

Parte I

Modelos, Desempenhos e Técnicas de Marcação D'Água Digital

2

Modelo do Problema de Marcação D'Água Digital

O modelamento da marcação d'água digital como um sistema de comunicação, onde a marca d'água representa o sinal a ser transmitido e o hospedeiro da marca, o sinal interferente, é muito útil quando analisa-se o desempenho e outras características da marcação d'água digital. Neste contexto, o problema do modelamento da marcação d'água digital já foi investigado em [4], [5] e [6], e como qualquer sistema de comunicações, surge a natural limitação da capacidade do sistema, exigindo o emprego de arquiteturas codificadas a fim de possibilitar o desempenho próximo à capacidade do sistema. Nosso objetivo neste capítulo é apresentar os principais modelos que permitirão o entendimento e o desenvolvimento dos capítulos subsequentes.

2.1

Modelo Básico

O problema de marcação digital possui muitos aspectos e etapas a serem considerados: o domínio hospedeiro e a seleção de coeficientes do mesmo para a marcação, o modelo de percepção humano (auditivo e visual), os possíveis ataques, sincronismo, segurança, requisitos específicos de uma aplicação, economicidade, entre outros. Neste capítulo, iremos considerar somente a etapa da marcação (modulação) do hospedeiro, e a correspondente recuperação da marca (deteção ou demodulação), levando em conta um modelo de ataque específico (ruído gaussiano).

O diagrama de blocos da Fig. 2.1 ilustra o modelo geral para a marcação d'água binária não codificada. Neste diagrama cada bit b , do bloco de bits de informação da marca d'água, deve marcar, através de um processamento específico no modulador, N amostras (coeficientes) distintas do sinal hospedeiro, o vetor $\mathbf{x} \in \mathbb{R}^N$, para produzir o sinal marcado \mathbf{s} . O

vetor \mathbf{x} é qualquer representação adequada de parte do sinal hospedeiro. No caso de uma imagem hospedeira, por exemplo, \mathbf{x} pode ser um vetor de valores de pixels, ou um vetor de coeficientes de uma transformada cosseno discreta (DCT).

O processamento do modulador fornece como saída o vetor $\mathbf{s}(b, \mathbf{x}) \in \mathbb{R}^N$. Devido a similaridade com o modelo de comunicação, refere-se também ao processo de marcação como modulação.

A taxa de modulação dos bits de informação (marca d'água) é $1/N$ bits por amostra do sinal hospedeiro. Naturalmente, entre outros requisitos, a técnica de modulação deve ser projetada para maximizar esta taxa de marcação, minimizando o comprimento N do vetor \mathbf{x} necessário para proceder a marcação com cada bit.

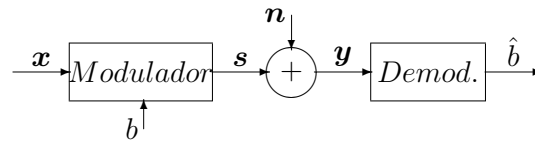


Figura 2.1: Modelo do problema da marcação d'água binária não codificada .

A distorção entre o sinal marcado \mathbf{s} e o hospedeiro \mathbf{x} , em consequência da modulação com o bit b , pode ser medida por

$$D_b = \frac{1}{N} \sum_{i=1}^N E\{(s_i - x_i)^2\}. \quad (2-1)$$

onde $E\{\cdot\}$ representa a expectativa. Note que D_b também pode ser interpretada como a medida da potência (σ_{wm}^2) da marca d'água. Assim, é possível determinar a energia do bit, E_b , responsável por provocar a correspondente distorção (devido a modulação), como sendo

$$E_b = ND_b = N\sigma_{wm}^2. \quad (2-2)$$

Diversos tipos inocentes de processamento de sinais, como a compressão, ou maliciosos, como o ruído aditivo, podem ser introduzidos no sinal marcado \mathbf{s} . Estes processamentos podem não intencionalmente, ou intencionalmente, remover a marca d'água digital. Estes processamentos são genericamente chamados de ataques. Nesta tese, o ataque será modelado por uma seqüência decorrelacionada de um ruído gaussiano aditivo $\mathbf{n} \in \mathbb{R}^N$,

com média zero, e variância $\sigma_n^2 = N_0/2$. Assim, na entrada do demodulador (detetor) tem-se

$$\mathbf{y} = \mathbf{s} + \mathbf{n}, \quad (2-3)$$

correspondendo ao sinal marcado que sofreu um ataque. Outra classe de ataque, não é direcionada à marca d'água propriamente, mas à capacidade de sincronização do detetor (o detetor precisa encontrar onde cada bit da marca d'água está escondido no sinal hospedeiro), e não é considerada neste modelo apresentado. Segmentação e transformadas geométricas são exemplos de ataques à sincronização do detetor que afetam a capacidade de recuperação da marca d'água.

O objetivo do demodulador (detetor) é produzir em sua saída, através da observação de \mathbf{y} , a melhor estimativa $\hat{\mathbf{b}}$ da marca d'água digital. A técnica de modulação/demodulação é dita “não cega”, quando \mathbf{x} está disponível no receptor para auxiliar o processamento da demodulação, ou “cega”, caso contrário. A maioria das aplicações práticas de interesse requerem o emprego de técnicas cegas, em virtude da necessidade de preservar a segurança do sinal hospedeiro original (não marcado), ou mesmo pela impossibilidade em disponibilizar o mesmo no demodulador para aplicações quase em tempo real. Contudo, a modulação/demodulação, no caso de técnicas cegas, não é uma tarefa simples em virtude da interferência que o sinal hospedeiro introduz no processo de detecção. Exemplos de implementação de técnicas cegas são a *spread transform dither modulation* (STDM) [4], o esquema Costa escalar (SCS) [6] e o espalhamento espectral avançado (ISS) [9].

Considerando o ruído \mathbf{n} estatisticamente independente das demais variáveis do problema, podemos expressar a distorção do sinal \mathbf{y} em relação a \mathbf{x} como

$$D_{\mathbf{y}} = \sigma_{wm}^2 + \sigma_n^2. \quad (2-4)$$

A tabela 2.1 relaciona alguns parâmetros, notações e definições, que serão empregados ao longo desta tese. Quando $N > 1$, a técnica de modulação é dita, de uma maneira geral, de espalhamento. Observa-se que da definição de WNR_N (razão marca d'água - ruído normalizada) obtém-se

$$WNR_N = 2E_b/N_0, \quad (2-5)$$

que representa uma correspondência simples com o parâmetro E_b/N_0 , largamente empregado em teoria da informação e da comunicação.

Tabela 2.1: Notação de Parâmetros

Parametro	Definição
Razão marca d'água - ruído	$WNR = \frac{D_b}{\sigma_n^2}$
Razão marca d'água - ruído normalizada	$WNR_N = \frac{E_b}{\sigma_n^2}$
Razão documento hospedeiro - marca d'água	$DWR = \frac{\sigma_x^2}{D_b}$
Razão documento hospedeiro - ruído	$DNR = \frac{\sigma_x^2}{\sigma_n^2}$

2.2

Modelo Super-Canal

Como já mencionado, as técnicas de detecção cega são as de maior interesse. Em seguida, um modelo alternativo para o problema de marcação d'água digital com demodulação cega é apresentado na Fig.2.2. Este modelo, que é equivalente ao modelo da Fig.2.1, quando é definido o sinal $\mathbf{e}(\mathbf{x}, b) \triangleq \mathbf{s}(\mathbf{x}, b) - \mathbf{x}$, como observado em [4], representa mais claramente o problema de marcação digital no contexto de sistemas de comunicações, como será explicado. O sinal \mathbf{e} pode ser interpretado como a entrada de um “super-canal” sujeito a uma interferência aditiva \mathbf{x} em cascata com um canal tradicional. Este sinal \mathbf{x} , que representa o estado deste “super-canal”, é conhecido pelo modulador. Neste modelo a distorção é dada por $\frac{1}{N} \|\mathbf{e}\|^2$.

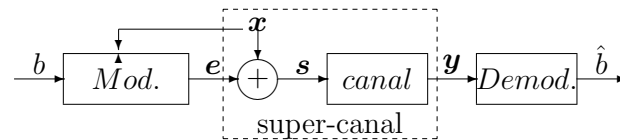


Figura 2.2: Modelo alternativo “super-canal” equivalente ao problema de marcação d'água digital.

A importância deste modelo equivalente reside na possibilidade de permitir o emprego do resultado alcançado por Costa em seu artigo *Writing on Dirty Paper* [7]. Neste artigo, ficou demonstrado que, sob algumas condições, a capacidade do “super-canal” ilustrado na Fig. 2.2, surpreendentemente, é independente da interferência (estado) \mathbf{x} , ainda que o mesmo não seja do conhecimento do demodulador. Provou-se que esta capacidade é dada por

$$C = \frac{1}{2} \log_2(1 + WNR) \text{ bits/amostra}, \quad (2-6)$$

a mesma capacidade de um canal sem interferência.

Interessante observar que na correspondência com um sistema de comunicações, o hospedeiro \mathbf{x} pode ser considerado o sinal interferente quando não há sua disponibilidade no processo de recuperação da marca (deteção cega). Nas aplicações onde é possível empregar o hospedeiro na deteção, o mesmo pode ser considerado a portadora da marca d'água.

2.3

Modelo com Codificação

A modulação binária codificada é genericamente modelada como ilustrado na Fig. 2.3. Neste diagrama, os bits de informação da marca d'água digital, representados por um bloco de bits b , são codificados (com uma taxa R) antes da marcação do sinal hospedeiro. Cada conjunto de N amostras do sinal hospedeiro, representado pelo vetor $\mathbf{x} \in \mathbb{R}^N$, é modulado por $1/R$ bits (quantidade de bits codificados na saída do codificador para cada bit de informação b da marca d'água na entrada do codificador), produzindo o sinal modulado \mathbf{s} na saída do modulador. Então, o processamento do modulador gera em sua saída o vetor $\mathbf{s}(b, \mathbf{x}) \in \mathbb{R}^N$. O valor $1/N$ (bits por amostra) chama-se de taxa de modulação (ou de marcação).

A diferença entre os vetores \mathbf{x} e \mathbf{s} é medida de acordo com um critério de distorção, esta distorção não deve exceder parâmetros bem restritivos a fim de não corromper a percepção original do sinal hospedeiro. Esta restrição é a razão principal para o emprego de códigos corretores de erros no esquema de marcação digital, possibilitando que a distorção introduzida seja minimizada, isto é, a potência da marca d'água necessária para a modulação pode ser bastante reduzida para um determinado nível de desempenho. Ainda, o emprego de códigos também permite maximizar a taxa de modulação, minimizando o comprimento N do vetor hospedeiro \mathbf{x} necessário para a modulação com cada bit, implicando no aumento da capacidade (quantidade total de bits que o hospedeiro pode ser marcado) da técnica. Assim, para um dado desempenho (probabilidade de erro de deteção), o “ganho de codificação” irá permitir a operação com a significativa redução da razão sinal (marca d'água) - ruído (ataque).

O objetivo do demodulador é fornecer a melhor estimativa dos bits codificados, e a do decodificador, a melhor estimativa, \hat{b} , dos bits da marca d'água b .

2.4 Análise de Capacidades

Antes de prosseguir para o próximo capítulo, uma interessante discussão e interpretação das capacidades envolvidas no problema de marcação d'água digital, orientados pelo resultado de Costa [7], serão conduzidos.

2.4.1

“Conservação” da Capacidade no Problema da Marcação D'Água

O modelo da marcação d'água digital representado na Fig.2.2 também pode ser interpretado como um canal possuindo 2 (dois) usuários. O usuário hospedeiro (ou interferente), com potência σ_x^2 , e o usuário marcador d'água, com potência σ_{wm}^2 (potência do sinal e) que também é a distorção introduzida no sinal s em relação a x em virtude da modulação. Assim, o canal suporta 2 (dois) usuários e sua capacidade ($C^{channel}$) é bem conhecida:

$$C^{channel} = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_x^2 + \sigma_{wm}^2}{\sigma_n^2} \right) \text{ bits/amostra}, \quad (2-7)$$

O usuário hospedeiro enxerga o canal possuindo duas fontes de ruído interferentes. Uma interferência é o ruído do canal, e a outra é a interferência da marca d'água. Considerando a marca d'água também modelada por uma variável gaussiana, pode-se expressar a capacidade vista pelo hospedeiro (C^{host}) como

$$C^{host} = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_x^2}{\sigma_n^2 + \sigma_{wm}^2} \right) \text{ bits/amostra}, \quad (2-8)$$

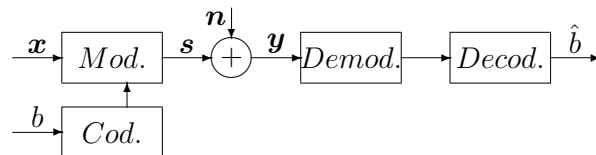


Figura 2.3: Modelo do problema de marcação d'água digital codificada.

Finalmente, empregando o resultado de Costa, apresentado na equação 2-6, a capacidade do usuário marcador d'água (C^{wm}), dado que este usuário possui conhecimento do sinal hospedeiro, é

$$C^{wm} = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_{wm}^2}{\sigma_n^2} \right) \text{ bits/amostra}, \quad (2-9)$$

Agora, é muito interessante reparar que

$$C^{channel} = C^{host} + C^{wm}, \quad (2-10)$$

sugerindo um tipo de conceito de “conservação de capacidade”.

Para muitas aplicações, é razoável considerar que a potência do sinal hospedeiro σ_x^2 é dada (fixa), e que uma limitação da distorção total (em virtude da interferência e do ruído de ataque), D^T , é exigida. Assim, no pior caso esta limitação pode ser expressa como $\sigma_n^2 + \sigma_{wm}^2 = D^T$. Desta forma podemos reescrever as expressões capacidades acima como

$$C^{channel} = \frac{1}{2} \log_2 \left(\frac{1/\psi + 1}{1 - \rho} \right) \text{ bits/amostra}, \quad (2-11)$$

$$C^{host} = \frac{1}{2} \log_2 (1 + 1/\psi) \text{ bits/amostra}, \quad (2-12)$$

$$C^{wm} = \frac{1}{2} \log_2 \left(\frac{1}{1 - \rho} \right) \text{ bits/amostra}. \quad (2-13)$$

Onde o fator de distorção (ψ) é definido como $\psi = D^T / \sigma_x^2$, representando o total da distorção permitida em relação a potência do sinal hospedeiro, e o fator de robustez (ρ), como $\rho = \sigma_{wm}^2 / D^T$, representando a contribuição relativa da marca d'água para a distorção total. Vale observar que o ruído de ataque também possui restrição de potência de forma a não provocar distorção que afete a percepção original do hospedeiro. Ambos fatores podem ser considerados parâmetros de projeto dependentes da aplicação. Esclarecemos que a distorção introduzida, respeitada a capacidade do canal, teoricamente pode ser eliminada no processo de demodulação/deteção, isto é, tanto o hospedeiro quando a marca d'água podem ser perfeitamente recuperados.

A Figura 2.4 mostra a relação gráfica entre as capacidades acima discutidas

Naturalmente, para aplicações de marcação d'água, objetiva-se o

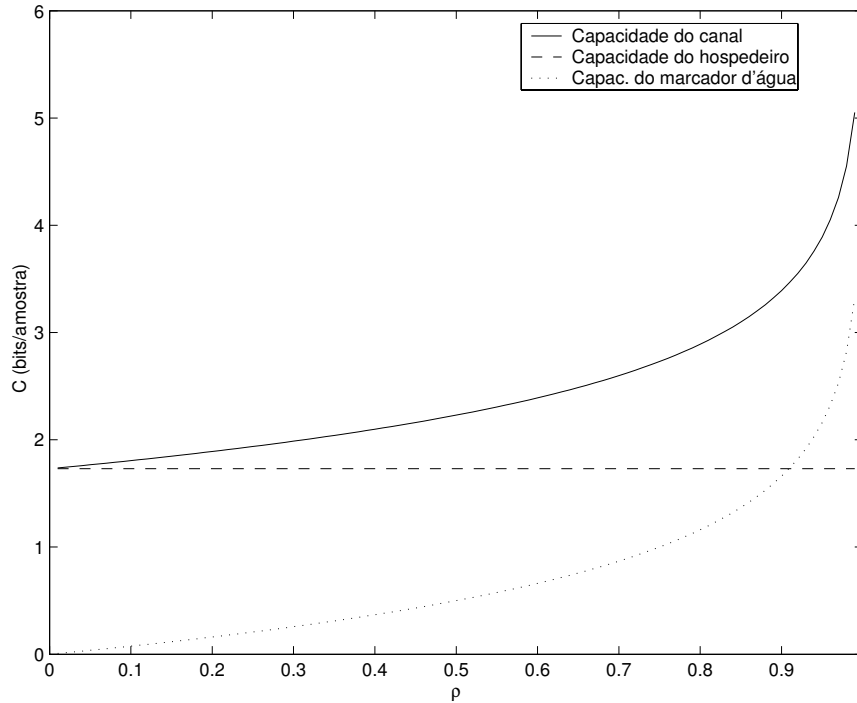


Figura 2.4: Capacidades do problema de marcação d'água como função do fator de robustez, parametrizada com o fator de distorção $\psi = 0, 1$.

emprego de um técnica que permita minimizar a distorção introduzida pela modulação. Então é necessário operar com um baixo ρ , significando que a capacidade disponível para o usuário marcador é relativamente baixa em relação a capacidade do canal. Para outras aplicações, em que este mesmo modelo pode ser empregado, como na transmissão com interferência conhecida (jamming), ou em um canal de comunicação multiusuário, a distorção introduzida na transmissão não é um requisito tão restritivo. Nestas aplicações basta garantir que os sinais distorcidos possam ser recuperados perfeitamente (ou quase perfeitamente) após a demodulação/deteção. Neste casos pode-se utilizar um valor maior para ρ , limitado apenas pela capacidade do canal.

2.4.2

Taxa excedente do hospedeiro

A discussão da seção anterior é bastante ilustrativa do ponto de vista didático, contudo na prática ocorre que o usuário hospedeiro não sabe que sofrerá uma marcação d'água, e assim o mesmo (o usuário hospedeiro)

entende que a capacidade do canal disponível ($C^{host_wm_free}$) é

$$C^{host_wm_free} = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_x^2}{\sigma_n^2} \right) \text{ bits/amostra.} \quad (2-14)$$

Nesta situação, quando o usuário marcador d'água também utiliza o canal, ocorre que o canal será utilizado além de sua capacidade. Este excedente em relação à real capacidade disponível do hospedeiro convencionamos de chamar de *taxa excedente* do usuário hospedeiro, e que pode ser determinado como

$$C^{host_wm_free} - C^{host} = \frac{1}{2} \log_2 \left(\frac{1 + \frac{1}{\psi^{(1-\rho)}}}{1 + 1/\psi} \right) \text{ bits/amostra.} \quad (2-15)$$

Esta *taxa excedente* implica que o sinal hospedeiro não poderá mais ser recuperado perfeitamente (sem erros), isto é será recuperado um sinal distorcido em relação ao sinal hospedeiro original \mathbf{x} . O termo recuperado refere-se a estimativa $\hat{\mathbf{x}}$ do hospedeiro original após a demodulação/deteção, e a distorção do sinal recuperado não deve ser confundida com a distorção do hospedeiro após a modulação e ataque presente no canal. Esta taxa excedente é motrada graficamente na Figura 2.5.

Observamos na Figura 2.5 que para possibilitar a recuperação do sinal hospedeiro, com maior fidelidade ao original, é necessário minimizar a *taxa excedente*, e assim, novamente deve-se operar com um baixo ρ , evidenciando a necessidade do emprego de códigos na marcação d'água.

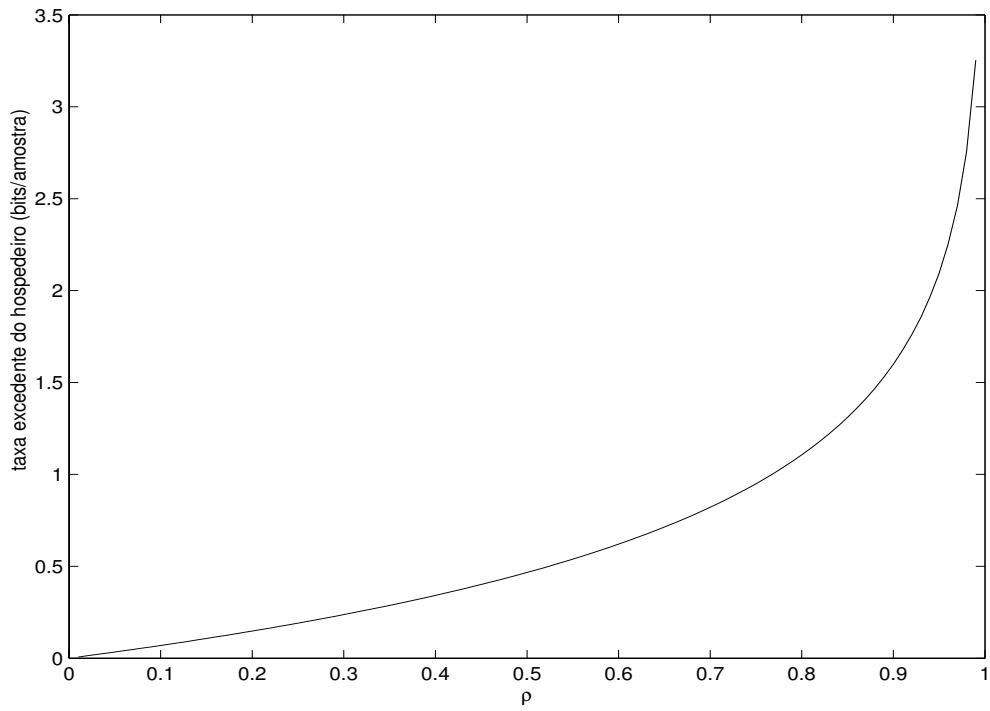


Figura 2.5: *Taxa excedente* em função do fator de robustez, parametrizado com o fator de distorção $\psi = 0.1$.