International Journal of Computer Applications (0975 - 8887)
Volume 53 - No. 18, September 2012

Improving Embedding Capacity by using the $\mathbb{Z}_4$-linearity of Preparata Codes

Houda JOUHARI
Laboratory of mathematics, informatics and applications
University Mohammed V Agdal
Faculty of Sciences
BP 1014 Rabat Morocco

EL Mamoun SOUIDI
Laboratory of mathematics, informatics and applications
University Mohammed V Agdal
Faculty of Sciences
BP 1014 Rabat Morocco

ABSTRACT

This paper presents a novel steganographic scheme based on non-linear Preparate codes that can achieve better performance for application in steganography than simple linear codes currently in use. The idea of this paper is to use the $\mathbb{Z}_4$-linearity of Preparata non-linear codes for the construction of a new steganographic scheme and to show that quaternary covering functions can provide embedding capacity higher than binary ones and can maintain good image quality as well.

Keywords:

Nonlinear codes, Codes over rings, Quaternary codes, Embedding efficiency, Preparata codes

1. INTRODUCTION

Internet is a popular communication channel nowadays. Transmitted data are easy to be copied or destroyed by unauthorized persons. Therefore, how to transmit data secretly by internet becomes an important topic. Encryption may provide a safe way, which transforms data into a ciphertext via cipher algorithms [1]. However, it makes the messages unreadable and suspicious enough to attract eavesdroppers attention. To overcome this problem, steganography offers different approaches to transmitting secret messages [2]. Steganography is a technique that imperceptibly hides secret data into cover media by altering its most insignificant components for covert communication, such that an unauthorized user will not be aware of the existence of secret data [3].
The most common and well-known steganographic method is called least significant bit (LSB) substitution, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly [4]. Many optimized LSB methods have been proposed to improve this work [5]. The human perceptibility has a property that it is sensitive to some changes in the pixels of the smooth areas, while it is not sensitive to changes in the edge areas. Not all pixels in a cover image can tolerate equal amount of changes without causing noticeable distortion. Hence, to improve the quality of stego images, several adaptive methods have been proposed. An interesting steganographic method is known as matrix embedding, introduced by Crandall[6] and analyzed by Bierbrauer [7] and independently discovered by van Dijk [8] and Galand [9]. Matrix encoding requires the sender and the recipient to agree in advance on a parity check matrix H, and the secret message is then extracted by the recipient as the syndrome (with respect to H) of the received cover object. This method was made popular by Westfeld [10], who incorporated a specific implementation using Hamming codes in his F5 algorithm, which can embed t bits of message in $2^t - 1$ cover symbols by changing at most, one of them.
There are two parameters which help to evaluate the performance of a steganographic method over a cover message of N symbols: the embedding rate $R = \frac{t}{N}$, which t is the amount of bits that can be hidden in a cover message and the embedding efficiency $E = \frac{t}{\rho}$, where the covering radius ρ is the largest number of possible changes. In general, for the same embedding rate a method is better when the embedding efficiency is larger. We acknowledge, though, that the number of changes is not the only important factor influencing the security of the steganographic scheme but the choice of the cover object and the character of modifications play an equally important role.
In this paper, a novel steganographic scheme based on the $\mathbb{Z}_4$-linearity of Praparata codes is described. The experimental results show that the proposed scheme can embed large amounts of information and can maintain good image quality as well.
The remainder of this paper is organized as follows. In Section II we recall the relationship between information hiding and coding theory, and we give a brief introduction to codes defined over $\mathbb{Z}_4$ and more especially Preparata codes. In section III, the embedding and extracting algorithms of the proposed method is presented. The experimental results will be in Section IV. Finally, conclusions are given in Section V.

2. CODING THEORY AND STEGANOGRAPHY

2.1 Notations

Throughout this paper, we will use some standard concepts and results from Coding Theory. Let $\mathbb{F}_2^N$ denote the vector space of all N-bit row vectors $x = (x_1, \cdots, x_N)$. A binary $[N, k]$ code C of block length N and dimension k is a k-dimensional vector subspace of $\mathbb{F}_2^N$, where the sum of two vectors and a multiplication of a vector by scalar are defined using the usual binary arithmetics. The $(N-k) \times N$ matrix H is called a parity check matrix of C if $xH^T = 0$ for each $x \in C$, where H^T denotes the transpose of H. For any $x \in \mathbb{F}_2^N$, the vector $s = xH^T \in \mathbb{F}_2^{N-k}$ is called the syndrome of x. For each syndrome $s \in \mathbb{F}_2^N$, the set $C(s) = \{x \in F_2^N | xH^T = s\}$ is called a coset. Note that $C(0) = C$. Obviously, cosets associated with different syndromes are disjoint. Also, from elementary linear algebra, we know that every coset can be written as $C(s) = x + C$, where $x \in C(s)$ arbitrary. Thus, there are 2^{N-k} disjoint cosets, each consisting of 2^k vectors. Any member of the coset $C(s)$ with the smallest Hamming weight is called a coset leader and will be de-

noted as $e_L(s)$.
The Hamming weight ω_H of a vector x is defined as the number of ones in x (i.e., $\omega_H(x) = x_1 + \cdots + x_N$).
The distance between two vectors x and y is defined as the Hamming weight of their difference $d_H(x, y) = \omega_H(x - y)$. For any $x \in C$, we denote by $\mathcal{B}(x, \rho)$ the ball with center x and radius ρ, $\mathcal{B}(x, \rho) = \{y \in \mathbb{F}_2^N | d_H(x, y) \leq \rho\}$.
The covering radius ρ of a code C is defined as

$$\rho = \max_{x \in \mathbb{F}_2^N} d_H(x, C)$$

where $d_H(x, C) = \min_{c \in C} d_H(x, c)$ is the distance between x and the code C.

2.2 Syndrome Coding (*Matrix Embedding*)

We now briefly review a few relevant known facts about embedding schemes and covering codes that appeared in [9] and [11] and establish some more terminology. Let $\mathfrak{M}$ be the set of all messages. An embedding scheme on $\mathbb{F}_2^N$ with a distortion bound T is a pair of embedding and extraction functions Emb and Ext:

$$Emb : \mathbb{F}_2^N \times \mathfrak{M} \to \mathbb{F}_2^N \text{ and } Ext : \mathbb{F}_2^N \to \mathfrak{M} \quad (1)$$

$$d_H(x, Emb(x, M)) \leq T, \quad \forall \quad M \in \mathfrak{M}, \text{ and } x \in \mathbb{F}_2^N \quad (2)$$

such that for all $M \in \mathfrak{M}$ and all $x \in \mathbb{F}_2^N$, $Ext(Emb(x, M)) = M$. In other words, (1) means that we can embed any message from $\mathfrak{M}$ in any binary N-tuple and (2) states that we can do it using at most T changes.

The matrix embedding theorem is taken from [12] and gives a recipe on how to use an $[N, k]$ code to communicate $(N - k)$ bits using at most ρ changes in a sequence of N bits.

THEOREM 1. *(Matrix embedding) Let C be an $[N, k]$ code with a parity check matrix H and covering radius ρ. The embedding scheme below can communicate $N - k$ bits $M \in \mathbb{F}_2^{N-k}$ in a sequence of N bits $x \in \mathbb{F}_2^N$ using at most ρ changes*

$$Emb(x, M) = x + e_L(M - xH^T) = y$$

$$Ext(y) = yH^T$$

where $e_L(M - xH^T)$ is a coset leader of the coset $C(M - xH^T)$.
Indeed, since C has a covering radius ρ, we know that $d_H(x, y) = \omega_H(e_L(M - xH^T)) \leq \rho$, which shows that the embedding scheme has (a tight) distortion bound ρ. To see that $Ext(Emb(x, M)) = M$, note that $Ext(Emb(x, M)) = yH^T = xH^T + e_L(M - xH^T)H^T = xH^T + M - xH^T = M$.
The goal is to deliberately modify x to y in a way that:

$$Ext(y) = M$$

Steganography technique should generally have two important properties : good visual/statistical imperceptibility and a sufficient payload. The first is essential for the security of hidden communication and the second ensures that a large quantity of data can be conveyed. Two levels of protection can be done if the message is encrypted before hiding it [13].

2.3 Quaternary Codes

Let $\mathbb{Z}_4$ be the ring of integers modulo 4 and $\mathbb{Z}_4^n$ be the set of n-tuples over $\mathbb{Z}_4$. By a quaternary code $\mathcal{C}$ of length n we shall mean a linear block code over $\mathbb{Z}_4$,i.e ., an additive subgroup of $\mathbb{Z}_4^n$.

DEFINITION 1. *A Lee weigth $\omega_L : \mathbb{Z}_4 \to \mathbb{Z}$ of an element in $\mathbb{Z}_4$ is defined as*

$$\omega_L(0) = 0, \ \omega_L(1) = \omega_L(3) = 1, \ \omega_L(2) = 2$$

and a Lee weight of a vector $c \in \mathbb{Z}_4^n$ is naturally : $\omega_L(c) = \sum_{i=1}^n \omega_L(c_i)$. The Lee distance is defined as $d_L(x, y) = \omega_L(x - y)$.
We define an inner product on $\mathbb{Z}_4^n$ by $\langle a, b \rangle = a_1 b_1 + \cdots + a_n b_n (mod 4)$ where $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$, and then the notions of dual code ($\mathcal{C}^\perp$), self-orthogonal code ($\mathcal{C} \subseteq \mathcal{C}^\perp$), and self-dual code ($\mathcal{C} = \mathcal{C}^\perp$) are defined in the standard way. We say that two codes are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called permutation-equivalent.
Any quaternary code is permutation-equivalent to a code $\mathcal{C}$ with generator matrix of the form

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{bmatrix}$$

where A and C are $\mathbb{Z}_2$-matrices and B is a $\mathbb{Z}_4$-matrix. The code is then an elementary abelian group of type $4^{k_1} 2^{k_2}$, containing $2^{2k_l + k_2}$ codewords. We shall indicate this by saying that $\mathcal{C}$ has type $4^{k_1} 2^{k_2}$, or simply that $|\mathcal{C}| = 4^{k_1} 2^{k_2}$.
If $\mathcal{C}$ has generator matrix G, the dual code $\mathcal{C}^\perp$ has generator matrix

$$H = \begin{bmatrix} -B^T - C^T A^T & C^T & I_{n-k_1-k_2} \\ 2A^T & 2I_{k_2} & 0 \end{bmatrix}$$

and type $4^{n-k_1-k_2} 2^{k_2}$

2.4 Gray Map

The vehicle by which binary codes are obtained from linear codes over $\mathbb{Z}_4$ is the Gray map $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ defined by $\phi(0) = 00, \ \phi(1) = 01, \ \phi(2) = 11$, and $\phi(3) = 10$.
Formally, we define three maps from $\mathbb{Z}_4$ to $\mathbb{F}_2$ by:

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

The Gray map is then extended componentwise to a map, also denoted ϕ, from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^{2n}$. The 2-adic expansion of $c \in \mathbb{Z}_4$ is

$$c = \alpha(c) + 2\beta(c) \quad (3)$$

We construct binary codes from $\mathbb{Z}_4$-linear codes using the Gray map $\phi : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n}$ given by

$$\phi(c) = (\beta(c), \gamma(c)) \ , \ c \in \mathbb{Z}_4^n.$$

LEMME 1. *The Gray map $\phi : (\mathbb{Z}_4^n, d_L) \to (\mathbb{F}_2^n, d_H)$ is an isometry of metric spaces, that is, ϕ is a bijection and $d_H(\phi(x), \phi(y)) = d_L(x, y)$ for all $x, y \in \mathbb{Z}_4^n$.*

If u and v are in $\mathbb{Z}_4^n$, then

$$\phi(u) + \phi(v) = \phi(u + v + 2(u * v))$$

Therefore if u and v are in $\mathbb{Z}_4^n$, then

$$\phi(u + v) = \phi(u) + \phi(v) + \phi(2\alpha(u) * \alpha(v))$$

where $u * v$ is the componentwise product of the two vectors u and v in $\mathbb{Z}_4^n$.
Knowing that all the digital files are binary, we simply use the inverse gray map for working on the support quaternary.

2.5 Preparata Codes

The binary Preparata codes are nonlinear codes that are distance invariant of length 2^{m+1} and minimal distance 6. It is known

that the Preparata code contains more codewords than any linear code with the same minimal distance [14].
We refer the reader to [15] for information concerning Galois rings and their use in the construction of codes over $\mathbb{Z}_4$.
Let $\mathcal{R}$ be a Galois ring of characteristic 4 with 4^m elements. The multiplicative group of units in $\mathcal{R}$ contains a unique cyclic subgroup of order (2^m-1). Let ξ be a generator of this subgroup and let $\mathcal{T} = \{0, 1, \xi, \cdots, \xi^{2^m-2}\}$. Let $\mu : \mathbb{Z}_4 \to \mathbb{F}_2$ denote the modulo 2 reduction map.
Our Preparata code is thus defined as $P = \phi(\mathcal{P})$, where $\mathcal{P}$ is the quaternary codes with parity-check matrix given by:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{2^m-2} \end{bmatrix}$$

where the entries in the second row are to be replaced by the corresponding m-tuples $(b_{0j}, b_{1j}, \cdots, b_{m-1,j})^T$. Then H is a matrix of $m+1$ rows and 2^m columns over $\mathbb{Z}_4$.
Then for odd $m \geq 3$ the binary image $P = \phi(\mathcal{P})$ of P under the Gray map is a nonlinear code of length $N = 2^{m+1}$, with 2^{N-2m-2} codewords and minimal distance 6.

3. THE PROPOSED STEGANOGRAPHIC SCHEME

Now taking a non-linear Preparata codes as example, it is shown that the performance of binary steganographic method can be improved by applying a non-linear codes on our information hiding method.
First a complete decoding algorithm for the $\mathbb{Z}_4$-linear Preparata code of length 2^m is presented.

3.1 Decoding the Quaternary Preparata Code in the $\mathbb{Z}_4$ Domain

There is a very simple decoding algorithm for the Preparata code $\mathcal{P}$, obtained by working in the $\mathbb{Z}_4$ domain. This is an optimal syndrome decoder: it corrects all error patterns of Lee weight at most 2, detects all errors of Lee weight 3, and detects some errors of Lee weight 4. We use the parity check matrix H given in (section 2.5), and assume m is odd and ≥ 3.
Let $v = (v_0, v_1, \cdots, v_{n-1}) \in \mathbb{Z}_4^n$ be the received vector. The syndrome Hv^T has two components, which we write as

$$t = \sum_{j=1}^{n-1} v_j + v_0,$$

$$A + 2B = \sum_{j=1}^{n-1} v_j \xi^j$$

where A, B in $\mathcal{T}$.
It follows that the covering radius of P is at most 4 ([16], Theorem 21 of ch. 6), i.e., the Lee distance $d_L(v, \mathcal{P})$ from a vector $v \in \mathbb{Z}_4^n$ to $\mathcal{P}$ satisfies $d_L(v, \mathcal{P}) \leq 4$. Note that $t = \pm 1$ if and only if $d_L(v, \mathcal{P}) = 1$ or 3.
Single errors of Lee weight 1 or 2: If $t = 1$ and $B = 0$, or if $t = -1$ and $A = B$, we decide that there is a single error of Lee weight 1 in column $(1, A)$. If $t = 1$ and $B \neq 0$, or if $t = -1$ and $A \neq B$, then $d_L(v, \mathcal{P}) = 3$. If $t = 2$ and $A = 0$, we decide that there is a single error of Lee weight 2 in column $(1, B)^T$.
Double errors of Lee weight 2: We begin by supposing that $t = 0$ and

$$A + 2B = X - Y$$

where X, Y in $\mathcal{T}$ and $X \neq Y$. Note that $A \neq 0$ since $X - Y$ is invertible. We have

$$A = X + Y + 2X^{2^{m-1}} Y^{2^{m-1}},$$

$$B \equiv Y + X^{2^{m-1}} Y^{2^{m-1}} (mod\ 2).$$

Let x, y, a, b, respectively, be the images of X, Y, A, B in $GF(2^m)$ after reduction mod 2 using the map μ. Then

$$a = x + y,\ b = y + x^{2^{m-1}} y^{2^{m-1}},$$

which we rewrite as

$$a = x + y,\ (b + y)^2 = xy.$$

The unique solution to these equations is $y = b^2/a$, $x = a + b^2/a$. Note that when $b = 0$ or $b = a$, the double error involves the first column of H. Next we suppose that $t = 2$ and that

$$A + 2B = X + Y$$

where $X, Y \in \mathcal{T}$, $X \neq Y$, $A \neq 0$. Proceeding as above we find

$$a = x + y,\ b^2 = xy$$

and so x and y are distinct roots of the equation

$$u^2 + au + b^2 = 0.$$

A necessary and sufficient condition for this equation to have distinct roots is that

$$tr(b^2/a^2) = tr(b/a) = 0$$

Finally we suppose that $t = 2$ and

$$A + 2B = -X - Y$$

where $X, Y \in \mathcal{T}$, $X \neq Y$, $A \neq 0$. We now find that

$$a = x + y,\ (b + a)^2 = xy,$$

and so x and y are distinct roots of the equation

$$u^2 + au + (a^2 + b^2) = 0.$$

A necessary and sufficient condition for this equation to have distinct roots is that

$$tr(\frac{a^2 + b^2}{a^2}) = tr(1 + \frac{b}{a}) = 1 + tr(\frac{b}{a}) = 0.$$

3.2 Embedding Process

Our proposed data hiding method is based on Preparata codes $P = \phi(\mathcal{P})$ of length 2^{m+1}, where m is odd and ≥ 3.
The embedding process consists of the following steps:

Algorithm 1 The Proposed Embedding Process

Inputs Let $x = (x_1, \cdots, x_{2^{m+1}})$ in $\mathbb{F}_2^{2^{m+1}}$ be a block of cover data,
$M = (M_1, \cdots, M_{2^{m+2}})$ in $\mathbb{F}_2^{2^{m+2}}$ the message to hide.

Outputs $y = (y_1, \cdots, y_{2^{m+1}})$ in $\mathbb{F}_2^{2^{m+1}}$, stego-data such that: $d_H(x, y) \leq \rho$.

(1) We compute $a = \phi^{-1}(x)$ and $\mathcal{M} = \phi^{-1}(M)$
(2) Compute the syndrome: $S = \mathcal{M} - aH^T$ over $\mathbb{Z}_4$
(3) If $S = 0$, then $e = 0$
else we look for an e such that $eH^T = S$ and $\omega_L(e) \leq \rho$ by using the decoding algorithm (in section 3.1) ;
(4) Put: $b = (a + e)\ mod\ 4$
(5) [`Embedding modifications`] y is the stego object $y = Emb(M, x) = \phi(b) = x + \phi(e) + \phi(2\alpha(a) * \alpha(e))$
(6) if we are at the end of the cover object, Stop; otherwise, go to 1.

In fact, this embedding process works because :

$$d_H(x, y) = d_H(\phi(a), \phi(b)) = d_L(a, b) = \omega_L(a-b) = \omega_L(e) \leq \rho$$

3.3 Extracting Process

The message embedded is retrieved from the stego-data by applying the proposed extracting function given as follows:

$$M = Ext(y) = \phi(\varphi(y).H^T)$$

M is the secret information which the receiver extract from the cover.

In fact:

$$\begin{aligned}\phi(\varphi(y).H^T) &= \phi(b.H^T) = \phi((a+e).H^T) \\ &= \phi(a.H^T + e.H^T) = \phi(a.H^T + \mathcal{M} - a.H^T) \\ &= \phi(\mathcal{M}) = \phi(\varphi(M)) = M\end{aligned}$$

3.4 Evaluation of image quality

For comparing stego-image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio[17].

3.4.1 Mean-Squared Error. The mean-squared error (MSE) between two images $I_1(i,j)$ and $I_2(i,j)$ is

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(I_1(i,j) - I_2(i,j))^2}{m \times n}$$

m and n are the number of rows and columns in the input images, respectively.

3.4.2 Peak Signal-to-Noise Ratio. Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range:

$$PSNR = 10log_{10}\left(\frac{I_{max}^2}{MSE}\right)$$

where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray-scale images, PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between image comparisons of PSNR are meaningless. Generally speaking, if the value of PSNR is more than 30dB, then people have difficulty to notice the difference between the cover image and the stego image.

3.4.3 Histogram. The histogram is a function that counts the number of observations that fall into each of the disjoint categories (known as bins). The height of the bins represents the number of values that fall within each range. An image histogram is a chart that shows the distribution of intensities in an indexed or intensity image.

4. EXPERIMENTAL RESULTS

For concreteness, we assume that the cover object used for communication is a gray-scale digital image whose pixels are integers between 0 and 255, then we assign 8 bits to each pixel value. Our steganographic scheme features two essential components. First, is the selection of places within the cover that might be modified and that used to hide the secret message. The second component is the steganographic protocol.
The best widely known steganography algorithm to embed secret information in Spatial and Transform domain of images is based on modifying the least significant bit layer of images, hence known as the LSB technique. This technique makes use of the fact that the least significant bits in an image could be thought of random noise and changes to them would not have any effect on the image.
For example for $m = 3$, let $\mathcal{P}_3$ be a $\mathbb{Z}_4$-linear Preparata code of length 2^3 and (correcting capacity 2), and witch has the parity-check matrix described below:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 1 \end{bmatrix}$$

By applying the non-linear Preparata code $P_3 = \phi(\mathcal{P}_3)$, we can hide 8 bits in a sequence of 16 bits by changing at most 4 bits. Thus, for our method we embed the message $(M_1, \cdots, M_8)$ in the LSBs 2^4 pixel gray values $(p_1, \cdots, p_{16})$ by at most 4 changes in the following manner

$$(M_1, \cdots, M_8) = (x_1, \cdots, x_{16}).H^T$$

where x_i denotes the LSB of p_i.

4.1 Design Details

The proposed scheme are implemented to visualize the data-hiding effect. In the following we describe the steps of our embedding algorithm implemented under Matlab:

(1) Read the host gray-scaling image A, which is to be modified and to embed data.
(2) The host image is partitioned into groups of 16 pixels.
(3) The size of the image and the number of bits to be embedded in each group of 16 pixels together determine the capacity of embedding.
(4) If the message size fits to the estimated capacity, the embedding proceeds (go to step 5), otherwise an error message showing the maximal possible length is displayed.
(5) The text message to be embedded is divided into segments of 8 bits that are embedded into a groups of 16 pixels along the embedding process.
(6) For each group of 16 pixels, do the following:
—Extract the cover-data $x = (x_1, \cdots, x_{16})$ of 16 bits from the group by concatenation the LSB of each pixel value;
—Hide the secret message $M = (M_1, \cdots, M_8)$ of 8 bits into the cover-data using the proposed method.
(7) Store the resulting image as Stego Image (S).

In this present implementation Lena grayscale image of 512×512 pixels and Baboon grayscale image of 298×298 pixels, has been taken as cover images as shown in Figures 1(a) and 2(a). For each image, we applied our method and we present a comparative study in Figures 1 and 2 of the proposed method with the syndrome coding based on the extended Hamming codes [16]and [18] with the same length.

4.2 Embedding Capacity of the proposed scheme

In the proposed scheme the bit numbers of the secret messages that carried in sequence of length N bits by using the $\mathbb{Z}_4$-linearity of Preparata codes is up to

$$log_2\left[\binom{N}{0} + \binom{N}{1} + \cdots + \binom{N}{4}\right]$$

In our example, using extended Hamming code of the same length $2^{m+1} = 16$ to carry secret messages in 512×512 pixels of Lena grayscale image, its rate of the embedding capacity is

$$\frac{log_2\left[\binom{16}{0} + \binom{16}{1} + \binom{16}{2}\right]}{16} = \frac{7.0980}{16} = 0.4436$$

The rate of the embedding capacity using the proposed method with $m = 3$ is

$$\frac{log_2\left[\binom{16}{0} + \cdots + \binom{16}{4}\right]}{16} = \frac{11.2975}{16} = 0.7061$$

(a) original host image

(b) After embedding 6920 bytes by the proposed scheme (PSNR=$44,55$)

(c) After embedding 3460 bytes by the Hamming method (PSNR=$44,55$)

Fig. 1: Embedding effect on Lena image

Therefore, about $131K$ bits of secret messages can be embedded into the 512×512 image applying the proposed method compared to $81K$ bits applying the syndrome coding based on the extended Hamming code.

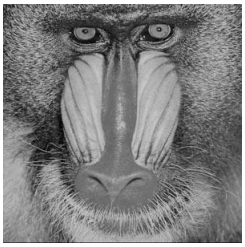
The proposed scheme has the following features:

—Applying the proposed method much amount of data could be embedded in the image. Therefore, a part of the image remains unused resulting in a distortion less image.

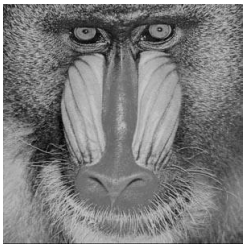
—The amount of data embedded using the proposed scheme leads indeed to a good results compared to the scheme based on extended Hamming code for embedding the secret data into a cover image, see Table 1.

—The effectiveness of the embedding process has been studied by calculating PSNR for the two digital images using the proposed method and the syndrome coding based on extended Hamming code as given in Table 2.

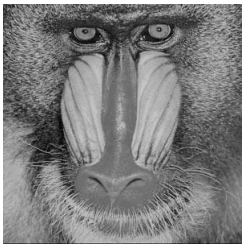
By comparing the histograms (See Figures 3, 4, 5 and 6) of the Lena image before and after the embedding, higher security performance was inferred applying our method. This improves the imperceptibility and enhances the embedding capacity.



(a) original host image



(b) After embedding 3460 bytes by the proposed scheme (PSNR=$58,79$)



(c) After embedding 2957 bytes by the Hamming method (PSNR=$58,79$)

Fig. 2: Embedding effect on Baboon image

Host Image	Amount of embedded data applying (in bytes)	
	The proposed scheme	Extended Hamming code
Lena	16.384	10.240
Baboon	5.550	3.468

Table 1. : Comparaison of amount of embedded data between the proposed method and the Extended Hamming syndrome coding

Host image	PSNR (dB)	
	The proposed scheme	Extended Hamming code
Lena	44,5580	44,5590
Baboon	58,7865	58,7048

Table 2. : Comparaison on PSNR values between the proposed method and the Extended Hamming syndrome coding method after embedding 3.460 bytes

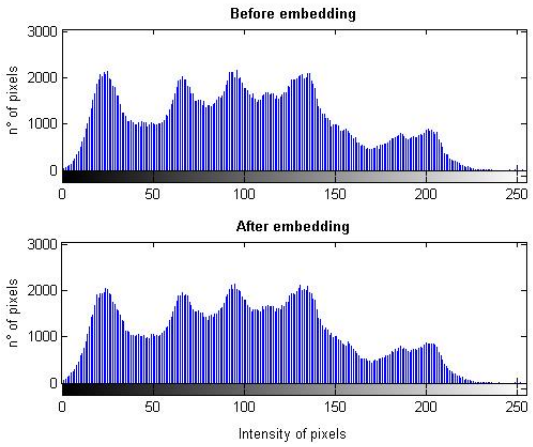


Fig. 3: Histogram of Lena for Our proposed method

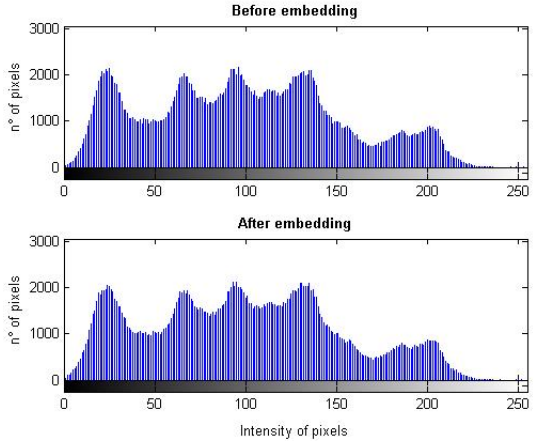


Fig. 4: Histogram of Lena for Extended Hamming method

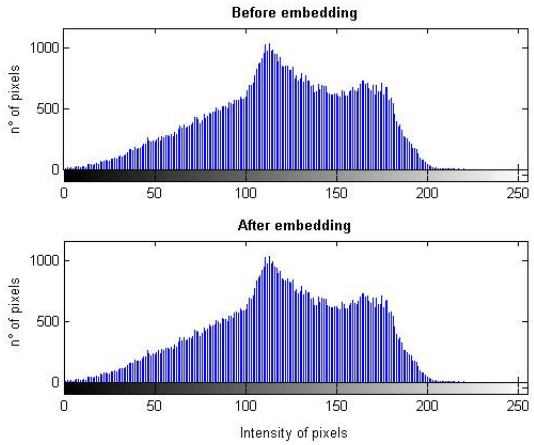


Fig. 5: Histogram of Baboon for Our proposed method

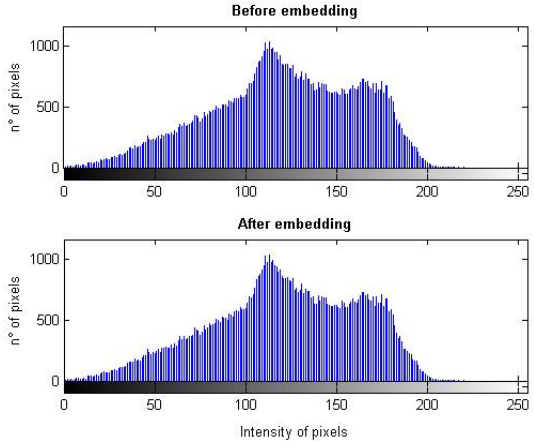


Fig. 6: Histogram of Baboon for Extended Hamming method

5. CONCLUSION

In this paper, we have presented a novel and adaptive method to embed the secret data in the cover image with a good imperceptibility and a high embedding capacity. The receiver does not need the original image to extract the information. Our testing results have shown that the proposed method based on $\mathbb{Z}_4$-linearity of Preparata codes leads indeed to good results compared to the syndrome coding method based on the Extended Hamming codes, and can maintain a good image quality which is seen in the PSNR value.
This paper has presented a novel steganography scheme capable of concealing a large amount of data in a binary image when compared to the Extended Hamming syndrome coding method.

6. REFERENCES

[1] H.J. Highland, Data encryption: a non-mathematical approach, Comput. Secur. 16 (1997) 369386.

[2] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding: a survey, Proc. IEEE Spec. Issue Prot. Multimedia Content 87 (7) (1999) 10621078.

[3] H. Wang, S. Wang, Cyber warfare: steganography vs. steganalysis, Commun. ACM 47 (10) (2004) 7682.

[4] D.W. Bender, N.M. Gruhl, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (1996) 313316.

[5] C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognit. 37 (3) (2004) 469474.

[6] R. Crandall, "Some notes on steganography". Posted on steganography mailing list, 1998, http://os.inf.tu-dresden.de/ westfeld/crandall.pdf.

[7] J. Bierbauer and J. Fridrich, "Constructing good covering codes for applications in steganography", in Transactions on Data Hiding and Multimedia Security III, Lecture Notes in Computer Science, Volume 4920, Pages 1-22, 2008.

[8] M. van Dijk and F. Willems, "Embedding information in grayscale images", in Proc. 22nd Symp. Information and Communication Theory Benelux, Enschede, The Netherlands, May 15-16, 2001, pp.147-154.

[9] F. Galand and G. KAbatiansky, "Information hiding by coverings", in Proc. ITW, Paris, France, 2003, pp. 151-154.

[10] A. Westfeld, : "$F5$: A steganographic algorithm: High capacity despite better steganalysis". In: Moskowitz, I.S. (ed) IH 2001. LNCS, vol. 2137, pp. 289-302. Springer, Heidelberg (2001).

[11] D. Schönfeld and A. Winkler : "Embedding with syndrome coding based on BCH codes:," in *Proceedings of the 8th workshop on Multimedia and security*, pp. 214–223, 2006.

[12] J. Bierbrauer, "On Crandalls Problem". 1998 [Online]. Available: http://www.ws.binghamton.edu/fridrich/covcodes.pdf, Personal Communication.

[13] W. Stalling, "Cryptography and Network Security". Englewood Cliffs, NJ: Prentice-Hall, 1999.

[14] R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A Sloane, and P. Sol, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," IEEE Trans. Inform. Theory, vol. 40, pp. 301319, Mar. 1994.

[15] B. R. MacDonald, Finite Rings with Identity. New York Marcel Dekker 1974.

[16] F. J. MacWilliams and N. I. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.

[17] Moerland, T., "Steganography and Steganalysis", Leiden institute of Advanced Computing Science, Silman, J., Steganography and Steganalysis: An Overview, SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18 : 01, 1999.

[18] J. Fridrich and D. Soukal, : "Matrix embedding for large payloads," *IEEE Trans. Inf. Security Forensics*, vol. 1, no. 3, pp. 390–394, Sept 2006.