AN IMPROVED SPREAD SPECTRUM TECHNIQUE FOR ROBUST WATERMARKING

Henrique S. Malvar and Dinei A. Florêncio

Microsoft Research
One Microsoft Way, Redmond, WA 98052

ABSTRACT

This paper introduces a new watermarking modulation technique, which we call improved spread spectrum (ISS). Unlike in traditional spread spectrum (SS), in ISS the carrier signal does not act as a noise source, leading significant performance gains. In typical examples, the gain of ISS over SS is 20 dB or more in signal-to-noise ratio or 20 orders of magnitude or more in error probability. The proposed method achieves roughly the same noise robustness gain as quantization index modulation (QIM). Nevertheless, while QIM is quite sensitive to amplitude variations, ISS is as robust in practice as traditional SS.

1. INTRODUCTION

With the widespread use of digital representation for images, video, audio and other signals, copyright protection by using digital watermarks became an active area of research. Watermarking in this new context is a complex problem, with issues that also involve system design, cryptography, and a series of economic and legal aspects. While we do appreciate the complexity of the problem, in this paper we will only deal with a specific aspect of the problem: that of "hiding" or transmitting information embedded in a signal (i.e., watermark modulation).

In most watermarking schemes, spread spectrum (SS) is the modulation technique used to embed the watermark [1–3]. In this case, the signal to be marked (the carrier signal) acts as a source of interference [1,4]. Because the carrier signal itself is generally much stronger than other interferences, its interference dominates the performance of watermark detection.

In [5], Chen and Wornell proposed a new embedding method, called quantization index modulation (QIM), which eliminates the interference from the carrier signal. However, QIM obtains its gains from embedding the watermark in a lattice, making the watermark sensitive to scaling of the signal. Change in the scale of the watermarked signal, such as dynamic range equalization typically used by radio stations, can effectively erase the watermark. Therefore, QIM may not be applicable to watermarking signals in scenarios where a malicious attack can take place.

In [4], Cox et al. present a framework where they indicate the need for removing the influence of the signal in the watermark detection process. Three different practical solutions based on that framework have been proposed [7]. Nevertheless, they do not handle the most important case under the communication point of view: how to insert the watermark to minimize the error rate at a given average distortion level.

In this paper, we propose a new technique, which we call improved spread spectrum (ISS). This technique essentially removes the signal as source of interference, producing a dramatic improvement in the quality of the watermarking process. The gains for the ISS are similar to those obtained by QIM, but ISS does not suffer from the same sensitivity to amplitude scaling. In fact, ISS is essentially as insensitive to amplitude scaling as traditional spread spectrum.

Practically any watermarking system currently using SS would immediately profit from using the proposed scheme. Gains will vary according to signal-to-noise ratio (SNR) and current error probability, but improvements of 20 dB in noise immunity or reduction in error probabilities of 20 orders of magnitude can be achieved.

In Section 2 we present our notation and analyze traditional SS, as it applies to watermarking. In section 3 we present our technique, including a simplified (linear) version, and the optimum ISS. In section 4 we compare the performance in terms of noise immunity of our technique to that of traditional spread spectrum, and in Section 5 we present some conclusions.

2. TRADITIONAL SS-BASED WATERMARKING

A simplified diagram of basic SS-based watermarking is shown in Fig. 1. A secret key *K*$ is used by a pseudo random number generator (PRN) to produce a "chip sequence" **u**, with zero mean, and whose elements are equal to $+\sigma_u$ or $-\sigma_u$. The sequence **u** is then added or subtracted to the signal **x** depending on to the variable *b*, which has the values of +1 or –1, according to the bit (or bits) to be transmitted. The watermarked signal is **s**.

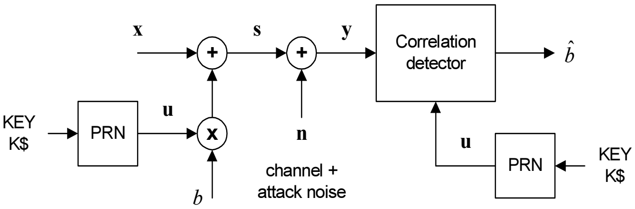

Figure 1. Spread-spectrum-based watermarking.

We now perform a simple analysis of the probability of error in the detector for SS-based watermarking. First, consider the definitions of inner product and norm:

$$\left\langle \mathbf{x},\mathbf{u}\right\rangle \triangleq \frac{1}{N}\sum_{i=0}^{N-1} x_i u_i \quad , \quad \text{and} \quad \left\|\mathbf{x}\right\| \triangleq \left\langle \mathbf{x},\mathbf{x}\right\rangle. \tag{1}$$

Without loss of generality, we assume that we are embedding one bit of information in a vector **s** of N signal samples[1]. Then, the bit rate is $1/N$ bits/sample. Embedding is performed by **s** = **x** + b **u**. The distortion D in the embedded signal is defined by $D = \|\mathbf{s} - \mathbf{x}\|$. It is easy to see that for the embedding equation above we have

$$D = \| b\mathbf{u} \| = \| \mathbf{u} \| = \sigma_u^2 . \tag{2}$$

The channel is modeled as additive noise, i.e. **y** = **s** + **n**. Detection is performed by first computing the (normalized) sufficient statistic r

$$r \triangleq \left\langle \mathbf{y},\mathbf{u}\right\rangle \big/ \left\|\mathbf{u}\right\| = \left\langle b\mathbf{u} + \mathbf{x} + \mathbf{n},\mathbf{u}\right\rangle \big/ \sigma_u^2 = b + x + n , \tag{3}$$

and then estimating the embedded bit by $\hat{b} = \operatorname{sign}(r)$, where $x \triangleq \left\langle \mathbf{x},\mathbf{u}\right\rangle \big/ \left\|\mathbf{u}\right\|$ and $n \triangleq \left\langle \mathbf{n},\mathbf{u}\right\rangle \big/ \left\|\mathbf{u}\right\|$.

We assume simple statistical models for the original signal **x** and the attack noise **n**. Namely, we assume both to be samples from uncorrelated white Gaussian random processes. Therefore, we have

$$x_i \sim N(0,\sigma_x^2), \quad n_i \sim N(0,\sigma_n^2) \tag{4}$$

Under those assumptions, it is easy to show that the sufficient statistic r is also Gaussian, i.e.

$$r \sim N(m_r,\sigma_r^2), \quad m_r = E[r] = b \quad \sigma_r^2 = \left(\sigma_x^2 + \sigma_n^2\right) \big/ N\sigma_u^2 . \tag{5}$$

In particular, let's consider the case when b = 1. Then, an error occurs when r < 0, and so the error probability p is given by

$$p = \Pr\left[r < 0 \mid b = 1\right] = \frac{1}{2}\operatorname{erfc}\left(\frac{m_r}{\sigma_r\sqrt{2}}\right) = \frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{\sigma_u^2 N}{2\left(\sigma_x^2 + \sigma_n^2\right)}}\right). \tag{6}$$

where erfc(·) is the complementary error function. The same error probability is obtained for $b = -1$.

3. IMPROVED SPREAD-SPECTRUM

The main idea behind the Improved Spread Spectrum (ISS) is that, by using the encoder knowledge about the signal **x** (or more precisely x, the projection of **x** on the watermark), we can enhance performance by modulating the energy of the inserted watermark to compensate for the signal interference. The new embedding approach is defined by a slight modification to the SS embedding equation, i.e., we vary the amplitude of the inserted chip sequence by a function $\mu(x, b)$

$$\mathbf{s} = \mathbf{x} + \mu(x,b)\mathbf{u} , \tag{7}$$

where, as before, $x \triangleq \left\langle \mathbf{x},\mathbf{u}\right\rangle \big/ \left\|\mathbf{u}\right\|$. Note that the traditional SS is a particular case of ISS, for $\mu(x, b) = b$, i.e. μ is independent of x.

We will now analyze two variations of the ISS approach. We first analyze a linear approximation to μ, as this allows for a simpler mathematical analysis and it's useful in practice. We also discuss the case of optimum ISS. These and a few other alternatives are discussed in detail in [8].

3.1 A linear approximation for μ

A simpler version of the ISS is to restrict μ to be a linear function. Not only this is much simpler to analyze, it will also provide a significant part of the gains in relation to traditional SS. In this case, and due to the symmetry of the problem in relation to b and x, we have:

$$\mathbf{s} = \mathbf{x} + \left(\alpha b - \lambda x\right)\mathbf{u} \tag{8}$$

The parameters α and λ control the distortion level and the removal of the carrier distortion on the detection statistic. Traditional SS is obtained by setting $\alpha = 1$ and $\lambda = 0$.

With the same channel noise model as before, the receiver sufficient statistic is

$$r = \left\langle \mathbf{y},\mathbf{u}\right\rangle \big/ \left\|\mathbf{u}\right\| = \alpha b + (1-\lambda)x + n . \tag{9}$$

So, the closer we make λ to 1, the more the influence of x will be removed from r. The detector is the same as in spread-spectrum, i.e., the detected bit is sign(r).

The expected distortion of the new system is given by

$$E[D] = E[\| \mathbf{s} - \mathbf{x} \|] = \left(\alpha^2 + \frac{\lambda^2\sigma_x^2}{N\sigma_u^2}\right)\sigma_u^2 . \tag{10}$$

To make the average distortion of the new system to equal that of traditional SS, we force $E[D] = \sigma_u^2$, and therefore

$$\alpha = \sqrt{\left(N\sigma_u^2 - \lambda^2\sigma_x^2\right) \big/ N\sigma_u^2} . \tag{11}$$

To compute the error probability, all we need is the mean and variance of the sufficient statistic r. They are given by

$$m_r = \alpha b, \quad \text{and} \quad \sigma_r^2 = \left(\sigma_n^2 + (1-\lambda)^2\sigma_x^2\right) \big/ N\sigma_u^2 . \tag{12}$$

We can therefore compute the error probability p by

$$p = \frac{1}{2}\operatorname{erfc}\left(\frac{m_r}{\sigma_r\sqrt{2}}\right) = \frac{1}{2}\operatorname{erfc}\left(\sqrt{\frac{N\sigma_u^2 - \lambda^2\sigma_x^2}{2\left(\sigma_n^2 + (1-\lambda)^2\sigma_x^2\right)}}\right). \tag{13}$$

In Fig. 2 we plot p as a function of λ for various values of SNR and $N\sigma_u^2/\sigma_x^2$. Remember that λ = 0 corresponds to SS. Note that by proper selection of the parameter λ, the error probability in the proposed method can be made several orders of magnitude better than using traditional SS. For example, with a signal to interference ratio of 10 (i.e., 10 dB), we get a reduction in the error rate from $p_o = 10^{-5}$ for traditional SS to $p_o = 1.55\times10^{-43}$ for the proposed method, a reduction of over 37 orders of magnitude in the error probability! Higher SNR (which can happen in practical applications) will yield even higher gains.

[1] The signal **x** is usually obtained from transformations on the original media signal to be marked [3].

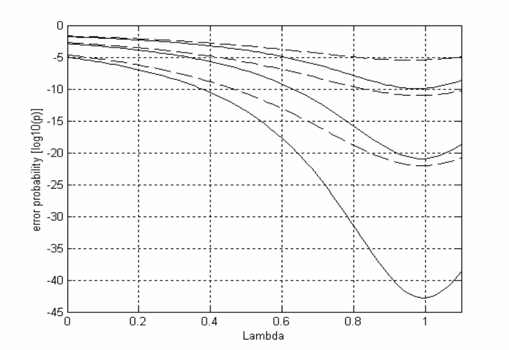

Figure 2. Error probability p as a function of λ. Solid lines correspond to 10 dB SNR, and dashed lines to 7 dB SNR. Lines correspond to values of $N\sigma_u^2/\sigma_x^2$ equal to 5, 10, and 20 (higher values having smaller p).

As it can be inferred from Fig. 2, the error probability achieves a minimum value for λ close to one. The expression for the optimum value for λ can be computed from the error probability p by setting $\partial p/\partial\lambda = 0$:

$$2\lambda_{opt} = \left(1+\frac{\sigma_n^2}{\sigma_x^2}+\frac{N\sigma_u^2}{\sigma_x^2}\right) - \sqrt{\left(1+\frac{\sigma_n^2}{\sigma_x^2}+\frac{N\sigma_u^2}{\sigma_x^2}\right)^2 - 4\frac{N\sigma_u^2}{\sigma_x^2}} \,. \quad (14)$$

Note also from this expression that $\lambda_{opt} \to 1$ as SNR $\to \infty$ (for N large enough).

3.2 Optimum ISS

We now analyze the more generic case, where the function $\mu(x, b)$ in (7) is not restricted to be linear. We can find the optimum solution for $\mu(x, b)$ that minimizes the probability detection error. We first note that since **x**, **n**, and b are independent, $\mu(x, b)$ will be odd symmetric, in the sense that $\mu(x, b) = -\mu(-x, -b)$. For simplicity, and without loss of generality, from now on we will assume $b = 1$, and write simply $\mu(x)$. We can show that the optimum value of $\mu(x)$ is either $\mu(x) = 0$ or it must satisfy

$$K\mu(x) = \exp\left(-\left(\frac{x+\mu(x)}{\sigma_n\sqrt{2}}\right)^2\right), \quad (15)$$

where K is a constant. Details of the derivation can be found in [8]. Unfortunately, there is no closed-form solution for $\mu(x)$, but we can solve the above equation numerically. The expected error probability will depend on the variance of the noise, and on the constant K. We can, therefore look at K as a parameter that controls the tradeoff between distortion and error probability. Depending on the values of K, σ_n , and x, the equation will have one, two or three solutions. Details on which is the optimum solution can also be found in [8].

Fig. 3 shows a plot of the optimum $\mu(x)$ for some different situations. In particular, we vary the SNR ratio, while keeping the average distortion constant. As it can be noted in the figure, $\mu(x)$ can be approximated by a straight line segment for a large number of situations. In particular, the higher the SNR (or the stronger the watermark), the better the linear approximation.

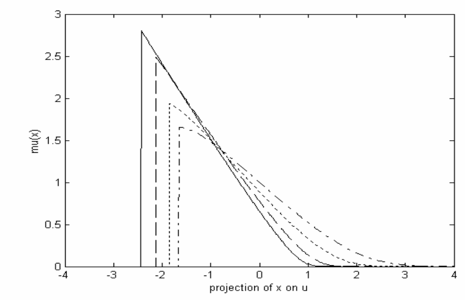

Figure 3. Optimal $\mu(x)$ for several SNRs. From left to right SNR is 10 dB, 7 dB, 3 dB, and 0 dB. In all cases, distortion is set to 20 dB below signal, and $N = 100$.

4. PERFORMANCE COMPARISONS

The proposed method improves the error ratio (or noise immunity) for any level of channel noise (signal editing or malicious attack), and for any level of desired error probability. We now select a more specific example to give an idea of the levels of improvement that can be achieved with the proposed ISS method. We recall that for the traditional SS system to work with a low probability of error, e.g. $p < 10^{-3}$, then we need to ensure $N\sigma_u^2 > 9\left(\sigma_n^2 + \sigma_x^2\right)$. For this case it follows 0.9 < λ_{opt} < 1. Also, let's call σ_{no}^2 the amount of noise supported by SS, Q the signal to channel noise ratio, i.e.

$$Q \triangleq \frac{\sigma_x^2}{\sigma_{no}^2} \quad (16)$$

and let's call P the noise tolerance gain of our system when compared to traditional SS

$$P \triangleq \frac{\sigma_n^2}{\sigma_{no}^2} \,. \quad (17)$$

Then, we can show that the noise tolerance gain for our new system is given by [8]

$$P = (1+\lambda_o Q) > (1+0.9Q) \,. \quad (18)$$

Therefore, for large Q the improvement in noise tolerance will be significant, since it will be approximately equal to 0.9Q. In Fig. 4 we plot P as a function of Q, all in dB.

We note that the performance of our new ISS system is quite close to that of QIM [5]. The noise tolerance improvement of QIM over SS is slightly above Q, whereas in our system it is slightly below Q. However, our ISS system is not sensitive to amplitude scaling of the received signal **y**, like QIM. So, ISS can work very well in practice.

In many applications, a desired error probability and a certain SNR are specified. In such cases, the objective is to minimize the energy of the watermark (i.e., the signal distortion). We will now use this situation to compare the linear ISS to traditional SS, to STDM (a particular form of QIM), and to a theoretical bound.

For a given signal and noise energy, and a desired error probability, inverting Eqn. (6) gives us the necessary energy in the watermark for traditional SS. A similar equation for the linear

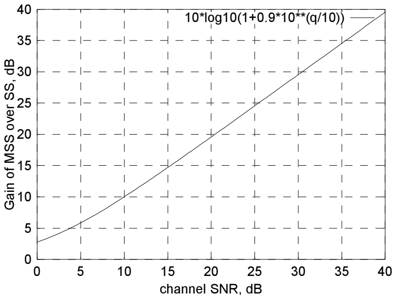

Figure 4. Improvement in noise robustness of ISS over traditional SS, in dB, as a function of the channel SNR. For a typical scenario of a channel SNR of 20 dB, the improvement is about 20 dB, i.e., ISS can tolerate 100 more times channel noise power than traditional SS.

ISS can be obtained by inverting Eqn. (13). The objective of ISS is to reduce the influence of the signal as a source of interference. A natural performance bound is therefore the result that could be achieved if the decoder had knowledge of the signal (and therefore could remove any influence from the detection statistic). In such situation, it has been shown that traditional SS is optimum. In [6], Chen and Wornell show that the performance of STDM is only 1.25 dB above this bound.

Fig. 5 shows a plot of these numbers for attacks corresponding to 5 dB and 10 dB SNR. In each figure, the solid line represents the theoretical bound, the dash-doted line represents the performance of traditional SS, the dashed line id for STDM, and the two dotted lines represent two versions of linear ISS: the simplest one ($\lambda = 1$), and with λ optimized according to Eqn. (14). Note that, in each case, traditional SS requires about the same extra energy in the watermark as the attack SNR. For error probabilities below 10^{-5} with attacks over 10 dB, the ISS performance is within 2 dB of the theoretical bound, and it even outperforms STDM for error probabilities below 10^{-8} (below 10^{-3} for a 5 dB attack). We note that other QIM methods, more elaborate than STDM would help reduce the gap to the theoretical bound. Nevertheless, all QIM methods suffer from the scale sensitivity problem. In summary, ISS is much simpler, robust to scaling attacks, does not require modifying an existing SS decoder, and its performance is similar to that of QIM.

5. CONCLUSION

In this paper we have proposed an improved spread spectrum technique for use in watermarking applications. We have shown that the proposed technique provides an exceptional improvement over traditional SS, with improvements in the error probability of several orders of magnitude for most typical scenarios. Spread spectrum is currently used by many watermarking schemes as the information embedding (or modulation) technology. The proposed technique can be readily applied to practically any watermarking technique currently using SS, taking immediate advantage of the gains. Furthermore, the proposed method does not require any change in the detection scheme, and in some cases it could be applied even to systems that are already deployed, as far as we still have access to the encoders (and this is often the case in media distribution schemes).

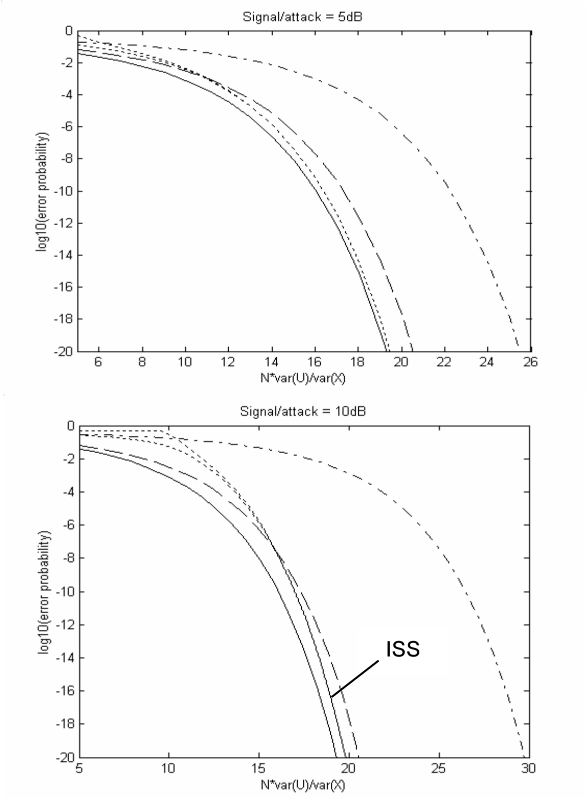

Figure 5. Error probability as a function of watermark energy. Error probability for ISS (optimum and linear, dotted lines) compared to SS (dash-dot lines), STDM (dashed line) and a theoretical bound (solid line). Top: SNR = 5dB; bottom: SNR = 10dB.

REFERENCES

[1] Z. Tirkel, C. F. Osborne, and R. G. van Schyndel, "Image watermarking – a spread spectrum application," *Proc. IEEE 4th Int. Symp. Spread Spectrum Techniques and Applications*, 1996.

[2] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: malicious attacks and counter-attacks," *Proc. SPIE Security and Watermarking of Multimedia Contents*, San Jose, CA, pp. 147–158, Jan. 1999.

[3] D. Kirovski and H. S. Malvar, "Robust spread-spectrum audio watermarking," *Proc. International Conference Acoustics, Speech, and Signal Processing,* Salt Lake City, UT, 2001.

[4] I. Cox, M. Miller, and A. McKellips, "Watermarking as Communications with Side Information," *Proc. of the IEEE,* vol. 87, n. 7, pp. 1127-1141, July 1999.

[5] B. Chen and G. Wornell, "Achievable Performance of Digital Watermarking Systems," *Proc. Int. Conf. Multimedia Computing and Systems,* June 1999.

[6] B. Chen and G. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Trans. Inform. Theory,* vol. 47, pp. 1423–14443, May 2001.

[7] M. Miller, I. Cox, and J. Bloom, "Informed Embedding: Exploiting Image and Detector Information during Watermark Insertion," *Proc. IEEE Int. Conf. Image Processing,* 2000.

[8] H. Malvar and D. Florêncio, "Improved spread spectrum: a new modulation technique for robust watermarking," preprint.