A HOST REJECTED SPREAD SPECTRUM EMBEDDING SCHEME FOR DATA HIDING

Amir Valizadeh and Z. Jane Wang

Department of Electrical and Computer Engineering
University of British Columbia
Canada

ABSTRACT
In this paper, a new spread spectrum-based embedding modulation approach, which we call host rejected spread spectrum (HRSS), is presented to efficiently remove the noise-source effect of the host signal in decoding the hidden message bits. The proposed HRSS could improve the decoding performance in terms of bit error rate. To further improve the decoding performance of the HRSS under distortions (which can be modeled as additive noise), an improved host rejected spread spectrum (IHRSS) is introduced. Simulation results demonstrate the superior performances of the proposed embedding schemes for data hiding.

Index Terms— Data hiding, watermarking, spread spectrum, information embedding.

1. INTRODUCTION
There has been an increasing use of digital multimedia during the last years. This explosion of using digital media is mostly due to the easy access to the Internet. However, this easy use of digital media also leads to copyright violation, unauthorized manipulation, malicious tampering, and thus poses additional challenges on intellectual property protection. One popular, promising way to address such challenges is watermarking. It is defined as embedding information into the digital media without significantly degrading the perceptual quality of the original digital content.

Depending on the specific application purposes, there are two main types of watermark-extraction problems at the receiver side: watermark decoding and watermark detection. In the first case, hidden information is embedded into the host content to communicate a specific message and such hidden message needs to be extracted accurately. For example, the hidden information can be a serial of binary identification numbers used for video distribution. The procedure of decoding the embedded bit information for extracting the hidden message is referred as watermark decoding. In the second case, a watermark is inserted into the host data and the detector only needs to verify whether a specific embedded water-

mark is present or not. For instance, a watermark representing the copyright information can be embedded into the media content and its presence should be verified by the detector. This verification procedure is called watermark detection. Since we are particularly interested in communicating hidden message, we focus on watermark decoding in this paper.

In [1] Cox et al. proposed the spread spectrum (SS) watermarking scheme, which is probably the most popular embedding scheme used today. In this scheme, the bits composing the message are modulated by a sequence and then added to the original host signal. This scheme was shown to be robust against distortions since the watermark signal is spread over a large number of host coefficients. Although SS watermarking has a simple embedding structure, the host signal usually is treated as a noise source at the decoder and consequently the decoding error is not zero even in the absence of noise/distortion. Quantization based schemes, which exploit the information of the host signal at the encoder, were proposed based on the Costa’s dirty paper code idea [2] to achieve high capacity watermarking. Scalar Costa scheme (SCS) [3] and quantization index modulation (QIM) [4] are example schemes in this group for watermarking. Among different embedding schemes, spread spectrum is still of great interest because of its robustness against the attacks and its simple embedding structure which can be extended to incorporate the human visual system (HVS) characteristics into embedding to achieve better imperceptibility [5]. However, one important challenge is how we can improve the traditional SS embedding to minimize the bit error rate in decoding.

In this paper, to reduce the source effect of the host signal in the traditional SS, we propose a host rejected scheme for spread spectrum watermarking, namely host rejected spread spectrum (HRSS). We demonstrate the interference effect of the host signal could be removed completely for watermark decoding in the noiseless (distortion less) cases. However, it could lead to high distortion. A modified version of HRSS, the improved host rejected spread spectrum (IHRSS), is presented to make a trade off between distortion and robustness. We show that IHRSS could improve both the channel capacity and watermark decoding performance in terms of bit error rate. Finally, simulations are carried out to demonstrate the performances of the proposed embedding schemes.

This work was supported by a SPG grant from the Natural Sciences and Engineering Research Council of Canada (NSERC).
2. PROPOSED EMBEDDING SCHEME AND ITS PERFORMANCE

A basic SS-based embedding for data hiding can be generally expressed as

\[
r = x + Ab \tag{1}
\]

where \(b\) represents the bit to be transmitted, \(s\) represents the watermark sequence, \(A\) declares the bit amplitude, and \(r\) represents the watermarked signal. For simplicity, the original host signal \(x = [x_1, x_2, ..., x_N]^T\) is generally assumed to have uncorrelated samples from Gaussian random process with zero mean and variance of \(\{\sigma_{n_i}^2\}\). The distortion \(D\) due to embedding is defined as \(D = E[|r - x|^2]\). Having introduced the distortion \(D\), the ratio of the host signal variance to the distortion \(D\) leads to the document to watermark ratio (DWR) as follows

\[
\text{DWR} = 10 \log \left( \frac{E[x^T x]}{D} \right) \tag{2}
\]

In the case of having additional noise/distortion due to attacks, which is represented by the noise vector \(n\) with coefficients of variance \(\sigma_{v_i}^2\), we can also define the watermark to noise ratio (WNR) as \(\text{WNR} = 10 \log \left( \frac{D}{\sigma_{v_i}^2} \right)\).

The basic idea of the proposed host rejected spread spectrum is that, by using the predetermined index knowledge of the disjoint pairs \(\{i_1, j_1\}\) from the host signal \(x\), we can enhance decoding performance by performing pair-wise embedding to compensate for the signal interference. The information embedding procedure of HRSS is as follows. First, \(M\) disjoint pairs of coefficients are pre-selected out of the \(N\) coefficients in \(x\). We denote the set \(\{I, J\}\) to denote the indices of the \(M\) pair coefficients, e.g. \(\{I(1), J(1)\}\) denotes the indices of the first pair coefficients. In HRSS embedding, the pair \((x_{I(i)}, x_{J(i)})\), for \(i = 1, ..., M\), is changed to the watermarked pair \((r_{I(i)}, r_{J(i)})\) as follows

\[
\begin{align*}
    r_{I(i)} &= x_{I(i)} + s_i Ab, \\
    r_{J(i)} &= x_{I(i)},
\end{align*}
\]

where \(s_i \in \{\pm 1\}\) represents the \(i\)th element of the signature code \(s\), and \(b \in \{\pm 1\}\) is the bit information embedded into the host signal. Using signature code could increase the security and also make the system capable of multi-message embedding. Due to space limit, we do not include the case of multi-message embedding in this paper. The distortion to the host signal pair \((x_{I(i)}, x_{J(i)})\) due to HRSS embedding defined in (3) can be calculated as

\[
D_P = E\{(r_{I(i)} - x_{I(i)})^2\} + E\{(r_{J(i)} - x_{J(i)})^2\} = A^2 + \sigma_{x_{I(i)}}^2 + \sigma_{x_{J(i)}}^2 \tag{4}
\]

by assuming the independence among \(x_i\)’s. When \(M\) pairs of coefficients are utilized for embedding, the overall distortion can be derived as

\[
D = A^2 M + \sum_{k \in I, J} \sigma_{x_k}^2. \tag{5}
\]

For the sake of simplicity, we assume that the \(M\) pair coefficients have the same variance \(\sigma_{x_k}^2\). Therefore, for a fixed distortion \(D\) and bit amplitude \(A\), the number of pairs \(M\) can be calculated as

\[
M = \left\lfloor \frac{D}{2 \sigma_{v_i}^2 + A^2} \right\rfloor \tag{6}
\]

where the \(\lfloor \cdot \rfloor\) operation rounds to the nearest integer value. Obviously, \(M\) should be greater than one, i.e. \(M \geq 1\). It could be shown that the maximum document to watermark ratio (DWR\(_{\text{max}}\)) achievable by the proposed embedding is

\[
\text{DWR}_{\text{max}} = \frac{\sigma_{x_i}^2}{A^2 + 2 \sigma_{v_i}^2}. \tag{7}
\]

Eqn. (7) suggests that selecting the pairs with lower power for information embedding could increase the maximum value of DWR. Furthermore, Eqn. (5) indicates that the major part of distortion is due to the power of the \(M\) pair coefficients selected for embedding. In practice, pre-determining the set \(\{I, J\}\) can be a challenging task since the watermarked signal should meet the imperceptibility requirement of embedding. The better choice of the set \(\{I, J\}\) leads to a better trade off between decoding and imperceptibility. We are currently working at this direction.

At the receiver side, a decoder is developed to extract the embedded information bit by using the \(M\) pairs of coefficients conveying the hidden bit. First, based on the watermarked signal \(r\), we define the signal \(y\) as the following form

\[
y = r_I - r_J = sAb \tag{8}
\]

where the vectors \(r_I = [r_{I(1)}, r_{I(2)}, ..., r_{I(M)}]^T\), \(r_J = [r_{J(1)}, r_{J(2)}, ..., r_{J(M)}]^T\), and \(s = [s_1, s_2, ..., s_M]^T\). Based on Eqn. (8), it is clear that the optimal decoder is the simple correlator defined as

\[
\hat{b} = \text{sign}(s^T y). \tag{9}
\]

From the expression (8) and the decoder (9), we can see that the HRSS is capable of completely removing the host signal as source of interference and leads to the zero error probability in the absence of additional noise/distortion.

However, in practical cases, the received watermarked signal \(r\) can be manipulated due to intentional and unintentional attacks and distortions. This can be modeled as that the received signal is corrupted by the noise. Therefore, the signal model at the receiver side could be generally represented as

\[
\begin{align*}
    \tilde{r}_{I(i)} &= x_{I(i)} + s_i Ab + n_{1i}, \\
    \tilde{r}_{J(i)} &= x_{J(i)} + n_{2i},
\end{align*}
\]

where
for \( i = 1, \ldots, M \), where \( n_{1i} \) and \( n_{2i} \) represent the additive noises added to the \( i \)-th-pair signals. For simplicity, it is assumed that the noise samples are independent and drawn from a Gaussian distribution with zero mean and variance \( \sigma^2_n \). In order to improve the decoding performance of the HRSS and also compensate the effects of the additive noises \( n_{1i} \)'s and \( n_{2i} \)'s, here we propose an improved HRSS (IHRSS) embedding scheme for data hiding. The IHRSS embedding model is defined by a slight modification as

\[
\begin{align*}
r_I(i) &= x_I(i) + s_i Ab, \\
r_J(i) &= x_J(i) + \alpha (x_I(i) - x_J(i)),
\end{align*}
\]

for \( i = 1, \ldots, M \), where \( \alpha \) is the improved factor determined at the encoder side. At the receiver side, with additive noise, the general received signal model can be expressed as

\[
\begin{align*}
\bar{r}_I(i) &= x_I(i) + s_i Ab + n_{1i}, \\
\bar{r}_J(i) &= x_J(i) + \alpha (x_I(i) - x_J(i)) + n_{2i}.
\end{align*}
\]

Let denote \( n_1 \) and \( n_2 \) as the noise vectors with length \( M \), representing respectively the additive noise in the first and second elements of the \( M \) pair bit-information-conveying coefficients. We also denote \( v_1 = [x_{I(1)}, \ldots, x_{I(M)}]^T \) and \( v_2 = [x_{J(1)}, \ldots, x_{J(M)}]^T \), representing the original \( M \) pair coefficients used for information embedding.

To decode the embedded bit information at the receiver, we define the signal \( y \), which is obtained as

\[
y = \bar{r}_I - \bar{r}_J = (1 - \alpha) (v_1 - v_2) + s Ab + n_1 - n_2
\]

where \( \bar{r}_I \) and \( \bar{r}_J \) together represent the received \( M \) pair signals. The optimal decoder for extracting the hidden bit information \( \hat{b} \) is the maximum likelihood (ML) decoder. With the assumption of independent and identical distributed (IID) samples for \( n_1, n_2, v_1 \) and \( v_2 \), the ML decoder is obtained as the correlator (match filter) in the form of \( \hat{b} = \text{sign}(s^T y) \).

At the encoding design stage, we need to determine the value of the improved factor \( \alpha \). We want to choose \( \alpha \) to minimize the decoding error. To achieve this optimum value of \( \alpha \), equivalently the signal to interference plus noise ratio (SINR) should be maximized. Using (13) and the decoder structure (9), the SINR could be expressed in the following form

\[
\text{SINR} = \frac{A^2 M}{2(1 - \alpha)^2 \sigma^2_n + 2 \sigma^2_n}.
\]

According to the IHRSS embedding scheme in (11), it is straightforward to show that the overall distortion due to IHRSS embedding is

\[
D = A^2 M + 2 \alpha^2 \sigma^2_v M.
\]

It leads to the SINR expression as follows

\[
\text{SINR} = \frac{D - 2 \alpha^2 \sigma^2_v M}{2(1 - \alpha)^2 \sigma^2_n + 2 \sigma^2_n}.
\]

Maximizing the SINR leads to the optimum value of the improved factor \( \alpha \) as

\[
\alpha = \frac{2M \sigma^2_n + 2M \sigma^2_v + D}{4M \sigma^2_v} - \sqrt{(2M \sigma^2_v + 2M \sigma^2_n + D)^2 - 8MD \sigma^2_v}. \tag{17}
\]

Therefore, the improved factor \( \alpha \) is determined first at the encoder ans as will be shown in the next section, the IHRSS could achieve a better performance than SS scheme.

3. CHANNEL CAPACITY OF THE IHRSS

The maximum possible host payload in bits that allows the recovery of information with small error is obtained by Shannon capacity, denoted as \( C = \max_I I(b; y) \). Here, \( I(b; y) \) declares the mutual information about the input variable \( b \) by the received vector \( y \) and \( f \) denotes the probability density function of the input variable. For Gaussian-distributed host signal \( x \) and average distortion \( D \), considering the received signal model (13), the capacity can be expressed as

\[
C = \frac{1}{2} \log_2 \det(I_M + \frac{A^2 ss^T}{2 \sigma^2_n + 2(1 - \alpha)^2 \sigma^2_v}). \tag{18}
\]

This capacity result is based on the assumption of IID samples for \( v_1 \) and \( v_2 \) with variance \( \sigma^2_v \). As an alternative way to determine the improved factor \( \alpha \), we could find the optimum value of \( \alpha \) by maximizing the capacity. Since \( \log(\cdot) \) is a strictly monotonic increasing function, we have the following maximization

\[
\alpha_{\text{opt}} = \arg \max_\alpha \det(I_M + \frac{A^2 ss^T}{2 \sigma^2_n + 2(1 - \alpha)^2 \sigma^2_v}). \tag{19}
\]

Using the Sylvester’s determinant theorem, we can simplify (19) to the following form

\[
\alpha_{\text{opt}} = \arg \max_\alpha (\frac{A^2 M}{2 \sigma^2_n + 2(1 - \alpha)^2 \sigma^2_v}). \tag{20}
\]

Comparing (20) with (14), we can see that maximizing the channel capacity leads to the same solution of the optimal value of \( \alpha \) as in (17). Therfore, it could be concluded that the optimal value of the improved factor minimizes the probability of error and maximizes the channel (13) capacity at the same time.

4. SIMULATION RESULTS

In order to demonstrate the decoding performances of the proposed IHRSS embedding scheme in comparison with the traditional SS watermarking, for data hiding, the bit error rate (BER), i.e. \( P_c = Pr\{\hat{b} \neq b\} \) where \( \hat{b} \) is the estimated bit,
Fig. 1. The left figure is the original “Boat” image and the right figure is the watermarked image with DWR=30dB.

Fig. 2. The plots of bit error rate versus DWR for SS and IHRSS embedding schemes where WNR=15dB.

Fig. 3. The plots of channel capacity versus DWR for SS and IHRSS embedding schemes where WNR=15dB.

5. CONCLUSION

In this paper, we proposed a host rejected spread spectrum scheme for information embedding. We showed that the HRSS is able to yield zero probability of error for the ideal noiseless case, even though leads to higher distortion. We also presented a modified version of HRSS to make a trade off between the robustness and decoding performance in data hiding. Moreover, the channel capacity for the proposed watermarking schemes were derived and it was shown that the IHRSS has higher capacity than the SS. The simulation results based on real images illustrated the good decoding performances of the proposed information embedding scheme.

6. REFERENCES


