Multiple Codebook Information Hiding

H. T. Sencar  
Electrical and Computer Engineering Department  
New Jersey Institute of Technology  
University Heights, Newark, NJ  
07102-1982  
e-mail: taha.sencar@njit.edu

M. Ramkumar  
AVWAY.COM Inc.  
IDT Corporation  
520 Broad Street, Newark, NJ  
07102  
e-mail: ramkumar@corp.idt.net

A. N. Akansu  
Electrical and Computer Engineering Department  
New Jersey Institute of Technology & NJCMR  
University Heights, Newark, NJ  
07102-1982  
e-mail: ali@megahertz.njit.edu

Abstract — We present a new embedding methodology for data hiding applications by employing multiple codebooks for embedding the watermark signal. The use of multiple codebooks offers a freedom in the choice of the codeword that is more "friendly" with the host signal for a particular message to be conveyed. In the proposed scheme, embedder searches among a set of unitary transformations of the cover signal that maximizes the correlation between the embedded and detected watermark signals at a fixed embedding distortion. The transform bases set is known to the embedder and detector while particular transform basis used for embedding is not revealed to the detector. We also derive the closed form expressions for the upper bound on the probability of error in detecting the wrong watermark signal for both single and multiple codebook cases. Simulation results show that hiding rate is improved with the use of multiple codebooks.

I. INTRODUCTION

Extensive availability of multimedia data and advanced processing tools brought data hiding applications into the realm of content providers and researchers to improve the tractability of their digital media assets. These concerns mainly evolved around issues like copyright protection and content authentication. Common to all of these motives is the likely presence of intruders willing to modify contents that has undergone such a processing with the intention of nullifying aforementioned efforts. Information hiding (Data hiding) solutions promise to address some of these concerns.

Gelfand et al. in [1] derived the capacity of a discrete memoryless channel with side information at the encoder such that at any transmission time encoder has the whole channel state information for all times. Their works have become a cornerstone for oblivious data hiding applications. Later research gained a considerable momentum by reinterpreting side information as the multimedia content that carries hidden information. Costa [2], was the first to present an information-theoretic analysis of the problem that applies to oblivious data hiding. He also proved that the capacity of the Gaussian channel is the same whether the side information is known to the decoder or not by using the results of [1] for iid Gaussian distributed cover-signal and side information.

In Ref. [3], Moulin et al. gave complementary analysis for hiding capacity considering all aspects of data hiding within a game theoretic perspective. That study also highlights some design criteria for practical systems. Cohen et al. [4] present a detailed discussion and results of hiding capacity assuming a Gaussian distributed cover-signal and squared error distortion.

Although fundamental limits of hiding rate are known for additive white Gaussian noise (AWGN) attack and mean squared error distortion measure, practical algorithms that achieve these limits are not well established yet. Costa in [2] outlined an encoder decoder structure that achieves the capacity by utilizing a codebook, although it was far beyond being practical. Ramkumar et al. [5], Eggers et al. [6] and Chen et al. [7] proposed schemes that are similar in principle and have better robustness vs. rate trade offs than the conventional data hiding methods.

Assuming a fixed distortion measure that is in compliance with the perceptual properties of the cover-signal, information hider has two degrees of freedom to improve hiding rate vs. robustness characteristics. These are of designing the codebooks and the embedder-detector set that utilizes them. In this paper, we investigate multiple codebook embedding technique. The use of multiple codebooks provides with the choice of the codebook that has favorable distortion properties. In general, embedders are nonlinear functions. Consequently, codewords from different codebooks corresponding to the same message may have different embedding distortions. In a typical application, embedding distortion is limited by some fixed value derived from the distortion measure, and the hider uses all available resources in order to increase the robustness. In other words, at the same level of embedding distortion, a message may be represented by codewords with different strengths and correspondingly different detection statistics. Embedder picks the codeword that is expected to yield highest correlation at the detector at a fixed embedding distortion. Each codebook is assumed to be generated through a unitary transformation of the cover-signal. We show that for AWGN channel, Gaussian distributed cover-signal and squared error distortion measure, the increase in probability of error due to use of multiple codebooks is compensated by an exponential reduction (in probability of error) due to the embedder’s ability to adapt the codeword to the cover-signal. We derived closed form expressions for the upper bound on the probability of error in terms of the number of codebooks and codeword size. The embedder described in Ref. [5] is incorporated with the proposed methodology. However, the concept is applicable to a wide range of embedders.

In the text, we denote vectors with boldfaced characters, random variables with capital letters and their realizations with the corresponding lower case letters. In the next section
we present details of the data hiding model used. We describe
the data hiding scheme in Section III and derive performance
analysis methodology for the one codebook and multiple code-
book embedding in the Section IV. Performance results are
presented in Section V.

II. DATA HIDING MODEL
In a generic data hiding application a message indexed by m,
from an alphabet $\mathcal{M}$, $1 \leq m \leq M$, is mapped out to a se-
quence $W \in \mathbb{R}^N$. Sequence $W$ (watermark signal) must be
embedded into the cover-signal, $S$, without any perceptual
distortion. Embedder, $E$, modifies signal $S$ with respect to
$W$ within some distortion constraint and generates the stego-
signal (watermarked signal) $\hat{S}$. The difference signal, $X$, be-
 tween $S$ and $\hat{S}$ is the embedding distortion corresponding to
message $m$, $X = \hat{S} - S$. Detector, $D$, extracts signal $\hat{W}$ from
$\hat{S}$ or from an “attacked” version $Y$ of $\hat{S}$. Signals $S$, $W$, $X$, $\hat{S}$, $Y$, and $\hat{W}$ are generalized to be vectors of length $N$. Em-
bedder and detector may be scalar or vector operations that
operate on these vectors based on the choice of designer.

By multiple codebook embedding we assume the presence of
$L$ number of $N \times N$ unitary transform bases at the embedder
and detector

$$I = T_i^T T_i, \quad i = 1, \ldots, L,$$  \hfill (1)

where $I$ is the identity matrix and $^T$ is the matrix transpose
operation. One selection criterion for $T_i$, $i = 1, \ldots, L$, is that
all transformations of a vector are maximally separated to
each other in $\mathbb{R}^N$ with respect to a pre-designated distance
measure. Among $L$ possible transformations of $S_i = T_i S$, $i = 1, \ldots, L$, let $k, 1 \leq k \leq L$ represent the index of transform
basis which will be used for embedding. Uninformed of partic-
ular $T_k$ used for embedding, detector generates $L$ transforms of
signal $Y$ and extracts message in a blind manner.

One consequence of using multiple codebooks is that embed-
ning is not strictly a scalar operation because for a message $m$ to
be conveyed choice of $T_k$ determines signal vector $\hat{S}_k$.

The overall information hiding system in an additive channel
model is outlined below

$$W : m \rightarrow W, \quad \hat{S}_k = E(T_k S, W) = \hat{S}_k + \hat{X}_k, \quad Y = T_k^T (E(T_k S, W)) + Z = S + X_k + Z, \quad \hat{W}_i = D(T_i^T Y), \quad i = 1, \ldots, L$$  \hfill (2)

where $m \in \mathcal{M}$ is the index of the hidden message, $X = X_k$ is
the distortion introduced by the embedder for the chosen trans-
f ormation basis $T_k$, and $Z$ is the intrusion of the attacker.
$W$ is a one to one mapping from $m$ to $W$ which transforms
message $m$ into a better representation for embedding. The
embedder, $E$, and the detector, $D$, may be linear or nonlinear
and not necessarily invertible functions ($D(E(S, W)) \neq W$).

Not evident in the model is the distortion constraints im-
p osed on information hider and attacker. We assume mean
squared error distance as the measure of distortions intro-
duced by information hider and attacker. Although power of a
difference signal is not a true distance in perceptual sense, it
may be deployed in accordance with the findings of multimedia
compression methods due to the ease in analytical tractability.
Imposing restrictions on the distortions introduced by the
information hider and attacker, such that these distortions have
much less power than the cover signal $S (\frac{1}{N} \sum_{j=1}^{j=N} X_j^2 \ll
\frac{1}{N} \sum_{j=1}^{j=N} X_j^2 \ll \frac{1}{N} \sum_{j=1}^{j=N} Y_j^2)$, will keep the
original content more or less intact and simplify the problem.

Analysis of data hiding rate is developed by projecting the
early theoretical studies in channel communication with side
information. Gelfand et. al [1] considered a discrete memory-
less channel with an input alphabet $X$ and output alphabet
$Y$, both of which depend on a given side information from
a finite set $S$ where $X, Y, S, \in \mathbb{R}^N$. Channel capacity is ex-
pressed in terms of random variables $X \in X, Y \in Y, S \in S$ and
an additional auxiliary random variable $U \in U$, $U$ being a
finite alphabet in $\mathbb{R}^N$, given the conditional joint probability
density $p(u, x|z)$ as

$$R = \max_{p(u|x)} (I(U; Y) - I(U, S)).$$ \hfill (3)

Costa in Ref. [2] had a design of $U = X + \alpha S$ by assuming
codewords satisfying the power constraint $\frac{1}{N} \sum_{j=1}^{j=N} X_j^2 \leq P$
and independent random variables $X, S, Z$ with probability
distribution functions $X \sim \mathcal{N}(0, P)$, $S \sim \mathcal{N}(0, \sigma^2_S)$,
$Z \sim \mathcal{N}(0, \sigma^2_Z)$, respectively. He showed that by setting
$\alpha = \frac{P}{\sigma^2_S}$ the optimal codebook that achieves the capa-
city $C = \frac{1}{2} \log_2 (1 + P/\sigma^2_Z)$ is designed. This is the capacity
of AWGN channel where $S$ is known to both encoder and decoder.

In data hiding applications, channel is unpredictably non-
linear. Practically, it is impossible to model the channel con-
sidering the vast variety of attack scenarios and their com-
binations, [8]. As discussed in [3] and [4] assuming indepen-
dent Gaussian distributed cover signal and codeword white
Gaussian noise is the optimal attack. These assumptions
provide means for characterizing hiding rate vs. robustness
features of a method. In the rest of the analysis all intru-
sions of the attacker to watermarked signal is represented by
AWGN. Corresponding hiding rates can be computed assuming
an $Mary$ symmetric channel with transition probabilities
$p(j|m) = 1 - P_\epsilon$ for $j = m$ and $p(j|m) = \frac{P_\epsilon}{2 - P_\epsilon}$ for $j \neq m$.

III. EMBEDDER

Data hiding methods may be categorized into three main types
based on how $(E, D)$ are designed. Type-I methods are very
common and simple to implement. Basically, stego-signal is
generated by adding the watermark signal or a non-uniform
scaled version of it to the cover signal. These methods suffer
from dramatically low hiding rates because of the non-optimal
design which assumes $S$ as a noise and tries to cancel it. Type-
I methods are preferable only when the attack is too severe.
However, they are ideal only for applications for which the
cover-signal is present at the detector.

Type-II methods are characterized by the use of quantizer
structures in the embedding and detection, [9], [10], [11]. Un-
like Type-I methods, watermark signal has restricted values
and detection is a many to one mapping such that stego-signal
values apart from each other at certain amounts have the same
detected value with respect to a periodic pattern. The distor-
tion, $X$, is a function of $S$ and $W$. Also, the embedder, $E$,
and detector, $D$, are inverses of each other. Disadvantage is
that the system performs well only if the attack is not se-
vere. These can also be employed with oblivious data hiding
systems at considerable hiding rates.

Type-I and Type-II methods are equivalent to designs of
$U = X$, $\alpha = 0$ and $U = X + \alpha S$, $\alpha = 1$, respectively. These
two choices of $U$ correspond to two extremes in hiding rate
vs. robustness curves. Within the context of data hiding this fact may be restated as Type-I and Type-II methods having preferable performances at “severe attack” and “no attack” cases. An optimal design is the one that designer has control over the operating characteristics of the method. In Refs. [5, 6, 7] modifications to the Type-II methods are proposed by removing the invertibility condition on the set ($E, D$). In Type-III methods added non-invertibility is designed in a particular way that hiding rate is maximized for a presumed attack level. Type-III methods utilize the design $U = X + \alpha S$, $0 < \alpha < 1$ which gives information hides a freedom to adapt the codeword to the channel. Type-III data hiding is optimal for oblivious data hiding applications.

The embedder being utilized by the data hiding technique is a quantizer characterized by a pair of parameters, period $\Delta$ and threshold $\beta$ where $0 < \beta \leq \Delta$. The form of quantizer used for implementation is a periodic continuous triangular function. Watermark signal values are limited by the peak values of the periodic function. Embedding is a translation of the input coefficient values by introducing distortions thresholded to $\pm \frac{\beta}{2}$ such that the mapping of embedded coefficient over the periodic function has a minimum Euclidean distance to the watermark signal. The period $\Delta$ and threshold $\beta$ of the quantizer are dictated by the preassigned embedding distortion, above which perceptual features of the cover signal will be considered changed. Among the $\Delta$, $\beta$ pairs that meet the distortion constraint, the one that maximizes hiding rate for a presumed distortion amount is picked. Detection of the watermark signal is similar to embedding. The stego-signal is mapped over the periodic function with the same $\Delta$ as used for embedding and with the fixed threshold $\beta = \Delta$, which adds non-invertibility to the $E, D$ set.

Figure 1 represents embedding of two different watermark signal coefficients, $x_0$ and $x_1$, to signal coefficient $s$. Embedding $x_0$ into $s$ generates the stego-signal $s_0$. Whereas, embedding $x_1$ into $s$ generates $s_\beta$ rather than $s_1$ due to thresholding by $\pm \frac{\beta}{2}$.

As $\Delta \to \infty$, for some finite $\beta$, hiding rate vs. robustness characteristics of this scheme gets similar to Type-I methods. When $\Delta = \beta$, this scheme becomes a Type-II method. For all other fractions of $\frac{\beta}{2}$, scheme performance is optimal for different attack powers. The distortion $X_\beta$ introduced by this embedder is a non-linear function of $S$ and $W$, $X = \mathcal{E}(S, W) - S$. However, it is statistics can be computed given the probability distributions of $S$ and $W$. Similarly, the statistics of the distortion $X_\beta$ on $X$ as a consequence of the un invertibility condition introduced by the Type-III method, due to thresholding $X$ by $\beta < \Delta$, can be computed.

IV. Multiple Codebooks

A codebook is the collection of sequences, codewords, each of which is generated through an intelligent combination of the cover-signal $S$ and watermark-signal $W$ corresponding to one of the $M$ possible messages (i.e. information of $\log_2 M$ bits to be conveyed.) Every codeword is required to comply with a perceptual distortion constraint. Ultimately, embedder generates the codebook for a fixed cover signal and a presumed attack level. Then, it picks the codeword that is pointed by the message index $m$ (i.e. decimal number that $\log_2 M$ bit sequence corresponds to) which is consequently delivered to the channel by adding it to $S$. Detector’s function is to decode the message $m$ which might be distorted intentionally or unintentionally.

Use of multiple codebook helps embedder by assuming a number of possible sequences all of which satisfy the power constraint. In other words, employing multiple codebooks correspond to a simplified way of generating $U$ sequences for practical applications where number of sequences in each bin (as described within random coding argument) is increased by the number of codebooks.

In a multiple codebook embedding each codebook is generated with a particular unitary transformation of the cover signal for the same message set. The embedder that makes use of $L$ codebooks embeds sequence $W_m$, corresponding to message $m$ with $L$ transformations of the cover signal, $S_i = T_i S$ for $i = 1, \ldots, L$, consecutively. Then, it decides on the transform basis $T_k$, $1 \leq k \leq L$ that maximizes the detection statistics. The codeword corresponding to the transform basis $T_k$, $X_k = \mathcal{E}(T_k S, W_m) - S_k$, is transmitted after backward transformation $\hat{S} = T_k^{-1} (X_k + S_k)$. Detector extracts $\hat{W} = D(\hat{T} Y)$ for all $k$ values, $1 \leq k \leq L$, from the received signal $Y$.

In a practical method, watermark signal detection is followed by matching the extracted signal to one of the known watermark signals in order to decide on the sent message. Given that the detector has no knowledge of the internal processing of the channel, use of normalized correlation is a practical approach but non-optimal. Normalized correlation is a similarity measure between two vectors which can be geometrically interpreted as the cosine of the angle between the vectors. Thus, detector computes the normalized correlation between the extracted vector $\hat{W}$ and all $W$ sequences corresponding to $M$ messages, and the message that yields the highest normalized correlation is defined as the sent message.

The embedder can decide on the transform basis $T_k$, $1 \leq k \leq L$, for embedding in two ways. In the first one, sequence $W_m$ is embedded into $S_i$, $i=1, \ldots, L$, based on the minimum distortion criterion. The index that yields the smallest distortion, $k = \arg \min \{d_i \}$, $i = 1, \ldots, L$ where $d_i = \frac{1}{2} \sum_{j=1}^{N} (X_{ij} - \hat{X}_{ij})^2$, is chosen as the index of the transform basis, $T_k$. Alternately, the embedder can use normalized correlation as the decision metric to choose the transform basis, maximum correlation criterion. In general, the amount of distortion that can be introduced to $S$ is limited. In this case, for each $S_i$, embedding parameters are chosen such that the resulting embedding distortion, $P_e$, is the same. Since the embedding and detection functions are not the inverses of each other, the embedded watermark signal $W_m$ and the detected watermark signal $\hat{W}_m$ are not the same. The embedder picks the transform basis $T_k$ that yields the highest correlation between $W_m$ and $\hat{W}_m$ at the embedder, $k = \arg \max \{\rho_i \}$, $i = 1, \ldots, L$ where $\rho_i = \frac{W_m^T \hat{W}_m}{|W_m||\hat{W}_m|}$. In this paper we use the
signal than the extracted signal \( \hat{W}_i \) will also have a zero covariance matrix with \( W_j \). Random variable \( \rho_{ij} \) can be generalized to,

\[
\rho_{ij} \sim \begin{cases} 
N(0, \frac{1}{N}), & 1 \leq i, j \leq M \text{ if } i \neq j \\
N(m_{p_{\text{dep}}}, \sigma^2_{\text{dep}}), & 1 \leq i, j \leq M \text{ if } i = j,
\end{cases}
\]

(8)

where \( m_{p_{\text{dep}}} \) and \( \sigma^2_{\text{dep}} \) can be computed given the statistics of \( X, X_1 \), and \( Z \).

In the rest of the analysis we will drop the first sub-script of \( \rho_{ij} \) and assume \( m \) is the index of the sent message for all cases. Eq. (7) can be rewritten using Eq. (8),

\[
P^{\text{err}} \leq \sum_{j=1}^{M} \int_{-\infty}^{\infty} f_{\rho_j}(\rho_j \geq p_{m,j}) f_{p_m}(p_m) dp_j dp_m,
\]

(9)

Inner integral in Eq. (9) can be expressed in terms of Gaussian Q function \( Q(x) = \frac{1}{\sqrt{2\pi}} \int_{x}^{\infty} e^{-t^2/2} dt \). Additionally, since statistics of \( p_j \) is independent of the index \( j \) for \( j \neq m \), sum operator in Eq. (9) can be dropped and it simplifies to

\[
P^{\text{err}} \leq (M - 1) \int_{-\infty}^{\infty} Q(p_j, \sqrt{N}) f_{p_m}(p_m) dp_m.
\]

(10)

IV. II Probability of Error for Multiple Codebook embedding

When \( L \) codebooks are used for embedding, one of the watermark signals \( \{W_1, \ldots, W_M\} \) is embeded in one of the \( L \) transformations of the cover signal \( S_i = T_i S, 1 \leq i \leq L \). We will use the super-script \( ^i \) to denote the transform basis \( T_i \) used for embedding and detection.

The embedder will decide on the transform basis \( T_i \), \( 1 \leq i \leq L \), based on the correlation between the embedded watermark signal \( W_{i,m} \) and detected watermark signal \( \hat{W}_m \) at the embedder. Since embedder-detector set is not invertible in the watermark signal \( W_{i,m} \) even in the absence of channel noise detected \( W_{i,m} \) will be different from \( W_{i,m} \), due to thresholding noise \( X_i, D(E(S_i, W_{i,m})) \neq W_{i,m} \). Among the watermark signals \( \{W_{1,m}, \ldots, W_{M,m}\} \) the one that yields the highest correlation, \( \max[p_{\text{m},1}, \ldots, p_{\text{m},M}] \), will be embedded where \( \rho_{\text{m},j} \) is the normalized correlation between \( W_{i,m} \) and \( W_{i,m} \). Accordingly, the index for transform basis is set by the index of the highest correlation, \( \arg \max_i \{\rho_{\text{m},i}\}, i = 1, \ldots, L \).

Assuming \( \hat{W}_{\text{m}} \) is the sent signal embedded using basis \( T_m \), the detector will extract the watermark signals \( \{\hat{W}_{1,m}, \ldots, \hat{W}_{M,m}\} \) from the \( L \) back transformations of the received signal, \( Y_i = T_i^T Y, 1 \leq i \leq L \). Let \( \rho_{\text{m},j} \) represent the normalized correlation between the signal \( W_{i,m} \) embedded into \( S_i \) and the signal \( \hat{W}_{i,m} \) detected form \( Y_i \). Among all indices \( i, j \), that maximize \( \rho_{\text{m},j} \) for \( 1 \leq j \leq M \) and \( 1 \leq i \leq L \), \( j \) is the detected message \( m, \hat{m} = \arg \max_i \max_j \{p_{\text{m},j}\}, 1 \leq j \leq M \) and \( 1 \leq i \leq L \).

Probability of error for multiple codebook embedding, \( P^{\text{err}} \), is due to any of the normalized correlation values \( \rho_{\text{m},j} \), \( 1 \leq j \leq M, j \neq m \) and \( 1 \leq i \leq L \) being greater than \( \rho_{\text{m},m} = \max[p_{\text{m},m}, \ldots, p_{\text{m},M}] \). Compared to the one codebook case, probability of error is expected to increase with the number of codebooks because there are \( L \) times more normalized...
correlation values that can exceed \( \rho_{m_2} \). Defining \( \hat{\rho}_{m,j} \) as the normalized correlation between the received watermark signal \( \hat{W}^i_m \) generated using \( T_i \) and the signal \( W_j \) than an event \( E_j \) that detector will prefer \( m \) to \( m \) as the detected message is denoted as (similar to Eq. \( (4) \))

\[
E_j^i = \{ \rho_{m,j} \geq \rho_{m_2} \}, \quad i = 1, \ldots, L, \quad j = 1, \ldots, M \text{ and } j \neq m. 
\]

The event \( E_j^m \) that detector makes an error is

\[
E_j^m = \bigcup_{i=1}^{L} \bigcup_{j'=1}^{M} \bigcup_{j \neq m} E_j^i. 
\]  

(11)

Hence, the probability of detecting a wrong message is obtained as

\[
P_e^m = Pr\{E^m\} = \sum_{i=1}^{L} \sum_{j=1}^{M} \sum_{j \neq m} Pr\{E_j^i\}. 
\]

(13)

The advantage of multiple codebook embedding stems from the difference in the distributions of the random variables \( \rho_{m,m} \) and \( \rho_{m_2} \) (in Eq. \( (7) \) and Eq. \( (14) \), respectively).

The distributions of \( \rho_{m,j} \) for \( 1 \leq j \leq M \) and \( 1 \leq j \leq L \), assuming message \( m \) is embedded using transform \( T_k \), is shown as

\[
\rho_{m,j} \sim \begin{cases} 
N(0, \frac{1}{L}), & 1 \leq j \leq M \text{ if } i \neq k; \\
N(0, \frac{1}{M}), & 1 \leq j \leq M \text{ if } i = k \text{ and } j \neq m; \\
N(m_{dep}, \sigma^2_{dep}), & 1 \leq j \leq M \text{ if } i = k \text{ and } j = m.
\end{cases}
\]

The probability density function of the r.v. \( \rho_{m_2} \) is determined using,

\[
\rho_{m_2} = \max\{\rho_{m,j} \mid 1 \leq j \leq L\},
\]

(15)

where \( \rho_{m,j} \) are iid Gaussian distributed random variables, \( \rho_{m,j} \sim N(m_{dep}, \sigma^2_{dep}) \).

The probability of error for multiple codebooks given in Eq. \( (14) \) can be rewritten using the above results by dropping the first subscript referring to sent message \( m \),

\[
P_e^m = \sum_{i=1}^{L} \sum_{j=1}^{M} \sum_{j \neq m} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{\rho_{j}^i}(\rho_j^i \geq \rho_{m_2}) f_{\rho_{m_2}}(\rho_{m_2}) \]

\[
d\rho_j^i d\rho_{m_2}.
\]

(16)

where \( \rho_j^i \sim N(0, \frac{1}{L}) \). Since the inner integral in Eq. \( (16) \) is the Gaussian Q function and does not depend on the index \( j \), Eq. \( (16) \) can be simplified to

\[
P_e^m \leq L(M - 1) \int_{-\infty}^{\infty} Q(\rho_j^i \rho_{m_2} \sqrt{N}) f_{\rho_{m_2}}(\rho_{m_2}) d\rho_{m_2}.
\]

(17)

V. RESULTS

Figures 3, 4 and 5 display the union bound on the probability of error vs. robustness computed by numerically solving Eq. \( (10) \) and \( (17) \) for various codebook numbers and sizes of \( M \times N \). The corresponding robustness measure \( R = \frac{\sigma^2_{ede}}{\sigma^2_{e}} \) is the ratio of the embedding distortion power to the channel noise distortion power. However, an exact comparison of single and multiple codebook embedding schemes is not possible for the actual probability of errors, results indicate that the upper bound on probability of error decreases exponentially to zero for multiple codebook embedding scheme.

We implemented multiple codebook embedding by designing a set of transform bases \( T_1, \ldots, T_L \), using Givens rotations. Givens rotations provide orthogonal transformations in \( \mathbb{R}^{N \times N} \) that rotates each vector with a fixed angle. A particular transform basis \( T_k \) is obtained by the consecutive multiplication of \( N(N-1)/2 \) number of orthogonal matrices all with determinant 1 so that resulting \( T_k \) is unitary. Each orthogonal matrix is derived from the identity matrix by introducing cos \( \theta_k \) terms at \( (i, i) \) and \( (j, j) \) locations with \( \sin \theta_k \) and \( -\sin \theta_k \) terms at \( (i, j) \) and \( (j, i) \) locations in order to rotate \( (i, j) \) coordinate plane with the designated angle \( \theta_k \). Rotation angles \( \theta_k \), \( k = 1, \ldots, L \), can be chosen by uniformly sampling \( 2\pi \) for maximum separation, before embedding. Setting watermark signal size to \( N \) and number of messages to \( M \), the size of the codebooks that will be utilized by embedder is fixed to \( M \times N \) where \( M = 2N \).

We fixed the embedding distortion \( P_e \) and optimized the embedding parameter \( \Delta \) for each \( R = \frac{P_e}{2\sigma^2} \) value. The latter is also revealed to the detector. With proper selection of \( \beta \) value, \( P_e \) is adjusted to the designated distortion amount. We assumed the cover signal \( S \) and channel noise \( Z \) are iid zero mean Gaussian vectors with variances \( \sigma^2_S \) and \( \sigma^2_Z \), respectively, satisfying \( \sigma^2_S \gg P_e \) and \( \sigma^2_Z \gg P_e \). \sigma^2_2.

The simulations are done by embedding and detecting randomly chosen messages with the use of different number of codebooks \( L \). The embedder chooses the message \( m \), \( 1 \leq m \leq M \) and embeds the corresponding \( W_m \) vector of length \( N \) to the cover-signal \( S \). Signal \( S \) is passed through AWGN channel with noise variance selected in way that \( R = \frac{P_e}{2\sigma^2} \) is satisfied for a range of \( R \) values. The detector extracts the signal \( \hat{W}_m \) and uses normalized correlation to match it to message \( m \). If the extracted message \( \hat{m} \) at the detector is same with \( m \), it’s called a success and otherwise an error. Resultant probability of success values are used to compute the hiding rate of the system within an Mary symmetrical channel assumption.

We performed embedding with up to 14 codebooks and codebook sizes of \( 32 \times 64, 64 \times 128, 128 \times 256 \). Results are evaluated within \( 0.1 \leq R \leq 0.8 \) range of embedding power to noise power ratios. Figures 6 and 7 display the probability of success and corresponding hiding rates for \( L = 4 \) and varying \( N \) values. The increase in the watermark signal size \( N \) improves the detection statistics because normalized correlation gives more reliable results with the larger signal sizes. Figures 8 and 9 display the probability of success and corresponding hiding rates for \( N = 128 \) and \( L = 1, 3, 5, 14 \).
Figure 3: Multiple codebook embedding and detection, N=64 and M=128.

Figure 4: Multiple codebook embedding and detection, N=1280 and M=2560.

Figure 5: Multiple codebook embedding and detection, N=8192m and M=16384.

Figure 6: Probability of success performance for 4-codebook embedding and detection for various watermark signal sizes of N = 32, 64, 128.

Figure 7: Data hiding rates for 4-codebook embedding and detection for various watermark signal sizes of N = 32, 64, 128.

Figure 8: Probability of success performance for multiple codebook embedding and detection, L = 1, 3, 5, 14 and N = 128.

Figure 9: Data hiding rates for multiple codebook embedding and detection for L = 1, 3, 5, 14 and N = 128.

It is observed that for the data hiding scheme described in Section III, as the ratio of $\frac{P_e}{2}$ changes in between 0.1 and 0.8 multiple codebook embedding has higher hiding rates. However, the concept is trivially applicable to all Type-III data hiding schemes.

REFERENCES


