Performances of Polar Codes in Steganographic Embedding Impact Minimization

Birahime Diouf, Idy Diop, Sidi Mohamed Farssi

Department of Computer Science, Polytechnic Institute (ESP) / Cheikh Anta Diop University (UCAD), Dakar, Senegal

dioufbira11@yahoo.fr, idydiop@yahoo.fr, farsism@yahoo.com

Abstract—Syndrome coding is used in practice by many authors to define steganographic schemes that minimize embedding impact. Polar Codes, recently introduced, are the first capacity-achieving codes with low complexity of encoding and decoding. In this paper we propose a new practical polar coding methodology for constructing steganographic scheme. We use syndrome coding with binary embedding operation. The approach exploits the form of the syndrome, calculated from cover and secret message. A connection between the syndrome decimal value and the embedding changes position is established and enables defining a new steganographic algorithm. The wet paper codes can also be implemented using this method. Experimental results prove that the scheme minimizes the embedding impact with a reduced time complexity compared to the first Polar Coding Steganography (PCS). The bit-reversal permutation matrix used in polar coding is also employed in practice to uniformly scatter the changes over the whole image.

Keywords—Embedding impact, matrix embedding, polar code, steganography, wet paper codes.

I. INTRODUCTION

The steganography is an information hiding technique that enables to conceal a message in a cover medium in such a way that it existence is kept secret [1]. The cover medium can be digital media such as an image (used in this paper), a sound or a video. The steganalysis aims to detect the existence of secret message. The sender, known as steganographer [2], should embed her covert communication or payload in a cover medium in such a way that only the receiver is aware of the existence of secret communication. The receiver can extract the messages without being aware of the sender choices. Steganography have both good and evil uses.

The embedding must be done by making the cover medium changes less noticeable as possible. In spatial domain, the bits of secret message can be inserted at the LSBs (Least Significant Bits) of the cover image pixels. To improve this so called LSB technique, several propositions exist. The most evident is (a): to make less changes as possible and (b): so that they were less detectable. To answer the first problem of minimizing the number of changes (a), Crandall introduced and conceptually described a steganographic technique [3]. A connection between codes and the problem of minimizing the number of changed pixels (the constant profile) is established by Bierbrauer [4]. The first implementation of this technique was created with the F5 algorithm of Westfield [5] in which the Hamming codes were used. Afterwards, several schemes have implemented this technique in steganography using Golay [6], BCH (Bose-Chaudhuri- Hocquenghem) [7], [8], LDGMs (Low Density Generator Matrices) [9] in combination with the ZZW (Zhang-Zhang-Wang) construction [10], STC ( Syndrome Trellis Codes) [11], [12] and LDPC (Low Density Parity Check) [13] codes. The second problem (b) can be solved using wet paper codes [14]. After having introduced polar codes in steganography PCS (Polar Coding Steganography) [15], we propose in this paper a new practical method for minimizing embedding impact with a reduced algorithmic time complexity. It exploits the relation between syndrome decimal value and embedding changes position. The originality of this work lies in defining an algorithm which gives stego medium in a single step compared to PCS [15] and without using lookup tables [16]. Moreover, this new methodology is applied on images in spatial domain. The images are beforehand randomly permuted to scatter the changes over isolated pixels.

This paper is organized as follows. Section II gives a brief review of basic concepts in steganography and polar coding. In Section III, we present PCS scheme. New steganographic scheme is studied in Section IV. Section V provides a time complexity comparison between PCS scheme [15] and the proposed new algorithm [17]. This section shows also the practical results of the permutation of images. Section VI concludes the paper.

II. STEGANOGRAPHY AND POLAR CODES BASIC CONCEPTS

We will denote by \( x = (x_1, \ldots, x_n) \in \mathcal{X} = \{0,1\}^n \) the LSBs of the cover 8-bits grayscale image and \( x_i \) its \( i \)-th LSB in in spatial domain. The secret message \( m = (m_1, \ldots, m_n) \in \mathcal{M} = \{0,1\}^n \) is embedded by slightly modifying the cover image. This create the LSB-stego-image.
y = (y₁, ..., yₙ) ∈ ℜ = I₁ × ... × Iₙ, where Iᵢ ⊂ ℜ such that xᵢ ⊂ Iᵢ. We will use the binary LSB replacement method where Iᵢ = {xᵢ, xᵢ⁻¹} (cardinality |Iᵢ| = 2, for all i), where xᵢ is xᵢ after flipping its value. We denote by e the embedding change vector (y = x + e) and H ∈ {0,1}ⁿ×m is a parity check matrix of the code.

A. Steganography and Basic Concepts

Matrix embedding is introduced in steganography by Crandall [3] to minimize the number of embedding changes. It is based on syndrome decoding of error correcting codes. Subsequently, several codes are used to implement this technique in steganography.

1) Distortion function:

The embedding impact produced by cancelling the secret message m in the cover vector x will be measured using a distortion function D. In this paper, we limit ourselves to an additive distortion [12]

\[ D(x, y) = \sum_{i=1}^{n} \rho_i(x, y_i) , \]

where \( \rho_i(x, y_i) \) is the cost of replacing the cover pixel \( x_i \) with stego pixel \( y_i \). Note that \( \rho_i \) may arbitrarily depend on the entire cover image \( x \). The independency of the value of \( \rho_i(x, y) \) to changes made at other pixels implies that the embedding changes do not interact. In others words, the change of a pixel has no effect on the other pixels. In the case of binary embedding operation, the distortion can be written as [11]

\[ D(x, y) = \sum_{i=1}^{n} |x_i - y_i| \]  \hspace{1cm} (3)

2) Minimizing embedding impact:

In this paper we use the PLS (Payload-Limited Sender) that that is to embed a fixed average payload while minimizing the average distortion opposed to DLS (Distortion-Limited Sender) that maximize the average payload while introducing a fixed average distortion [12]. The PLS is more commonly used in steganography when compared to the DLS. For a PLS, the sender tries to embed her secret message \( m \) so that the total distortion \( D \) is minimized; that make the resulting stego-system less detectable (more secure). This problem has been approached using variants of syndrome coding [5]–[13]. The sender and the receiver, respectively, implement the embedding and extraction functions \( \text{Emb}: X \times M \rightarrow \mathcal{Y} \) and \( \text{Ext}: \mathcal{Y} \rightarrow M \) satisfying

\[ \text{Ext}(\text{Emb}(x, m)) = m \hspace{0.5cm} \forall x \in X, \forall m \in M, \]  \hspace{1cm} (4)

The embedding is seen as being universal because the distortion function \( D \) is unknown at the receiver. For a binary linear code \( \mathcal{C} \) of length \( n \) and dimension \( n - m \)

\[ \text{Emb}(x, m) = \arg \min_{x \in \mathcal{C}(m)} D(x, y) \]

\[ \text{Ext}(y) = yH^T = m \]  \hspace{1cm} (5)

where \( \mathcal{C}(m) = \{ z \in \{0,1\}^n \mid zH^T = m \} \) is the coset corresponding to syndrome \( m \) and all operations are in binary arithmetic. The extraction function is equivalent to

\[ \text{Ext}(y) = yH^T = m \iff \text{Ext}(e) = eH^T = m - xH^T. \]  \hspace{1cm} (6)

Then, in constant profile, searching the stego vector \( y \) amounts to search the change vector \( e \) of minimal weight in the coset \( \mathcal{C}(m - xH^T) \). Syndrome coding is capacity achieving for the PLS problem if random linear codes are used. Unfortunately, random linear codes are not practical due to the exponential complexity of the optimal binary coset quantizer (4), which is the most challenging part of the problem.

3) Wet Paper Codes:

The wet paper channel is based on pixels selection technique which consists in choosing pixels whose change is less perceptible by human visual system and having less statistical effects on the cover image. In the case where all pixels are assigned \( \rho_i = 1 \) (the so called constant profile), minimizing the distortion \( D \) is reduced to minimize the number of embedding changes. However, in practice some pixels of the cover image can be more sensitive to change than others. The first called wet pixels (with \( \rho_i = \infty \)); we must force the embedding algorithm to keep such pixels unchanged. The second called dry pixels (with \( \rho_i = 1 \)) can be changed. In this case we say that we have a wet paper channel [15]. The syndrome coding is also applied to this type of channel using wet paper codes [11], [12] and [15]. The polar code design for wet paper channel with a given relative wetness \( \tau = [i : \rho_i = \infty]/n \), with \( |X| \) denotes the cardinality of the set \( X \), is described in Section IV-B.

B. Polar Codes

Based on a new paradigm of coding, polar codes are defined as the first codes that achieve the channel capacity, limit established by Shannon. A polar code of length \( n = 2^k \) and dimension \( k \) will be denoted by \( PC(n,k) \). W is a B-DMC (Binary-input Discrete Memoryless Channel). The symmetric capacity [18] of \( W \) is denoted by \( I(W) \) and the reliability parameter is \( Z(W) \). Let \( \Lambda \) and its \( \Lambda' \) respectively denote information and frozen bits sets. The construction of polar codes is based on channel polarization. It consists in synthesizing of \( n \) independent copies of a given B-DMC \( W \) to create \( n \) others channels \( \{W^{(i)}_n \}_{i=1}^{n} \) . It is made up two steps: channel combining and channel splitting [18] with we summarize as follows:

\[ \begin{align*}
(W, W, \ldots, W) &\longrightarrow W_n \longrightarrow \{W^{(i)}_n \}_{i=1}^{n} .
\end{align*} \]  \hspace{1cm} (7)

The channel combining combines \( n \) copies of a given B-DMC \( W \) in a vector channel \( W_n \). It is done recursively by
combining two copies of $W_{n^2}$. During channel splitting we subdivide $W_n$ into $n$ channels $W_{n^i}^{(i)}$, $1 \leq i \leq n$. Channel polarization can be seen as a recursive channel transformation process which can be represented as follows [15], [17]:

$$\left( W_n^{(i)}, W_n^{(i)} \right) \xrightarrow{\text{we construct}} \left( W_{2n^{2-i}}^{(2i-1)}, W_{2n^{2-i}}^{(2i)} \right). \quad (8)$$

The polar coding is done using the following relationships:

$$x_i^* = u_i^* G_u,$$
$$G_n = B_n \odot G_{2}^{\otimes p} = B_n \begin{bmatrix} G_{n/2} & 0 \\ 0 & G_{n/2} \end{bmatrix}, \quad (9)$$

with $B_n$ is a bit-reversal permutation matrix, $G_n$ is a generator matrix, $u_i = (u_1, \ldots, u_i)$, with $1 \leq i \leq n$ and $G_1 = [1]$ and $G_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$. The Kronecker product between matrix $A = [A_j]$, $1 \leq i \leq n$ and $1 \leq j \leq m$ and $B = [B_q]$, $1 \leq i \leq q$ and $1 \leq j \leq r$ is defined by

$$A \otimes B = \begin{bmatrix} A_1 B & \cdots & A_n B \\ \vdots & \ddots & \vdots \\ A_{m1} B & \cdots & A_{m1} B \end{bmatrix}, \quad (10)$$

which is a $mn \times nr$ matrix. The Kronecker power is defined by $A^{\otimes p} = A \otimes A^{(p-1)}$, for all $p \geq 1$, with $A^{\otimes 0} = [1]$.

For polar code PC$(8,4)$, we have:

$$G_2^{\otimes p} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad G_n = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \quad (11)$$

The information word $u_i^*$ is transformed in a code word $x_i^*$. Each bit $x_i$ of $x_i^*$ borrows a copy of $W$ and the gives the bit $y_i$ of the received word $y_i^*$ as shown in Fig. 1.

In polar coding if $u_i^*$ has a uniform distribution then $W_n^{(i)}$ is the channel really seen by $u_i$ (Fig. 2).

The most reliable $W_n^{(i)}$ are used to carry the information bits and the least reliable ones contain the frozen bits $Z(W_n^{(i)}) \leq Z(W_n^{(j)})$, for any $i \in A$ and $j \in A^c$.

Polar codes are several applications in information theory and have been recently introduced in steganography [15].

III. FIRST PCS (POLAR CODING STEGANOGRAPHY) METHOD

Denote by $S_{\text{PCS}}(n,m=n-k)$ the steganography based on polar code $PC(n,k)$.

A. Construction of Polar Codes in Steganography

The construction of polar codes for the purposes of steganography can be summed up in three steps [15] as shown in Fig. 3.

We calculate the reliability parameters as follows [15]:

$$Z(W^{(j)}) = 2Z(W^{(j+1)/2}) - Z(W^{(j+1)/2})^2 \quad \text{if} \ j \text{ is even},$$
$$Z(W^{(j)}) = Z(W^{(j+1)/2})^2 \quad \text{if} \ j \text{ is odd}. \quad (12)$$

The initial value is calculated with

$$Z(W^{(1)}) = Z(W) = 2\sqrt{W(0)W(1)} = 2\sqrt{p_c(1-p_c)} \quad (13)$$

where $p_c$ is the error probability of the channel $W$, $p_c = W(0\mid 1) = W(1\mid 0)$ and $1 - p_c = W(0\mid 0) = W(1\mid 1)$.

To obtain $A$ and $A^c$ we select channels with the parameters of the lowest reliabilities for data bits. The indices of these channels form the information bits $A$. Its cardinality is equal to the dimension $k$ of the considered polar code. The $n-k$ other channels carry redundancy bits. Their indices constitute $A^c$.

To determinate a parity check matrix of a polar code, we use the lemma given by Goela et al. [19, Lemma 1] which states that if the frozen bits are equal to 0 then the transpose of the parity check matrix $H$ of the polar code is given by the columns of the generator matrix $G_n$ whose indices are in $A^c$.

As examples, we use a polar code $PC(4,1)$ for the steganography $S_{\text{PCS}}(4,3)$ and $PC(8,4)$ for $S_{\text{PCS}}(8,4)$.
For $PC(4,1)$, $A = \{4\}$, $A' = \{1, 2, 3\}$ and a parity check matrix is:

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

and its transpose $H^T = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 \\
\end{bmatrix}$ \hspace{1cm} (14)

If we use $PC(8,4)$ then $A = \{4, 6, 7, 8\}$, $A' = \{1, 2, 3, 5\}$ and from (11) we have:

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

and $H^T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\end{bmatrix}$ \hspace{1cm} (15)

The steganographic scheme is made up two steps.

B. First Step

By making the most of the particular form of $H$ and its transpose $H^T$, we can transform the equations of the relation $yH^T = m$ in a system allowing calculating the coefficients of the stego vector $y$ (see [15]):

$$y = y_n H^T_{(j=1),j} + \cdots + y_n H^T_{(j=4),j} + m_j ; j = n-k \text{ down to } 1 \hspace{1cm} (16)$$

with $i$ the position of first 1 on column $j$ of $H^T$. For each $j$, we calculate the corresponding $y_i$. The vector $y$ must be initialized to the cover vector $x$ before the calculations. With (16), we obtain a stego vector $y_p$ verifying $yH^T = m$ but it is not the closest to the cover vector $x$.

C. Optimization of the First Solution

The objective of this step is to find the stego vector $y$ closest to $x$ by using the polar code $PC(n,k)$. Let $e_p$ be the embedding change vector corresponding to the stego vector $y_p$ found with the first step. The distortion (3) can be written:

$$D(e) = \sum_{i=1}^{m} \rho_i e_i$$ \hspace{1cm} (17)

where $|x_i - y_i| = e_i$ and $\rho_i = 1$ for constant profile and $\rho_i = \{1, \infty\}$ for wet paper channels. The insertion and extraction functions become:

$$Emb(x, m) = \text{arg min}_{e \in C(s)} D(e)$$

$$Ext(y) = yH^T = m \iff eH^T = s = m-xH^T$$ \hspace{1cm} (18)

Considering the problem in the following three points [15]:

- we have a first solution $e_p \rightarrow$ initial solution,
- we have to minimize the distortion $D(e) \rightarrow$ minimization problem,
- verifying $eH^T = m - xH^T = s \rightarrow$ constraints,

we have a minimization problem with equalities constraints and initial solution $e_p$. The problem can be formalized as follows:

$$\text{arg min}_{e \in \{0,1\}^n} f(e) = D(e) = <p,e> = p^T e$$ \hspace{1cm} (19)

with $f$ the objective function and $p = \{ \rho_i \}_{1 \leq i \leq n}$ the change cost vector. This is a problem of linear programming written in standard form. It can be solved using the methods simplex or interior points [15].

IV. NEW POLAR CODING STEGANOGRAPHIC ALGORITHM

In [16], we have proposed two approaches for complexity reducing. The first use lookup tables and the second exploits the form of the syndrome but its definition is based on lookup tables. Additionally, only the second approach was implemented in practice. In this section we propose a new version of the second approach which does not need lookup tables, which is implemented in practice and compared to PCS. We will consider constant profile case and wet paper codes.

A. New PCS for Constant Profile

Consider the polar code $PC(4,1)$ for the steganography $S_{PC}(4,3)$. According to (14), the columns $H$, $1 \leq j \leq 4$, of the parity check matrix $H$ satisfy the following equations:

$$H_1 + H_2 = H_3 + H_4 = (01)^T$$
$$H_1 + H_2 = H_3 + H_4 = (01)^T$$
$$H_1 + H_2 = H_3 + H_4 = (01)^T$$

(20)

(21)

(22)

When using polar code $PC(8,4)$ for steganography $S_{PC}(8,4)$, the inequalities verified by the columns $H$, $1 \leq j \leq 8$ of the parity check matrix $H$ (15) are:

$$H_1 + H_2 = H_3 + H_4 = H_5 + H_6 = (0001)^T$$
$$H_1 + H_2 = H_3 + H_4 = H_5 + H_6 = (0001)^T$$
$$H_1 + H_2 = H_3 + H_4 = H_5 + H_6 = (0001)^T$$
$$H_1 + H_2 = H_3 + H_4 = H_5 + H_6 = (0001)^T$$

(23)

(24)

(25)

(26)

First calculate the syndrome $s = m - xH^T$. If it is equal to:

- **Synd. 1**: zero vector then the embedding change vector $e$ is also equal to zero vector;
- **Synd. 2**: one column of $H$ let be $H_j(s = H_j)$, then it has as first element 1 and the embedding change vector $e$ has only one 1 at position $j$. The columns $H_j(1 \leq j \leq n)$ of $H$ represent the binary values of the numbers between $n$ and $2n-1$ (see, for example, (20) and (21)). Thus, on column $j$, we have the binary representation of $n+j-1$. The decimal value $dec(H_j) = n + j - 1$. Hence, $j = dec(s) - n + 1$;
- **Synd. 3**: sum of two columns of $H$ ($H_j$ and $H_k$) then it has a 1 as first coefficient, see (20) and (21). The decimal value varies between 1 and $n-1$. The embedding change vector has two 1; the first at the first position and the second at
position \( j \). The decimal value of the sum of the two columns \( H_1 \) and \( H_2 \) is equal to \((n) + (n+1) \mod 2n = j-1\). Then \( \text{dec}(H_1 + H_2) = j - 1 \). Hence, \( f = \text{dec}(s) + 1 \).

These three cases are also valid for the equivalent\(^1\) systems. According to these observations, there is a relationship between the decimal value of syndrome \( s \) and the position of the \( 1 \) of the embedding change vector \( e \). A necessary condition is \( 2^{n-k} = 2n-2^{p+1} \). Then \( n-k = p+1 \). Hence \( k = n-\log(n) = 2^{p}-1-p \). The validity of these observations concerns the values:

\[
    p \in \{2, 3, 4, 5, 6, 7\} = \mathcal{P}
\]

\[
    n \in \{4, 8, \ldots, 128\} = \mathcal{N}
\]

\[
    k \in \{1, 4, \ldots, 120\} = \mathcal{K}
\]

with \( n = 2^p, k = 2^p - 1 - p \) and \( p \in \mathcal{P} \).

For an arbitrary polar code \( PC(n,k) \) \[^{18}\], the length \( n \) is a power of 2 and the dimension \( k \) is a positive integer in \( \{1, 2, \ldots, n-1\} \). For a polar coding steganographic scheme, the optimality condition \[^{15}\] is \( m = n - k > p = \log_2 n \). The parameters of our polar code in the proposed approach satisfy this optimality condition because we have \( n-k = p+1 > p \).

Consider a given \( PC(N=2^p,K) \) for steganography \( S_{Pr}(N,N,K) \). If \( N \not\in \mathcal{N} \) (i.e. \( p \in \{8, 9, \ldots \} = N \not\in \mathcal{N} \cup \{0, 1\}) \) or \( K \not\in \mathcal{K} \), we can always come down to a validity case. For \( N \in \mathcal{N} \), if \( K \in \mathcal{K} \) then we apply directly the steganographic method with \( S_{Pr}(N,N,K) \) else we normalize \( K \). For \( N \not\in \mathcal{N} \), we normalize \( N \) and then \( K \).

### Normalization of \( N \):

- Subdivide \( N \) in several integers \( n \) so that \( n \in \mathcal{N} \). Since \( N \) and \( n \) are both power of 2 (\( N = 2^p \) and \( n = 2^q \)), with \( N > n \), then \( N \) is divisible by any \( n \in \mathcal{N} \). The ratio \( \frac{N}{n} = \frac{2^p}{2^q} = 2^{p-q} = 2^r \) is a power of 2. Thus, we obtain \( 2^r \) segments of size \( n \in \mathcal{N} \) each.

### Normalization of \( K \):

- We aim to bring \( K \) back to an integer \( k \in \mathcal{K} \). But, since we are interested in the size \( m = n-k \) of the message for steganography rather than \( k \), then we will subdivide \( N-K \) in \( n-k = p+1 \) parts such as \( n = 2^q \in \mathcal{N} \) and \( k = (n-1) - \log(n) \in \mathcal{K} \). Since we know \( n \), we can determine \( k \). \( N-K \) is not always divisible by \( n-k \). Let \( N-K = (n-k)q+r \), with \( 0 \leq r < n-k \). If \( r = 0 \) then we subdivide \( N-K \) in \( q \) segments of size \( n-k \). Otherwise (i.e. \( 0 < r < n-k \)), we have \( q \) segments of size \( n-k \) and another one of size \( r \). In this case, we complete this segment with \( (n-k)-r \) bits to 0 to have a size equal to \( n-k \).

The embedding is done by pair of a cover medium segment and a message segment. The number of cover segments must be equal to or greater than the number of message segments.

The following algorithm (Algorithm 1) calculates a coset leader for a given syndrome \( s \).

---

\(^1\) Equivalent denotes the system obtained for another polar coding steganographic parameter \( n \) different to \( 8 \).

---

### Algorithm 1 Calculation of a syndrome coset leader.

**Inputs:** cover vector \( x \), message \( m \) and parity check matrix \( H \).

**Outputs:** syndrome coset leader \( e \).

1. Initialization:
   2. \( p \leftarrow \text{an element of } \mathcal{P}; n = 2^p; k \leftarrow n-1-p; \)
   3. \( e \leftarrow (0, \ldots, 0); y \leftarrow x; \)
   4. Calculation:
   5. \( \text{If } xH^T \neq m \text { then} \)
   6. \( s \leftarrow m - xH^T; \)
   7. \( \text{calculate decimal value of binary syndrome vector} \)
   8. \( \text{(dec}\leftarrow \text{decimalConversion}(s)) \)
   9. \( \text{if } 1^\text{th} \text{coefficient of syndrome } s \text{ is equal to } 1 \text { then} \)
   10. \( \text{affect the } (\text{dec}+1\text{-th}) \text{ coefficient of } e \text{ to } 1; \)
   11. \( \text{else} \)
   12. \( \text{affect } 1^\text{th} \text{ and } (\text{dec}+1\text{-th}) \text{ coefficients of } e \text{ to } 1; \)
   13. \( \text{end (if)} \)
   14. \( \text{End (If)} \)

The function \( \text{decimalConversion}(s) \) converts a binary vector \( s \) into its decimal value.

For a given parameter \( p \) not in validity domain, we can always come down to valid parameter by subdividing it to one of the valid parameters in \( \mathcal{P} \). Furthermore, we can choose one of the valid parameters \( p \in \mathcal{P} \) and subdivide the cover medium size \( N \) to \( n \in \mathcal{N} \) and the secret message size to \( n-k \) with \( k \in \mathcal{K} \). This implies that we can choose the parameter \( p \), which minimizes well the embedding impact.

### B. Wet Paper Polar Codes

In this section, we explain how polar codes can be used for the wet paper channel. Give first two theorems that make applicable polar codes for wet paper.

**Theorem 1** (Rank of the parity check matrix): The rank of a parity check matrix \( H \) of a polar code of block length \( n \) and dimension \( k \) is

\[
    \text{rank}(H) = n-k \quad (23)
\]

**Proof:** The generator matrix of the polar code \( G_n \) is invertible \[^{18}\] i.e. the columns of \( G_n \) are linearly independents (none of the columns is linear combination of the others). This is equivalent to \( \text{rank}(G_n) = n \). The matrix \( H^T \) is obtained by pruning the \( k \) columns of \( G_n \), whose indices are in the information set \( A \) \[^{19}\]. Then \( G_n \) is the matrix \( H^T \) at which we add \( k \) others columns which none is linear combination of the others columns of \( H^T \). Thus \( \text{rank}(H^T) + k = \text{rank}(G_n) = n \). Since \( \text{rank}(H^T) = \text{rank}(H) \). Then \( \text{rank}(H) + k = n \). Finally \( \text{rank}(H) = n-k \).

Consider still the set of wet elements \( J \). The maximum number of positions that we can lock for the wet paper steganography is \( n - \text{rank}(H) = k \).

**Theorem 2** (Maximum number of locked elements): Let \( S_{Pr}(n,m,n-k) \) denote the polar coding steganography such that \( n \in \mathcal{N} \) and \( k \in \mathcal{K} \). The maximum number \( \ell_{\max} \) for which we are always able to lock any combination of \( \ell_{\max} \) positions is

\[
    \ell_{\max} = \frac{n}{2} - 1 \quad (24)
\]

---

Copyright © 2016 GiRI (Global IT Research Institute)
Proof: Consider, for example, the lock of \( n/2 \) last positions of the cover vector. This amounts to prune the \( n/2 \) last columns of the parity check matrix \( H \) for the matrix product \( yH^T = m \). In this case, the second row of the matrix \( H \) has all its elements equal to 0 and may then, be written as linear combination of the others (see for example (14) and (15)). This means that we can’t always lock \( n/2 \) positions or more. The maximal number of positions that we can always lock, for any combination, is then less than \( n/2 \). It is between 1 and \( n/2-1 \). Let \( \ell \) be the number of locked positions, then \( 1 \leq \ell \leq n/2-1 \). In our steganographic problem, we must look a number of positions such that \( yH^T = m \) has, at least, one solution. Then, the system must have a number of unknowns more than or equal to the number of equations. The number of unknowns after locking is equal to \( n-\ell \) and the number of equations is \( n-k = 1+\log_2(n) = 1+p \). Thus, we must have \( n-\ell \geq n-k \) then \( \ell \leq k \).

The value of \( \ell \) have two constraints \( (\ell \leq n/2-1 \text{ and } \ell \leq k) \). So \( \ell_{\text{max}} = \min(k, \ n/2-1) = \min(n-1-\log_2(n), \ n/2-1) \). Prove that \( \ell_{\text{max}} = \ n/2-1 \). This amounts to demonstrate that \( n/2-1 \leq r \log_2(n) \). That is equivalent to prove that their difference \( r \log_2(n) \geq d \). Let \( f(p) = (p-1)^{2^{-d-1}} \geq 0 \), for \( p \geq 2 \). This mean that \( f \) is monotonic and \( f(2) = 0 \). Then \( f(p) \geq 0 \) for any \( p \geq 2 \). Consequently \( n-\log_2(n) \geq n/2-1 \). Finally, we have \( \ell_{\text{max}} = n/2-1 \).

On the one hand, we can lock \( k \) positions but not any ones. On the other hand, any combination of \( n/2-1 \) positions can be chosen for the locking. Then, to ensure to always succeed the locking, we will not exceed \( \ell_{\text{max}} \).

Let \( J \) be the set of wet elements, then:

- If syndrome \( s \) is in \textbf{Synd. 1} then we do nothing because \( e \) is also a zero vector;
- If \( s \) is in \textbf{Synd. 2} then consider, by quadruplets, the decimal values of the \( n \) syndromes whose embedding change vectors have a single 1. These syndromes correspond to the \( n \) columns of \( H \) and constitute the half of all possible \( 2^n = 2n \). We have \( n/4 \) quadruplets and each consists of four consecutive syndromes:

\[
Q_i = \{n+4i-4; n+4i-3; n+4i-2; n+4i-1\}, \ i = 1, \ldots, \ n/4
\]  

(25)

Searching to know the quadruplet \( Q \) of a given syndrome \( s \), we calculate its index \( i \) by:

\[
i = \left\lfloor (\text{dec}(s)+n+1)/4 \right\rfloor
\]  

(26)

where \( \lfloor \rfloor \) denote the ceil operator and \( \text{dec}(s) \) is the decimal value of the syndrome \( s \).

Proof: According to (25), \( \text{dec}(s) \) varies between \( n+4i-4 \) and \( n+4i-1 \) for quadruplet \( Q_i \). Therefore \( (\text{dec}(s)+n+1)/4 \) is included between \( i-3/4 \) and \( i \). Thus, when applying the round to the upper bound then \( \lfloor (\text{dec}(s)+n+1)/4 \rfloor \) is between \( i-3/4 \equiv i \) and \( i \). This gives (26).

Let \( s, s_1, s_2 \) and \( s_3 \) be the syndromes forming a quadruplet \( Q \) and \( e, e_1, e_2, e_3 \) their corresponding embedding change vectors, \( e_i H^T = s_i \) for \( i = 1, 2, 3 \). In each quadruplet, a syndrome is equal to the sum of the three other; therefore \( s = s_1 + s_2 + s_3 \). Let \( e_0 = e_1 + e_2 + e_3 \), then \( e_i H^T = e_i H_i^T + e_i H_1^T + e_i H_2^T = s_i + s_2 + s_3 = s \). Thus \( e_i \) is in the coset of \( s \). Consequently, to lock the position \( j \), we choose as embedding change vector \( e_i \). Each of the vectors \( e_1, e_2, e_3 \) has only one 1 respectively at different positions \( j, h, t \) and \( t \). Then \( e_i \) has three 1 at positions \( h, l \) and \( l \). If at least one of these three positions is in \( J \), then we search another embedding change vector with 1 at positions not in \( J \). To do so, we choose a pair in the triplet containing one or two elements belonging to \( J \). The chosen pair, let \( (h, l) \), is then replaced by another pair \( (f, g) \) which is not included in \( J \) with the equality of an equivalent system of (21) (see Algorithm 2). The new embedding change vector will have 1 at positions \( f, g \) and \( t \) and 0 at replaced positions \( h \) and \( l \).

- If \( s \) is in \textbf{Synd. 3} (i.e. \( e \) has two 1 at positions \( j \) and \( j \) which at least one is in \( J \)), then we search with (21) or an equivalent, the pair \( (h, l) \) not included in \( J \) using Algorithm 2.

The embedding change vector will have then two 1 at positions \( h \) and \( l \).

For position replacement, the algorithm is as follows:

**Algorithm 2** Replacement of a pair by another not in \( J \).

- **Inputs**: pair to replace \((i, j)\) the set of wet element \( J \).
- **Outputs**: the new pair obtained \((l, t)\).

1. **While** (not found and not end of \( J \))
2. Search a first position \( l \) (from 1 to \( n \)) not in \( J \)
3. Search a second position \( t \) (\( t > l \)) not in \( J \)
4. If \((l, t)\) verifies with \((i, j)\) one of the equalities of (21):
   5. **End (If)**
   6. \( l \leftarrow l; \quad t \leftarrow t; \quad \text{return} \ (l, t) \)
7. **Else If** (not end of \( J \))
   8. Go to line 3.
9. **End (If)**
10. **End (If)**
11. Go to line 2.
12. **End (If)**
13. Repeat until having a good pair \((l, t)\)
14. \( l \leftarrow l; \quad t \leftarrow t; \quad \text{return} \ (l, t) \)
15. **End (While)**

with \( \text{bin}(a) \) is the binary value of the number \( a \).

The new proposed scheme can be summarized as follows:

![Fig. 4. New polar coding steganographic scheme.](image)
The upper part of the scheme deal with the constant profile case with the three possible cases. In the case of wet paper channel we continuous with the lower side by replacing the wet elements indices. After replacement, the new positions are set to 1 and the old reset to 0 in the embedding change vector $e$. After calculating $e$, we can obtain the stego vector by $y = x + e$.

V. EXPERIMENTAL RESULTS

We have represented in Fig. 5 the embedding efficiency $\epsilon = m/D(x,y)$ of the proposed method in wet paper channel according to relative wetness $\tau = ||\{i : \rho_i = \infty\}||/n$. We have looked $n/2$ elements and then $\tau = (n/2-1)/n$.

For relative wetness $\tau$ varying between 0.25 and 0.5, the embedding efficiency increases from 2.4 to 5.9. The increasing is faster than the relative wetness is great. This proves the goodness of the embedding efficiency.

![Fig. 5. Embedding efficiency for wet paper codes.](image)

We have also given the complexity variation of the steganographic scheme based on polar codes [15] and those of the algorithm proposed in this paper. To compare the complexity of algorithm PCS with the new algorithm, we measure the required time resources amount for solving the problem of minimizing the embedding impact (here, research of the embedding change vector). For that, we observe their execution time on a computer. We perform several tests on Dual Core CPU running at 3.46 GHz with 2 GB RAM. We chose a polar code of block length $n \in \mathcal{N}$ and dimension $k \in \mathcal{K}$ because our algorithm is applied to these values (see (22)). For each pair $(n,k) \in (\mathcal{N},\mathcal{K})$, 20 cover vectors and 20 messages are randomly generated. Then, we calculate the execution times average (in seconds) of messages embedding in cover vectors. This calculation is done for the two algorithms.

The obtained results for constant profile and wet paper channel cases are respectively represented by Fig. 5 and Fig. 6. Each curve represents specifically the average execution times of the research algorithm of the embedding change vector corresponding to the syndrome calculated from randomly generated cover vector and message. The execution time curve of PCS algorithm is blue and the red one represents the proposed new algorithm.

![Fig. 6. The execution time of the two schemes for constant profile.](image)

The execution time of the new algorithm is lower than the PCS scheme [15] in constant profile (Fig. 6) as well as in wet paper channel (Fig. 7). The difference between the two curves increases with the size of the cover vector $n$. This allows us to pronounce on complexity reducing. Therefore, the scheme proposed in this paper allows minimizing the embedding impact with a reduced time complexity when compared to first PCS.

![Fig. 7. The execution time of the two schemes for wet paper channel.](image)

We can test the embedding scheme with cover images coming from BOSSbase database version 1.01 (Break Our Stego System) [21] containing 10,000 512×512 8-bit grayscale images of $pgm$ format coming from rescaled and cropped natural images of various sizes of eight different cameras.

To make the message less detectable, we choose to permute the pixels of the cover image before embedding. Because the images have a fixed size of 512×512 pixels and 512 is a power of 2, we can use the bit-reversal permutation matrix $B_{512}$, described in Section II-B, for permutation. This permutation matrix $B_{512}$ can be used to permute the rows and the columns of the cover images before embedding the secret message as shows by Fig. 8. After permutation the obtained image is splitting in $512/n=2^p$ blocs because the bloc length $n=2^p$ of the used polar code is also a power of 2. Further, we can permute the rows and the columns of these $n \times n$ pixels bloc images using bit-reversal permutation matrix $B_n$. Then, we repeat the same process as in Fig. 8 with bloc images $I'_{i,s}$ and $B_r$. 

Copyright © 2016 GiRI (Global IT Research Institute)
Fig. 8. Permutation and splitting images.

Thus the changes will be scattered over isolated pixels of the image making less detectable the secret message and allowing a more secure insertion. After insertion, it is necessary to find the original order of pixels of the cover image. To achieve this, we still use the matrix $B_n$ since it is invertible and equal to its own inverse. Note that permutation technique was used in the pass but it depended on a key derived from a password. The receiver needed the correct secret key to be able to repeat the permutation which had linear time complexity $O(n)$ in [5]. Our permutation technique depends only on the bit-reversal permutation matrix $B_n$ which is already used in the construction of the polar code.

In this manner, we have four images choices to embed the secret message. We can choose the original cover image $I$, or the rows permuted image $I_R$, or the columns permuted image $I_C$, or rows and columns permuted image $I_{RC}$. This secret choice can be shared with the receiver and is unknown to all another person. The image ‘28.pgm’ of BOSSbase is used to illustrate the permutation effects. The original image and the three permuted images are shows in Fig. 9 (top-left the original image, top-right the rows permuted image, bottom-left the columns permuted image and bottom-right the rows and columns image).

As we can see, the black band on the right columns of the original image is also visible on the rows permuted image. In the same, the white pixels on the top remains on the top rows of the columns permuted image. Conversely, for the rows and columns permuted image the pixels are uniformly distributed.

In Fig. 10, white pixels correspond to changes by $+1$ or $-1$ and the black ones correspond to pixels that did not change. For the rows and columns permuted image, the changes are uniformly distributed over the whole image (right) when compared to the image without permutation (left) in which the changes are all at the top of the image. The changes in the stego rows and columns permuted matrix will, of course, more hard to be detected by an attacker.

Fig. 9. Original image and different permuted images.

Fig. 10. Positions of the embedding changes on non-permuted image (left) and rows and columns permuted image (right) when 0.2 bpp (bit per pixel) is embedded in ‘28.pgm’.

VI. CONCLUSION

We proposed, in this paper, new practical steganographic methodology based on polar codes that significantly reduce the complexity of PCS scheme [15] without using lookup tables [16]. This approach exploits the form of the syndrome calculated from the cover medium and the secret message, to determine the embedding change minimizing the distortion function. A relationship between the decimal value of the syndrome and the position of non-zero elements of the embedding change vector is established. This relationship is used to evaluate the changes position on the cover vector. As PCS, this method allows minimizing the embedding impact with a reduced time complexity. The algorithm proposed in this paper provides good performance in terms of embedding efficiency and has a lower time complexity than PCS for both constant profile and wet paper cases as shown by the execution time comparison curves of the two schemes. We have also applied the scheme on images in spatial domain. We have chosen to permute the pixels of images before embedding the private message. The permutation can be done only on the rows or only on the columns or both on the rows and columns of the cover image. This allowed scattering the changes at isolate pixels of the image and made the stego-system more secure.

As part of our future research, we plan to propose an adaptive steganographic scheme based on polar codes using adaptive linear programming decoding of polar codes. We also plan to propose a method of steganalysis.

REFERENCES


