# 3
# Técnicas e Desempenho da Marcação D'Água Digital

Neste capítulo, as principais técnicas de marcação d'água digital são apresentadas, com maior ênfase na discussão das técnicas baseadas no espalhamento espectral (*Spread Spectrum* - SS), incluíndo o desempenho das mesmas. Novas técnicas derivadas do tipo SS são propostas e os respectivos desempenhos são derivados.



## 3.1
## Abordagem Tradicional para a Marcação Binária por Espalhamento Espectral

A marcação d'água digital binária por espalhamento espectral (SS) é ilustrada na Figura 3.1. Uma chave secreta $K$ é utilizada por um gerador de vetores aleatórios (PRV) para produzir um vetor $\boldsymbol{u}$ com energia

$$E_b = \sum_{i=1}^{N} u_i^2 = N\sigma_u^2. \tag{3-1}$$

Outros condicionamentos específicos podem ser considerado para o gerador PRV dependendo dos requisitos da aplicação. Em seguida, o vetor $\boldsymbol{u}$ é adicionado, ou subtraído, ao sinal $\boldsymbol{x}$, de acordo como o sinal da variável $b \in \{\pm 1\}$. O sinal $\boldsymbol{s}$ é o sinal marcado.

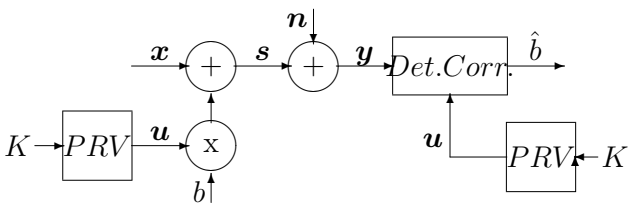


**Figura 3.1:** Modelo da técnica de marcação por Espalhamento Espectral.

A análise da técnica tipo SS binária conduz a uma simples expressão para a probabilidade de erro na deteção correspondendo ao desempenho da técnica. A modulação com o bit $b$ produz o sinal marcado

$$\boldsymbol{s} = \boldsymbol{x} + b\boldsymbol{u} \tag{3-2}$$

com $D_b = \sigma_u^2$.

Considerando a definição de produto interno

$$< \boldsymbol{x}, \boldsymbol{u} >= \frac{1}{N}\sum_{i=1}^{N} x_i u_i, \tag{3-3}$$

a deteção é realizada primeiramente calculando a estatística suficiente normalizada (detetor de correlação)

$$r = \frac{< \boldsymbol{y}, \boldsymbol{u} >}{\sigma_u^2} = \frac{< b\boldsymbol{u} + \boldsymbol{x} + \boldsymbol{n}, \boldsymbol{u} >}{\sigma_u^2} = b + x + n \tag{3-4}$$

onde $x =< \boldsymbol{x}, \boldsymbol{u} > /\sigma_u^2$ e $n =< \boldsymbol{n}, \boldsymbol{u} > /\sigma_u^2$. Repare aqui a forte interferência do hospedeiro no processo de deteção . Em seguida o bit $b$ é estimado como

$$\hat{b} = \text{sign}(r). \tag{3-5}$$

Em nosso modelo, vamos supor que $\boldsymbol{x}$ e $\boldsymbol{n}$ são amostras descorrelacionadas de vetores de um processo aleatório gaussiano branco. Assim, $x_i \sim N(0, \sigma_x^2)$ e $n_i \sim N(0, \sigma_n^2)$, e é simples demonstrar que o desempenho é expresso por

$$p_e = \frac{1}{2}\text{erfc}\left(\sqrt{WNR_N/2(1 + DNR)}\right). \tag{3-6}$$

## 3.2
## Espalhamento Espectral Otimizado

A idéia chave da modulação por espalhamento espectral otimizado (ISS), como apresentada em [9], é que através do conhecimento do sinal $\boldsymbol{x}$ pelo modulador , uma grande melhora no desempenho (em relação ao SS tradicional) é obtida. Esta melhora é alcançada por meio da modulação da energia da marca d'água a fim de compensar a interferência na deteção. A

abordagem da modulação ISS é conduzida introduzindo uma pequena modificação na modulação SS tradicional, e consiste em controlar a amplitude de cada vetor $\boldsymbol{u}$, representando cada bit da marca d'água, com a função $\mu(x, b)$

$$\boldsymbol{s} = \boldsymbol{x} + \mu(x, b)\boldsymbol{u} \tag{3-7}$$

onde $x =< \boldsymbol{x}, \boldsymbol{u} > /\sigma_u^2$. Assim, podemos reparar que a modulação SS tradicional é um caso particular da modulação ISS, quando a função $\mu = b$. A solução geral para determinar a função $\mu(x, b)$ ótima é discutida em [9]. Nesta tese consideraremos apenas a aproximação linear, pois além de ser bastante eficiente na melhora do desempenho, fornece expressões simples para análise. A modulação ISS linear é definida como

$$\boldsymbol{s} = \boldsymbol{x} + (\alpha b - \lambda x)\boldsymbol{u}. \tag{3-8}$$

Como veremos, o parâmetro $\alpha$ e $\lambda$ controlam respectivamente, o nível de distorção, e a redução da interferência do hospedeiro na deteção. Utilizando o mesmo modelo de canal da seção anterior, a estatística suficiente normalizada do receptor é

$$r = \frac{< \boldsymbol{y}, \boldsymbol{u} >}{\sigma_u^2} = \alpha b + (1 - \lambda)x + n. \tag{3-9}$$

Para que a distorção $D_b$ introduzida pela modulação ISS seja a mesma daquela introduzida pela modulação SS, condiciona-se que $D_b = \sigma_u^2$, o que resulta na determinação de $\alpha$ como

$$\alpha = \sqrt{\frac{N\sigma_u^2 - \lambda^2\sigma_x^2}{N\sigma_u^2}}. \tag{3-10}$$

Considerando novamente $\hat{b} = \text{sign}(r)$, o desempenho do ISS linear é facilmente derivado, e é expresso por

$$p_e = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{WNR_N - DNR\ \lambda^2}{2(1 + DNR(1 - \lambda)^2)}}\right) \tag{3-11}$$

A determinação do valor ótimo para o parâmetro $\lambda$ é obtido por meio da mimimização da probabilidade de erro $p_e$ fazendo $\partial p_e/\partial\lambda = 0$, resultando em

$$\lambda_{opt} = \frac{1}{2}\left(1 + \frac{1}{DNR} + \frac{WNR_N}{DNR} - \sqrt{(1 + \frac{1}{DNR} + \frac{WNR_N}{DNR})^2 - 4\frac{WNR_N}{DNR}}\right) \tag{3-12}$$

Nota-se que da expressão acima que para altos valores de $DNR$ e $WNR_N > DNR$, resulta $\lambda_{opt} \approx 1$. Estas considerações fornecem a expressão aproximada de desempenho para ISS linear como descrito na Tabela 4.1. Repara-se ainda que para altos valores de $DNR$ e $WNR_N < DNR$, resulta em $\lambda_{opt} \approx E_b/\sigma_x^2$.

## 3.3 Outras Técnicas

Outras importantes técnicas de marcação d'água digital binária são a modulação indexada por quantização (QIM) [4] e o esquema Costa escalar (SCS) [6], e as correspondentes técnicas variantes. Estas técnicas também utilizam o conhecimento do sinal hospedeiro na modulação para que, na deteção, a interferência do mesmo seja significativamente reduzida, podendo ser teoricamente eliminada. Como o desenvolvimento desta tese apoia-se essencialmente nas técnicas do tipo SS, ao leitor interessado no detalhamento das técnicas QIM e SCS é recomendado consultar as citadas referências. Na seção seguinte propõe-se novas técnicas de marcação, variantes das técnicas do tipo SS e ISS.

## 3.4 Modulação SS Unidimensional M-Ária

Até o momento, nossa discussão de técnicas de marcação d'água digital restringiu-se à modulação binária, onde um bit $b$ da marca d'água (bit de informação) é empregado na marcação das $N$ amostras do sinal $\boldsymbol{x}$. Quando uma maior taxa de marcação é pretendida, especialmente quando considera-se a operação com uma razão marca d'água-ruído elevada, o desempenho mais próximo à capacidade do canal é obtido através da modulação de um mesmo conjunto de $N$ amostras do sinal $\boldsymbol{x}$ com mais de um bit. Com este objetivo, é proposto a modulação SS unidimensional $M$-ária como

$$\boldsymbol{s} = \boldsymbol{x} + m\boldsymbol{u}, \tag{3-13}$$

onde $m \in \{\pm 1, \pm 3, ..., \pm(M-1)\}$, $M$ é o número de símbolos (níveis) disponíveis, e $\log_2(M)$ é a quantidade de bits de informação a serem uti-

lizados por marcação de $N$ amostras de $\boldsymbol{x}$.

Cada símbolo introduz na marcação uma distorção média $D_s = E_s/N$, que também representa a potência da marca d'água, onde $E_s$ é a energia média dos símbolos. A energia média do bit é $E_b = E_s/\log_2(M)$, e a sua contribuição para a distorção é $D_b = E_b/N$, que também representa a potência média do bit. Repare que a energia média do bit não é mais $N\sigma_u^2$, como no caso binário. Agora, a energia média do bit é dada por $E_b = \frac{M^2-1}{3\log_2(M)} N\sigma_u^2$, onde $N\sigma_u^2$ é a energia do vetor $\boldsymbol{u}$.

Na deteção, considerando a introdução do ruído do canal, a estatística suficiente normalizada correspondente é

$$r = \frac{< \boldsymbol{y}, \boldsymbol{u} >}{\sigma_u^2} = m + x + n. \tag{3-14}$$

O correspondente problema de deteção é equivalente ao do problema $M$-$ASK$ (Amplitude Shift Keying) de comunicação, onde podemos verificar na equação 3-14 a presença do sinal $m$ formando um constelação colinear. Contudo, na deteção $M$-$ASK$ normalmente considera-se somente a presença do ruído do canal. Assim, a equivalencia deve ser entendida de forma que o ruído resultante é $x + n$, evidenciando a contribuição (interferência) do sinal hospedeiro no processo de deteção. Assim, como veremos em seguida, podemos derivar facilmente o desempenho para esta técnica, e a correspondente técnica otimizada, aplicando convenientemente a expressão de desempenho da modulação $M$-$ASK$ [12]

$$p_e = \frac{M-1}{M} \mathrm{erfc}\left(\frac{d}{2\sqrt{N_0}}\right), \tag{3-15}$$

onde $d$ representa a distância entre sinais consecutivos da constelação colinear da modulação $M$-$ASK$, e a potência total (resultante) do ruído gaussiano é $\sigma_{nt}^2 = N_0/2$.

Assim, podemos derivar o desempenho da técnica de modulação SS unidimensinal M-ária cosiderando o ruído total (normalizado) interferindo na deteção como $(\sigma_n^2 + \sigma_x^2)/(N\sigma_u^2)$, e que $d = 2$. Desta forma, da equação 3-15, obtém-se o seguinde desempenho para a técnica de modulação SS

unidimensinal M-ária:

$$p_e = \frac{M-1}{M}\text{erfc}\left(\sqrt{\frac{3\log_2(M)}{M^2-1}\frac{WNR_N}{2(1+DNR)}}\right). \quad (3\text{-}16)$$

## 3.5 Modulação SS Unidimensional M-Ária Otimizada

Utilizando abordagem semelhante a da técnica ISS binária, é possível reduzir a interferência do hospedeiro na deteção definindo a modulação como

$$\boldsymbol{s} = \boldsymbol{x} + (\alpha m - \lambda x)\boldsymbol{u}, \quad (3\text{-}17)$$

que representa a técnica ISS unidimensional M-ária. O parâmetro $\alpha$, também é determinado de forma a manter a mesma distorção média, e é expresso por

$$\alpha = \sqrt{\frac{3}{M^2-1}\frac{(\frac{M^2-1}{3})N\sigma_u^2 - \lambda^2\sigma_x^2}{N\sigma_u^2}}. \quad (3\text{-}18)$$

Na deteção, considerando a introdução do ruído do canal, a estatística suficiente normalizada correspondente é

$$r = < \boldsymbol{y}, \boldsymbol{u} > /\sigma_u^2 = \alpha m + (1-\lambda)x + n. \quad (3\text{-}19)$$

Assim, a potência total (normalizada) do ruído interferindo na deteção é

$$(\sigma_n^2 + (1-\lambda)^2\sigma_x^2)/(N\sigma_u^2),$$

e tem-se agora $d = 2\alpha$. Desta forma, da equação 3-15, o desempenho da técnica de modulação ISS unidimensional M-ária é

$$p_e = \frac{M-1}{M}\text{erfc}\left(\sqrt{\frac{3}{2(M^2-1)}\frac{\log_2(M)WNR_N - \lambda^2 DNR}{(1+(1-\lambda)^2 DNR)}}\right). \quad (3\text{-}20)$$

A otimização do parâmetro $\lambda$ para minimização da probabilidade de erro também é ralizada da mesma forma como para a técnica ISS, e é

expresso como

$$\lambda_{opt} = \frac{1}{2}\left(1 + \frac{1}{DNR} + \frac{\log_2(M)WNR_N}{DNR}\right) - \frac{1}{2}\left(\sqrt{(1 + \frac{1}{DNR} + \frac{\log_2(M)WNR_N}{DNR})^2 - 4\frac{\log_2(M)WNR_N}{DNR}}\right). \tag{3-21}$$

Observar que para altos valores de $DNR$, $\lambda_{opt}$ depende somente do valor $(E_b/\sigma_x^2)\log_2(M)$.

## 3.6 Modulação SS M-Ária Multidimensional

Em sistemas de comunicações, o desempenho da modulação M-ária pode ser melhorado utilizando modulação multidimensional, ao invés da unidimensional, como pode ser observado quando comparamos os desempenhos das modulações $M$-$ASK$ e $M$-$PSK$ [12]. Assim, nesta tese, naturalmente propõe-se uma nova técnica de marcação d'água tipo SS considerando a modulação multidimensional. Para simplificar nossa análise, somente o caso bidimensional 4-ária será considerado, mas a extensão para outros valores de $M$ e para outras dimensões é direta, podendo inclusive aproveitar alguns resultados já alcançados em modelos equivalentes a determinados sistemas de comunicações. Em seguida descreve-se a técnica proposta.

Um gerador de vetores pseudo aleatório (PRV) fornece um vetor $\boldsymbol{u_1}$, como para a modulação SS binária tradicional. Em seguida, um segundo vetor $\boldsymbol{u_2}$ é gerado tal que o mesmo seja ortogonal a $\boldsymbol{u_1}$ e $||\boldsymbol{u_2}|| = ||\boldsymbol{u_1}||$. A geração deste segundo vetor pode ser realizada com uma outra chave num PRV distinto, elevando o grau de segurança do sistema de marcação. Como exemplo, se $N = 3$, $\boldsymbol{u_1}$ pode ser selecionado de uma esfera de raio $\sqrt{N}\sigma_u$, e $\boldsymbol{u_2}$ pode ser selecionado de um círculo, com mesmo raio, pertencendo a um plano ortogonal a $\boldsymbol{u_1}$ na origem.

Vamos representar os quatros símbolos por um par de bits $(b_1, b_2)$, onde $b_i \in \{-1, 1\}$. Assim, estamos aptos a definir a modulação bidimensional como

$$\boldsymbol{s} = \boldsymbol{x} + b_1\boldsymbol{u_1} + b_2\boldsymbol{u_2}. \tag{3-22}$$

Esta implementação específica de modulação bidimensional ortogonal 4-ária designa-se de marcação $QSS$ ( $SS$ quaternária ). Observe que a potência do símbolo é $D_s = 2\sigma_u^2$, e que a potência média do bit é $D_b = \sigma_u^2$. O ruído do canal (ataque) é o mesmo do modelo SS tradicional.

Na demodulação, a deteção é conduzida computando a estatística suficiente normalizada $r_i$ para cada dimensão:

$$r_1 = \frac{< \boldsymbol{y}, \boldsymbol{u_1} >}{\sigma_u^2} = b_1 + x_1 + n_1 \tag{3-23}$$

e

$$r_2 = \frac{< \boldsymbol{y}, \boldsymbol{u_2} >}{\sigma_u^2} = b_2 + x_2 + n_2 \tag{3-24}$$

e estimando cada símbolo utilizado na marcação (par de bits) como

$$(\hat{b_1}, \hat{b_2}) = (\text{sign}(r_1), \text{sign}(r_2)) \tag{3-25}$$

onde $x_i =< \boldsymbol{x}, \boldsymbol{u_i} > /\sigma_u^2$ e $n_i =< \boldsymbol{n}, \boldsymbol{u_i} > /\sigma_u^2$ .

O problema de deteção acima descrito é equivalente ao problema de deteção da modulação $QPSK$ da teoria dos sistemas de comunicações, onde o par $(b_1, b_2)$ representa uma constelação quadradada de símbolos, e o ruído total resultante é composto pelas contribuições da interferência do hospedeiro e do ruído do canal (ataque). O desempenho da modulação $QPSK$ [12], com lado da constelação quadrada $d$, é

$$p_e = \text{erfc}\left(\frac{d}{2\sqrt{N_0}}\right) - \frac{1}{4}\left(\text{erfc}(\frac{d}{2\sqrt{N_0}})\right)^2, \tag{3-26}$$

onde a potência do ruído gaussiano total (contribuições do hospedeiro e do canal) é, para cada dimensão, $\sigma_{nt}^2 = N_0/2$.

Assim, considerando $d = 2$, e a potência total (normalizada) do ruído interferindo na detação

$$\sigma_{nt}^2 = (\sigma_n^2 + \sigma_x^2)/(N\sigma_u^2),$$

para cada dimensão, pode-se aplicar diretamente a Eq. 3-26 para obter

o desempenho da técnica de marcação $QSS$ como

$$p_e = \text{erfc}\left(\sqrt{WNR_N/2(1+DNR)}\right) - \frac{1}{4}\left(\text{erfc}(\sqrt{WNR_N/2(1+DNR)}\ )\right)^2. \tag{3-27}$$

## 3.7
## Modulação SS M-Ária Multidimensional Otimizada

Utilizando abordagem semelhante a da técnica ISS binária, é possível reduzir a interferência do hospedeiro na deteção definindo a modulação como

$$\boldsymbol{s} = \boldsymbol{x} + (\alpha_1 b_1 - \lambda_1 x_1)\boldsymbol{u_1} + (\alpha_2 b_2 - \lambda_2 x_2)\boldsymbol{u_2}, \tag{3-28}$$

que representa a técnica QSS otimizada (IQSS). Os parâmetros $\alpha_i$, são também determinados de forma a manter a mesma distorção média introduzida pela marcação, e ambos os parâmetros são igualmente expressos pela equação 3-10.

Na deteção, considerando a introdução do ruído do canal, a estatística suficiente normalizada correspondente é

$$r_i = \frac{< \boldsymbol{y}, \boldsymbol{u_i} >}{\sigma_u^2} = \alpha_i b_i + (1-\lambda_i)x_i + n_i. \tag{3-29}$$

Assim, a potência total (normalizada) do ruído interferente na deteção é

$$(\sigma_n^2 + (1-\lambda)^2\sigma_x^2)/(N\sigma_u^2),$$

para cada dimensão, e tem-se agora $d = 2\alpha$. Desta forma, pode-se aplicar diretamente a equação 3-26, e o desempenho otimizado da técnica de modulação IQSS é determinado como

$$p_e = \text{erfc}\left(\sqrt{\frac{(WNR_N - \lambda_{opt}^2 DNR)}{2(1+(1-\lambda_{opt})^2 DNR)}}\right) - \frac{1}{4}\left(\text{erfc}(\sqrt{\frac{(WNR_N - \lambda_{opt}^2 DNR)}{2(1+(1-\lambda_{opt})^2 DNR)}}\ )\right)^2, \tag{3-30}$$

onde $\lambda_{opt}$ é o valor ótimo para os parâmetros $\lambda_i$ (para a minimização de $p_e$) e ambos são igualmente expressos pela equação 3-12.

## 3.8 Comentários

A investigação futura de outras técnicas de marcação possuindo constelações de sinais com equivalência de deteção a conhecidos modelos de modulação/demodulação em sistemas de comunicação é de interesse. Ainda, a facilidade em operar com dimensões maiores no problema de marcação d'água, possibilita otimizar as técnicas tradicionais no plano bidimensional usualmente empregadas em sistemas de comunicação. Por exemplo, caso venhamos a operar com três dimensões, e com uma técnica quaternária (quatro símbolos), a constelação de sinais formando um tetraedro fornece um desempenho superior a constelação quadrática no plano bidimensional (QPSK).