Parte II

Influência da Codificação na Marcação D'Água Digital

5
Modelamento da Fragilidade e Robustez de Marcas D'Água digital e a Influência da Codificação

Neste capítulo será introduzida uma nova metodologia para projeto e análise de sistemas de marcação d'água digital que, utilizando um enfoque prático da teoria da informação, incorpora as importantes propriedades de robustez e fragilidade das marcas d'água. A metodologia proposta é desenvolvida pela análise da curva de desempenho da técnica de marcação, considerando o efeito da codificação na mesma, em não só proporcionar o ganho de codificação, mas também na influência das características de robustez e fragilidade da marca d'água. Este novo conceito requer o resgate da análise e investigação de técnicas de codificação para também incluirem os requisitos de robustez e fragilidade nas respectivas implementações, e neste sentido será inicialmente investigado o código turbo.

5.1
Modelo de Projeto e Análise para as características de Robustez e Fragilidade de Marcas D'Água Digitais

Dois conceitos são fundamentais em nossa discussão: robustez e fragilidade. A robustez da marca d'água refere-se à capacidade da técnica em extrair confiavelmente (baixa probabilidade de erro na deteção) a marca, após ter sofrido ataques, mesmo quando presente ataques considerados de alta intensidade. Esta condição de robustez é muito importante em aplicações de proteção dos direitos (*copyright protection*) relacionados ao sinal hospedeiro. Por outro lado, a fragilidade de um esquema de marcação digital refere-se à capacidade de impedir que a marca d'água seja detetada, mesmo que o ataque seja considerado de baixa intensidade. Esta condição de fragilidade é bastante desejada em aplicações de verificação de autenticidade e integridade do sinal hospedeiro.

Em seguida, a análise do comportamento da fragilidade e da robustez será conduzida com o foco na dependência destes comportamentos com a curva de desempenho da técnica de marcação digital. Refere-se aqui ao desempenho da técnica como a probabilidade de erro de deteção (p_e) em função de WNR_N. Na prática, p_e é estimado pela medida da taxa de bits errados (BER), correspondendo a razão entre os bits estimados erroneamente na deteção, e o número total de bits da marca d'água.

Vamos agora introduzir alguns parâmetros de projeto que consideram as caracterísitcas de fragilidade e robustez. O primeiro parâmetro, D^M , estabelece um limitante superior da distorção admissível no sinal hospedeiro. Acima desta distorção, o sinal hospedeiro é considerado sem utilidade (ou sem valor), isto é a percepção original do hospedeiro está significativamente corrompida, não havendo mais sentido proteger os direitos em relação ao mesmo.

O segundo parâmetro estabelece um limiar p_e^M para a probabilidade de erro na deteção da marca d'água. Acima deste limiar, a marca d'água recuperada (detectada) pelo detetor não é mais considerada uma estimação confiável. Assim, por exemplo, em uma deteção com $BER > p_e^M$, uma aplicação de verificação de autenticidade indicará ao usuário que o hospedeiro foi corrompido por um ataque.

Assim, considerando os conceitos apresentados, e os parâmetros introduzidos, podemos inferir que um esquema de marcação opera em modo robusto quando a probabilidade de erro de deteção da marca d'água é inferior a p_e^M ($p_e < p_e^M$), mesmo com $D_y > D^M$ (distorção total superior a máxima admissivel). Da mesma maneira, o esquema opera em modo frágil quando $p_e > p_e^M$ (marca d'água corrompida), mesmo com $D_y < D^M$. Em seguida vamos aprofundar a análise de robustez e fragilidade.

O parâmetro condicionante da distorção máxima traduz-se pela expressão

$$D_{\boldsymbol{y}} = \sigma_{wm}^2 + \sigma_n^2 < D^M \ , \tag{5-1}$$

Vamos definir o fator de robustez (ρ) como

$$\rho = \sigma_{wm}^2 / D^M \ . \tag{5-2}$$

Este fator representa a parcela relativa da contribuição da marcação para a distorção total, e é fácil verificar que $0 < \rho < 1$. Assim a equação 5-1 pode ser reescrita como

$$WNR_N > N\rho/(1-\rho) = WNR_N^{D^M} \ , \tag{5-3}$$

significando que o hospedeiro será considerado utilizável (não corrompido) desde que WNR_N seja superior ao valor $WNR_N^{D^M}$ acima definido.

O parâmetro condicionante da máxima probabilidade de erro admissível, como já visto, traduz-se pela expressão

$$p_e < p_e^M \ . \tag{5-4}$$

Como a função de desempenho $p_e = f(WNR_N)$ é uma função decrescente em WNR_N, este condicionante pode ser reescrito como

$$WNR_N > f^{-1}(p_e^M) = WNR_N^{p_e^M} \ , \tag{5-5}$$

significando que para deteção confiável da marca d'água, WNR_N deve ser maior do que o valor $WNR_N^{p_e^M}$ acima definido. Assim, as desigualdades (5-3) and (5-5) vão balizar o projeto do sistema de marcação como será discutido a seguir.

Na ausência do ataque (ruído), a razão normalizada marca d'água - ruído (WNR_N) é infinita, e a probabilidade de erro p_e é zero, supondo um técnica de deteção cega ideal (o hospedeiro não interfere na deteção). Na medida em que a intensidade do ataque aumenta, a razão sinal-ruído (WNR_N) diminui, enquanto a probabilidade de erro p_e cresce, descrevendo a curva de desempenho do esquema. Assim, à medida que o ataque é incrementado (reduzindo WNR_N), se WNR_N atinge o valor $WNR_N^{D^M}$ antes de atingir o valor $WNR_N^{p_e^M}$, o esquema é robusto. De outro modo, se WNR_N assume primeiramente o valor $WNR_N^{p_e^M}$, o esquema é frágil. Resumindo, temos:

- Robustez : Mesmo após ter havido distorção crítica no hospedeiro ($D_y > D^M$), ainda é possível recuperar a marca d'água com confiabilidade ($p_e < p_e^M$).
- Fragilidade : A deteção confiável da marca d'água é perdida ($p_e > p_e^M$) antes de se ter atingido a distorção crítica no hospedeiro ($D_y < D^M$), i.e., a autenticidade/integridade do hospedeiro é medida como a

capacidade do esquema detetar confiavelmente a marca d'água, e a adulteração do hospedeiro é indicada quando essa capacidade é perdida.

Ainda, o valor $WNR_N^{D^M} - WNR_N^{p_e^M}$ pode ser utilizado para representar uma medida de robustez ou fragilidade. Assim, se deseja-se projetar um esquema bastante robusto $WNR_N^{D^M}$ deve ser bem superior a $WNR_N^{p_e^M}$, e para um esquema frágil, $WNR_N^{D^M}$ deve ser bem inferior a $WNR_N^{p_e^M}$.

A Figura 5.1 ilustra a discussão anterior. O desempenho da técnica STDM [4] não codificada foi utilizado neste exemplo.
O parâmetro de deteção confiável foi escolhido ser $p_e^M = 10^{-5}$, fornecendo

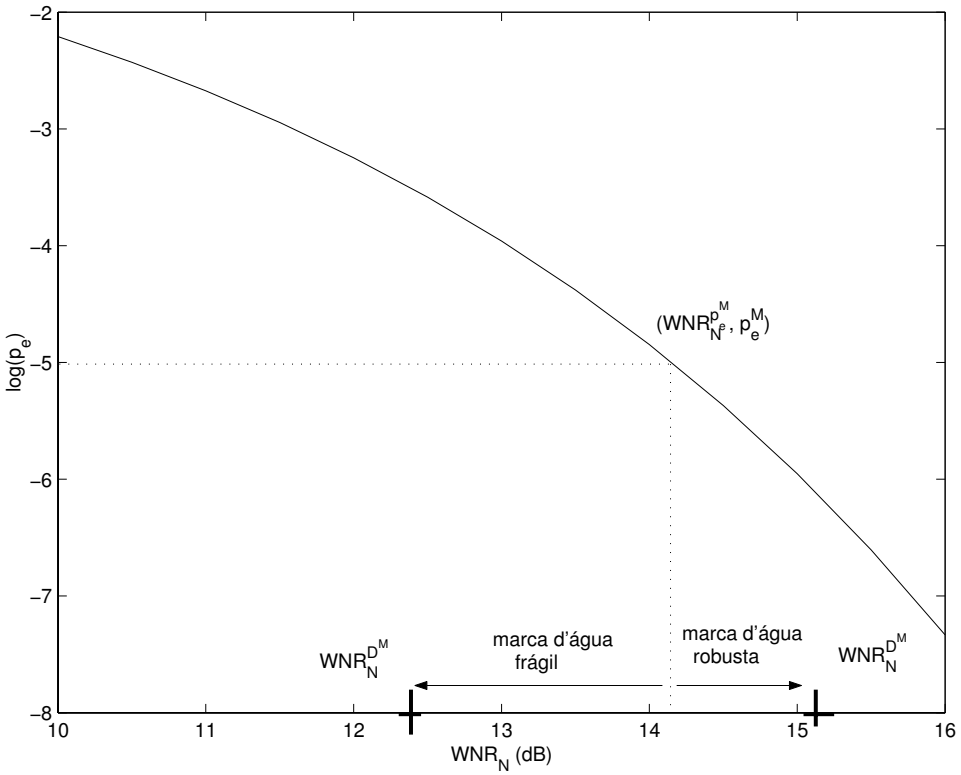

Figura 5.1: Parâmetros de projeto empregando desempenho da técnica STDM de marcação d'água digital.

$WNR_N^{p_e^M} = 14.1dB$. O projeto pode agora ser conduzido através da escolha apropriada dos parâmetros N e ρ. Se um sistema robusto é desejado, o valor de $WNR_N^{D^M}$ deve ser ajustado, de acordo com a equação 5-3, tal que $WNR_N^{D^M} > 14.1dB$. Por outro lado, se o objetivo é projetar um esquema frágil, este ajuste deve ser tal que $WNR_N^{D^M} < 14.1dB$. A Figura 5.1 ilustra as duas alternativas de projeto. A seta orientada para a direita (esquerda) do ponto $WNR_N = 14.1dB$ até $WNR_N = WNR_N^{D^M}$ mede

a robustez (fragilidade) do esquema. Assim, verificamos que a curva de desempenho da técnica tem um papel importante na projeto do esquema, e pode ser utilizada para ajustar tanto um esquema frágil quanto um robusto.

5.2 Influência da Codificação na Robustez e na Fragilidade da Marcação D'Água Digital

Um aspecto importante da robustez e fragilidade, não tratado na seção anterior, é a sensitividade, medida pela inclinação (derivada) da curva de desempenho. A idéia pode ser melhor entendida quando comparamos dois sistemas de marcação A e B operando no modo robusto (frágil). O sistema A é mais robusto (frágil) do que o sistema B, se ao incrementar a intensidade do ataque (reduzindo WNR_N), no mesmo valor nos dois sistemas, resulta num incremento de p_e, para o sistema A, inferior (superior) ao incremento correspondente para o sistema B. Assim, nesta comparação, verifica-se que inclinação da curva de desempenho é fundamental, tendo em vista que os mencionados incrementos de p_e estão diretamente relacionados a mesma.

Assim, a curva de desempenho (p_e^M versus WNR_N) possui importante influência não só na definição do modo de operação (robusto ou frágil), como descrito na seção 5.1, mas também na sensitividade do correspondente modo de operação. Lembrando que as técnicas de codificação podem afetar significativamente a forma da curva de desempenho, leva-nos a considerar que investigar a influência destas técnicas na sensitividade do modo (robusto ou frágil) é importante. De fato, como será visto em seguida, e também no próximo capítulo, esta influência pode ser convenientemente utilizada no projeto do sistema para, além de proporcionar o conhecido ganho de codificação (veja apêndice A), também obter a sensitividade adequada ao modo de operação (robusto ou frágil). Assim, o projeto de técnicas de codificação deve ser revisitado para também considerar este novo cenário de emprego em marcação d'água digital.

Aprofundando nossa discussão, vamos considerar, como exemplo, que o codificador empregado na Figura 2.3 é um típico código turbo [13] com desempenho conforme representado no gráfico da Figura 5.2 (para

implementações de marcação d'água codificada referir-se a [6]).

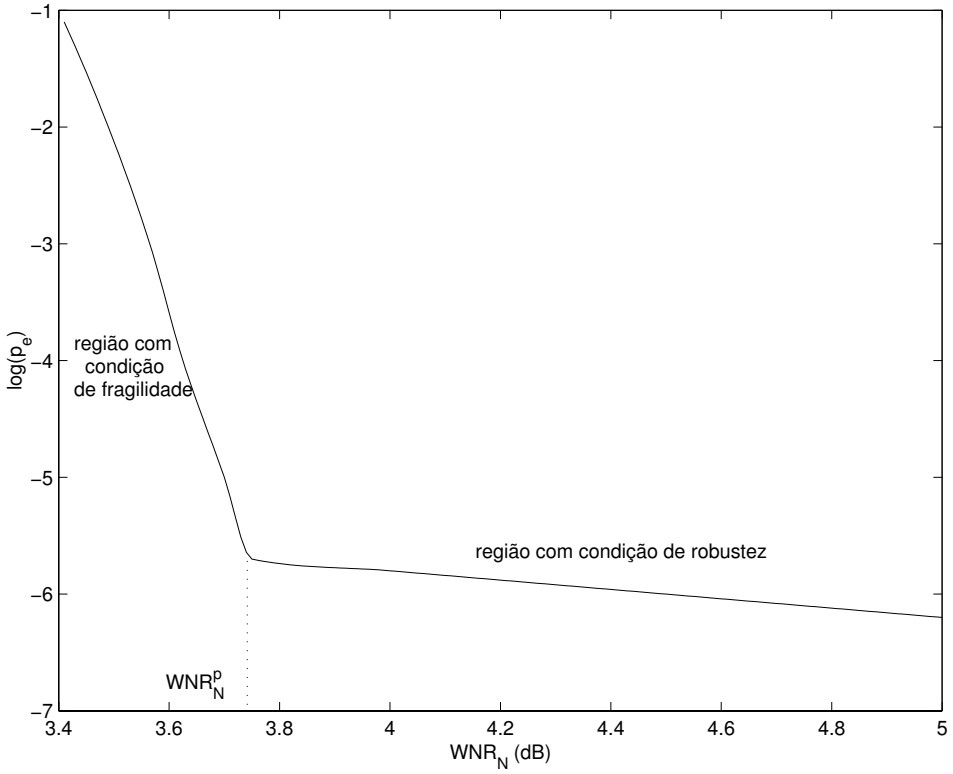

Figura 5.2: Desempenho de um codificador turbo típico com taxa 1/2.

Observando a figura 5.2 podemos conluir que a codificação turbo pode ser diretamente empregada para um esquema de marcação d'água robusta, pois a curva de desempenho possui uma inclinação (derivada) bastante reduzida no domínio $WNR_N > 3.75dB$, representando a região com condição de robustez, para este exemplo em particular. Assim, para projetar um sistema operando com baixa sensitividade em modo robusto, com $p_e^M < 10^{-6}$, basta ajustarmos os parâmetros de projeto (N e ρ) tais que $WNR_N^{D^M} > 3.75dB$.

Quanto a operação em modo frágil, a primeira impressão do codificador turbo é de que o mesmo não é diretamente apropriado para tanto. A dificuldade em garantir adequada fragilidade à marca d'água reside no fato de ser necessária uma alta intensidade de ataque, até que a região de alta sensitividade (região com condição de fragilidade) seja alcançada, de forma a degradar a confiabilidade de deteção da mesma. Uma solução

para superar tal dificuldade (o objetivo de um esquema frágil é garantir a perda de deteção da marca d'água para baixas intensidades do ataque) será apresentada no próximo capítulo.