Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking


Information Technologies for IPR Protection
Spread-spectrum based watermarking, where $b$ is the bit to be embedded
• **u**: the chip sequence (reference pattern), with zero mean and whose elements are equal to $+\sigma_u$ or $-\sigma_u$ (1-bit message coding)

• inner product: $\langle x, u \rangle \triangleq \frac{1}{N} \sum_{i=0}^{N-1} x_i u_i$

• norm: $\langle x, x \rangle \triangleq ||x||$

• Embedding: $s = x + bu$

• Distortion in the embedded signal:
  $$D = ||s - x|| = ||bu|| = ||u|| = \sigma_u^2$$

• Channel noise: $y = s + n$
Detection is performed by first computing the (normalized) sufficient statistic $r$:

**normalized correlation**

$$r \triangleq \frac{\langle y, u \rangle}{\langle u, u \rangle} = \frac{\langle bu + x + n, u \rangle}{\sigma_u^2}$$

$$= b + \frac{\langle x, u \rangle}{\|u\|} + \frac{\langle n, u \rangle}{\|u\|} = b + \tilde{x} + \tilde{n}$$

and estimating the embedded bit by

$$\hat{b} = \text{sign}(r)$$
We usually assume simple statistical models for the original signal $x$ and the attack noise $n$:

both to be samples from uncorrelated white Gaussian random process

\[
x_i \sim N(0, \sigma_x^2)
\]

\[
n_i \sim N(0, \sigma_n^2)
\]
Then, it is easy to show that the sufficient statistic $r$ is also Gaussian, i.e.,

$$r \sim N(m_r, \sigma_r^2)$$

where

$$m_r = E(r) = b \quad b \in \{0, 1\}$$

$$\sigma_r^2 = \frac{\sigma_x^2 + \sigma_n^2}{N \sigma_u^2}$$
Let’s consider the case when \( b = 1 \).

Then, an error occurs when \( r < 0 \), and therefore, the error probability \( p \) is given by

\[
p = \Pr(\hat{b} < 0 \mid b = 1)
\]

\[
= \frac{1}{2} \text{erfc} \left( \frac{m_r}{\sigma_r \sqrt{2}} \right)
\]

\[
= \frac{1}{2} \text{erfc} \left( \sqrt{\frac{\sigma_u^2 N}{2(\sigma_x^2 + \sigma_n^2)}} \right)
\]

\[
= \frac{1}{2} \text{erfc} \left( \frac{1}{\sqrt{2}} \sqrt{\frac{N \sigma_u^2}{\sigma_x^2 + \frac{\sigma_n^2}{\sigma_x^2}}} \right)
\]

where \( \text{erfc} (\cdot) \) is the complementary error function.
The same error probability is obtained under the assumption that \( b = -1 \) but \( \hat{r} > 0 \)

\[
\text{If we want an error prob. Better than } 10^{-3}, \text{ then we need}
\]

\[
m_r/\sigma_r > 3
\]

\[
N\sigma_u^2 > 9(\sigma_x^2 + \sigma_n^2)
\]

\[
\log_{10}\text{error probability}
\]

SNR in detection variable \( r \) \( (m_r/\sigma_r) \)
In general, to achieve an error probability $p$, we need

$$N \sigma_u^2 > 2 (\text{erfc}^{-1}(p))^2 (\sigma_x^2 + \sigma_n^2)$$

One can trade the length of the chip sequence $N$ with the energy of the sequence $\sigma_u^2$!!
Main idea:
by using the encoder knowledge about the signal $x$ (or more precisely, the projection of $x$ on the watermark), one can enhance performance by modulating the energy of the inserted watermark to compensate for the signal interference.
We vary the amplitude of the inserted chip sequence by a function \( \mu(x,b) \):

\[
s = x + \mu(\tilde{x},b)u
\]

where, as before

\( \tilde{x} \uparrow <x,u> / ||u|| : \text{signal interference} \)

\( \Rightarrow \) SS is a special case of the ISS in which the function \( \mu \) is made independent of \( \tilde{x} \).
Linear Approximation:

\[ \mu \text{ is a linear function of } x \]

\[ s = x + (\alpha b - \lambda \tilde{x})u \]

The parameters \( \alpha \) and \( \lambda \) control the distortion level and the removal of the carrier distortion on the detection statistics. Traditional SS is obtained by setting \( \alpha = 1 \) and \( \lambda = 0 \).
With the same channel noise model as before, the receiver sufficient statistic is

\[ r = \frac{\langle y, u \rangle}{\|u\|} = \alpha b + (1 - \lambda) \tilde{x} + \tilde{n} \]

The closer we make \( \lambda \) to 1, the more the influence of \( \tilde{x} \) is removed from \( r \).

The detector is the same as in SS, i.e., the detected bit is \( \text{sign}(r) \).
The expected distortion of the new system is given by

\[
E[D] = E \left[ \|s - x\| \right] \\
= E \left[ |\alpha b - \lambda \bar{x}|^2 \sigma_u^2 \right] \\
= \left( \alpha^2 + \frac{\lambda^2 \sigma_x^2}{N \sigma_u^2} \right) \sigma_u^2 \\
= 1
\]

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

\[
\alpha = \sqrt{\frac{N \sigma_u^2 - \lambda^2 \sigma_x^2}{N \sigma_u^2}}
\]
To compute the error probability, all we need is the mean and variance of the sufficient statistic \( r \). They are given by \( m_r = \alpha b \)

\[
\sigma_r^2 = \frac{\sigma_n^2 + (1 - \lambda)^2 \sigma_x^2}{N \sigma_u^2} \]

Therefore, the error probability \( p \) is

\[
p = \Pr\{r < 0 \mid b = 1\} \\
= \frac{1}{2} \text{erfc} \left( \frac{m_r}{\sigma_r \sqrt{2}} \right) \\
= \frac{1}{2} \text{erfc} \left( \frac{\sqrt{N \sigma_u^2 - \lambda^2 \sigma_x^2}}{2(\sigma_n^2 + (1 - \lambda)^2 \sigma_x^2)} \right)\]
We can also write $p$ as a function of the relative power of the SS sequence $N \sigma_u^2 / \sigma_x^2$ and the SNR $\sigma_x^2 / \sigma_n^2$

$$p = \frac{1}{2} \operatorname{erfc} \left( \frac{1}{\sqrt{2}} \sqrt{\frac{N \frac{\sigma_u^2}{\sigma_x^2} - \lambda^2}{\frac{\sigma_n^2}{\sigma_x^2} + (1 - \lambda)^2}} \right) = \frac{1}{2} \operatorname{erfc} \left( \frac{1}{\sqrt{2}} \sqrt{\frac{1}{\text{power} - \text{ss}} - \lambda^2} \left( \frac{1}{\text{SNR}} + (1 - \lambda)^2 \right) \right)$$

By proper selection of the parameter $\lambda$, the error probability in the proposed method can be made several orders of magnitude better than using traditional SS.
The three lines correspond to values to 5, 10, and 20dB SNR (with higher values having smaller error probability).

SIR: Signal-to-interference ratio

Solid lines represent a 10-dB SIR and dash lines represent a 7-d SIR.
As can be inferred from the above figure, the error probability varies with $\lambda$, with the optimum value usually close to 1.

The expression for the optimum value for $\lambda$ can be computed from the error probability $p$ by \[ \frac{\partial p}{\partial \lambda} = 0 \]
and is given by

\[
\lambda_{opt} = \frac{1}{2} \left( 1 + \frac{n^2}{\sigma_x^2} + \frac{N\sigma_u^2}{\sigma_x^2} \right) - \sqrt{\left( 1 + \frac{n^2}{\sigma_x^2} + \frac{N\sigma_u^2}{\sigma_x^2} \right)^2 - 4 \frac{N\sigma_u^2}{\sigma_x^2}}
\]

Note: for $N$ large enough, $\lambda_{opt} \rightarrow 1$ as $\text{SNR} \rightarrow \infty$