# Limitante Inferior da Marcação D'Água Digital não Codificada

Marcos de Castro Pacitti* e Weiler Alves Finamore**

***Resumo*— Neste artigo é proposto um novo limitante inferior para orientar o desenvolvimento de técnicas de marcação d'água digital cega (blind) não codificadas, introduzindo, em conseqüência, uma nova metodologia de projeto para as mesmas, com fundamento proveniente da teoria da informação. A metodologia proposta consiste de duas etapas que contemplam, na primeira etapa, a otimização do ganho de modulação, e na segunda etapa, a maximização do ganho de codificação. Na primeira etapa, o desenvolvimento da técnica de modulação da marca d'água no sinal hospedeiro objetiva minimizar a interferência do hospedeiro na saída do demodulador. É proposto um limitante de projeto para esta primeira etapa, denominado de limitante inferior de modulação não codificada, considerando um ataque ou ruído gaussiano. Na segunda etapa, a marca d'água é codificada e emprega-se a técnica de modulação no sinal hospedeiro com a marca codificada. A codificação da marca nesta etapa objetiva a operação próxima à capacidade do sistema, já que a interferência do hospedeiro foi minimizada. Casos particulares de implementações existentes das técnicas de modulação via espalhamento espectral ($SS$) e modulação indexada por quantização ($QIM$) são analisadas e comparadas ao proposto limitante de modulação não codificada, e alguns limites práticos de projeto são calculados considerando a codificação turbo.**

***Palavras-Chave*— Marca d'água digital, camuflagem da informação, segurança da informação, modulação indexada pela quantização, espalhamento espectral, códigos turbo, ganho de codificação.**

***Abstract*— This paper introduces a new lower bound to guide the analysis and development of non coded digital watermarking modulation techniques, based on a simple equivalence with a binary communication system. This non coded lower bound introduces a new methodology on the techniques design. When compared with others results we observe that the proposed lower bound is more accurate and general. Practical bounds for digital watermarking under turbo coding are examined in the context of the proposed non coded lower bound.**

***Keywords*— Digital watermarking, information hiding, information security, quantization index modulation, spread spectrum, turbo codes, coding gain, covert communication.**

## I. INTRODUÇÃO

A utilização de marca d'água, onde permeia-se a informação (a marca) em um documento hospedeiro de forma a não ser imediatamente percebida e a dificultar a sua reprodução, já vem sendo bastante empregada, objetivando reprimir a falsificação. Estas técnicas já são utilizadas em documentos e dinheiro há séculos. Atualmente, com a ampla utilização da representação digital de documentos, imagens, áudio, e outros sinais, a proteção de direitos de reprodução e autorais utilizando técnicas de marcação d'água digital tornou-se uma área muito ativa de pesquisa (veja extensa bibliografia em [1]). Naturalmente, muitas outras aplicações surgiram nesta nova perspectiva digital do assunto [2], incluindo as aplicações de segurança nacional como as para verificação de integridade/autenticidade da mídia, para "comunicação camuflada" (*covert communication*) da informação, e para "rastreamento de traidor" (*traitor tracing*).

A marcação d'água neste novo contexto é um problema complexo, com questões que envolvem não somente a marcação digital e fatores subjetivos da percepção humana, mas também o projeto sistêmico, segurança, e uma série de aspectos econômicos e legais. Em nosso artigo, tratamos apenas de parte do problema: os limitantes de parâmetros utilizados em projetos de marcação (modulação) da informação em um sinal hospedeiro, isto é, de técnicas de marcação d'água digital. Estes limitantes de desempenho correspondem a etapas de minimização da energia da marca d'água necessária para operação com uma especificada probabilidade de erro na recuperação da mesma.

O limitante inferior de desempenho de um sistema de marcação d'água digital já foi estudado em [3], e para almejar alcançá-lo, na prática, propostas de utilização de códigos corretores de erro foram implementadas [10]. Para algumas técnicas de modulação não codificada, aproximações ou limitantes superiores de desempenho foram realizados ([3], [4], [5]). Contudo, pelo conhecimento dos autores, carece na literatura pesquisas quanto ao limitante inferior de desempenho destas técnicas antes de efetuar-se a codificação. É proposto em [8] um limitante inferior, com base nos resultados da referência [3], para as técnicas derivadas da modulação tipo "Spread Spectrum" ($SS$) não codificadas.

Fundamentado no trabalho de Costa [6], e no relacionamento do problema de marcação digital com a transmissão em um sistema de comunicação, neste artigo é proposto um limitante inferior de projeto para qualquer técnica sob consideração, antes de se efetuar a codificação da marca, introduzindo um nova metodologia de projeto para as técnicas de modulação digital. Uma vez encontrada a técnica de modulação que se aproxime deste limitante, emprega-se as já conhecidas técnicas de codificação para correção de erros objetivando a operação do sistema próximo a capacidade canal.

Na seção II, apresentamos o modelamento do problema de marcação d'água digital, incluindo a descrição dos diversos parâmetros envolvidos na análise e no projeto das técnicas

Este trabalho foi parcialmente financiado pela Comissão de Implantação do Sistema de Controle do Espaço Aéreo Brasileiro (CISCEA)- Comando da Aeronáutica - Ministério da Defesa.

*Marcos de Castro Pacitti, CISCEA, Rio de Janeiro, Brasil, E-mail: pacitti@cc.sivam.gov.br.

**Weiler Alves Finamore, CETUC / PUC - RJ, Rio de Janeiro, Brasil, E-mail: weiler@cetuc.puc-rio.br

de modulação. Na seção III, apresentamos nossa proposta do limitante inferior de projeto para a modulação digital não codificada, e na seção IV, comparamos e analisamos este limitante proposto em relação as principais técnicas existentes de modulação de marca d'água digital. Na seção V, introduzimos uma nova metodologia de projeto de técnicas de marcação digital, incluindo as considerações de um exemplo prático para codificação turbo.

## II. Modelo do Problema

O problema de modulação ou marcação d'água binária é genericamente descrito na fig. 1. Nesta figura o sinal hospedeiro é representado por um vetor $\mathbf{x} \in \mathbb{R}^N$ que é modulado por um bit de informação $b$, gerando o vetor $\mathbf{s}(b, \mathbf{x}) \in \mathbb{R}^{\mathbb{N}}$ na saída do modulador.[1] A taxa de marcação é de $1/N$ bits por dimensão (amostra do sinal hospedeiro), e o vetor $\mathbf{s}$ normalmente possui uma restrição de distorção.

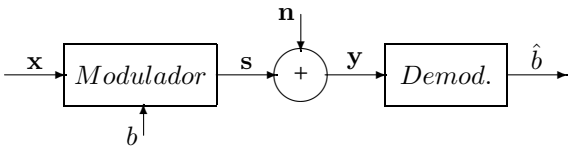


Fig. 1. Modelo do problema de marcacação/estimação do bit de informação $b$ no hospedeiro $\mathbf{x}$.

A distorção ($D_b$) do sinal $\mathbf{s}$ , em relação a $\mathbf{x}$ , provocada pela modulação com o bit $b$, é definida por

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

assim, podemos considerar que a energia do bit ($E_b$) necessária para provocar a correspondente distorção é

$$E_b = ND_b \tag{2}$$

O sinal marcado $\mathbf{s}$ está sujeito a diversas manipulações comuns de processamento de sinal e de tentativas voluntárias de remover a informação marcada. Estas manipulações são denominadas de ruído ou ataque, e também estão restritas pela distorção provocada no sinal. Em nosso artigo consideraremos que o ataque é resumido a um ruído gaussiano aditivo $\mathbf{n} \in \mathbb{R}^N$ cujas componentes são descorrelacionadas, possuem média nula e variância $\sigma_n^2$ . Assim na entrada do domodulador temos o sinal $\mathbf{y} = \mathbf{s}+\mathbf{n}$. O demodulador processa o sinal $\mathbf{y}$ em função da técnica de modulação utilizada, e fornece como saída uma estimativa $\hat{b}$ do bit de informação $b$. É interessante notar que o modelo apresentado é análogo a um sistema de comunicação onde há um sinal interferente $\mathbf{x}$ e um ruído aditivo $\mathbf{n}$.

Na Tabela I introduz-se algumas notações a fim de padronizar os parâmetros de análise, para facilitar a comparação de resultados. Nesta tabela $\sigma_x^2 = E[x_i^2]$, e foi considerado que $E[x_i] = 0$.

[1]O vetor $\mathbf{x}$ é qualquer representação conveniente de todo ou parte do sinal hospedeiro. No caso do sinal hospedeiro ser uma imagem, o vetor $\mathbf{x}$ pode possuir componentes correspondentes a valores selecionados de pixels ou coeficientes de uma transformada ($DCT$ ou $DWT$, por exemplo).

TABELA I
NOTAÇÃO DOS PARÂMETROS DE ANÁLISE

| Parâmetro | Definiçao |
|---|---|
| Razão marca-ruído | $WNR = \frac{D_b}{\sigma_n^2}$ |
| Razão marca-ruído normalizada | $WNR_N = \frac{E_b}{\sigma_n^2}$ |
| Razão documento hospedeiro-marca | $DWR = \frac{\sigma_x^2}{D_b}$ |
| Razão documento hospedeiro-ruído | $DNR = \frac{\sigma_x^2}{\sigma_n^2}$ |

## III. Limitante inferior de modulação não codificada

Costa [6] demonstrou que, sob determinadas condições, a capacidade do canal de um sistema de comunicação, com conhecido sinal interferente, independe do mesmo e é a mesma capacidade do canal na ausência da interferência, ainda que o sinal interferente não seja conhecido no receptor. Este resultado trouxe grande motivação no desenvolvimento das técnicas de marcação d'água digital. Conforme o modelo apresentado na fig. 1, o sinal hospedeiro pode ser considerado como um sinal interferente conhecido pelo transmissor, e é altamente desejável para diversas aplicações que na recepção, a detecção ocorra sem o conhecimento do mesmo (técnica cega).

O entendimento do conceito apresentado no parágrafo anterior, possibilita-nos conjecturar que a técnica de modulação/demodulação ideal fornecerá ao estimador do correspondente demodulador apenas o sinal que representa o bit $b$ de energia $E_b$, adicionado do ruído gaussiano (distribuição $N(0, \sigma_n^2)$ ), e livre de qualquer tipo de interferência do hospedeiro $\mathbf{x}$, mesmo que o sinal hospedeiro não seja conhecido no demodulador. Assim, considerando os sinais antipodais, o modelo de marcação ideal é equivalente ao sistema BPSK de comunicação [11], e a correspondente probabilidade de erro ($p_e$) é dada por

$$p_e = \frac{1}{2}erfc(\sqrt{E_b/N_o}) \tag{3}$$

Considerando $\sigma_n^2 = N_0/2$, teremos:

$$WNR_N = 2E_b/N_o \tag{4}$$

e

$$p_e = \frac{1}{2}erfc(\sqrt{WNR_N/2}) \tag{5}$$

Assim, a expressão acima estabelece o limitante inferior para modulação binária não codificada sob ataque de ruído gaussiano aditivo.

Considerando a equivalência da técnica de marca d'água digital com um sistema de comunicação, é interessante também interpretar $\mathbf{x}$ como a portadora da marca d'água digital, e que o objetivo no desenvolvimento da técnica de modulação é eliminar a interferência da portadora $\mathbf{x}$ no processo de demodulação/estimação.

## IV. ANÁLISE E COMPARAÇÃO DO LIMITANTE INFERIOR DA MODULAÇÃO NÃO CODIFICADA COM EXISTENTES TÉCNICAS DE MODULAÇÃO

Na tabela II é sintetizado o resultado para diversos tipos marcação digital. Consideramos a tradicional técnica de espalhamento espectral ($SS$) introduzida em [7] e a correspondente técnica aperfeiçoada ($ISS$) [8] em que a interferência do hospedeiro é significantemente reduzida. Também consideramos as técnicas derivadas da modulação indexada por quantização ($QIM$) analisadas em [3]: A "*Spread-Transform Dither Modulation*"($STDM$) e "*Low Bit Modulation*"($LBM$). A técnica de projeção quantizada ($QP$) introduzida em [9] combina elementos das técnicas de modulação $SS$ e $QIM$.

TABELA II

DESEMPENHO DE TÉCNICAS DE MODULAÇÃO DIGITAL

| **Técnica** | $p_e$ |
|---|---|
| limitante | $\frac{1}{2}erfc(\sqrt{WNR_N/2})$ |
| $SS$ | $\frac{1}{2}erfc(\sqrt{WNR_N/2(1+DNR)})$ |
| $ISS$ linear | $\frac{1}{2}erfc(\sqrt{WNR_N - DNR)/2})$ |
| $STDM$ | $erfc(\sqrt{\frac{3}{8}WNR_N})$ |
| $LBM$ | $erfc(\sqrt{\frac{3}{14}WNR_N})$ |
| $QP$ | $\frac{1}{2}erfc(\sqrt{WNR_N/2(1+DWR/N)})$ |

Na fig. 2 estão representadas todas as curvas de desempenho ($log(p_e)$ x $WNR_N(dB)$) para todas as técnicas de modulação relacionadas na tabela II, incluindo também o limitante inferior de modulação não codificada. Fica evidente a facilidade de análise de projeto, e de comparação, utilizando o limitante de marcação não codificado introduzido neste artigo.

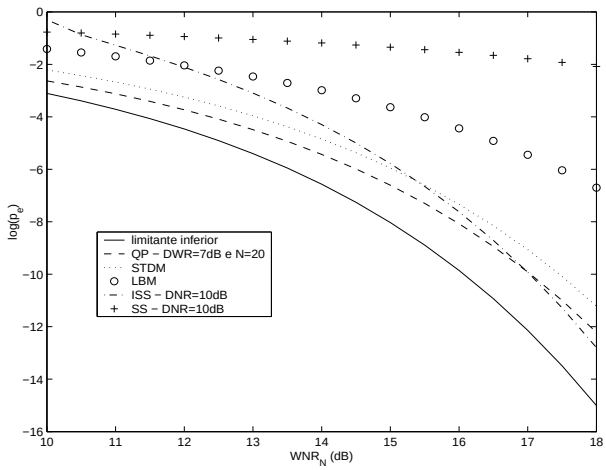


Fig. 2. Curvas de desempenho para as técnicas de modulação não codificadas consideradas na tabel II, incluindo o limitante inferior proposto neste artigo.

É interessante verificarmos o desempenho de cada técnica de modulação em termos de $\Delta WNR_N(dB)$, que corresponde a distância ou variação (em $dB$) da técnica em relação ao limitante inferior não codificado. Na Tabela III são consolidados os resultados obtidos para as técnicas consideradas.

TABELA III

COMPARAÇÃO DO LIMITANTE INFERIOR COM TÉCNICAS DE MARCAÇÃO

| **Técnica** | $\mathbf{\Delta WNR_N(dB)}$ | **Condições** |
|---|---|---|
| $SS$ | $10log(1+DNR)$ | $\forall\ p_e$ |
| $ISS$ | 0 | $WNR_N \gg DNR$ e $\forall\ p_e$ |
| $STDM$ | 1.25 | $p_e \to 0$ |
| $LBM$ | 3.68 | $p_e \to 0$ |
| $QP$ | 0 | $N \gg DWR$ e $\forall\ p_e$ |

Assim na técnica $SS$ constata-se uma forte interferência do hospedeiro, já nas modulações $ISS$ e $QP$ a interferência é minimizada, podendo ser arbitrariamente reduzida, e para as modulações $STDM$ e $LBM$ existe sempre um "gap" para o limitante inferior de modulação não codificada.

É interessante constatar que o limitante proposto, também baliza as técnicas de modulação não codificadas com compensação de distorção ($DC$). Em [10] é utilizado esta técnica de compensação de distorção para a modulação $STDM$ ($DC - STDM$) que fornece ganho de $1\ dB$ em relação a técnica $STDM$ em $p_e = 10^{-6}$. Assim, a técnica $DC - STDM$ reduz o "gap" para o limitante de marcação não codificada para aproximadamente $0.5\ dB$, naquele ponto de operação, apresentando desempenho superior as demais técnicas relacionadas, sob as condições consideradas.

Vale observar que o "gap" ($1.25\ dB$) obtido para a modulação $STDM$ é idêntico ao obtido em [3] quando compara esta modulação à técnica $SS$ sem interferência do hospedeiro, na operação com $p_e \to 0$. Em [8] é utilizado este mesmo resultado ("gap" de $1.25\ dB$ do $STDM$) como referência do limitante inferior das técnicas tipo $SS$, para operação em qualquer valor de $p_e$ , na análise dos resultados da técnica $ISS$, o que introduz uma discrepância de mais de $0.5\ dB$, para médias probabilidades de erro, em relação ao limitante inferior proposto neste artigo.

Entendemos assim, que o proposto limitante inferior de modulação não codificada é consistente com resultados já obtidos para as técnicas consideradas, e corresponde a uma referência mais precisa e geral para análise de qualquer técnica de modulação digital, e em qualquer ponto de operação.

## V. METODOLOGIA DE PROJETO

Da fig. 2, fica evidente que podemos segmentar o projeto de um sistema de marcação em duas etapas:

1) *Ganho de Modulação*: Objetiva a aproximação de operação para o limitante inferior de marcação d'água não codificada. Nesta etapa busca-se adaptar, na transmissão, a marca ao conhecido sinal hospedeiro de forma a eliminar sua interferência no processo de estimação, conforme apresentado na seção III.
2) *Ganho de Codificação*: Objetiva a utilização de códigos corretores de erro a fim de promover a operação próxima a capacidade do sistema (canal), resultando em um novo ganho em $WNR_N$ ( ou em $E_b/N_0$).

Na fig. 3 ilustramos o processo completo para obtenção de uma marcação ótima. No modelo foram incluídos um

codificador e um decodificador para obtenção do ganho de codificação. O codificador recebe bits de informação da marca d'água e entrega bits codificados ao modulador. O decodificador recebe os bits codificados junto com a interferência, que no caso ideal (limitante e inferior de modulação não codificada) é representado apenas por um ruído aditivo gaussiano, e fornece em sua saída uma estimativa dos bits de informação.

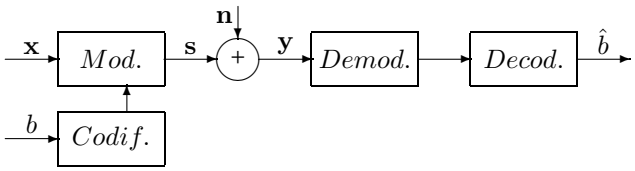


Fig. 3. Modelo do problema de marcacação/estimação do bit de informação $b$ no hospedeiro $\mathbf{x}$, incluindo a codificação da marca d'água.

Devemos observar que outras técnicas poderão integrar as etapas de modulação e codificação em um único processamento o que denominamos de marcação d'água codificada, contudo, na literatura investigada, ainda não foi constatada algum tipo de implementação prática da mesma.

A capacidade do canal é derivada da fórmula de Shannon e, para uma dada taxa $R$ do código, é diretamente obtida da seguinte desigualdade [11]:

$$E_b/N_0 > (2^{2R} - 1)/2R \tag{6}$$

Assim, o ganho máximo de codificação é obtido para $R \to 0$ em $WNR_N = 1.4\ dB$ (observar que de (4) temos $WNR_N(dB) = E_b/N_0(dB) + 3\ dB$). Já no emprego de um código com taxa $R = 1/2$, o maior ganho de codificação é obtido para operação com $WNR_N = 3\ dB$.

Como referência, é interessante verificarmos os limites de operação para $p_e < 10^{-5}$ . Neste caso, para a marcação não codificada, utilizando (5), obtem-se que $WNR_N^{limitante}(dB) > 12,5\ dB$. Assim, da tabela I, temos

$$N^{limitante}(D_b/\sigma_n^2) > 17,8 \text{ amostras}, \tag{7}$$

indicando que, para $WNR = 1$, deve-se utilizar no mínimo $18$ amostras do sinal hospedeiro para cada bit de informação da marca d'água.

Considerando agora a utilização de um código turbo, com $R = 1/2$, é possível obter para a modulação binária um ganho aproximado de $8.8\ dB$, em $E_b/N_0$ (ou $WNR_N$), conforme apresentado em [12], deslocando a operação para $WNR_N = 3.7\ dB$, estando a $0.7\ dB$ da capacidade do canal. Assim a operação para $p_e < 10^{-5}$ ocorrerá em $WNR_N^{turbo} > 3,7\ dB$, implicando em

$$N^{turbo}(D_b/\sigma_n^2) > 2,3 \text{ amostras }, \tag{8}$$

significando que, mantendo $WNR$ constante, é possível reduzir em mais de 7 vezes a quantidade de amostras, por bit de informação, em relação ao caso sem codificação. Observar que como a taxa do código é $R = 1/2$ , cada bit codificado utilizará $N^{turbo}/2$ amostras. Conclusões semelhantes podem ser derivadas para o aumento da robustez ($\sigma_n^2$) ou redução da distorção (ou $E_b$ necessário) quando empregado o código turbo, mantendo demais parâmetros fixos.

Finalmente, vale observar que, para este exemplo analisado, o ganho máximo de codificação, para operação com $p_e = 10^{-5}$, é de $11.1\ dB\ (12.5 - 1.4)$, já quando utilizamos o código com taxa $R = 1/2$, reduzimos o ganho de codificação alcançável ("gap") para $9.5\ dB\ (12.5 - 3.0)$.

## VI. Conclusões

Neste artigo, propusemos um novo limitante inferior para balizar o desenvolvimento e análise de técnicas de modulação com marca d'água digital não codificada, fundamentado na simples equivalência com um sistema de comunicações binário, introduzindo uma nova metodologia de projeto destas técnicas. Foi verificado que este limitante é mais preciso e mais geral do que o limitante utilizado em [8], podendo ser aplicado para análise de qualquer tipo de técnica. A utilização do mesmo raciocínio apresentado neste artigo, fundamentado no trabalho de Costa [6], pode ser usado, para estabelecer o limitante inferior destas técnicas para outros modelamentos do ataque — que neste artigo foi considerado aditivo gaussiano. O estudo do comportamento destes limitantes inferiores quando aplicado algum tipo de restrição de distorção ao hospedeiro é também de interesse, assim como a investigação das técnica integradas de marcação d'água codificada citada na seção V.

## Referências

[1] R. J. Anderson and F. A. Petitcolas,"Information hiding: an annotated bibliography" *[online]. Available: www.petitcolas.net/fabien/steganography/bibliography/*, 1999.

[2] M. D. Swanson, M. Kobayashi,and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies" *Proc. IEEE*, v. 86, p. 1064-1087, June 1998.

[3] B. Chen and G. W. Wornell, "Quantization Index Modulation: A class of provably good methods for digital watermarking and information embedding" *IEEE Trans. Inform. Theory*, v. 47, No. 4, p. 1423-1443, May 2001.

[4] F. Perez-González, F. Balado, and J. R. Hernández, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels"*IEEE Trans. on Signal Processing*, v. 51, No. 4, p. 960-980, April 2003. Special Issue on Signal Processing for Data Hiding in Digital Media & Secure Content Delivery.

[5] F. Perez-González, P. Comesaña, and F. Balado, "Dither-Modulation Data hiding with distortion-compensation: exact performance analysis and an improved detector for JPEG attacks" *In International Conference on Image Processing, Barcelona, Spain*, September 2003, IEEE.

[6] M. H. M. Costa, "Writing on dirty paper" *IEEE Trans. Inform. Theory*, v. IT-29, p. 439-441, May 1983.

[7] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for mutimedia" *IEEE Trans. Image Processing*, v. 6, p. 1673-1687, Dec 1997.

[8] H. S. Malvar and D. A. F. Florêncio, "Improved Spread Spectrum: A new modulation Technique for robust watermarking" *IEEE Trans on Signal Processing*, v. 51, No. 4, p. 898-905, April 2003.

[9] F. P. González and F. Balado, "Quantized projection data hiding" *In Proc. of the IEEE International Conference on Image Processing (ICIP)*, Rochester (NY), USA, September 2002.

[10] B. Chen and G. W. Wornell, "Implementations of Quantization Index Modulation methods for digital watermarking and information embedding of multimedia" *J. VLSI Signal Processing Syst. Signal, Image, and Video Technol. (Special Issue on Multimedia Signal Processing)*, v. 27, p. 7-33, Feb 2001.

[11] R. Johannesson and K. S. Zigangirov, "Fundamentals of Convolutional Coding" *Wiley-IEEE Press*, March 1999, ISBN 0-7803-3483-3.

[12] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes" *in ICC'93*,Geneva, Switzerland,p. 1064-1070, May 1993.