# Pixel-Sensitive and Robust Steganography Based on Polar Codes

Yujun Ji*, Jinsheng Li*, Ling Liu†, Qi Cao† and Tao Dai*
* College of Computer Science and Software Engineering, Shenzhen University, China
† Guangzhou Institute of Technology, Xidian University, Guangzhou, China
Email: {jiyujun2023, lijinsheng2020}@email.szu.edu.cn, {liuling, caoqi}@xidian.edu.cn, daitao@szu.edu.cn



***Abstract*—Steganography is an information hiding technique for covert communication. The core issue in steganography design is the rate-distortion coding problem. Polar codes, which have been proven to achieve the rate-distortion bound for any binary symmetric source, are utilized to design a steganographic scheme that can reach the embedding capacity for the Distortion-Limited Sender problem in certain cases. In adaptive steganography, for attack scenarios where each noise element can have different intensities, existing steganographic coding methods fail to resist such attacks. In this paper, we propose a pixel-sensitive and robust steganographic scheme based on polar codes. Our steganographic scheme not only matches the adaptive distortion well but is also robust against sophisticated noise attacks. Futher, it is proven that our scheme achieves the embedding capacity in certain cases. Experimentally, a steganographic scheme can be designed and implemented with a secret message error rate at the $10^{-5}$ level when the attack noise is known to both the sender and the receiver. This demonstrates its significant robustness.**

## I. Introduction

In recent years, the rapid development of computer networks, including wireless networks, has increased the security risks of information dissemination, drawing more attention to information security [1]. As an information hiding technique for covert communication, steganography secures data transmission in digital networks. Steganography hides secret messages in ordinary covers (e.g. image, audio and text.), making it difficult for eavesdroppers to notice the presence of secret messages [2]–[4].

Steganalysis is a technique antagonistic to steganography, aiming to detect the presence of secret messages in a carrier. To counter steganalysis, steganography needs to minimize the distortion to the cover caused by embedding messages at a given payload rate, which is known as the Payload-Limited Sender (PLS) problem. The Distortion-Limited Sender (DLS) problem is the dual of the PLS problem, where the goal is to maximize the payload rate given a certain level of distortion caused by embedding messages. The core issue in steganography design is the rate-distortion coding problem, which can be solved using steganographic codes [5]–[7]. In adaptive steganography, a distortion function that represents the modification distortion weight of each cover element is defined. When the modification of each cover element is independent, the distortion function is additive. Currently, distortion functions can be derived using advanced deep learning techniques [8]–[10]. For adaptive steganography, Syndrome-Trellis Codes (STC) [11] are most widely used, as they can asymptotically approach the bounds for a large range of distortion functions.

Polar coding, introduced by Arıkan [12], is a channel coding method that can be proven to achieve the symmetric capacity of Binary Discrete Memoryless Channels (B-DMCs). It has also been extended to the field of source coding [13], [14]. In lossy source coding, Korada and Urbanke proved that polar codes can achieve the rate-distortion bound for any binary symmetric source (BSS) [15]. Therefore, using polar codes as steganographic codes is highly suitable. Diouf *et al.* were the first to use a SC decoder as a steganographic encoder [16], and experimentally demonstrated better embedding performance compared to STC. Subsequent works [17]–[19] further optimized and expanded the steganography based on polar codes.

However, in practical applications, the stego sequence may suffer from noise attacks due to various factors, such as adversary-originated noise or transmission through a noisy communication channel, leading to secret information loss. Therefore, robust steganography is required. The steganographic methods in [16]–[19] cannot withstand noise attacks. For attack scenarios where each noise element has the same intensity, Li and Liu proposed robust schemes based on polar codes for the constant distortion (where the modification distortion weight of each cover element is the same) [20]. Yao *et al.* proposed reliable robust adaptive steganographic coding based on nested polar codes for the adaptive distortion [21]. In this paper, for generalized attack scenarios where each noise element can have different intensities, we propose a pixel-sensitive and robust steganographic scheme based on polar codes. Our steganographic scheme not only matches the adaptive distortion well but is also effective against more sophisticated noise attacks. More suitable construction algorithms and better-performing decoders of polar codes are employed in our scheme. We theoretically prove that our scheme achieves the embedding capacity in certain cases.

All random variables (RVs) are denoted by capital letters, and their realizations are denoted by the corresponding lowercase letters. $[N]$ denotes the set $\{1, 2, \ldots, N\}$. We use the notation $x_i^j (i \leq j)$ as a shorthand for the vector $(x_i, ..., x_j)$, which is a realization of the RVs $X_i^j = (X_i, ..., X_j)$. The vector$(x_i : i \in \mathcal{A})$ is denoted by $x_{\mathcal{A}}$. The Shannon entropy of $X$ is denoted by $H(X)$, and the binary entropy function is denoted by $h_2(\cdot)$. For a set $\mathcal{I}$, $\mathcal{I}^c$ denotes its complement, and $|\mathcal{I}|$ represents its cardinality. If $X$ follows a Bernoulli distri-

bution with $P(X=1)=p$, we denote it by $X \sim Ber(p)$. The capacity of channel $W$ is denoted by $C(W)$. We denote the binary logarithm and natural logarithm by $\log$ and $\ln$, respectively, and information is measured in bits.

## II. Preliminaries

### A. Adaptive Steganographic Model

We use $X$ to denote the cover random variable and use $Y$ to denote the stego random variable after embedding. The stego sequence $y_1^N$ is obtained by embedding the secret message sequence $m_1^q$ into the cover sequence $x_1^N$. Typically, images are used as data carriers for both the cover and stego. In this paper, we consider binary embedding, hence $x_1^N$,$y_1^N$, and $m_1^q$ are binary sequences, with $x_i$ and $y_i$ being the Least Significant Bit (LSB) of the $i$-th pixel of the cover and stego, respectively. Note that the $q$-ary embedding can be implemented using multi-layered binary embedding [11], [22].

We define the embedding modification probability for $x_i$ as $p_i \triangleq P(y_i \neq x_i \,|\, x_i)$. The distortion caused by embedding is measured by Hamming distortion, with a positive weight $\rho_i$. In additive distortion model, the total distortion is the sum of the distortion of each pixel given by

$$D\left(x_1^N, y_1^N\right) = \sum_{i=1}^{N} \rho_i \cdot (x_i \oplus y_i), \tag{1}$$

where $\oplus$ denotes the XOR operation. The formulations of the PLS and DLS problems are introduced in the following.

1) PLS: given a fixed number of embedded message bits $q$, minimize the total average distortion:

$$\underset{p_1^N}{\text{minimize}} \quad E(D) = \sum_{i=1}^{N} p_i \rho_i, \tag{2}$$

$$\text{subject to} \quad H(p_1^N) = \sum_{i=1}^{N} h_2(p_i) = q. \tag{3}$$

2) DLS: given a fixed total average distortion $D_\epsilon$, maximize the number of embedded message bits:

$$\underset{p_1^N}{\text{maximize}} \quad H(p_1^N) = \sum_{i=1}^{N} h_2(p_i), \tag{4}$$

$$\text{subject to} \quad E(D) = \sum_{i=1}^{N} p_i \rho_i = D_\epsilon. \tag{5}$$

For the PLS problem, the optimal embedding has the form of a Gibbs distribution [23]:

$$P_\lambda\left(y_i | x_i\right) = \frac{\exp\left(-\lambda \rho_i \cdot (x_i \oplus y_i)\right)}{\sum_{t_i \in \{0,1\}} \exp\left(-\lambda \rho_i t_i\right)},\ 1 \leq i \leq N, \tag{6}$$

where $\lambda \in [0, \infty)$ can be determined by (3). In practice, $H(p_1^N)$ is a monotonically decreasing function of $\lambda$, which can be found using a simple binary search. The PLS and DLS problems are dual problems of each other. The optimal embedding distribution for the DLS problem is also given by (6). In this case, $\lambda$ can be determined in the same way by (5).

### B. Polar Codes

For channel polarization, $N$ independent copies of a given B-DMC $W$ are combined into a vector channel $W_N$, which is split into $N$ subchannels $W_N^{(i)}$, $1 \leq i \leq N$ [12]. As $N$ increases to infinity, almost all subchannels have capacity close to 0 or 1, and the proportion of the subchannels with capacity close to 1 approaches $C(W)$.

*1) Polar Encoding:* Polar codes can be identified by a parameter tuple $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$, where $N = 2^n$ for a positive integer. $\mathcal{A}$ is the set of indices for the $K$ information bits, and $u_{\mathcal{A}^c}$ represents the $N-K$ frozen bits.

The construction of $(N, K)$ polar codes refers to selecting the $K$ most reliable subchannels to transmit the information bits $u_{\mathcal{A}}$. One usually uses the Bhattacharyya parameter [12] to evaluate the reliability of the subchannels. The Bhattacharyya parameter of $i$-th subchannel $W_N^{(i)}$ is defined as

$$Z(W_N^{(i)}) \triangleq \sum_{\substack{(y_1^N, u_1^{i-1}) \in \\ \mathcal{Y}^N \times \{0,1\}^{i-1}}} \sqrt{W_N^{(i)}\left(y_1^N, u_1^{i-1} | 0\right) W_N^{(i)}\left(y_1^N, u_1^{i-1} | 1\right)}.$$

For binary symmetric channel (BSC), $Z(W_N^{(i)})$ can be recursively approximated by Equivalent Bhattacharyya Parameter Construction [24]. The degrading merging algorithm [25] is more commonly used, as it can estimate $Z(W_N^{(i)})$ with arbitrary precision.

After acquiring the information indices $\mathcal{A}$, the generator matrix is calculated by $G_N = B_N \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]^{\otimes n}$, where $B_N$ is known as the *bit-reversal* permutation matrix and $\otimes$ denotes the Kronecker product. For encoding, $u_{\mathcal{A}^c}$ and $u_{\mathcal{A}}$ are combined into the vector $u_1^N = [u_{\mathcal{A}^c}, u_{\mathcal{A}}]$, where $u_{\mathcal{A}}$ represents the information bits and $u_{\mathcal{A}^c}$ represents the frozen bits known to both the encoder and decoder. Then, the codeword is given by $x_1^N = u_1^N G_N$.

*2) Polar Decoding:* Consider the polar code represented by $(N, K, \mathcal{A}, u_{\mathcal{A}^c})$. The decoder's task is to generate an estimate $\hat{u}_{\mathcal{A}}$ of $u_{\mathcal{A}}$ from the received $y_1^N$. The Successive Cancellation (SC) decoder, introduced by Arıkan [12], uses Log-Likelihood Ratio (LLR) to decide the value of $\hat{u}_i (i \in \mathcal{A})$ sequentially. The LLR can be calculated recursively from equations (75) and (76) presented in [12].

The Successive Cancellation List (SCL) [26], [27] decoder is an enhancement based on the SC decoder. The SCL decoder extends the single decoding path of the SC decoder to $L$ paths. In the decoding process, the SCL decoder retains at most $L$ decoding paths with the best path metrics at each step. Upon completion of decoding, the SCL decoder selects the most reliable path as the output of the decoder. The complexities of the SC and SCL decoders are $O(N \log N)$ and $O(L \cdot N \log N)$, respectively. The notation $\text{SCL}(y_1^N, W^N, u_{\mathcal{A}^c}, \mathcal{A}^c, L)$ represents the decoding estimate of an SCL decoder with list size $L$, given the output $y_1^N$, channel $W^N$, frozen bits $u_{\mathcal{A}^c}$ and frozen indices $\mathcal{A}^c$.

## III. Polar Codes for adaptive steganography

Let $M$ represent the secret message. Embedding $M^q$ into $X^N$ can be viewed as passing $X^N$ through

$(W_1, W_2, \cdots, W_N)$, where $W_i$ is a BSC with the crossover probability of $p_i$, denoted by BSC($p_i$), representing the $i$-th embedding channel. The embedding capacity of $W_i$ is complementary to the channel capacity, given by $h_2(p_i)$. The adaptive steganography process is shown in Fig. 1. Let $\mathbf{E} = (E_1, E_2, \ldots, E_N)$, where $E_i$ is the RV corresponding to $W_i$ and $E_i \sim Ber(p_i)$. Notice that the cover $X$ is a BSS and the stego $Y$ is also a BSS since the embedding channel is symmetric, demonstrating the distribution-preserving property of the steganography. Based on the aforementioned symmetry, $X_i$ can also be considered as obtained from $Y_i$ through $W_i$. The channel polarization of $(W_1, W_2, \cdots, W_N)$ is represented as $(W_1, W_2, \cdots, W_N) \mapsto (W_N^{(1)}, W_N^{(2)}, \cdots, W_N^{(N)})$.

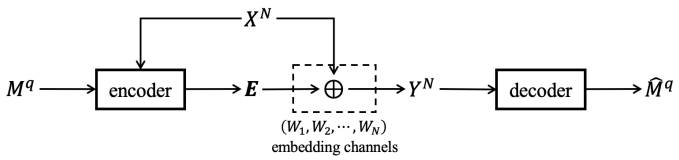



Fig. 1. Illustration of the adaptive steganography.

For $0 < \beta < \frac{1}{2}$, partition $[N]$ into

$$\mathcal{F} \triangleq \left\{ i \in [N] : Z(W_N^{(i)}) \geq 1 - 2^{-N^\beta} \right\}$$

and $\mathcal{I} = \mathcal{F}^c$, where $\mathcal{F}$ is the indices corresponding to $M^q$. Equivalent Bhattacharyya Parameter Construction can be generalized to the case of parallel channels [28]. Therefore, $Z(W_N^{(i)})$ can still be recursively approximated.

For message embedding, we obtain $u_{\mathcal{F}}$ by $u_{\mathcal{F}} = m_1^q$. For each $i \in \mathcal{I}$,

$$\hat{u}_i = \underset{u \in \{0,1\}}{\operatorname{argmax}} P_{\hat{U}_i | \hat{U}_1^{i-1}, X_1^N} \left( u \mid \hat{u}_1^{i-1}, x_1^N \right). \tag{7}$$

Finally, we derive the stego sequence as $y_1^N = u_1^N G_N$. Using the SCL decoder, we have

$$(u_{\mathcal{F}}, u_{\mathcal{I}}) = u_1^N = \text{SCL}\left( x_1^N, (W_1, W_2, \cdots, W_N), m_1^q, \mathcal{F}, L \right).$$

The decoder calculates the LLR with the initial value $L_1^{(1)}(x_i) = (1 - 2x_i) \ln \frac{1-p_i}{p_i}$.

For message extraction, after receiving the stego sequence $y_1^N$, the receiver uses the same construction method as the sender to obtain $\mathcal{F}$ and $\mathcal{I}$. Given $G_N^{-1} = G_N$ for the 2-by-2 binary kernel [12], we have $u_1^N = y_1^N G_N$, then $m_1^q = u_{\mathcal{F}}$.

Given a set of $N$ parallel channels $\{W_1, W_2, \cdots, W_N\}$, each component channel is used $J$ times. Let $w_{r,t}$ denote the $t$-th use of component channel $W_r$, that is, $w_{r,t} \Leftrightarrow W_r$, where the equivalence relation $\Leftrightarrow$ indicates the two channels have the same transition probability for $r = 1, 2, \cdots, N$ and $t = 1, 2, \cdots, J$. We use notation $w_1^{NJ}$ to denote a vector of $NJ$ independent channels, where $w_i$ is related to the channel uses $w_{r,t}$ with a one-to-one mapping

$$\pi : \{1, 2, \cdots, NJ\} \to \{1, 2, \cdots N\} \times \{1, 2, \cdots J\}, \tag{8}$$

that is, $\pi(i) = (r, t)$, and

$$w_i \Leftrightarrow w_{\pi(i)} \Leftrightarrow w_{r,t} \Leftrightarrow W_r, \tag{9}$$

where $i \in \{1, \cdots, NJ\}, r \in \{1, \cdots, N\}$ and $t \in \{1, \cdots, J\}$.

By modifying the decision rule to the randomized rounding where $\hat{u}_i$ is obtained from $Ber(\frac{1}{1+\exp(L_N^{(i)})})$, we can derive Theorem 1, with its proof given in the Appendix. Likewise, Lemma 1 can be adapted from [14] Lemma 3.14, owing to the symmetry of the embedding channel and distortion function.

**Theorem 1.** Let the cover $X$ be a BSS. Consider any independent parallel embedding channel BSCs $\{W_1, W_2, \cdots, W_N\}$, where $N = 2^n$, for a fixed positive integer $n$. For each embedding channel $W_i$, the crossover probability is $p_i \in [0, \frac{1}{2}]$. Using each of the $N$ channels $J$ times, where $J = 2^j$ and $j$ is a non-negative integer, we obtain $NJ$ channels $w_1^{NJ}$. Fix the design distortion $D = \frac{1}{N} \sum_{i=1}^N p_i \rho_i$ and $0 < \beta < \frac{1}{2}$. For any embedding rate $R < \frac{1}{N} H(Y_1^N | X_1^N) = \frac{1}{N} \sum_{r=1}^N h_2(p_r)$, there exists a sequence of polar codes of length $NJ$ with rates $R_{NJ} \geq R$ so that under SC encoding using randomized rounding they achieve expected distortion $D_{NJ}$ satisfying

$$D_{NJ} \leq D + O(2^{-(NJ)^\beta}).$$

The encoding as well as decoding complexity of this scheme is $O(NJ \log(NJ))$.

**Lemma 1.** The average distortion $D_{NJ}(F, u_F)$ is independent of the choice of $u_F \in \{0, 1\}^{|F|}$.

## IV. Polar Codes for Pixel-Sensitive and Robust Steganography

In practical applications, the receiver may acquire noisy stego due to various reasons, such as noise attacks from an adversary or communication through a specific channel. For convenience, these are collectively called the *attack channels* in this paper. The aforementioned adaptive steganography cannot resist noise, making it difficult to extract accurate secret messages. To protect secret messages from noise attacks, we propose pixel-sensitive and robust steganography. In this paper, we consider only noise that independently follows a Bernoulli distribution. Note that many other types of attack channels can be approximated as a BSC.

Equations (2)-(5) provide the forms of adaptive steganography. Here, we redefine the formulations in robust scenarios of adaptive steganography. The $i$-th attack channel $Q_i$ is assumed to BSC($\theta_i$), with the corresponding noise RV $Z_i \sim Ber(\theta_i)$. Restate the PLS and DLS problem as follows.

1) PLS:

$$\underset{p_1^N}{\text{minimize}} \quad E(D) = \sum_{i=1}^N p_i \rho_i, \tag{10}$$

$$\text{subject to} \quad \sum_{i=1}^N h_2(p_i) - \sum_{i=1}^N h_2(\theta_i) = q. \tag{11}$$

2) DLS:

$$\underset{p_1^N}{\text{maximize}} \quad H(p_1^N) = \sum_{i=1}^N h_2(p_i) - \sum_{i=1}^N h_2(\theta_i), \tag{12}$$

$$\text{subject to} \quad E(D) = \sum_{i=1}^N p_i \rho_i = D_\epsilon. \tag{13}$$

It is evident that our scheme achieves noise robustness by sacrificing some embedding rate due to the additional attack.

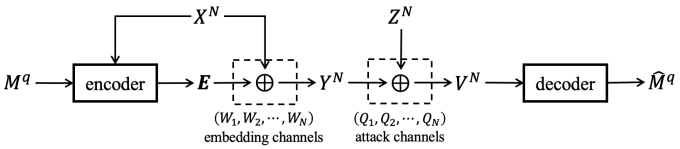



Fig. 2. Illustration of the pixel-sensitive and robust steganography.

Below, we present the pixel-sensitive and robust steganographic scheme based on polar codes. For $0 < \beta < \frac{1}{2}$, the index sets are obtained as follows:

$$\mathcal{F}_1 \triangleq \left\{ i \in [N] : Z\left(W_N^{(i)}\right) \geq 1 - 2^{-N^\beta} \right\} \tag{14}$$

$$\mathcal{F}_2 \triangleq \left\{ i \in [N] : Z\left(Q_N^{(i)}\right) \geq 2^{-N^\beta} \right\}. \tag{15}$$

Next, we partition $[N]$ into $\mathcal{F} \triangleq \mathcal{F}_1 \cap \mathcal{F}_2$, $\mathcal{I} \triangleq \mathcal{F}_1 \setminus \mathcal{F}_2$, and $\mathcal{P} \triangleq \mathcal{F}_1^c$. For the construction of parallel channels, the Monte Carlo construction proposed by Arıkan [12], which statistically estimates the decoding error rate of subchannels through experimental simulation, is more effective. The Monte Carlo construction algorithm is detailed in the pseudocode of Algorithm 1 in the Appendix. As the number of simulation runs increases, the statistical results become more effective in reflecting the reliability of the subchannels.

For message embedding, with the random frozen bits $F \sim Ber\left(\frac{1}{2}\right)$, we obtain $u_\mathcal{F}$ and $u_\mathcal{I}$ by $u_\mathcal{F} = f^{|\mathcal{F}|}$ and $u_\mathcal{I} = m_1^q$, where $u_\mathcal{F}$ is a vector of frozen bits pre-shared between sender and receiver. For each $i \in \mathcal{P}$, we compute

$$\hat{u}_i = \underset{u \in \{0,1\}}{\operatorname{argmax}} P_{\hat{U}_i | \hat{U}_1^{i-1}, X_1^N}\left(u \mid \hat{u}_1^{i-1}, x_1^N\right). \tag{16}$$

Finally, we derive the stego sequence as $y_1^N = u_1^N G_N$. Using the SCL decoder, we have

$$(u_\mathcal{F}, u_\mathcal{I}, u_\mathcal{P}) = u_1^N = \text{SCL}\left(x_1^N, (W_1, W_2, \cdots, W_N), (f^{|\mathcal{F}|}, m_1^q), (\mathcal{F}, \mathcal{I}), L\right).$$

The decoder calculates the LLR with the initial value $L_1^{(1)}(x_i) = (1 - 2x_i) \ln \frac{1-p_i}{p_i}$.

For message extraction, after receiving the sequence $v_1^N$ from attack channels $(Q_1, Q_2, \ldots, Q_N)$, the receiver uses the same construction method as the sender to obtain $\mathcal{F}_1$ and $\mathcal{F}_2$, thus deriving $\mathcal{F} \triangleq \mathcal{F}_1 \cap \mathcal{F}_2$, $\mathcal{I} \triangleq \mathcal{F}_1 \setminus \mathcal{F}_2$, and $\mathcal{P} \triangleq \mathcal{F}_1^c$. We obtain $\hat{u}_\mathcal{F} = u_\mathcal{F}$. For each $i \in \mathcal{I} \cup \mathcal{P}$,

$$\hat{u}_i = \underset{u \in \{0,1\}}{\operatorname{argmax}} P_{\hat{U}_i | \hat{U}_1^{i-1}, V_1^N}\left(u \mid \hat{u}_1^{i-1}, v_1^N\right). \tag{17}$$

$\hat{u}_\mathcal{I}$ is the extracted secret message. Using the SCL decoder, we have

$$(u_\mathcal{F}, \hat{u}_\mathcal{I}, \hat{u}_\mathcal{P}) = \hat{u}_1^N = \text{SCL}\left(v_1^N, (Q_1, Q_2, \cdots, Q_N), u_\mathcal{F}, \mathcal{F}, L\right).$$

The decoder calculates the LLR with the initial value $L_1^{(1)}(v_i) = (1 - 2v_i) \ln \frac{1-\theta_i}{\theta_i}$.

Let $W \preccurlyeq Q$ denote that channel $W$ is degraded with respect to channel $Q$, as defined in [25]. The following lemma can be easily adapted from [25]. For brevity, we omit the proof.

**Lemma 2.** For B-DMCs $W_1, W_2, Q_1$ and $Q_2$, $W^-$ and $W^+$ are obtained from the polarization process $(W_1, W_2) \mapsto (W^-, W^+)$, while $Q^-$ and $Q^+$ are obtained from the polarization $(Q_1, Q_2) \mapsto (Q^-, Q^+)$. If $W_1 \preccurlyeq Q_1$ and $W_2 \preccurlyeq Q_2$, then

$$W^- \preccurlyeq Q^- \quad \text{and} \quad W^+ \preccurlyeq Q^+. \tag{18}$$

**Corollary 1.** For B-DMCs $W_i$ and $Q_i$ for $i \in [N]$, $W_N^{(i)}$ and $Q_N^{(i)}$ are obtained from the polarization process $(W_1, W_2, \ldots, W_N) \mapsto (W_N^{(1)}, W_N^{(2)}, \ldots, W_N^{(N)})$ and $(Q_1, Q_2, \ldots, Q_N) \mapsto (Q_N^{(1)}, Q_N^{(2)}, \ldots, Q_N^{(N)})$, respectively. If $W_i \preccurlyeq Q_i$ for $i \in [N]$, then

$$W_N^{(i)} \preccurlyeq Q_N^{(i)}, \text{ for } i \in [N]. \tag{19}$$

**Theorem 2.** Let the cover $X$ be a BSS. Consider sets of independent parallel BSCs $\{W_1, W_2, \cdots, W_N\}$ and $\{Q_1, Q_2, \cdots, Q_N\}$ for embedding and attack channels, respectively, where $N = 2^n$, for a fixed positive integer $n$, and the crossover probability pair $(p_i, \theta_i)$ of each pair $(W_i, Q_i)$ satisfy $0 \leq \theta_i \leq p_i \leq \frac{1}{2}$. Using each pair of $N$ channels $(W_i, Q_i)$ $J$ times, where $J = 2^j$ and $j$ is a non-negative integer, we obtain $NJ$ pairs of channels $(w_1^{NJ}, q_1^{NJ})$. Fix the design distortion $D = \frac{1}{N}\sum_{i=1}^N p_i \rho_i$ and $0 < \beta < \frac{1}{2}$. For any embedding rate $R < \frac{1}{N} H(Y_1^N | X_1^N) - \frac{1}{N} H(Y_1^N | V_1^N) = \frac{1}{N}\sum_{r=1}^N h_2(p_r) - \frac{1}{N}\sum_{r=1}^N h_2(\theta_r)$, there exists a sequence of polar codes of length $NJ$ with rates $R_{NJ} \geq R$ so that under SC encoding with randomized rounding, they achieve expected distortion $D_{NJ}$ satisfying

$$D_{NJ} \leq D + O(2^{-(NJ)^\beta}).$$

Futher, the block error probability satisfies

$$P_{NJ} \leq O(2^{-(NJ)^\beta}).$$

The encoding as well as decoding complexity of this scheme is $O(NJ \log(NJ))$.

**Remark 1.** Based on the assumptions of Theorem 2, the proposed pixel-sensitive and robust steganography, in which the polar codes are constructed by the degrading merging algorithm [25], can achieve the per-bit average embedding capacity in Equation (12) when $J$ and the limit of the output alphabet size are both sufficiently large. The expected distortion under SC encoding using randomized rounding and the block error probability under SC decoding are respectively upper bounded by $D + O(2^{-(NJ)^\beta})$ and $O(2^{-(NJ)^\beta})$, for $0 < \beta < \frac{1}{2}$.

**Remark 2.** Similarly to Lemma 1, the average distortion $D_{NJ}(F, u_F)$ and average block error probability $P_{NJ}(F, u_F)$ are independent of the choice of $u_F \in \{0,1\}^{|F|}$, respectively.

For cases not satisfying the conditions of Theorem 2, $\mathcal{F}_1$ and $\mathcal{F}_2$ lack a clear nested relationship. This issue could potentially be addressed by universal polar codes [29], [30], which represents a promising direction for future research. However, in practice, $\frac{|\mathcal{F}_2 \setminus \mathcal{F}_1|}{N}$ is typically small. Moreover,

a larger $\frac{|\mathcal{F}_2 \backslash \mathcal{F}_1|}{N}$ is associated with reduced robustness.

We analyze two attack models below. The first model involves scenarios where the attacker launches attacks with the same intensity, or where the stego is transmitted over a channel. The second model describes scenarios where the attacker launches hidden linear attacks. The more complex the image texture surrounding a pixel, the better concealed higher-intensity attacks on that pixel become.

1) Attack Model 1 (AM1): Assume $Z_i \sim Ber(\theta)$, $i \in [N]$, i.e., the attack model for each $i$ is fixed. The equation (11) becomes $\sum_{i=1}^{N} h_2(p_i) - Nh_2(\theta) = q$. We ensure that $\theta$ is known to both the sender and receiver. Thus, the optimal embedding distribution of $p_i$ remains as in (6). Clearly, we cannot guarantee that $p_i \geq \theta$ for all $i \in [N]$.

2) Attack Model 2 (AM2): Assume $R_a = \frac{\theta_i}{p_i} \in [0, 1]$ is a constant. We have $p_i \geq \theta_i$ and $Z_i \sim Ber(R_a p_i)$. The equation (11) becomes $\sum_{i=1}^{N} h_2(p_i) - \sum_{i=1}^{N} h_2(R_a p_i) = q$. If $R_a$ is directly known to both the sender and receiver, solving for the optimal embedding distribution of $p_i$ becomes difficult. Therefore, to simplify the problem, we propose a two-phase approach, initially assuming that $R_a$ is unknown, based on the reasonable assumption that the embedding loss due to robustness in AM2 is the same as in AM1. The proposed approach consists of the following phases:

- **Phase 1:** Based on our assumption, we set $\sum_{i=1}^{N} h_2(R_a p_i) = Nh_2(\theta)$, where $\theta$ is known to both the sender and receiver, and $R_a$ is a variable to be solved. Consequently, the equation (11) simplifies to $\sum_{i=1}^{N} h_2(p_i) - Nh_2(\theta) = q$. At this point, solving for the optimal embedding distribution of $p_i$ reverts to solving under AM1;
- **Phase 2:** With the optimal embedding distribution of $p_i$ already known, we determine $R_a$ by solving $\sum_{i=1}^{N} h_2(R_a p_i) = Nh_2(\theta)$. Thus, $\theta_i = R_a p_i$.

In fact, AM1 and AM2 yield the same optimal distribution of $p_i$ for the same problem, albeit with different noise parameters. Since AM2 satisfies the conditions in Theorem 2, our scheme is validated. As for AM1, the effectiveness of our scheme will be assessed experimentally in the next section.

## V. SIMULATION EXPERIMENTS

Next, we will conduct two simulation experiments. The first is to verify that the proposed pixel-sensitive and robust steganographic scheme can approach the theoretical bounds, and the second is to demonstrate that the scheme exhibits good robustness.

### A. Per-Bit Average Embedding Distortion

We choose the PLS form for message embedding under AM1. The theoretical bound, $E_b = \frac{1}{N} \sum_{i=1}^{N} p_i \rho_i$, is given by (10). We denote the distortion profile by the function $c(\cdot)$. Three common distortion profiles are considered: the constant profile $c(x) = 1$, linear profile $c(x) = x$, and square profile $c(x) = x^2$. The value of $\rho_i$ is then computed as $c\left(\frac{i}{N}\right)$. The embedding rate $R = \frac{q}{N}$ is measured in bit per pixel (bpp).

The results for the constant distortion profile are provided in [20]. Here, we consider the linear and square distortion profiles. For both linear and square distortion profiles, $E_b$ is monotonically non-increasing as $N$ increases. This phenomenon is illustrated in Fig. 3. As $N$ increases, $E_b$ converges to a fixed value. Therefore, we use $E_b$ at $N = 2^{22}$ as the theoretical bound in our experiments. With $\theta = 0.05$ and $R$ varying from 0.1 to 0.5, we use the SCL decoder with $L = 16$, and the results are averaged over 100 simulations. The simulation results are shown in Fig. 4. It shows that the performance achieved by polar codes approaches the theoretical bound as $N$ increases.

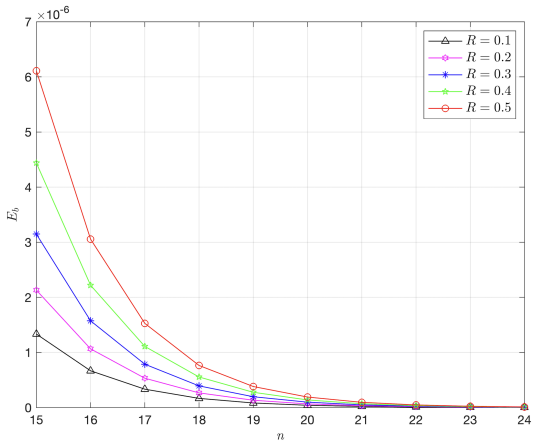



Fig. 3. $E_b$ variation with $N = 2^n$ under linear distortion profile.

### B. Robustness

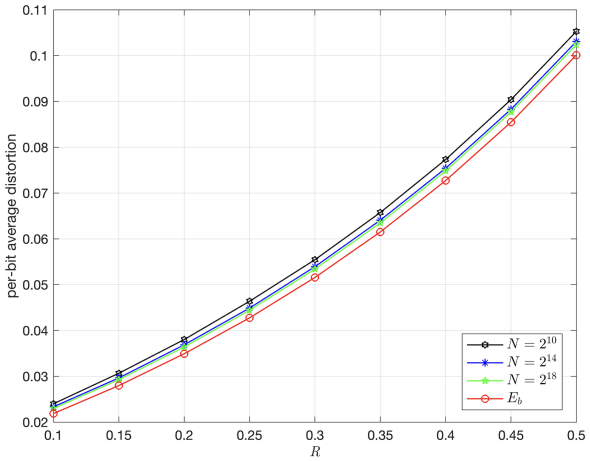
Recall that $\theta$ is the preset attack noise parameter for designing polar codes, not the actual attack noise parameter. For AM1, the actual attack noise $\widetilde{Z}_i \sim Ber(\widetilde{\theta})$, and for AM2, $\widetilde{Z}_i \sim Ber(\widetilde{\theta}_i)$, $i \in [N]$. We define the constant $R_{\theta=b} = \frac{\widetilde{\theta}_i}{\theta_i}$, where $\theta_i$ is the value determined under AM2 for $\theta = b$. The relationship between the actual noise $\widetilde{\theta}_i$ and the preset noise $\theta_i$ can be characterized as follows:

- $R_{\theta=b} < 1$: the actual noise is less than the preset noise;
- $R_{\theta=b} = 1$: the actual noise is equal to the preset noise;
- $R_{\theta=b} > 1$: the actual noise is greater than the preset noise.

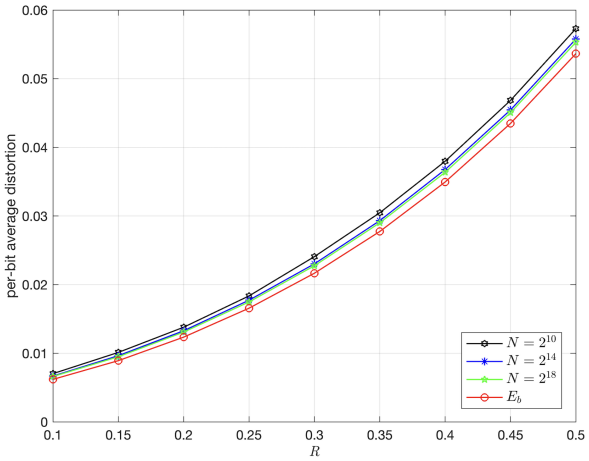
For $N = 2^{16}$ and $R = 0.1$, the simulations of our scheme using an SCL decoder with $L = 16$ are averaged over 200 runs. The simulation results are shown in Tables I and II, where '0' denotes an average bit error rate of less than $10^{-5}$. Under the constant distortion profile, AM1 and AM2 are identical, thus omitted in Table II. The adaptive steganography performs poorly across the three common distortion profiles. In contrast, our proposed pixel-sensitive and robust steganographic scheme shows improved robustness against noise attacks, with robustness increasing as the preset attack noise $\theta$ increases.

## VI. CONCLUSION

In this paper, we introduce adaptive steganographic schemes based on polar codes and present the embedding capacity-achieving theorem for the adaptive distortion. We redefine




(a) Linear distortion profile




(b) Square distortion profile

Fig. 4. Per-bit average distortion.

TABLE I
AVERAGE SECRET MESSAGE BIT ERROR RATE (AM1)

| Profiles | $\widetilde{\theta}$ | 0.001 | 0.002 | 0.004 | 0.006 |
|---|---|---|---|---|---|
| Constant | Adaptive | 0.19023 | 0.48943 | 0.49883 | 0.49962 |
| | Ours($\theta = 0.005$) | **0.00000** | 0.00062 | 0.12212 | 0.49782 |
| | Ours($\theta = 0.01$) | **0.00000** | **0.00000** | **0.00011** | **0.00123** |
| Linear | Adaptive | 0.16633 | 0.48138 | 0.49581 | 0.49888 |
| | Ours($\theta = 0.005$) | **0.00000** | 0.00017 | 0.11720 | 0.49678 |
| | Ours($\theta = 0.01$) | **0.00000** | **0.00000** | **0.00003** | **0.00041** |
| Square | Adaptive | 0.15917 | 0.48110 | 0.49573 | 0.49901 |
| | Ours($\theta = 0.005$) | **0.00000** | 0.00036 | 0.13071 | 0.49645 |
| | Ours($\theta = 0.01$) | **0.00000** | **0.00000** | **0.00003** | **0.00071** |

TABLE II
AVERAGE SECRET MESSAGE BIT ERROR RATE (AM2)

| Profiles | $R_{\theta=0.005}$ | 0.2 | 0.4 | 0.8 | 1.2 |
|---|---|---|---|---|---|
| Linear | Adaptive | 0.46863 | 0.49109 | 0.49805 | 0.49973 |
| | Ours($\theta = 0.005$) | **0.00000** | 0.00064 | 0.17693 | 0.49782 |
| | Ours($\theta = 0.01$) | **0.00000** | **0.00000** | **0.00002** | **0.00039** |
| Square | Adaptive | 0.46857 | 0.49101 | 0.49836 | 0.49964 |
| | Ours($\theta = 0.005$) | 0.00008 | 0.00058 | 0.17746 | 0.49892 |
| | Ours($\theta = 0.01$) | **0.00000** | **0.00000** | **0.00000** | **0.00044** |

the mathematical formulations of the PLS and DLS problem in robust scenarios of adaptive steganography, propose a corresponding steganographic scheme based on polar codes, and present the embedding capacity-achieving theorem in these robust scenarios. Additionally, We describe two attack models and their solutions. We show our proposed scheme can approach the theoretical bounds and demonstrate strong robustness. Furthermore, this scheme is applicable to other attack and steganographic models as well.

## APPENDIX

### A. *Proof of Theorem 1*

Prior to the proof of the theorem, essential notations must be formally defined. In the channel polarization of $(W, W, \cdots, W) \mapsto (W_N^{(1)}, W_N^{(2)}, \cdots, W_N^{(N)})$, $b_1, \cdots, b_n$ denote the $n$-bit binary expansion of $i$ and $W_{(b_1,\cdots,b_n)} \triangleq W_N^{(i)}$. Let $\{B_n : n \geq 1\}$ be a sequence of i.i.d. symmetric Bernoulli RVs defined over a probability space $(\Omega, \mathcal{F}, P)$. Let $\mathcal{F}_0 = \{\phi, \Omega\}$ denote the trivial $\sigma$-field and let $\{\mathcal{F}_n, n \geq 1\}$ denote the $\sigma$-fields generated by the RVs $(B_1, \cdots, B_n)$. Assume that $\mathcal{F}$ is such that $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}$. Let $W_0 = W$ and $\{W_n, n \geq 0\}$ denote a tree process. We are required to use the Bhattacharyya parameters random process $\{Z_n : n \geq 0\} := \{Z(W_n) : n \geq 0\}$.

*Proof.* Consider a specific channel mapping $\pi(i) = r + (t-1)N, r \in [N], t \in [J]$. The polarization of $NJ$ channels $w_1^{NJ}$ is divided into two stages. The first stage is the polarization of parallel channels. For each $t \in [J]$, the parallel polarization of $N$ channels is denoted by $(w_{1,t}, w_{2,t}, \cdots, w_{N,t}) \mapsto (W_N^{(1)}, W_N^{(2)}, \cdots, W_N^{(N)})$. The second stage is the polarization of identical channels. For each $r \in [N]$, the polarization of $J$ uses of $W_N^{(r)}$ is denoted by $(W_N^{(r)}, W_N^{(r)}, \cdots, W_N^{(r)}) \mapsto (W_{NJ}^{(1+(r-1)J)}, W_{NJ}^{(2+(r-1)J)}, \cdots, W_{NJ}^{(rJ)})$. The $NJ$ subchannels $W_{NJ}^{(i)} (i \in [NJ])$ are obtained through two-stage polarization.

For the second-stage polarization, According to [14] Theorem 3.15,

$$\lim_{J=2^j, j\to\infty} Pr(Z_{j,r} \geq 1 - 2^{-J^{\beta_r}}) = 1 - C(W_N^{(r)}),$$

where $0 < \beta_r < \frac{1}{2}, r \in [N]$ and $Z_{j,r}$ denotes the RV representing the identical channel polarization of $W_N^{(r)}$. Let

$\beta' = min(\beta_1, \cdots, \beta_N)$, then

$$\lim_{J=2^j, j\to\infty} Pr\left(Z_{nj} \geq 1 - 2^{-J^{\beta'}}\right) = 1 - \frac{1}{N}\sum_{r=1}^{N} C(W_N^{(r)}) = \frac{1}{N}\sum_{r=1}^{N} h_2(p_r),$$

where $Z_{nj}$ denotes the RV representing the channel polarization of $w_1^{NJ}$. Let $\beta = \frac{\ln J}{\ln(NJ)}\beta', 0 < \beta \leq \beta' < \frac{1}{2}$, then

$$\lim_{J=2^j, j\to\infty} Pr\left(Z_{nj} \geq 1 - 2^{-(NJ)^{\beta}}\right) = \frac{1}{N}\sum_{r=1}^{N} h_2(p_r). \quad (20)$$

According to parallel channel polarization theorem [28] Theorem 2, it is readily apparent that [14] Lemma 3.5-3.8 remain valid.

For $0 < \beta < \frac{1}{2}$ and $\delta_{NJ} = \frac{1}{2NJd_{max}} 2^{-(NJ)^{\beta}}$, $d_{max} = \max_{r\in[N], \rho_r \neq \infty} \rho_r$, Consider a polar code with frozen set $F_{NJ}$,

$$F_{NJ} = \left\{ i \in [NJ] : Z(W_{NJ}^{(i)}) \geq 1 - 2\delta_{NJ}^2 \right\}.$$

For $J$ sufficiently large there exists a $\beta' < \frac{1}{2}$ such that $2\delta_{NJ}^2 > 2^{-(NJ)^{\beta'}}$. Equation (20) implies that

$$\lim_{NJ=2^{n+j}, j\to\infty} \frac{|F_{NJ}|}{NJ} = \frac{1}{N}\sum_{r=1}^{N} h_2(p_r). \quad (21)$$

The above equation implies that for any $\epsilon > 0$ and for $J$ sufficiently large there exists a set $F_{NJ}$ such that

$$\frac{|F_{NJ}|}{NJ} \geq \frac{1}{N}\sum_{r=1}^{N} h_2(p_r) - \epsilon.$$

From [14] Lemma 3.6, we know that

$$D_{NJ}(F_{NJ}) \leq D + 2\,|F_{NJ}|\, d_{max}\delta_{NJ} \leq D + O(2^{-(NJ)^{\beta}}), \quad (22)$$

for $0 < \beta < \frac{1}{2}$. □

Recall that $D_{NJ}(F_{NJ})$ is the average of the distortion over all choices of $u_{NJ}$. Since the average distortion fulfills (22) it follows that there must be at least one choice of $u_{NJ}$ for which

$$D_{NJ}(F_{NJ}, u_{F_{NJ}}) \leq D + O(2^{-(NJ)^{\beta}}), 0 < \beta < \frac{1}{2}.$$

### *B. Proof of Theorem 2*

*Proof.* Consider a specific channel mapping $\pi(i) = r + (t-1)N$,$r \in [N]$,$t \in [J]$. We apply two-stage polarization to the $NJ$ channel $q_1^{NJ}$. For the second-stage polarization, According to [31] Theorem 1,

$$\lim_{J=2^j, j\to\infty} Pr(Z_{j,r} < 2^{-J^{\beta_r}}) = C(Q_N^{(r)}),$$

where $0 < \beta_r < \frac{1}{2}, r \in [N]$ and $Z_{j,r}$ denotes the RV representing the identical channel polarization of $Q_N^{(r)}$. Let $\beta' = min(\beta_1, \cdots, \beta_N)$, then

$$\lim_{J=2^j, j\to\infty} Pr\left(Z_{nj} < 2^{-J^{\beta'}}\right) = \frac{1}{N}\sum_{r=1}^{N} C(Q_N^{(r)}) = 1 - \frac{1}{N}\sum_{r=1}^{N} h_2(\theta_r).$$

where $Z_{nj}$ denotes the RV representing the channel polarization of $q_1^{NJ}$. Let $\beta = \frac{\ln J}{\ln(NJ)}\beta', 0 < \beta \leq \beta' < \frac{1}{2}$, then

$$\lim_{J=2^j, j\to\infty} Pr\left(Z_{nj} < 2^{-(NJ)^{\beta}}\right) = 1 - \frac{1}{N}\sum_{r=1}^{N} h_2(\theta_r)$$

and

$$\lim_{J=2^j, j\to\infty} Pr\left(Z_{nj} \geq 2^{-(NJ)^{\beta}}\right) = \frac{1}{N}\sum_{r=1}^{N} h_2(\theta_r). \quad (23)$$

Let $\epsilon > 0$ and $0 < \beta < \frac{1}{2}$ be some constants. Let $\delta_{NJ} = \frac{1}{NJ} 2^{-(NJ)^{\beta}}$. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ denote the sets

$$\mathcal{F}_1 \triangleq \left\{ i \in [NJ] : Z\left(W_{NJ}^{(i)}\right) \geq 1 - 2^{-(NJ)^{\beta}} \right\}$$
$$\mathcal{F}_2 \triangleq \left\{ i \in [NJ] : Z\left(Q_{NJ}^{(i)}\right) \geq 2^{-(NJ)^{\beta}} \right\}.$$

Equation (20) implies that for $J$ sufficiently large

$$\frac{|\mathcal{F}_1|}{NJ} \geq \frac{1}{N}\sum_{r=1}^{N} h_2(p_r) - \frac{\epsilon}{2}.$$

Similarly, equation (23) implies that for $J$ sufficiently large

$$\frac{|\mathcal{F}_2|}{NJ} \leq \frac{1}{N}\sum_{r=1}^{N} h_2(\theta_r) + \frac{\epsilon}{2}.$$

Since each pair $(W_r, Q_r)$ satisfy $0 \leq \theta_r \leq p_r \leq \frac{1}{2}$ for $r \in [N]$, we know

$$W_{NJ}^{(i)} \preccurlyeq Q_{NJ}^{(i)}, \text{ for } i \in [NJ].$$

When $J$ is sufficiently large,

$$\mathcal{F}_2 \subseteq \mathcal{F}_1.$$

Partition $[NJ]$ into $\mathcal{F} \triangleq \mathcal{F}_1 \cap \mathcal{F}_2$, $\mathcal{I} \triangleq \mathcal{F}_1 \setminus \mathcal{F}_2$, and $\mathcal{P} \triangleq \mathcal{F}_1^c$. Therefore,

$$\frac{|\mathcal{F}|}{NJ} \leq \frac{1}{N}\sum_{r=1}^{N} h_2(\theta_r) + \frac{\epsilon}{2}, \quad (24)$$

$$\frac{|\mathcal{I}|}{NJ} \geq \frac{1}{N}\sum_{r=1}^{N} h_2(p_r) - \frac{1}{N}\sum_{r=1}^{N} h_2(\theta_r) - \epsilon, \quad (25)$$

$$\frac{|\mathcal{P}|}{NJ} < 1 - \frac{1}{N}\sum_{r=1}^{N} h_2(p_r) + \frac{\epsilon}{2}. \quad (26)$$

The embedding rate is $\frac{|\mathcal{I}|}{NJ}$, satisfing (25).

For message embedding, the polar code constructed based on $\mathcal{F}_1$ and $\mathcal{I}_1 = \mathcal{F}_1^c$ is the same as that of the adaptive steganographic scheme. In conjunction with equation (22) and Lemma 1, we know

$$D_{NJ}(F_{NJ}) \leq D + 2\,|F_1|\,\delta_{NJ} \leq D + O(2^{-(NJ)^{\beta}}). \quad (27)$$

For message extraction, the polar code constructed based on $\mathcal{F}_2$ and $\mathcal{I}_2 = \mathcal{F}_2^c$ is a channel code for attack channels $q_1^{NJ}$. The block error probability satisfies

$$P_{NJ} \leq \sum_{i \in \mathcal{I}_2} Z(Q_{NJ}^{(i)}) \leq O(2^{-(NJ)^\beta}). \tag{28}$$

□

**Algorithm 1** Monte Carlo Construction

**Input:** code length $N$, information length $K$, BSCs $(W_1, W_2, \cdots, W_N)$, simulation runs $T$

**Output:** information indices set $\mathcal{A}$, frozen indices set $\mathcal{A}^c$

define $e_1^N = 0_1^N$
**for** $i = 1$ to $T$ **do**
  $u_1^N \leftarrow \text{randi}([0,1], 1, N)$
  $x_1^N = u_1^N G_N$
  generate noise $z_1^N$ from BSCs $(W_1, W_2, \cdots, W_N)$
  $y_1^N = x_1^N \oplus z_1^N$
  calculate $L_N^{(i)}\left(y_1^N, \widehat{u}_1^{i-1}\right)$ using equations (75) and (76) from [12]
  **if** $L_N^{(i)}\left(y_1^N, \widehat{u}_1^{i-1}\right) \geq 0$ **then**
    $\hat{u}_i = 0$
  **else**
    $\hat{u}_i = 1$
  **end if**
  **if** $u_i \neq \hat{u}_i$ **then**
    $e_i = e_i + 1$
    $\hat{u}_i = u_i$
  **end if**
**end for**
Sort $e_1^N$ in ascending order and store the indices in $idx_1^N$
$\mathcal{A} = idx_1^K$, $\mathcal{A}^c = idx_{K+1}^N$
**return** $(\mathcal{A}, \mathcal{A}^c)$

## REFERENCES


[1] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[2] P. Moulin and R. Koetter, "Data-hiding codes," *Proceedings of the IEEE*, vol. 93, no. 12, pp. 2083–2126, 2005.

[3] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications*. Cambridge university press, 2010.

[4] W. Mazurczyk and L. Caviglione, "Steganography in modern smartphones and mitigation techniques," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 334–357, 2014.

[5] W. Zhang and S. Li, "A coding problem in steganography," *Designs, Codes and Cryptography*, vol. 46, pp. 67–81, 2008.

[6] R. Zhang, V. Sachnev, M. B. Botnan, H. J. Kim, and J. Heo, "An efficient embedder for bch coding for steganography," *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7272–7279, 2012.

[7] I. Diop, S. Farss, K. Tall, P. Fall, M. Diouf, and A. Diop, "Adaptive steganography scheme based on ldpc codes," in *16th Int. Conf. Advanced Communication Technology*. IEEE, 2014, pp. 162–166.

[8] D. Huang, W. Luo, M. Liu, W. Tang, and J. Huang, "Steganography embedding cost learning with generative multi-adversarial network," *IEEE Trans. Inf. Forens. Security*, 2023.

[9] D. Huang, W. Luo, P. Zheng, and J. Huang, "Automatic asymmetric embedding cost learning via generative adversarial networks," in *Proc. 31st ACM Int. Conf. Multimedia*, 2023, pp. 8316–8326.

[10] X. Mo, S. Tan, W. Tang, B. Li, and J. Huang, "Reload: Using reinforcement learning to optimize asymmetric distortion for additive steganography," *IEEE Trans. Inf. Forens. Security*, vol. 18, pp. 1524–1538, 2023.

[11] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 920–935, 2011.

[12] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[13] ——, "Source polarization," in *2010 IEEE International Symposium on Information Theory*. IEEE, 2010, pp. 899–903.

[14] S. B. Korada, "Polar codes for channel and source coding," EPFL, Tech. Rep., 2009.

[15] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, 2010.

[16] B. Diouf, I. Diop, K. W. Keita, M. Diouf, S. M. Farsi, K. Tall, and O. Khouma, "Polar coding steganographic embedding using successive cancellation," in *Innovation and Interdisciplinary Solutions for Underserved Areas: 1st Int. Conf., InterSol 2017 and 6th Collogue Nat. sur la Recherche en Informatique et ses Applications, CNRIA 2017, Dakar, Senegal, April 11–12, 2017, Proc. 1*. Springer, 2018, pp. 189–201.

[17] W. Li, W. Zhang, L. Li, H. Zhou, and N. Yu, "Designing near-optimal steganographic codes in practice based on polar codes," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 3948–3962, 2020.

[18] H. Fu, X. Zhao, and X. He, "High-performance steganographic coding based on sub-polarized channel," in *Int. Workshop on Digital Watermarking*. Springer, 2022, pp. 3–19.

[19] H. Fu, Y. Cao, and X. He, "On the performance bounds of steganographic polar codes," in *2024 16th Int. Conf. Wireless Communications and Signal Processing (WCSP)*. IEEE, 2024, pp. 115–120.

[20] J. Li and L. Liu, "Robust steganography based on polar codes," in *2021 13th Int. Conf. Wireless Communications and Signal Processing (WCSP)*. IEEE, 2021, pp. 1–5.

[21] Q. Yao, K. Zeng, W. Zhang, and K. Chen, "Reliable robust adaptive steganographic coding based on nested polar codes," *IEEE Trans. Signal Process.*, 2024.

[22] T. Filler and J. Fridrich, "Using non-binary embedding operation to minimize additive distortion functions in steganography," in *2nd IEEE Int. Workshop on Information Forensics and Security*, 2010.

[23] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Trans. Inf. Forens. Security*, vol. 5, no. 4, pp. 705–720, 2010.

[24] E. Arıkan, "A performance comparison of polar codes and reed-muller codes," *IEEE Commun. Lett.*, vol. 12, no. 6, pp. 447–449, 2008.

[25] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6562–6582, 2013.

[26] A. Balatsoukas-Stimming, M. B. Parizi, and A. Burg, "Llr-based successive cancellation list decoding of polar codes," *IEEE Trans. Signal Process.*, vol. 63, no. 19, pp. 5165–5179, 2015.

[27] K. Chen, K. Niu, and J. Lin, "List successive cancellation decoding of polar codes," *Electronics letters*, vol. 48, no. 9, pp. 500–501, 2012.

[28] K. Chen, K. Niu, and J.-R. Lin, "Practical polar code construction over parallel channels," *Iet Communications*, vol. 7, no. 7, pp. 620–627, 2013.

[29] S. H. Hassani and R. Urbanke, "Universal polar codes," in *2014 IEEE Int. Symp. Information Theory*. Ieee, 2014, pp. 1451–1455.

[30] E. Şaşoğlu and L. Wang, "Universal polarization," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 2937–2946, 2016.

[31] E. Arıkan and E. Telatar, "On the rate of channel polarization," in *2009 IEEE Int. Symp. Information Theory*. IEEE, 2009, pp. 1493–1495.