Optimization of Error Pattern Embedding Steganography within Error-Correcting Code Frameworks

Yongkyu Jang*, Minglong Zhang†, Andre Kirchner†, Bryan A. Jones†, Vuk Marojevic†,
Taejoon Kim‡ and David J. Love*
*Purdue University †Mississippi State University ‡The University of Kansas
Email: {jang216, djlove}@purdue.edu, {mz354, amk694, bjones, vuk.marojevic}@msstate.edu, taejoonkim@ku.edu

***Abstract*—The importance of secure wireless communication is increasing as adversaries' eavesdropping capabilities become more advanced. In this paper, we propose a novel steganography method that utilizes error pattern embedding to minimize the likelihood of detection by eavesdroppers. Unlike existing error pattern embedding steganography, we introduce a secret codebook generation algorithm designed to maximize the secret codebook size. Our algorithm is applicable to any coding scheme that possesses a predefined maximum number of correctable errors. In addition, we propose a novel steganalysis scheme for error pattern embedding steganography. Our method is based on comparing two distinct empirical relative entropies: one derived from the empirical probability mass function (pmf) of observed transmitted signals and the other from the empirical pmf of randomly generated signals following a Bernoulli($\frac{1}{2}$) distribution. Simulation results indicate that our algorithm enhances security by effectively reducing the detection probability by the eavesdropper while simultaneously increasing the capacity for secret information.**

***Index Terms*—Steganography, Steganalysis, Error Control Coding, Secret Codeword, Secret Codebook.**

I. Introduction

Wireless networks have seen exponential growth in popularity due to the inherent accessibility provided by the broadcast nature of the wireless medium. However, this ease of reception also introduces significant security vulnerabilities. Within the range of wireless transmissions between transmitters and legitimate receivers, passive eavesdroppers can intercept signals without risk of detection [1]. To enhance security in wireless communications, the employment of cryptography and steganography stands as an effective strategy. Cryptography is the technique of securing information using mathematical concepts and rule-based calculations, ensuring that only the intended recipient can read the message. Conversely, steganography aims to conceal the very existence of the secret message within the transmitted signal, thereby preventing the eavesdropper from recognizing that a message is being sent, maintaining its confidentiality.

Information-theoretical analysis of steganography is comprehensively examined in [2]–[4]. The fundamental structure of steganography involves 'cover data' and 'stego data.' The transmitter embeds the secret message into the cover data, resulting in the stego data. The goal is to ensure that the probability distribution of the stego data closely resembles that of the cover data, making it difficult for an eavesdropper to distinguish between the two. Relative entropy, or Kullback-Leibler (KL) divergence, is commonly employed as a metric for measuring the similarity between the two probability distributions.

In practical steganography studies, images are often chosen as the cover data. The most prevalent scheme in image steganography involves embedding the secret message into the least significant bit (LSB) of each pixel data [5], [6]. Correspondingly, steganalysis techniques, which aim to detect hidden messages within given data, have been developed specifically for LSB steganography [7]–[9].

Error-correcting codes are extensively employed in steganography. These can be classified into two categories: syndrome embedding and error pattern embedding. In syndrome embedding steganography, it is assumed that the transmitter and receiver share a parity check matrix $\mathbf{H}$. The transmitter embeds secret messages by flipping the bits of the cover data so that the syndrome of each codeword conveys secret information. The Bose–Chaudhuri–Hocquenghem (BCH) code is utilized in [10], [11], with [10] focusing on minimizing the time complexity of embedding the secret message, and [11] aiming to reduce distortion in JPEG images. Filler et al. [12] proposed syndrome-trellis code steganography with a general non-binary embedding operation, presenting a near-optimal solution for minimizing additive distortion in steganography while ensuring that the time and space complexity increase linearly with the cover data size.

The utilization of error patterns in error-correcting codes for steganography has been explored in several studies [13], [14]. Reed-Solomon (RS) codes and BCH codes are employed in [13] and [14], respectively. Both studies leverage the redundant data in error-correcting codes as containers for secret messages. In [13], secret messages are embedded by flipping bits in the RS codeword, ensuring the number of flipped bits is within the error-correcting capability of the RS code. In [14],

This work is supported by the National Science Foundation (NSF) and Office of the Under Secretary of Defense (OUSD) – Research and Engineering, Grant ITE2226447, ITE2326898 and CNS2212565.

the locations for embedding secret messages are determined using a pseudo-random number generator, with a shared secret key between the transmitter and receiver. These studies assumed that nearly evenly distributed errors in the codeword due to secret message embedding will be sufficient to deceive eavesdroppers. However, they fail to present any steganalysis schemes to counteract their methodologies. Additionally, the maximum capacity of secret information per codeword is not investigated.

In this paper, we propose a method for steganography and steganalysis specifically designed for error pattern steganography. Additionally, we present an algorithm for generating a secret codebook with nearly maximum size, thereby increasing the capacity for secret information. By maximizing the size of the secret codebook, the codewords containing the embedded secret message achieve a broader dispersion within the $\{0,1\}^n$ space, where n is the codeword size. This dispersion makes it more difficult for eavesdroppers to identify the coding scheme used, thereby enhancing its confidentiality. Our simulation results demonstrate that increasing the size of the secret codebook reduces the detection probability of our steganalysis scheme. Moreover, our steganography method is flexible and can be applicable to a wide range of error-correcting codes, including RS codes and BCH codes, where the maximum correctable errors are known.

Notation: In our notation, uppercase calligraphic letters denote sets, lowercase letters represent real values, and boldface letters indicate vectors. For binary vectors $\mathbf{a}, \mathbf{b} \in \{0,1\}^n$, $\mathbf{a}+\mathbf{b}$ denotes an element-wise XOR operation. The Hamming distance between two vectors is defined as $d_H(\mathbf{a},\mathbf{b}) = \sum_{i=1}^{n} \mathbb{1}_0(a_i - b_i)$, where $\mathbb{1}_y(x) = 1$ if $x = y$, and $\mathbb{1}_y(x) = 0$ otherwise, with a_i and b_i representing the i-th entry of $\mathbf{a}$ and $\mathbf{b}$, respectively. The weight of a vector is defined as its one-norm, expressed as $\|\mathbf{a}\|_1 = d_H(\mathbf{a},\mathbf{0})$, where $\mathbf{0} \in \{0,1\}^n$ is the all-zero vector. $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. $\hat{\mathbf{a}}$ denotes the estimated vector of $\mathbf{a}$, and $\hat{a}$ denotes the estimated scalar value of a. The set of natural numbers is represented by $\mathbb{N}$. The binary random variable u follows the Bernoulli(p) distribution implies that $P(u=0) = 1-p$ and $P(u=1) = p$.

II. System model

The proposed steganographic communication system is illustrated in Fig.1. The transmitter has two encoders: the forward error correction (FEC) encoder and the secret message encoder, $f_n(\cdot)$. The normal binary source is modeled as generating a *normal binary vector* $\mathbf{x} \in \{0,1\}^k$ with each entry drawn from independently from Bernoulli($\frac{1}{2}$) distribution. Subsequently, the FEC encoder converts $\mathbf{x}$ into a *FEC codeword* $\mathbf{y} \in \{0,1\}^n$. Simultaneously, the secret message $m \in \mathcal{M} = \{1,2,...,M\}$ is encoded into a *secret codeword* $\mathbf{s}_m \in \{0,1\}^n$ by $f_n(\cdot)$. The set of all secret codewords is referred to as the secret codebook, $\mathcal{S}$. Thus, the size of the secret codebook is M, i.e. $|S| = M$, meaning $\log_2 M$ bits of secret information are conveyed per codeword. To embed the secret message into the FEC codeword, $\mathbf{s}_m$ is XORed with $\mathbf{y}$, i.e. $\mathbf{s}_m + \mathbf{y}$, and this vector is referred to as a *stealth codeword*. It should be noted that in our scheme, the error-correcting capabilities of FEC significantly affect the recovery performance of both the normal binary vector $\mathbf{x}$ and the secret message m.

The discrete memoryless channel (DMC) in Fig.1 introduces error bits $\mathbf{e} \in \{0,1\}^n$, leading to $\mathbf{r} = \mathbf{y} + \mathbf{s}_m + \mathbf{e}$ at the receiver. The FEC decoding process aims to simultaneously extract both $\mathbf{x}$ and m at the receiver. It begins immediately by FEC decoding the received signal $\mathbf{r}$, generating the estimated normal binary vector $\hat{\mathbf{x}}$. If the total error per FEC codeword, $\|\mathbf{s}_m + \mathbf{e}\|_1$, is less than or equal to the maximum correctable errors of the FEC, then $\hat{\mathbf{x}} = \mathbf{x}$, indicating successful decoding of the normal binary vector. Otherwise, a decoding failure of normal binary vector occurs, leading to the decoding failure of the secret message as well. For secret message decoding, $\hat{\mathbf{x}}$ is first FEC encoded to produce $\hat{\mathbf{y}}$, which is added with $\mathbf{r}$ to yield $\hat{\mathbf{s}}_m + \hat{\mathbf{e}}$. The secret message decoder $g_n(\cdot)$ then subsequently decodes it to generate the estimated secret message, $\hat{m}$.

Assuming the FEC decoder successfully decodes the normal binary vector, i.e., $\hat{\mathbf{x}} = \mathbf{x}$, the input to $g_n(\cdot)$ can be expressed as $\mathbf{s}_m + \mathbf{e}$. Since $g_n(\cdot)$ must accurately extract the secret message from the corrupted secret codeword $\mathbf{s}_m + \mathbf{e}$, it is essential to design the secret codeword such that it can be correctly recoverd from the channel error $\mathbf{e}$. Otherwise, the errors from the DMC will pose confusion at $g_n(\cdot)$ in distinguishing whether the observed errors originate from $\mathbf{s}_m$ or from the channel-induced errors, $\mathbf{e}$.

III. Secret message encoder/decoder design

For successful extraction of the secret message m from the corrupted secret codeword $\mathbf{s}_m + \mathbf{e}$, we develop the secret message encoder $f_n(\cdot)$, considering both the maximum correctable error bits of the FEC scheme and the upper bound of weight of $\mathbf{e}$.

Let t denote the largest number of correctable error bits per codeword, and let the weight of the channel error per stealth codeword be upper bounded with high probability, $\|\mathbf{e}\|_1 \leq \ell$, signifying that $\|\mathbf{e}\|_1$ could exceed ℓ albeit such occurrences are rare. Our objective is to devise $f_n(\cdot)$ and $g_n(\cdot)$ capable of successfully encoding and decoding secret messages under the assumption that $\|\mathbf{e}\|_1 \leq \ell$. Furthermore, we aim at maximizing the size of the secret codebook $|S|$, thereby increasing the dispersion of the stealth codeword $\mathbf{y}+\mathbf{s}_m$ in the $\{0,1\}^n$ space. This will make it more challenging for the eavesdropper to discern which error control coding method is employed at the transmitter.

1) Secret Message Encoder $f_n(\cdot)$: The generation of the secret codebook $\mathcal{S}$ can be expressed as the following optimization problem:

$$
\begin{aligned}
\text{(P1)} \quad & \underset{M \in \mathbb{N}}{\text{maximize}} \quad |\mathcal{M}| \\
& \text{subject to} \quad \|\mathbf{s}_m + \mathbf{e}\|_1 \leq t, \quad \forall m \in \mathcal{M}, && \text{(1a)} \\
& \qquad\qquad d_H(\mathbf{y}+\mathbf{s}_i, \mathbf{y}+\mathbf{s}_j) > 2\|\mathbf{e}\|_1, \\
& \qquad\qquad \forall i,j \in \mathcal{M}, i \neq j. && \text{(1b)}
\end{aligned}
$$

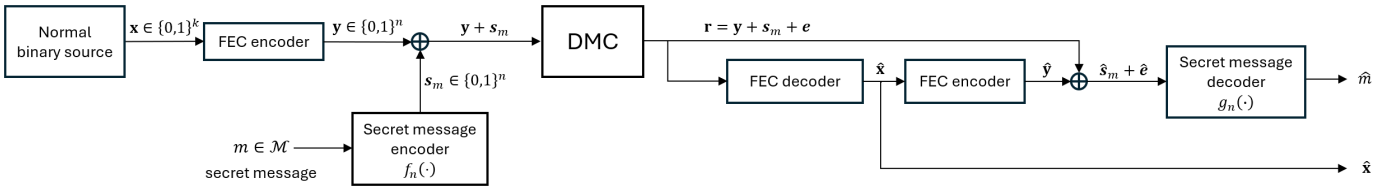

Fig. 1. Error-control code-based steganography communication system.

Successful decoding of $\mathbf{x}$ requires that the total weight of errors to the FEC codeword, i.e., $\|\mathbf{s}_m + \mathbf{e}\|_1$, is no greater than t in (1a). Furthermore, to distinguish two distinct stealth codewords conveying different secret messages, the Hamming distance between them must exceed $2\|\mathbf{e}\|_1$ in (1b). Otherwise, two distinct stealth codewords may exist within a Hamming distance of $\|\mathbf{e}\|_1$ from the received signal $\mathbf{r}$, resulting in a failure to decode the secret message. To ensure the worst-case error correction capability of $f_n(\cdot)$ and $g_n(\cdot)$, we substitute $\|\mathbf{e}\|_1$ with ℓ. Then (P1) is simplified to

$$\begin{aligned} \text{(P2)} \quad & \underset{M \in \mathbb{N}}{\text{maximize}} \quad |\mathcal{M}| \\ & \text{subject to} \quad 0 \le \|\mathbf{s}_m\|_1 \le t - \ell, \quad \forall m \in \mathcal{M}, \quad \text{(2a)} \\ & \qquad\qquad d_H(\mathbf{s}_i, \mathbf{s}_j) \ge 2l + 1, \quad \forall i, j \in \mathcal{M}, i \ne j. \\ & \qquad\qquad \text{(2b)} \end{aligned}$$

Our approach to secret codebook generation relies on the random generation of codewords that adhere to specified constraints. In each generation of a random codeword, we assess the compatibility of newly generated secret codewords by comparing them with those already present in the secret codebook S. The process for generating this secret codebook is detailed in Algorithm 1.

Although Algorithm 1 does not guarantee that S will contain the maximum feasible number of secret codewords, iterating Algorithm 1 a sufficiently large number of times can yield an S with a sufficiently large achievable secret codebook size.

2) Secret Message Decoder $g_n(\cdot)$: Given that we have already devised the secret codewords to adhere to the constraint $d(\mathbf{s}_i, \mathbf{s}_j) \ge 2\ell + 1$, we can employ a minimum distance decoder as the secret message decoder. The pseudocode for the minimum distance decoder for secret messages is outlined in Algorithm 2.

IV. Threat Model

To quantitatively evaluate our steganography method, we propose a novel steganalysis scheme specifically designed for error pattern steganography. Since relative entropy, $D(p\|q)$, also known as KL divergence, represents the statistical distance between two probability distribution, it is widely used for steganography in many other studies [2], [4], [15]–[17]. However, in our system, conventional steganalysis schemes applied to the distribution of individual bits result in poor performance. This is because, for most linear block codes, the occurrence of 0's and 1's is statistically equi-probable. Consequently, it becomes challenging for an eavesdropper to distinguish between random bit streams and error control

Algorithm 1: Generation of secret codebook $\mathcal{S}$

Input : n - codeword length, t - maximum correctable error bits per codeword, ℓ - maximum channel error bits per codeword
Output: $\mathcal{S}$ - secret codebook
▷ sc_weight: weight of a newly generated secret codeword
▷ sc_new: newly generated secret codeword

$\mathcal{S} \leftarrow \emptyset$;
sc_weight $\leftarrow$ randomly pick one from $\{0, 1, \cdots, t - \ell\}$;
sc_new $\leftarrow$ length n binary vector where total sc_weight 1's are located randomly with 0's elsewhere;
$\mathcal{S} \leftarrow \mathcal{S} \cup \{\text{sc\_new}\}$;
for *n=1:sufficiently large number of iteration* **do**
  sc_weight $\leftarrow$ randomly pick one from $\{0, 1, \cdots, t - \ell\}$;
  sc_new $\leftarrow$ length n binary vector where total scWeight 1's are located randomly with 0's elsewhere;
  if *sc_new satisfies minimum Hamming distance constraint for current* $\mathcal{S}$ **then**
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{\text{sc\_new}\}$;
  else
    discard sc_new;
  end
end

Algorithm 2: Pseudo code 2 - Secret message decoder $g_n(\cdot)$

Input : $\mathbf{s}_m + \mathbf{e}$, $\mathcal{S}$ - Secret codebook
Output: $\hat{m}$ - decoded secret message

for *i=1:*$|\mathcal{S}|$ **do**
  temp$\leftarrow \mathbf{s}_m + \mathbf{e} + \mathbf{s}_i$
  $P(i) \leftarrow$ sum of all elements in temp. ; `// Find the Hamming distance between` $\mathbf{s}_m + \mathbf{e}$ `and` $\mathbf{s}_i$.
end
if *the minimum element in* P *is unique* **then**
  $\hat{m} \leftarrow$ index of the minimum element in P;
else
  decoding error occurs;
end

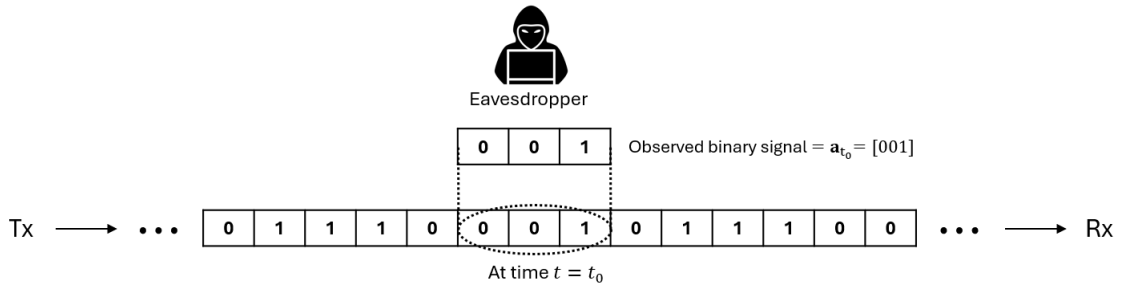

Fig. 2. The threat model of eavesdropper when the window size is $w = 3$.

codes. In our study, we propose a more sophisticated threat model to enable the eavesdropper to differentiate between random binary data and codewords.

As illustrated in Fig.2, we place the eavesdropper in a scenario where it observes transmitted bits with specific window sizes, denoted by w. Let $\mathbf{a}_t$ be a random observed binary signal at time $t \in \mathbb{N}$ with a window size w. The total number of observations at the eavesdropper is denoted by obs_{num}. The number of events that the observation matches to $\mathbf{u} \in \{0,1\}^w$ is given by $\sum_{t=1}^{obs_{\text{num}}} \mathbb{1}_{\mathbf{a}_t}\mathbf{u}$. Thus, the empirical probability mass function (pmf) of the observed vectors from the transmitted signals is defined as $p(\mathbf{u}) = \frac{\sum_{t=1}^{obs_{\text{num}}} \mathbb{1}_{\mathbf{a}_t}\mathbf{u}}{obs_{\text{num}}}, \quad \forall \mathbf{u} \in \{0,1\}^w$. We denote q as the theoretical pmf of $\mathbf{u}$ where every component independently follows the Bernoulli($\frac{1}{2}$) distribution, i.e., $q(\mathbf{u}) = \left(\frac{1}{2}\right)^w, \quad \forall \mathbf{u} \in \{0,1\}^w$.

After a total of obs_{num} binary observations, each with a length w, the eavesdropper calculates the relative entropy between $p(\mathbf{u})$ and $q(\mathbf{u})$ which is denoted as A:

$$\begin{aligned} A &= D(p(\mathbf{u})\|q(\mathbf{u})), \\ &= \sum_{\mathbf{u}\in\{0,1\}^w} p(\mathbf{u}) \log \frac{p(\mathbf{u})}{q(\mathbf{u})}, \\ &= \sum_{\mathbf{u}\in\{0,1\}^w} p(\mathbf{u}) \log \left(p(\mathbf{u})2^w\right). \end{aligned} \tag{3}$$

Thus, the value of A varies depending on the realizations of the transmitted signals of a total number of bits $obs_{\text{num}} \times w$.

Prior to the observation of the transmitted signals, the eavesdropper generates total $obs_{\text{num}} \times w$ bits, where each bit independently follows the Bernoulli($\frac{1}{2}$) distribution. Similarly in the Fig.2, the eavesdropper observes the generated signal with window size w. Let $\mathbf{b}_t \in \{0,1\}^w$ be a random observed binary vector at time t for $1 \le t \le obs_{\text{num}}$. The count of events where $\mathbf{b}_t$ matches $\mathbf{u} \in \{0,1\}^w$ is given by $\sum_{t=1}^{obs_{\text{num}}} \mathbb{1}_{\mathbf{b}_t}\mathbf{u}$. Consequently, the empirical pmf of $\mathbf{b}_t$, referred to as the empirical Bernoulli pmf, is defined as $p_{\text{EB}}(\mathbf{u}) = \frac{\sum_{t=1}^{obs_{\text{num}}} \mathbb{1}_{\mathbf{b}_t}\mathbf{u}}{obs_{\text{num}}}, \quad \forall \mathbf{u} \in \{0,1\}^w$.

Therefore, the $p_{\text{EB}}(\mathbf{u})$ value depends on the specific generation of random $obs_{\text{num}} \times w$ bits, but is independent of the transmitted signals. Subsequently, the eavesdropper finds the relative entropy between $p_{\text{EB}}(\mathbf{u})$ and $q(\mathbf{u})$, which is denoted as B:

$$\begin{aligned} B &= D(p_{\text{EB}}(\mathbf{u})\|q(\mathbf{u})), \\ &= \sum_{\mathbf{u}\in\{0,1\}^w} p_{\text{EB}}(\mathbf{u}) \log \frac{p_{\text{EB}}(\mathbf{u})}{q(\mathbf{u})}, \\ &= \sum_{\mathbf{u}\in\{0,1\}^w} p_{\text{EB}}(\mathbf{u}) \log \left(p_{\text{EB}}(\mathbf{u})2^w\right). \end{aligned} \tag{4}$$

Readily, the eavesdropper conducts a hypothesis test, with the null hypothesis H_0 suggesting that the observed signals are derived from a Bernoulli($\frac{1}{2}$) distribution. Conversely, the alternative hypothesis H_1 represents that the signals have undergone alterations, raising suspicions of potential inclusion of a concealed message. The determination of H_0 and H_1 depends on the threshold value of γ according to

$$|A - B| \underset{H_0}{\overset{H_1}{\gtrless}} \gamma. \tag{5}$$

One could have query regarding why we do not simply set a steganalysis metric as $A = D(p(\mathbf{u})\|q(\mathbf{u}))$ and perform the hypothesis test $A \underset{H_0}{\overset{H_1}{\gtrless}} \epsilon$. This approach appears plausible since a smaller value of A suggests that p is statistically closer to q. However, the value of A alone is not a stable metric for determining whether the transmitted signal follows a Bernoulli($\frac{1}{2}$) distribution. Assume each bit of the transmitted signals independently follows a Bernoulli ($\frac{1}{2}$) distribution, but obs_{num} is not sufficiently large for a fixed window size w. Due to these restricted observations, the observed vectors $\mathbf{a}_t$, for $1 \le t \le obs_{\text{num}}$, are unlikely to be evenly distributed over the $\{0,1\}^w$ space, causing the A value to be larger. Consequently, when obtaining the A value from a transmitted signal with an unknown distribution, it is challenging to discern whether the modified FEC code or the observation constraints primarily affect A. This ambiguity complicates setting the threshold value ϵ. To mitigate this issue, we compare A and B. Note that A is equivalent to B when each bit of the transmitted signal independently follows a Bernoulli($\frac{1}{2}$) distribution. The difference between A and B, i.e., $|A-B|$, effectively removes the influence of restricted observations at the eavesdropper from A.

Assuming that the prior probabilities of H_0 and H_1 are equal, i.e., $P(H_0) = P(H_1) = \frac{1}{2}$, the decision error probability at the eavesdropper is given by $P_{error} =$

$P(H_0)P(H_1|H_0) + P(H_1)P(H_0|H_1) = \frac{1}{2}[P_{FA} + P_{MD}]$, where $P_{FA} = P(H_1|H_0)$ stands for false alarm probability and $P_{MD}P(H_0|H_1)$ stands for mis-detection probability.

By computing the values of A and B over m iterations using different observed data, we can obtain a distribution of A and B. In this context, we assume the eavesdropper can select the optimal threshold γ' to minimize the decision error probability, P_{error}, based on the decision rule $D(p(\mathbf{u})\|q(\mathbf{u})) \gtrless_{H_0}^{H_1} \gamma'$. Conversely, the transmitter's objective is to maximize P_{error}.

Eve's overall performance will vary depending on the window size w and the number of observation obs_{num}. We could expect that when w is substantially smaller than the codeword length n, there will be a very small difference between A and B, making it almost impossible to differentiate them. When w equals n, then it is much more likely to differentiate between A and B. The simulation outcomes are detailed in the subsequent section.

V. Simulation

The Bose–Chaudhuri–Hocquenghem (BCH) code is used as an error control code in our stealth communication simulation. Thus, the *BCH codeword* can be regarded as a specific instance of the FEC codeword. We set the codeword length $n = 31$, and input data length $k = 11$. Then, the maximum correctable error bits per codeword is $t = 5$. We set the stealth codeword can correct an error per codeword, so the secret codebook is generated based on the following optimization problem:

$$\text{(P3)} \quad \underset{M\in\mathbb{N}}{\text{maximize}} \quad |\mathcal{M}|$$
$$\text{subject to} \quad 0 \le \|\mathbf{s}_m\|_1 \le 4, \quad \forall m \in \mathcal{M} \tag{6a}$$
$$d(\mathbf{s}_i, \mathbf{s}_j) \ge 3, \quad \forall i, j \in \mathcal{M}, i \ne j. \tag{6b}$$

Throughout the experimentation, we generated a secret codebook of size 981 using Algorithm 1, indicating that approximately 9.938 bits of secret information are conveyed per codeword ($\log_2 981 \simeq 9.938$).

To investigate the impact of observation window size w on relative entropy, we varied the window size from 1 to 32 while maintaining a fixed total observed bit count of $31 \times 2^{15} = 1,015,805$ bits. The selection of observation bit count was empirically determined to ensure minimal variation in relative entropy across different realizations of transmitted signals. Any remaining bits beyond the observed $\lfloor \frac{1015805}{w} \rfloor$ vectors were discarded, as their effect on relative entropy values was found to be negligible. We compared the relative entropy, $D(p(\mathbf{u})\|q(\mathbf{u}))$, for different types of observed signals.

1) A_1: This indicates the relative entropy value in (3) when the transmitted signals are concatenated BCH codewords. These transmitted signals do not contain any secret information.

2) A_2, A_3, A_4, A_5: These represent the relative entropy values in (3) for transmitted signals that are concatenated stealth codewords. However, the stealth codewords corresponding to each A_i for $i = 2, 3, 4, 5$ utilize different size of the secret codebook. The size of the secrete codebook is determined by the formula $\lfloor 981 \times \frac{x}{100} \rfloor$ for $x = 1, 5, 30, 100$, respectively.

3) B_1: This indicates the relative entropy value in (4) when each bit of the generated signals independently follows a Bernoulli($\frac{1}{2}$) distribution.

Fig.3 presents a comparative analysis of A_1, A_2, A_3, A_4, A_5 and B_1 for varying window sizes. Additionally, Table I provides the exact values of the differences between A_i and B_1 for the selected window sizes.

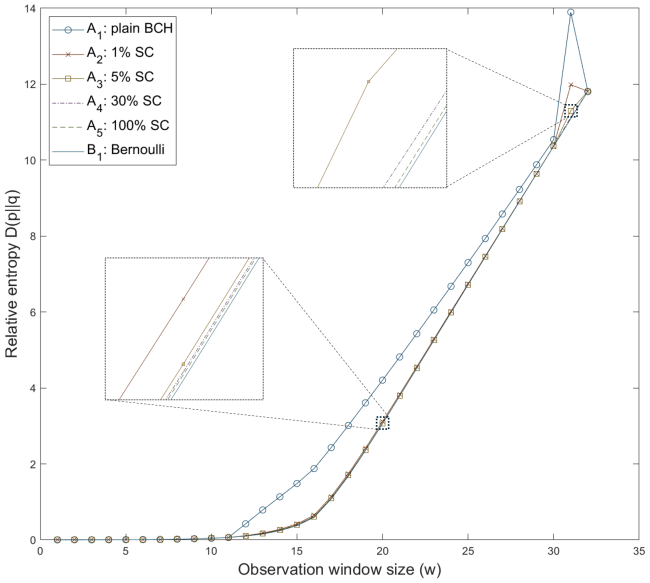

Fig. 3. The relative entropy values for different types of transmitted signals across various observation window sizes are shown. Enlarged images are provided for window sizes around $w = 20$ and $w = 31$.

$\lvert A_i - B_1 \rvert$ for $i = 1, ..., 5$						
i	$w = 15$	$w = 20$	$w = 25$	$w = 30$	$w = 31$	$w = 32$
1	1.1111	1.1452	0.5853	0.1748	**2.8046**	0.0100
2	0.0497	0.0561	0.0255	0.0068	**0.8948**	0.0035
3	0.0226	0.0112	0.0031	0.0010	**0.2092**	7.9e-04
4	0.0221	0.0057	9.4e-04	2.2e-04	**0.0360**	4.3e-05
5	0.0148	0.0036	4.1e-04	1.6e-04	**0.0103**	8.7e-05

TABLE I
Difference between A_i and B_1 for different window sizes.

The curves in Fig.3 demonstrate consistent values of the relative entropies for window sizes ranging from 1 to 11. However, for the window sizes between 11 and 29, a noticeable deviation is observed in A_1 compared to other values, while A_2, A_3, A_4, A_5 and B_1 exhibit similar distances. This suggests that within the window size ranging from 11 to 29, the eavesdropper can readily identify plain BCH codewords from the Bernoulli($\frac{1}{2}$) distribution given a sufficient number of observed bits, but can struggle to distinguish the stealth codeword from the Bernoulli($\frac{1}{2}$) distribution. Notably, for the window size $w = 31$, which matches the codeword size $n = 31$, the difference between A_1 and B_1 is significant compared to other window sizes. Additionally, the values of $|A_i - B_1|$ for $i = 2, 3, 4, 5$ are relatively large. As i increases, or equivalently, as the secret codebook size increases, $|A_i - B_1|$ becomes smaller, making it more challenging for the eavesdropper to differentiate the signals. This phenomenon occurs

because the embedded secret codewords effectively disperse the distribution of plain BCH codewords across the entire $\{0,1\}^n$ space. For window sizes $w = 30$ and 32, all A_i values closely align with B_1. This likely arises from the significant least common multiple of w and n, where the observation window size introduces greater randomness to the observed vectors.

Now, we analyze the worst-case scenario where $w = n$ under the constraint of limited observation bits. Due to the high precision achieved by eavesdroppers with sufficiently large observations in distinguishing between Bernoulli($\frac{1}{2}$) signals and those that have undergone alterations, we limit the number of observation windows to $obs_{\text{num}} = 512$ for the calculation of the relative entropy value A_i. Consequently, the eavesdropper observes a total of $w \times obs_{\text{num}} = 115,872$ bits to calculate each A_i. We conducted tests on 50 different realizations for each A_i and B_1. The simulation results are depicted in Fig.4.

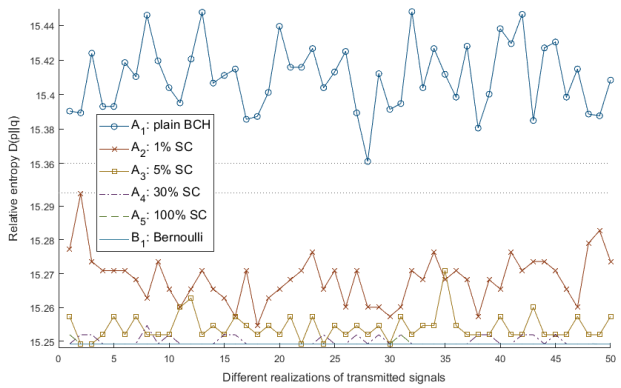

Fig. 4. Relative entropy values under $w = 31$ and $obs_{\text{num}} = 512$.

	Optimal γ'	P_{FA}	P_{MD}	P_{error}
A_1	15.28	0	0	0
A_2	15.2517	0	0	0
A_3	15.2506	0	0.1	0.05
A_4	15.2506	0	0.7	0.35
A_5	15.2506	0	0.96	0.485

TABLE II
OPTIMAL THRESHOLD VALUE γ' AND MINIMUM ERROR PROBABILITY AT THE EAVESDROPPER.

Based on our simulations, $B_1 = 15.2492$ for all 50 different realizations. Since all A_i values are greater than or equal to B_1, the eavesdropper can appropriately choose a threshold value γ' to achieve $P_{FA} = 0$ while minimizing P_{error}. The optimal threshold value γ' and the minimum error probability P_{error} for different types of transmitted signals A_i are summarized in Table II. It is observed that as the secret codebook size increases, the eavesdropper's decision error probability also increases. Therefore, it can be concluded that the transmitter can effectively reduces the detection probability by increasing the secret codebook size.

VI. CONCLUSION

In this paper, we proposed a novel error-pattern embedding steganography method and its corresponding steganalysis approach. The proposed secret codebook generation algorithm meets the necessary constraints for correct recovery at the receiver while ensuring a sufficiently large secret codebook size. Under the observation data constraints faced by the eavesdropper, we demonstrated that increasing the secret codebook size effectively reduces the detection probability by the eavesdropper.

REFERENCES

[1] E. Ruzomberka, D. J. Love, C. G. Brinton, A. Gupta, C.-C. Wang, and H. V. Poor, "Challenges and Opportunities for Beyond-5G Wireless Security," *IEEE Security Privacy*, vol. 21, no. 5, pp. 55–66, 2023.

[2] C. Cachin, "An information-theoretic model for steganography," in *International Workshop on Information Hiding*. Springer, 1998, pp. 306–318.

[3] T. Mittelholzer, "An information-theoretic approach to steganography and watermarking," in *International Workshop on Information Hiding*. Springer, 1999, pp. 1–16.

[4] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2706–2722, 2008.

[5] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits," in *2006 1st International Conference on Digital Information Management*, 2007, pp. 173–178.

[6] V. L. Reddy, A. Subramanyam, and P. C. Reddy, "Implementation of LSB steganography and its evaluation for various file formats," *Int. J. Advanced Networking and Applications*, vol. 2, no. 05, pp. 868–872, 2011.

[7] A. D. Ker, "Improved detection of LSB steganography in grayscale images," in *International workshop on information hiding*. Springer, 2004, pp. 97–115.

[8] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proceedings of the 2001 workshop on Multimedia and security: new challenges*, 2001, pp. 27–30.

[9] T. Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference image histogram," in *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03).*, vol. 3. IEEE, 2003, pp. III–545.

[10] R. Zhang, V. Sachnev, and H. J. Kim, "Fast BCH syndrome coding for steganography," in *Information Hiding: 11th International Workshop, IH 2009, Darmstadt, Germany, June 8-10, 2009, Revised Selected Papers 11*. Springer, 2009, pp. 48–58.

[11] V. Sachnev, H. J. Kim, and R. Zhang, "Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding," in *Proceedings of the 11th ACM Workshop on Multimedia and Security*, 2009, pp. 131–140.

[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, pp. 920–935, 2011.

[13] F. R. Ishengoma, "The art of data hiding with reed-solomon error correcting codes," *arXiv preprint arXiv:1411.4790*, 2014.

[14] E. Medvedeva, I. Trubin, and E. Blinov, "Steganography method in error-correcting codes," in *2022 24th International Conference on Digital Signal Processing and its Applications (DSPA)*. IEEE, 2022, pp. 1–4.

[15] K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Provably Secure Steganography: Achieving Zero K-L Divergence using Statistical Restoration," in *2006 International Conference on Image Processing*, 2006, pp. 125–128.

[16] J. Fridrich and J. Kodovský, "Multivariate gaussian model for designing additive distortion for steganography," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 2949–2953.

[17] P. Schöttle and R. Böhme, "Game Theory and Adaptive Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 760–773, 2016.