detected in the set of thousand original images. Nowadays such search is a big challenge.

Methods developed to detect stego image among original cover images are called steganalysis. Steganalysis deeply analyses all input images and identifies artificial changes done by steganography. If such changes are detected, steganalysis is successful. Modern steganalysis contains two parts: feature extractions and stego/cover image classifier based on modern machine learning techniques. Feature extraction is a key component of the modern steganalysis. Efficiency of the steganalysis mostly depends on the extracted features. In order to increase accuracy of the stego/cover image classifier modern steganalysis uses extremely large feature sets (10.000 – 40.000 features) [16], [17]. The extra large features set has higher chance to define artificial changes done by steganography. Hence, new steganography technique with better data hiding properties, suitable to survive against powerful steganalysis is needed. In this paper, we present a novel data hiding technique based on ternary BCH for JPEG steganography.

Among all possible covers, digital image is more suitable for steganography. Users exchange millions of photos through social networks and various chats. Among all image formats, JPEG is the most popular. Thus, developing the JPEG steganography methods becomes an important research direction in the steganography area[21].

JSteg [1] is very first JPEG steganography method designed specifically for JPEG images. JSteg hides data to LSB values of each DCT coefficients in JPEG image. Histogram of DCT coefficients becomes heavily damaged, which makes statistical detection of JSteg possible. Later [2], [4], [5] researchers balanced modification of DCT coefficients such that histogram shape becomes unchanged. Such strategy makes steganalysis based on statistical analysis of histogram of DCT coefficients less accurate. Solanki et. al. [6] hide data to spatial domain using robust watermarking. Cross domain data hiding preserves original statistical relationships in JPEG domain, which causes extra difficulties for steganalysis.

Another discovered way to survive against powerful steganalysis bases on using advanced coding, which spreads modifications through entire image and hides more data with less number of modified coefficients. Westfeld [3] developed famous F5 steganography technique based on Hamming code. Schonfeld and Winkler [7] used BCH code for data hiding purposes. Zhang et. al [8] significantly simplified JPEG steganography based on BCH. Later Sachnev et. al. [9] significantly improved BCH based steganography by applying advanced heuristic optimization. Filler et. al. [10] utilized Syndrome Trellis code (STC) for steganography. Hence, new code with even better performance is needed. In this paper, new ternary BCH code for steganography is presented.

The concept of using "minimal distortion" significantly improved modern JPEG steganography. The concept was introduced by Fridrich et al. [10], [11], [12], [13], [14], [15], [19]. The method creates JPEG images from original bitmap image and utilizes side information from bitmap image to choose DCT

coefficients which cause minimum distortion effect. The combination of using concept of "minimum distortion" and advanced codes creates a basis for modern steganography.

In this paper a novel ternary data hiding technique is presented. Sachnev et. al. [18] introduced ternary data for JPEG steganography based on Hamming code. It was proven in [7], [8] and [9] that BCH code has higher potential for improvement compared to Hamming code [3]. Ternary data hiding based on Hamming code [18] showed significant improvement compared to traditional binary Hamming code.

This paper is organized as follows. Section 2 presents ternary BCH with t = 2. Section 3 presents the proposed look up table approach for ternary BCH. In section 4 a data hiding framework is presented. Section 5presents experimental results. Section 6 concludes the paper.

2. Ternary Data Hiding using BCH(t = 2)

Proposed ternary data hiding using BCH with t = 2 first converts DCT coefficients to set of ternary coefficients. Ternary coefficients are calculated as follows:

$$v_i = d_i \bmod 3 \quad (1)$$

where d_i is the i-th DCT coefficients, v_i is a i-th ternary coefficient.

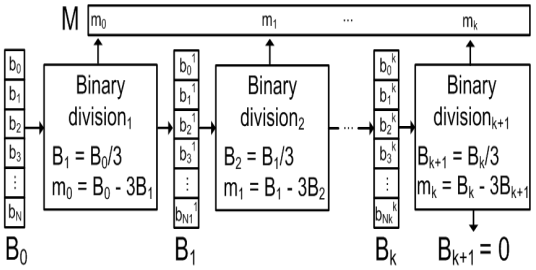
Modified coefficient is computed as follows:

$$D_i' = \begin{cases} d_i + 1 \; if \; m_i - v_i = 1 \; and \; m_i - v_i = -2 \\ d_i - 1 \; if \; m_i - v_i = -1 \; and \; m_i - v_i = 2 \\ d_i \quad otherwise \end{cases} \quad (2)$$

where m_i is the corresponding i-th ternary message coefficients.

Given messages are mostly given in binary shape. Hence, conversion from binary to ternary is required.

Assume $B = \{b_0, b_1, b_2, \dots, b_N\}$ is a binary message, N is the number of bits in the message (Figure 1) shows a systematic way to convert binary message B to a set of ternary coefficients $M = \{m_0, m_1, m_2, \dots, m_k\}$, where k is the length of ternary message.



(Figure. 1) Binary to ternary converter

Given binary message B_{i-1} is iteratively processed using "Binary division" (see Figure 1.). "Binary division" computes binary quotient B_i and ternary reminder m_{i-1}, which is (i-1)-th ternary coefficient of the ternary message M. "Binary division" stops when division is not longer possible and quotient B = 0.

Any q-ary BCH code in GF(q^m) with length $n = q^m - 1$has parity check matrix presented as follows:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & (\alpha)^2 & (\alpha^2)^2 & \dots & (\alpha^{n-1})^2 \\ \vdots & & \vdots & & \\ 1 & (\alpha)^{2t} & (\alpha^2)^{2t} & \dots & (\alpha^{n-1})^{2t} \end{pmatrix} \quad (3)$$

Parit-check matrix for t = 2:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(n-1)} \end{pmatrix} \quad (4)$$

Ternary data hiding based on BCH with t = 2 needs vector of the original ternary coefficients: $V = \{v_0, v_1, v_2, \dots, v_{n-1}\}$ computed using Equation 1. Corresponding polynomial is computed as follows:

$\mathbf{T}(x) = t_0 + t_1 \cdot x + t_2 \cdot x^2 + \cdots + t_{n-1} \cdot x^{n-1}$.

Vector of the original ternary coefficients has size equal to $n = q^m - 1$.

Ternary data hiding based on BCH with t = 2 hides ternary message $\mathbf{m} = [\mathbf{m}_1\ \mathbf{m}_2], \mathbf{m} \in [0, \mathrm{n}]$. Ternary message $\mathbf{m}$ is computed from a vector of ternary coefficients M using binary to ternary convertor as follows:

$$\boldsymbol{m}_1 = m_0 + 3^1 \cdot m_1 + 3^2 \cdot m_2 + \cdots + 3^{m-1} \cdot m_{m-1}$$
$$\boldsymbol{m}_2 = m_m + 3^1 \cdot m_{m+1} + 3^2 \cdot m_{m+2} + \cdots + 3^{m-1} \cdot m_{2m}$$

Data hiding using ternary BCH with t = 2 searches a vector of modified ternary coefficients R such that following equation holds:

$$\mathbf{m} = R \cdot H^T \qquad (5)$$

where modified vector of ternary coefficients: $R = \{r_0, r_1, r_2, \ldots, r_{n-1}\}$ is constructed from the vector of the original ternary coefficients V with minor modifications. Corresponding polynomial R like below:

$\mathbf{R}(x) = r_0 + r_1 \cdot x + r_2 \cdot x^2 + \cdots + r_{n-1} \cdot x^{n-1}$.

Error location polynomial is a difference between original polynomial V and modified polynomial R

$$\mathbf{E} = \mathbf{V} - \mathbf{R} \qquad (6)$$

or

$$\mathbf{E} = e_{u_1} \cdot x^{u_1} + e_{u_2} \cdot x^{u_2} + e_{u_3} \cdot x^{u_3} + \cdots + e_{u_l} \cdot x^{u_l} \qquad (7)$$

where $u = \{u_1, u_2, u_3, \ldots, u_l\}$ are indexes of the ternary coefficients which need to be replaced to $E = \{e_{u_1}, e_{u_2}, e_{u_3}, \ldots, e_{u_l}\}$. Assume that $\sigma_i = e_{u_i}$, then $E = \{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_l,\}$

The syndrome is calculated as follows:

$$\mathbf{S} = \mathbf{m} - V \cdot H^T = \mathrm{E} \cdot H^T = [S_1\ S_2]^T \qquad (8)$$

or,

$$S_1 = \sigma_1 \cdot \alpha^{u_1} + \sigma_2 \cdot \alpha^{u_2} + \sigma_3 \cdot \alpha^{u_3} + \cdots + \sigma_l \cdot \alpha^{u_l}$$

$$S_2 = \sigma_1 \cdot \alpha^{2u_1} + \sigma_2 \cdot \alpha^{2u_2} + \sigma_3 \cdot \alpha^{2u_3} + \cdots + \sigma_l \cdot \alpha^{2u_l}$$

where $\{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_l,\}$ and $\{u_1, u_2, u_3, \ldots, u_l\}$ are unknown values.

Thus, hiding data $\mathbf{m}$ to vector of original ternary coefficients V searches for unknown $\{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_l,\}$ and $\{u_1, u_2, u_3, \ldots, u_l\}$.

Vector V with modified coefficients $\{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_l,\}$ in the positions $\{u_1, u_2, u_3, \ldots, u_l\}$ creates modified vector R such that $\mathbf{R} \cdot H^T = \mathbf{m}$. Hence, special technique for searching necessary $\{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_l,\}$ has to be developed.

3. Look up table approach for ternary BCH with t = 2

In this section, look up table approach for searching $\{\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_l,\}$ is presented. In the proposed look up table approach all possible solutions including 1-flip $\{u_1\}$, 2-flip $\{u_1, u_2\}$, 3-flip $\{u_1, u_2, u_3\}$ and 4-flip $\{u_1, u_2, u_3, u_4\}$ solutions for all possible syndromes $\mathbf{S} = [S_1\ S_2]^T$ are stored in a set of look up tables Lu(m) created for various m by using an algorithm displayed in (Figure 2).

The proposed algorithm is a brute-force search for all possible syndromes $\mathbf{S} = [S_1\ S_2]^T$ by modifying flip locations for 1-flip $\{u_1\}$, 2-flip $\{u_1, u_2\}$, 3-flip $\{u_1, u_2, u_3\}$ and 4-flip $\{u_1, u_2, u_3, u_4\}$ and applying all possible variation of $\sigma \in [0, m-1]$. In the proposed algorithm flip locations and coefficients σwere combined together for more compact shape. If q = 3 and m = 3 or 4, coefficients $\{u_1, u_2, u_3, u_4\}$ are combined with necessary modification coded by corresponding coefficient

σ. The coefficient may either request to modify the ternary coefficient by adding 1 or subtracting 1 from corresponding coefficient in vector V. Thus, the flip locations stored in look up table are either positive or negative $\{\pm u_1, \pm u_2, \pm u_3, \pm u_4\}$ positive flip locations indicate modification by adding 1, negative flip locations indicate modification by subtracting 1.

The proposed algorithm for creating look up table is computational extensive with complexity increasing exponentially for higher m. However, the proposed lookup table can be calculated once and all other calculations necessary to obtain flip locations according to predefined syndrome are relatively simple (see Figure 3).

Example: Assume q = 3, m = 3, then $n = q^m - 1 = 3^3 - 1 = 26$, secret message $\mathbf{m} = \{6\ 3\}^T$, and the set of 26 DCT coefficients taken from JPEG image produces vector of original ternary coefficients V = { 0, 1, 0, 1, 2, 2, 1, 0, 0, 2, 0, 2, 1, 2, 0, 1, 0, 2, 0, 2, 2, 2, 0, 1, 0, 2}. Parity – check matrix $H_{2\times 26}$ for q = 3 and m = 3 is given below:

$$H = \begin{pmatrix} 1\,3\,9\,5\,15\,23\,13\,17\,20\,4\,12\,14\,11\,26\,18\,7 \ldots 19 \\ 1\,9\,15\,13\,20\,12\,11\,6\,7\,16\,22\,8\,25\,1\,9\,15\,13 \ldots 25 \end{pmatrix}$$

1-flip:

```
for u1 = 0 to n
 for σ1 = 0 to m-1
      S1 = σ1 ·q^u1
      S2 = σ1 ·q^2·u1
     Lu(m, S1, S2, "1-flip",c) = u1, σ1
      c ++
 end
end
```

2-flip:

```
for u1 = 0 to n
  for u2 = 0 to n
    for σ1 = 0 to m-1
      for σ2 = 0 to m-1
        S1 = σ1 ·q^u1+σ2 ·q^u2
        S2 = σ1 ·q^2·u1+σ2 ·q^2·u2
        Lu(m, S1, S2, "2-flip",c) = {u1, u2, σ1, σ2}
        c ++
      end
    end
  end
end
```

3-flip:

```
for u1 = 0 to n
  for u2 = 0 to n
    for u3 = 0 to n
      for σ1 = 0 to m-1
        for σ2 = 0 to m-1
          for σ3 = 0 to m-1
            S1 = σ1 ·q^u1+σ2 ·q^u2+σ3 ·q^u3
            S2 = σ1 ·q^2·u1+σ2 ·q^2·u2+σ3 ·q^2·u3
            Lu(m, S1, S2, "3-flip",c) = {u1, u2, u3,
                                         σ1, σ2, σ3 }
            c ++
          end
        end
      end
    end
  end
end
```

4-flip:

```
for u1 = 0 to n
  for u2 = 0 to n
    for u3 = 0 to n
      for u4 = 0 to n
        for σ1 = 0 to m-1
          for σ2 = 0 to m-1
            for σ3 = 0 to m-1
              for σ4 = 0 to m-1
                S1 = σ1 ·q^u1+σ2 ·q^u2+σ3 ·q^u3+σ4 ·q^u4
                S2 = σ1 ·q^2·u1+σ2 ·q^2·u2+σ3 ·q^2·u3+σ4 ·q^2·u4
                Lu(m, S1, S2, "4-flip",c) = {u1, u2, u3, u4,
                                             σ1, σ2, σ3 , σ3 }
                c ++
              end
            end
          end
        end
      end
    end
  end
end
```

(Figure 2) Algorithm to create look up table for various q and m

$V \cdot H^T = \{26\ 23\}$, then syndrome can be computed using Equation 8.

$$\mathbf{S} = \mathbf{m} - V \cdot H^T = [6\ \ 3]^T - [26\ \ 23]^T = [10\ \ 10]^T$$

Note that all calculation presented in this paper are processed through Galois Field GF (3^3). Summation and substruction tables for ternary calculation are presented in Table 1.

Transformation from decimal to ternary is presented as follows:

$$N_{10} = v_0 + v_1 3^1 + v_2 3^2 + v_3 3^3 + \cdots + v_m 3^m$$

where $(v_0\ v_1\ v_2 \ldots v_m)_3$ is a ternary representation of the decimal number N.

Summation				
x+y	x			
y		0	1	2
	0	0	1	2
	1	1	2	0
	2	2	0	1

Substruction				
$x - y$	x			
y		0	1	2
	0	0	1	2
	1	2	0	1
	2	1	2	0

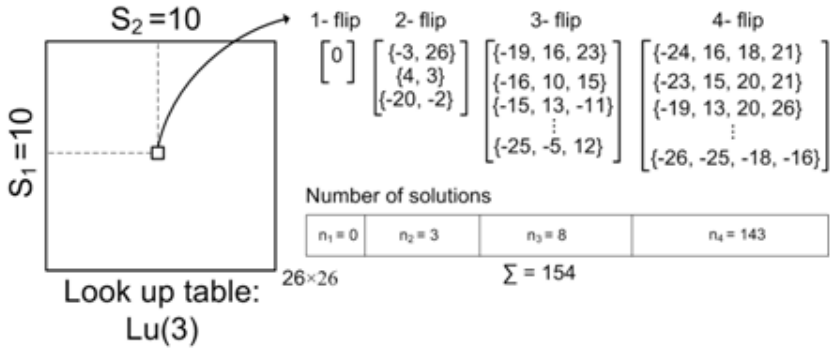
<Table 1> Summation and Subtraction

Then, $6=2 \cdot 3^1=(0\ 2\ 0)_3$, $3=1 \cdot 3^1=(0\ 1\ 0)_3$, $26=2 \cdot 3^2+2 \cdot 3^1+2=(2\ 2\ 2)_3$, $23=2 \cdot 3^2+1 \cdot 3^1+2=(2\ 1\ 2)_3$.

$$[6\ 3]^T - [26\ 23]^T = \left[\begin{pmatrix}0\\2\\0\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix}\right]^T - \left[\begin{pmatrix}2\\2\\2\end{pmatrix}\begin{pmatrix}2\\1\\2\end{pmatrix}\right]^T$$

$$= \left[\begin{pmatrix}0-2\\2-2\\0-2\end{pmatrix}\begin{pmatrix}0-2\\1-1\\0-2\end{pmatrix}\right]^T = \left[\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\right]^T = [10\ \ 10]^T$$

where $(1\ \ 0\ \ 1)_3 = 2 \cdot 3^2 + 1 = 10$.



(Figure 3) Look up table for m = 3, Lu(3)

All possible solutions can be taken from look up table Lu(3) (see Figure 3.). (Figure 3) displays all possible solutions for $\mathbf{S} = [10\ \ 10]^T$. For syndrome $\mathbf{S} = [10\ \ 10]^T$ there is no "1-flip" solutions, there are 3 "2-flip"solutions, 8 "3-flip" solutions and 143 "4-flip solutions", together 154 solutions.

Let's choose the first "2-flip" solution $\{-3,26\}$. Note that negative index implies $r_i = v_i - 1$, and positive index implies $r_i = v_i + 1$.

Coefficients with indexes 3 and 26 in the set of ternary coefficients V = { 0, 1, 0, 1, 2, 2, 1, 0, 0, 2, 0, 2, 1, 2, 0, 1, 0, 2, 0, 2, 2, 2, 0, 1, 0, 2}should be modified as follows: $r_3 = v_3 - 1$ and $r_{26} = v_{26} + 1$.

Then, modified vector of ternary coefficients is R = { 0, 1, 2, 1, 2, 2, 1, 0, 0, 2, 0, 2, 1, 2, 0, 1, 0, 2, 0, 2, 2, 2, 0, 1, 0, 0}. Modified coefficients are marked as bold.

Verification: $\mathbf{m} = R \cdot H^T = [6\ \ 3]^T$ is our hidden message.

The rest 153 solutions from look up table Lu(3) hide the same message.

4. Data hiding framework using ternary BCH with t = 2

Recent advantages in multimedia, communication, internet and etc. create various threats and JPEG steganography utilizes bitmap image I and hides binary message B to the set of DCT coefficients. JPEG steganography creates a stego JPEG image with hidden binary message B. Parameter q is 3.

Encoder:

1) Divide image into 8 by 8 blocks $\mathbf{BI_{8\times8}}$. Compute non rounded and rounded DCT as follows:

$$d^0 = \frac{\mathrm{DCT}(\mathbf{BI_{8\times8}})}{Q}, \qquad d = \mathrm{round}(d^0)$$

where DCT() is a Discrete Cosine Transformation, Q is a quantization matrix, d^0 and d are non rounded and rounded DCT coefficients respectively.

2) Define a set V of ternary coefficients using theEquation 1. Compute distortions $\mathbf{D_{plus}}$ and $\mathbf{D_{minus}}$ as follows:

$$D_{plus} = E_{\Gamma_{plus}} \cdot Q_t \qquad D_{minus} = E_{\Gamma_{minus}} \cdot Q_t$$

$$D_{plus} = \begin{cases} |d^0| + 1 - |d|, if\ d \neq -1 \\ NaN, \qquad if\ d = -1 \end{cases}$$

$$D_{minus} = \begin{cases} |d| - (|d^0| - 1), if\ d \neq 1 \\ NaN, \qquad if\ d = 1 \end{cases}$$

3) Convert binary message B to ternary message M using "Binary to ternary convertor" presented in (Figure 1).

4) Define minimum parameter m such that following inequality holds:

$$\frac{2 \cdot m}{3^m - 1} > \frac{k}{\text{Num}}$$

where k is the number of ternary coefficients in ternary message M, Num is the number of available DCT coefficients.

5) Divide all DCT coefficients into $n = 3^m - 1$ blocks; divide ternary message M into 2m coefficients' blocks, create messages $\mathbf{m} = [\mathbf{m}_1\ \mathbf{m}_2]$

6) Hide data in each block

6.1) Compute syndrome $\mathbf{S} = \mathbf{m} - V \cdot H^T$

6.2) Read all possible solutions from look up table Lu(3, S_1, S_2) for "1-flip", "2-flip", "3-flip" and "4-flip".

6.3) For each solution define total distortion using distortions $\mathbf{D}_{plus}$ and $\mathbf{D}_{minus}$. Choose a solution with the lowest distortion.

6.4) Modify DCT coefficients according to Equation 2.

7) Build JPEG image I_{jpeg} from modified DCT coefficients.

Decoder:

Hidden message B can be recovered from I_{jpeg} as follows:

1) Extract DCT coefficients from I_{jpeg}

2) Define set of ternary coefficients using Equation 1.

3) Extract hidden message block by block using Equation 5.

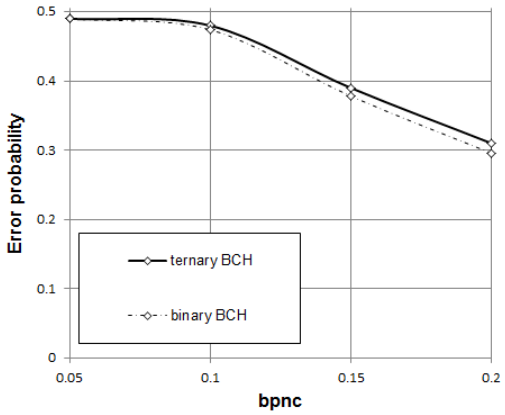
4) Convert the ternary message into binary.

5. Experimental results

The proposed method has been tested by using powerful ensemble classifier steganalysis proposed by Kodovski [17]. Ensemble classifier steganalysis uses a set of 22510 features [16]. A set of 20000 images from BOSS image data [20]has been used for experiments. Proposed ternary data hiding approach based on ternary BCH with t=2 was used to hide various amount of data to the set of 20000 images from BOSS data. The payload has been counted as follows: the number of non-zero DCT coefficients is counted for each image from BOSS data set, payload (0.05 bpnc), 0.1 bpnc, 0.15 bpnc and 0.2 bpnc)identifies the number of bits pear non-zero coefficients. Based on total number of DCT coefficients the number of bits for data hiding is different, but the message size is connected to the predefined payload given in bits per non-zero coefficient. Set of 22510 features is extracted 1) from original 20000 images from BOSS data set, 2) from 20000 modified images for payload 0.05 bpnc, 3) 0.1 bpnc, 4) 0.15 bpnc and 5) 0.2 bpnc. Thus, ensemble classifier [17] has been trained 4 times for different experiments with payloads 1) 0.05 bpnc, 2) 0.1 bpnc, 3) 0.15bpnc and 4) 0.2 bpnc. Each experiment holds 20000 original images and 20000 modified images. Steganalysis does not allow to train the classifier by using a pair (cover image - stego image), in this case performance of steganalysis dropped significantly. Thus, the training set is the random choice of 10,000 images from cover set and another set of 10,000 stego images which does not make a pair with chosen cover images. The rest images are used for testing. The performance of the ensemble classifier is analyzed by using error probability computed as follows:

$$E_p = \frac{1}{2}(P_a + P_b)$$

Where $\mathbf{P_a}$ is the probability of mis-detection (i.e., the cover image is classified as stego) and P_b is the probability of misclassification (i.e., the stego image is classified as cover).



(Figure 4) Error probabilities vs. payload (bpnc)

(Figure 4) shows the experimental results of applying ensemble classifier steganalysis against proposed data hiding based on ternary BCH with t = 2 and JPEG steganography method based on binary BCH with t = 2 [8]. Proposed method shows insignificant improvement for all examined payloads compared to JPEG steganography method based on binary BCH [8].

In this paper a novel steganography technique based on ternary BCH with t = 2 is presented. Proposed method efficiently utilizes a powerful ternary BCH code for data hiding. Few key techniques such as binary to ternary convertor, look up table approach for searching solutions and detailed data hiding framework necessary for implementing ternary BCH with t=2 for data hiding are presented. The proposed ternary data hiding approach produces a large number of possible solutions, and, as a result, shows lower detectability against powerful steganalysis. The experimental results clearly indicate advantage of using ternary data hiding based on BCH with t = 2 compared to binary BCH. Ternary data hiding may be a promising research direction for future research.

References

[1] D. Upham: http://www.funet.-/pub/crypt/steganography/jpeg-jsteg-v4.di®.gz.

[2] N. Provos: Defending against statistical steganalysis. Proc. of 10th USENIX Security Symposium, Washington, DC, 2001.

[3] A. Westfeld: High capacity despite better steganalysis (F5 - a steganographic algorithm). Lecture Notes in Computer Science, vol. 2137, pp. 289 - 302, 2001.

[4] J. Eggers, R. Bauml, and B. Girod: A communications approach to steganography. Proc. of EI SPIE, vol. 4675, pp. 26 - 37, San Jose, CA, 2002.

[5] H.Noda, M. Niimi, and E. Kawaguchi: Application of QIM with dead zone for histogram preserving JPEG steganography. Proc. of ICIP, Genova, Italy, 2005.

[6] K. Solanki, A. Sakar, and B.S. Manjunath. YASS: Yet another steganographic scheme that resists blind steganalysis. Information Hiding, 9th International Workshop Saint Malo, 2007.

[7] D. SchÄonfeld and A. Winkler: Reducing the complexity of syndrome coding for embedding. Lecture Notes in Computer Science, vol. 4567, 2008, 145 - 158.

[8] R. Zhang, V. Sachnev, and H. J. Kim: Fast BCH syndrome coding for steganography. Lecture Notes in Computer Science, vol. 5806, pp. 48 - 58, 2009.

[9] V. Sachnev, H. J. Kim, R. Zhang, Less Detectable JPEG Steganography Method Based on Heuristic Optimization and BCH Syndrome Coding, Proceeding of the 11th ACM workshop on Multimedia and Security, pp 131 - 140, Princeton, 2009.

[10] T. Filler, J. Judas, and J. Fridrich, "Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes," IEEE Transaction on Information Forensics and Security, vol. 6, n. 3, pp. 920-935, 2011.

[11] J. Fridrich, "Minimizing the embedding impact in

steganography," Proceedings of ACM Multimedia and Security Workshop, pp. 2-10, 2006.

[12] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," Proceedings of SPIE, vol. 6505, pp. 2-3, 2007.

[13] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography," ACM Multimedia and Security Journal, vol. 11, no. 2, pp. 98-107, 2005.

[14] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography using wet paper codes," Proceedings of ACM Workshop on Multimedia and Security, pp. 4-15, 2004.

[15] J. Fridrich, T. Pevny, and J. Kodovsky, "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities," Proceedings of ACM Workshop on Multimedia and Security, pp. 3-15, 2007.

[16] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images", IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 868 - 882, 2012.

[17] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," IEEE Transactions on Information Security and Forensics, Vol. 7, No. 2, pp. 432-444, 2012.

[18] V. Sachnev, H. J. Kim, Ternary Data Hiding Technique for JPEG Steganography, Lecture Notes and Computer Science, vol. 6526, pp 202 - 210.

[19] Y. H. Kim, Z. Duric, and D. Richards, Modi-ed matrix encoding technique for minimal distortion steganography. Information Hiding, 8th International Workshop, vol. 4437, pp. 314 - 327, Springer-Verlag, Berlin, 2006

[20] P. Bass, T. Filler, T. Pevny, "Break Our Steganographic System - the ins and outs of organizing BOSS", In proceedings of 13th Information Hiding Conference, Prague, 2011.

[21] Y. S. Choi and J. H. Kim, "A Steganography Method Improving Image Quality and Minimizing Image Degradation," J. of Digital Contents Society, Vol.17, No.5, 2016

Vasily Sacnev

2002년 : Komsomolsk-na-Amure State Tech. University, (B.S)
2004년 : Komsomolsk-na-Amure State Tech. University, (M.S)
2009년 : Korea University (PhD)

2010년~현재: Catholic University, Assistant Professor
관심분야 : Multimedia Security, Steganography, Steganalysis, Machine learning and Bio-informatics

최용수

1998년 강원대학교 제어계측공학과 공학사
2000년 강원대학교 제어계측공학과 공학석사
2006년 강원대학교 제어계측공학과 공학박사
2006년~2007년 연세대학교 첨단융합건설연구단 연구교수
2007년~2013년 고려대학교 정보보호대학원 연구교수
2013년~현재 성결대학교 교양교직부 (멀티미디어) 조교수
관심분야 : Multimedia Hashing, Information Hiding, Watermarking, Steganography, Image Forensics, Forgery Detection 등