combining two copies of $W_{n/2}$. During channel splitting we subdivide W_n into n channels $W_n^{(i)}$, $1 \le i \le n$. Channel polarization can be seen as a recursive channel transformation process which can be represented as follows [15], [17]:

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

The polar coding is done using the following relationships:

$$x_1^n = u_1^n G_n$$
$$G_n = B_n G_2^{\otimes p} = B_n \begin{bmatrix} G_{n/2} & 0 \\ G_{n/2} & G_{n/2} \end{bmatrix}, \quad (9)$$

with B_n is a bit-reversal permutation matrix, G_n is a generator matrix, $u_1^i = (u_1, \ldots, u_i)$, with $1 \le i \le n$ and $G_1 = [1]$ and $G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. The Kronecker product between matrix $A = [A_{ij}]$, $1 \le i \le n$ and $1 \le j \le m$ and $B = [B_{ij}]$, $1 \le i \le q$ and $1 \le j \le r$ is defined by

$$A \otimes B = \begin{bmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{bmatrix} \quad (10)$$

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

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

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

The information word u_1^n is transformed in a code word x_1^n. Each bit x_i of x_1^n borrows a copy of W and the gives the bit y_i of the received word y_1^n as shown in Fig. 1.

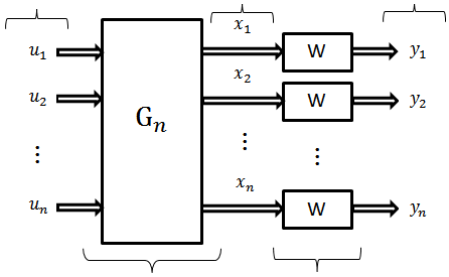


Fig. 1. Polar coding scheme.

In polar coding if u_1^n has a uniform distribution then $W_n^{(i)}$ is the channel really seen by u_i (Fig. 2).

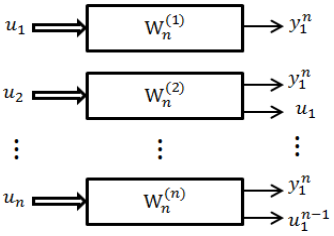


Fig. 2. Equivalent of polar coding scheme.

The most reliable $W_n^{(i)}$ are used to carry the information bits and the least reliable ones contain the frozen bits $Z(W_n^{(i)}) \le Z(W_n^{(j)})$, 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 $\mathcal{S}_{PC}(n,m=n-k)$ 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.

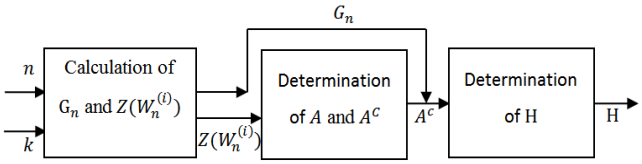


Fig. 3. Construction of polar codes for steganographic purposes.

We calculate the reliability parameters as follows [15]:

$$Z\left(W_n^{(j)}\right) = 2Z\left(W_{n/2}^{((j+1)/2)}\right) - Z\left(W_{n/2}^{((j+1)/2)}\right)^2 \quad \text{if } j \text{ is even}$$
$$Z\left(W_n^{(j)}\right) = Z\left(W_{n/2}^{(j/2)}\right)^2 \quad \text{if } j \text{ is odd} \quad (12)$$

The initial value is calculated with

$$Z\left(W_1^{(1)}\right) = Z(W) = 2\sqrt{W(0|0)W(0|1)} = 2\sqrt{p_e(1-p_e)}, \quad (13)$$

where p_e is the error probability of the channel W, $p_e = W(0|1) = W(1|0)$ and $1 - p_e = W(0|0) = W(1|1)$.

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 $\mathcal{S}_{PC}(4,3)$ and *PC(8,4)* for $\mathcal{S}_{PC}(8,4)$.

For *PC(4,1)*, $A = \{4\}$, $A^c = \{1, 2, 3\}$ and a parity check matrix is:

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

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

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

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]):

$$y_i = y_{i+1}H^T_{(i+1),j} + \cdots + y_n H^T_{nj} + m_j \; ; j = n-k \text{ down to } 1 \quad (16)$$

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:

$$D(e) = \sum_{i=1}^{n} \rho_i e_i \quad (17)$$

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:

$$\begin{aligned} &Emb(x, m) = \arg \min_{e \in C(s)} D(e) \\ &Ext(y) = yH^T = m \Leftrightarrow eH^T = s = m - xH^T \end{aligned} \quad (18)$$

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:

$$\begin{aligned} \underset{e}{\text{argmin}} \quad & f(e) = D(e) = \langle \rho, e \rangle = \rho^T e \\ \text{s.t} \quad & \begin{cases} e \in \{0,1\}^n \text{ binary vector} \\ eH^T = m - xH^T = s \\ e_p \text{ initial solution} \Leftrightarrow e_p H^T = s \end{cases} \end{aligned} \quad (19)$$

with f the objective function and $\rho = \{\rho_i\}_{1 \le i \le n}$ 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 $\mathcal{S}_{PC}(4,3)$. According to (14), the columns $H_{.j}$, $1 \le j \le 4$, of the parity check matrix H satisfy the following equations:

$$\begin{aligned} H_{.1} + H_{.2} &= H_{.3} + H_{.4} = (001)^T \\ H_{.1} + H_{.3} &= H_{.2} + H_{.4} = (010)^T \\ H_{.1} + H_{.4} &= H_{.2} + H_{.3} = (011)^T \end{aligned} \quad (20)$$

When using polar code *PC(8,4)* for steganography $\mathcal{S}_{PC}(8,4)$, the inequalities verified by the columns $H_{.j}$, $1 \le j \le 8$ of the parity check matrix H (15) are:

$$\begin{aligned} &H_{.1} + H_{.2} = H_{.3} + H_{.4} = H_{.5} + H_{.6} = H_{.7} + H_{.8} = (0001)^T \\ &H_{.1} + H_{.3} = H_{.2} + H_{.4} = H_{.5} + H_{.7} = H_{.6} + H_{.8} = (0010)^T \\ &H_{.1} + H_{.4} = H_{.2} + H_{.3} = H_{.5} + H_{.8} = H_{.6} + H_{.7} = (0011)^T \\ &H_{.1} + H_{.5} = H_{.2} + H_{.6} = H_{.3} + H_{.7} = H_{.4} + H_{.8} = (0100)^T \\ &H_{.1} + H_{.6} = H_{.2} + H_{.5} = H_{.3} + H_{.8} = H_{.4} + H_{.7} = (0101)^T \\ &H_{.1} + H_{.7} = H_{.2} + H_{.8} = H_{.3} + H_{.5} = H_{.4} + H_{.6} = (0110)^T \\ &H_{.1} + H_{.8} = H_{.2} + H_{.7} = H_{.3} + H_{.6} = H_{.4} + H_{.5} = (0111)^T \end{aligned} \quad (21)$$

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 $H_{.j}$ ($j = 1{:}n$) 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, $\boldsymbol{j = dec(s) - n + 1}$;
- **Synd. 3**: sum of two columns of H ($H_{.1}$ and $H_{.j}$) then it has a 0 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 $H_{.j}$ is equal to $((n) + (n+j-1)) \bmod 2n = j-1$. Then $dec(H_{.1}+H_{.j}) = j - 1$. Hence, $\boldsymbol{j = dec(s) + 1}$.

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 $2^{n-k}=2\cdot n=2^{p+1}$. Then $n-k=p+1$. Hence $k=n-1-\log_2 n=2^p-1-p$. The validity of these observations concerns the values:

$$\begin{aligned} p &\in \{2,3,4,5,6,7\} = \mathcal{P} \\ n &\in \{4,8,\ldots,128\} = \mathcal{N} \\ k &\in \{1,4,\ldots,120\} = \mathcal{K} \end{aligned} \tag{22}$$

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, …, 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 $\mathcal{S}_{PC}(N,N-K)$. If $N \notin \mathcal{N}$ (i.e. $P \in \{8,9,\ldots\} = \mathbb{N} \setminus (\mathcal{P} \cup \{0,1\})$) or $K \notin \mathcal{K}$, 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 $\mathcal{S}_{PC}(N,N-K)$ else we normalize K. For $N \notin \mathcal{N}$, 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 $n=2^p$), with $N > n$, then N is divisible by any $n \in \mathcal{N}$. The ratio $\frac{N}{n} = \frac{2^P}{2^p} = 2^{P-p} = 2^a$ is a power of 2. Thus, we obtain 2^a 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 $n = 2^p \in \mathcal{N}$ and $k = (n-1-\log_2 n) \in \mathcal{K}$. Since we know n, we can determine k. N-K is not always divisible by $n-k$. Let $N-K = (n-k)\cdot q+r$, with $0 \le r < n-k$. 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 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.

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

The function *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

$$\text{rank(H)} = n - k \tag{23}$$

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 $\mathcal{J}$. 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 $\mathcal{S}_{PC}(n,m=n-k)$ 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

$$\ell_{max} = \frac{n}{2} - 1 \tag{24}$$

[1] Equivalent denotes the system obtained for another polar coding steganographic parameter n different to 8.

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 ℓ be the number of locked positions, then $1 \le \ell \le n/2$-1. In our steganographic problem, we must lock 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-ℓ and the number of equations is n-k = 1+$\log_2(n)$ = 1+p. Thus, we must have n-$\ell \ge n$-k then $\ell \le k$. The value of ℓ have two constrains ($\ell \le n/2$-1 and $\ell \le k$). So ℓ_{max} = min{k, $n/2$-1} = min{n-1-$\log_2(n)$, $n/2$-1}. Prove that ℓ_{max} = $n/2$-1. This amounts to demonstrate that $n/2$-1 ≤ n-1-$\log_2(n)$. That is equivalent to prove that their difference d = n-1-$\log_2(n)$-$n/2$+1 = $n/2$-$\log_2(n)$ = 2^{p-1}-p is positive or null. Consider the following function $f : \mathbb{N} \setminus \{0,1\} \to \mathbb{Z}$ such that $f(p) = 2^{p-1}$-p. This function is continuous and differentiable. Its derivative is $f'(p)=(p-1)\cdot 2^{p-2}$-1 ≥ 0, for $p \ge 2$. This mean that f is monotonic and $f(2) = 0$. Then $f(p) \ge 0$ for any $p \ge 2 \Rightarrow d \ge 0$. Consequently n-1-$\log_2(n) \ge n/2$-1. Finally, we have ℓ_{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 ℓ_{max}.

Let $\mathcal{J}$ be the set of wet elements, then:

- If syndrome s is in **Synd. 1** then we do nothing because e is also a zero vector;
- If s is in **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 $2^{n-k} = 2n$. We have $n/4$ quadruplets and each consists of four consecutive syndromes:

$$Q_i = \{n+4i-4;\ n+4i-3;\ n+4i-2;\ n+4i-1\},\ i = 1,\ldots,n/4 \quad (25)$$

Searching to know the quadruplet Q_i of a given syndrome s, we calculate its index i by:

$$i = \lceil (dec(s) - n + 1)/4 \rceil \quad (26)$$

where $\lceil\ \rceil$ denote the ceil operator and dec(s) is the decimal value of the syndrome s.

Proof: According to (25), dec(s) varies between n+4i-4 and n+4i-1 for quadruplet Q_i. Therefore (dec(s)+n+1)/4 is included between i-3/4 and i. Thus, when applying the round to the upper bound then $|(dec(s)+n+1)/4|$ is between $|i-3/4| = i$ 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, $e_i \cdot H^T = s_i$, 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 $e_4 = e_1 + e_2 + e_3$, then $e_4 \cdot H^T = e_1 \cdot H^T + e_2 \cdot H^T + e_3 \cdot H^T = s_1 + s_2 + s_3 = s$. Thus e_4 is in the coset of s. Consequently, to lock the position j, we choose as embedding change vector e_4. Each of the vectors e_1, e_2, e_3 has only one 1 respectively at different positions j, h, and t. Then e_4 has three 1 at positions h, l and t. If at least one of these three positions is in $\mathcal{J}$, then we search another embedding change vector with 1 at positions not in $\mathcal{J}$. To do so, we choose a pair in the triplet containing one or two elements belonging to $\mathcal{J}$. The chosen pair, let be (h, l), is then replaced by another pair (f, g) which is not included in $\mathcal{J}$ 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 which and 0 at replaced positions h and l.

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

Inputs: pair to replace (i, j) the set of wet element $\mathcal{J}$.
Outputs: the new pair obtained (l, t).

1: **While** (not *found* and not end of $\mathcal{J}$)
2: Search a first position l_1 (from 1 to n) not in $\mathcal{J}$
3: Search a second position t_1 ($t_1 > l_1$) not in $\mathcal{J}$
5: **If** ((l_1, t_1) verifies with (i, j) one of the equalities of (21))
6: $l \leftarrow l_1$; $t \leftarrow t_1$; **return** (l, t);
7: **Else If** (not end of $\mathcal{J}$)
8: Go to line 3.
9: **End (If)**
10: **if** (no good pair (l_1, t_1) is found)
11: Go to line 2.
12: **end (if)**
13: Repeat until having a good pair (l_1, t_1)
14: $l \leftarrow l_1$; $t \leftarrow t_1$; **return** (l, t);
14: **End (While)**

with $bin(a)$ is the binary value of the number a.

The new proposed scheme can be summarized as follows:

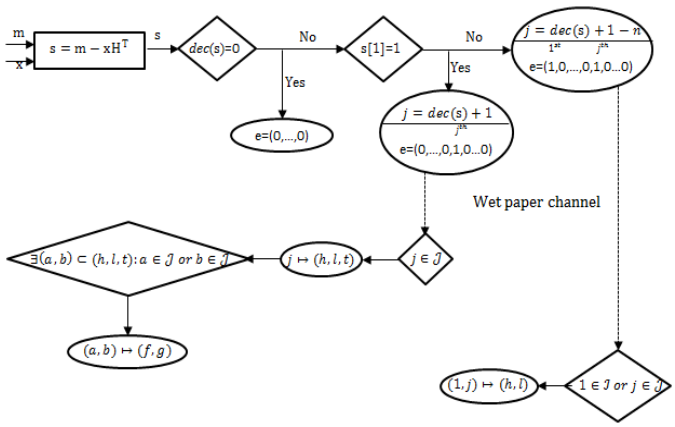


Fig. 4. New polar coding steganographic scheme.

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

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

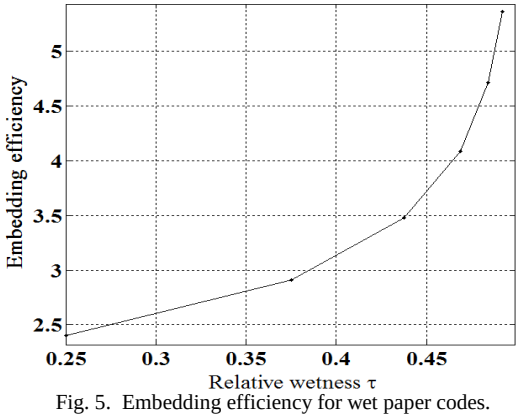


Fig. 5. Embedding efficiency for wet paper codes.

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.

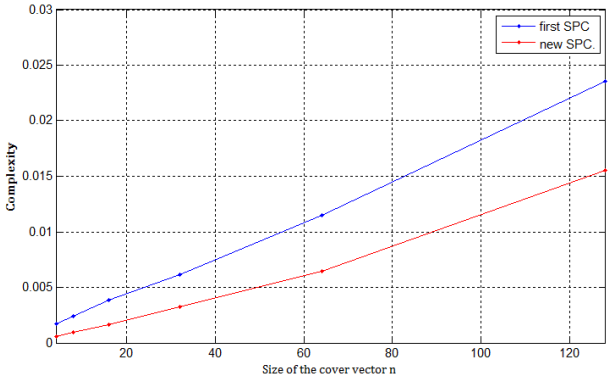


Fig. 6. The execution time of the two schemes for constant profile.

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.

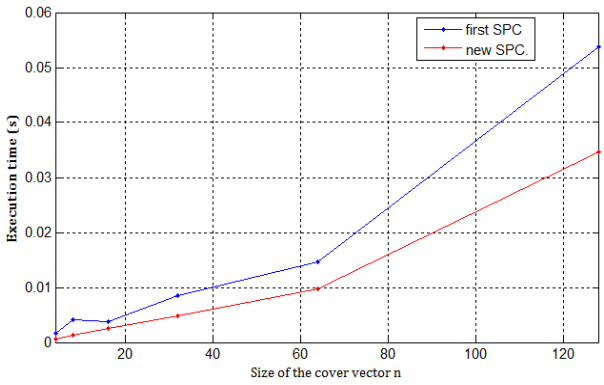


Fig. 7. The execution time of the two schemes for wet paper channel.

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 $512/n=2^{9-p}$ 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_{RC} and B_n.

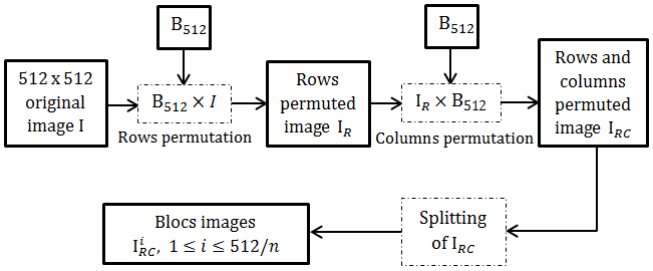


Fig. 8. Permutation and splitting images.

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 de 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.

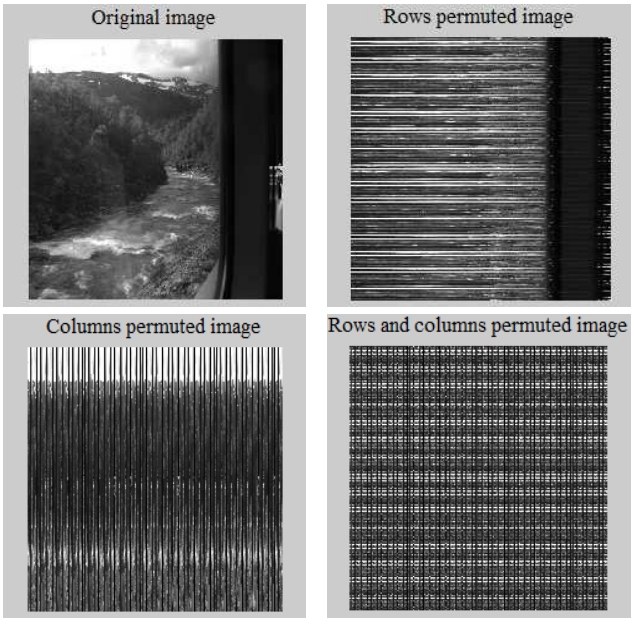


Fig. 9. Original image and different permuted images.

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.

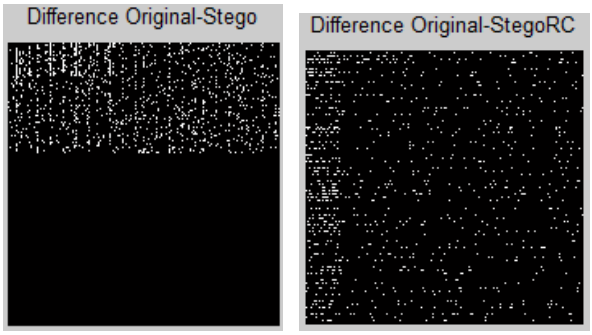


Fig.10. Positions of the embedding changes on non-permuted image (left) and rows and columns permuted image (right) when 0.2 bpp (bit per pixel) is embedded in '28.pgm'.

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

[1] V. Holub, "Content Adaptive Steganography – Design and Detection," *PhD thesis, Binghamton University*, May, 2014.

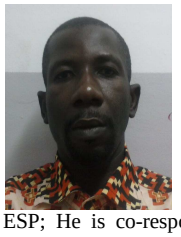
[2] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich and T. Pevný, "Moving Steganography and Steganalysis from laboratory to Real World," In *Proceedings of the ACM IH&MMSec'13, ACM*, pp.ACM 978-1-4503-2081-8/13/06, Montpellier, France, June, 2013.

[3] R. Crandall, "Some notes on steganography," in Steganography *Mailing List* [Online]. Available: http://os.inf.tu-dresden.de/ westfeld/crandall.pdf 1998.

[4] J. Bierbrauer, "On Crandall's Problem," [Online]. Available: http://www.ws.binghamton.edu/fridrich/covcodes.pdf 1998.
[5] A. Westfeld, "High capacity despite better steganalysis (F5 – a steganographic algorithm)," In: *Moskowitz, I.S. (ed.) IH 2001. LNCS*, vol. 2137, pp. 289–302, Springer, Heidelberg, 2001.
[6] M. van Dijk and F. Willems, "Embedding information in grayscale images," in *Proceedings of the 22nd Symposium on Information Communication Theory, Enschede, The Netherlands*, pp. 147–154, May 15–16, 2001.
[7] D. Schönfeld and A. Winkler, "An Embedding with syndrome coding based on BCH codes," in *Proceedings of the 8th ACM Workshop on Multimedia and Security*, pp. 214 – 223, 2006.
[8] R. Zhang, V. Sachnev, H. J. Kim, "Fast BCH syndrome coding for steganography," *S. Katzenbeisser and A.-R. Sadeghi (Eds.), IH 2009, LNCS 5806*, pp. 44-58, Springer-Verlag Berlin Heiderbelg, 2009.
[9] T. Filler and J. Fridrich, "Binary quantization using belief propagation over factor graphs of LDGM codes," presented at the *45th Annual. Allerton Conference Communication, Control and Computing, Allerton, IL*, September, 2007.
[10] W. Zhang and X. Wang, "Generalization of the ZZW embedding construction for steganography," *IEEE Transactions Information Forensics Security*, vol. 4, pp. 564–569, September, 2009.
[11] T. Filler, J. Judas and J. Fridrich, "Minimizing Embedding Impact in Steganography using Trellis-Coded Quantization," *Department of Electrical and Computer Engineering SUNY Binghamton*, USA, 2010.
[12] T. Filler, J. Judas and J. Fridrich, "Minimizing Additive Distortion in steganography Using Syndrome-Trellis Codes," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, September 2011.
[13] I. Diop, S. M. Farssi, M. Chaumont, O. Khouma, et H. B. Diouf, « Utilisation des codes LDPC en stéganographie, », *COmpression et REprésentation des Signaux Audiovisuels (CORESA)*, pp. 98-104, Lille, France, Mai, 2012.
[14] J. Fridrich, M. Goljan, P. Lisonek and D. Soukal, "Writing on wet paper," *In IEEE Transactions on Signal Processing Third Supplement on Secure Media*, vol. 53, pp. 3923–3935, October, 2005.
[15] B. Diouf, I. Diop, S. M. Farssi, K. Tall, P. A. Fall, A. K. Diop and K. Sylla, "Using of Polar Codes in Steganography," In *Proceedings of the 2nd International Conference on Advances in Computer Science and Engineering (CSE 2013)*, vol. 42, pp. 262-266, Atlantis Press, Los Angeles, July, 2013.
[16] B. Diouf, I. Diop, S. M. Farssi and O. Khouma, "Minimizing Embedding Impact in Steganography Using Polar Codes," In *Proceedings of 4rd IEEE International Conference on Multimedia Computing and Systems (ICMCS'14)*, pp. 105–111, Marrakesh, Morocco, April, 2014.
[17] B. Diouf, I. Diop, S. M. Farssi and O. Khouma, "Practical Polar Coding Method to Minimize the Embedding Impact in Steganography," In *Proceedings of the IEEE International Science and Information (SAI) Conference*, London, United Kingdom, July, 2015.
[18] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions Information Theory*, vol. IT-55, pp. 3051-3073, July, 2009.
[19] N. Goela, S. B. Korada, and M. Gastpar, "On LP Decoding of Polar Codes," *Submitted to IEEE Transaction Information Theory Workshop-ITW*, Dublin, 2010.
[20] T. Pevnỳ, T. Filler and P. Bas, "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography," *Czech Technical University, Prague, Czech Republic; State University, New York in Binghamton, NY, USA; CNRS-LAGIS, Lille, France*, 2010.
[21] T. Filler, T. Pevný, and P. Bas. BOSS (Break Our Steganography System). http://www.agents.cz/boss, July 2010.
[22] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," in *Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX (E. J. Delp and P. W. Wong, eds.)*, vol. 6505, pp. 02–03, San Jose, CA, January 29–February 1, 2007.
[23] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *Proceedings 8th International Workshop Information Hiding, J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, Eds., Alexandria, VA*, vol. 4437, Lecture Notes in Computer Science, pp. 314–327, July 10–12, 2006.

Birahime Diouf received the Electronic and Telecommunications Engineering Degree from Gaston Berger University (UGB), Saint-Louis, Senegal in 2012, and the M.Sc. in Computer Science, Modeling and Simulation of Complex Systems from Polytechnic Institute, Cheikh Anta Diop University (UCAD), Dakar, Senegal in 2013. He is currently working towards the Ph.D. degree.

He is currently a Researcher at the Department of Computer Science, Polytechnic Institute, Cheikh Anta Diop University. His research interests include data hiding, information theory, coding theory, image processing and signal processing.



Idy DIOP graduated from the University of Dakar. He received his engineering degree from Electronic and telecommunication in 2006 to the Gaston Berger University of Saint-Louis of Senegal, and a Diploma of master research: Physics for Engineers in Ecole Supérieure Polytechnique (ESP), Dakar-Senegal (2007). He holds a PhD in Engineering Thesis (2011): watermarking medical image based on JPEG 2000 ESP; He is co-responsible of several memories of Master in Computer Science and Telecommunications, author of several publications in international journals and several studies reported with publications in the proceedings of International Congresses with peer and scientific committee member of several international conferences. His research interests include steganography, steganalysis, compression, watermarking, information and coding theory and wireless communications.

Sidi Mohammed FARSSI graduated from the University of Dakar. He received his engineering degree from Electrical Engineering Design option (EEAI) in 1988 to the ESP, and a Diploma of Advanced Studies: Physics for Engineers in Paris XII (1989). He holds a PhD in Engineering Thesis (1993): Biomedical image processing in ESP (Ecole Supérieure Polytechnique de Dakar- Senegal) and then PhD State es-sciences (1997): Biomedical Image Processing, Dakar ESP. He is Director of several doctoral theses in Information Processing, Director of several DEA in Computer Science and Telecommunications, Director of several memories of Master in Computer Science and Telecommunications, author of several publications in international journals and several studies reported with publications in the proceedings of International Congresses with peer, expert player in international scientific journals, scientific committee member of several international conferences, participating in several workshops and training expertise, expert for the United Nations University for Education and Scientific Research, Member of the reflection of TOKTEN project, Expert of 'World ORT Union, Member of Networks of Excellence SIMILAR, Member of the Society of African scientists, Expert for the recognition and equivalence of degrees to African schools CAM, Expert for the Association of Francophone universities AUF..