Investigação de Entrelaçadores para Aplicação em Codificação Homofônica Universal

Daniel R. Simões e Valdemar C. da Rocha Jr.

***Resumo*— Dois esquemas de codificação homofônica universal são analisados neste artigo, para uma taxa de informação do usuário igual a $1/2$, com o emprego do gerador de números pseudo-aleatórios de Park-Miller-Carta e de vários entrelaçadores. A validação de tais esquemas é feita utilizando a versão 2.1.2 da suite de testes estatísticos adotada pelo *National Institute of Standards and Technology*. Os resultados dos ensaios são apresentados, os quais permitiram identificar desvios estatísticos em alguns esquemas e indicar a melhor escolha para o período de cada tipo de entrelaçador em função da aplicação desejada.**

***Palavras-Chave*— Criptografia, Codificação Homofônica Universal, Entrelaçamento**

***Abstract*— Two universal homophonic coding schemes are analyzed in this paper, considering a user information rate equal to $1/2$, employing the Park-Miller-Carta pseudo-random generator and various interleavers. Validation tests of the analyzed schemes are performed using the 2.1.2 version of the statistical test suite adopted by the National Institute of Standards and Technology. Test results are presented which allowed identification of statistical deviations in some schemes and indicate the best choice for the period of each type of interleaver as a function of the desired application.**

***Keywords*— Cryptography, Universal Homophonic Coding, Interleaving**

I. Introdução

A criptografia é uma ferramenta que tem como objetivo garantir o sigilo, a integridade e a autenticidade de dados e entidades [1], sendo inicialmente utilizada somente para fins militares e diplomáticos. Devido ao desenvolvimento dos meios de comunicação, as técnicas de criptografia passaram a ser mais acessíveis, sendo disseminadas a várias áreas e encontrando diversas aplicações. Paralelamente ao avanço de técnicas de cifragem, desenvolveram-se também os métodos de criptoanálise. Na prática, os dados a serem protegidos por meio da criptografia possuem, em geral, um comportamento estatístico muito diferente daquele de símbolos estatisticamente independentes e uniformemente distribuídos (IID). Tal comportamento representa uma vulnerabilidade que, caso não tratada adequadamente, certamente poderá ser explorada por terceiros.

A excessiva redundância do texto cifrado resultou na quebra de alguns cripto-sistemas, motivando assim o aparecimento da codificação homofônica. Essa técnica é utilizada na criptografia para combater ataques que exploram desvios na estatística do texto cifrado, daquela obtida para símbolos IID, tornando os cripto-sistemas de chave secreta mais resistentes à criptoanálise. Isso faz com que um usuário não autorizado, por meio de um ataque apenas ao texto cifrado, não consiga obter informação sobre a chave secreta utilizada na cifra e nem sobre o texto claro analisando apenas o texto cifrado.

Daniel R. Simões e Valdemar C. da Rocha Jr., Grupo de Pesquisa em Comunicações, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Recife, 50740-550, E-mail: {daniel.simoes, vcr}@ufpe.br.

A codificação homofônica consiste na substituição de cada símbolo da mensagem original por um ou mais símbolos, pertencentes a um alfabeto maior, de forma a produzir símbolos IID. Essa técnica reduz a redundância da mensagem a ser cifrada tendo como custo uma expansão do texto claro. Na sua forma clássica, esse procedimento necessita do conhecimento prévio da estatística do texto claro para realizar a codificação. Günther [2] de modo pioneiro descreveu um algoritmo para a realização da codificação homofônica, no qual as palavras representando homofonemas podem ter comprimento variável.

Na maioria das aplicações práticas, em geral, não se tem *a priori* o conhecimento da estatística da fonte, de modo que procedimentos de codificação homofônica para fontes específicas tornam-se bastante ineficientes nessa situação. Surge então a necessidade de se desenvolver sistemas que realizem a codificação de forma universal, ou seja, que não necessitem do conhecimento *a priori* da estatística da fonte para realizar a codificação. Massey [3] propôs um esquema de codificação homofônica universal, que utiliza um multiplexador e um codificador universal de fonte. Esse esquema foi analisado em [4], considerando o algoritmo LZW como codificador de fonte. Como uma alternativa mais eficiente ao esquema em [3], foi proposto um codificador homofônico universal empregando um sistema de bloco descartável combinado com um multiplexador e um entrelaçador [5]. Um refinamento desta técnica foi proposto em [6], na qual o codificador homofônico universal emprega codificação diferencial e um entrelaçador, com desempenho semelhante ao do esquema apresentado em [5]. A referência [7] aborda com detalhes a codificação homofônica universal e alguns esquemas são investigados.

Neste artigo é analisado o desempenho estatístico dos codificadores universais propostos em [5] e [6], considerando diferentes entrelaçadores e uma taxa de informação de $R = 0,5$ *bits* por símbolo. Para cada um dos casos, as sequências de saída dos codificadores são analisadas utilizando a suite de testes estatísticos do *National Institute of Standards and Technology* (NIST) na versão 2.1.2 [8], [9].

II. Motivação para o uso da codificação homofônica

Uma cifra de chave secreta é dita não-expansiva quando o texto claro e o texto cifrado possuem o mesmo alfabeto e existe uma sequência infinita de inteiros positivos $n_1, n_2, n_3, \ldots$ tal que os primeiros n_i símbolos $Y_1, Y_2, \ldots, Y_{n_i}$ do texto

cifrado junto com a chave secreta determinam unicamente os primeiros n_i símbolos $X_1, X_2, \ldots, X_{n_i}$ do texto claro para $i = 1, 2, 3, \ldots$ [10]. Como exemplo de cifra não-expansiva pode ser citada a cifra de fluxo aditiva, em que $Y_i = X_i \oplus Z'_i$. A sequência $Z'_1, Z'_2, Z'_3, \ldots$ é uma chave de sessão gerada a partir da chave secreta Z. Outro exemplo é a cifra de bloco, em que os blocos de texto claro e de texto cifrado possuem o mesmo comprimento N. Para o caso da cifra de fluxo aditiva, tem-se $n_i = i$ e para o caso da cifra de bloco, tem-se $n_i = iN$. As cifras de chave secreta não-expansivas possuem a seguinte importante propriedade.

Proposição 2.1: Se uma sequência de texto claro X^n, cifrada por uma cifra de chave secreta não-expansiva, for completamente aleatória então a sequência de texto cifrado Y^n é também completamente aleatória para qualquer escolha z da chave Z. Além disso, Y^n é estatisticamente independente da chave secreta Z.

Uma demonstração da Proposição 2.1 encontra-se em [10]. Shannon definiu uma cifra *fortemente ideal* como aquela cifra para a qual $H(Z|Y^n) = H(Z)$, ou seja, para a qual a entropia da chave secreta condicionada a n símbolos do texto cifrado é igual à entropia da chave secreta [11].

Corolário 2.1: Se uma sequência de texto claro X^n, cifrada por uma cifra de chave secreta não-expansiva, for completamente aleatória, então o cripto-sistema é fortemente ideal, independentemente da distribuição de probabilidade da chave secreta Z.

O Corolário 2.1 implica que um ataque de apenas texto cifrado não consegue extrair informação alguma sobre a chave secreta Z, não importando quantos símbolos do texto cifrado sejam examinados. O objetivo da codificação homofônica é justamente o de transformar uma sequência de símbolos de saída emitidos por uma fonte de informação não aleatória em uma sequência completamente aleatória, transformando qualquer cifra de chave secreta não-expansiva em um cripto-sistema fortemente ideal.

III. Dois codificadores universais

A seguir descrevemos dois codificadores homofônicos universais. O primeiro deles denomina-se codificador universal com Bloco Descartável, Multiplexador e Entrelaçador (BDME), cujos principais componentes estão ilustrados na Figura 1. A ideia no codificador universal BDME é formar na saída do multiplexador palavras de comprimento $n + 1$, em que cada uma destas palavras consiste de um bit da fonte aleatória z_j, seguido de n bits $u_i \oplus z_j$, sendo que para cada valor do índice j o índice i assume n valores consecutivos.

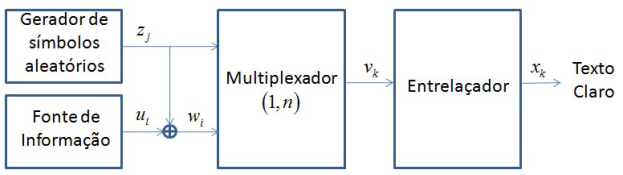

Fig. 1. Diagrama de blocos do codificador universal com Bloco Descartável, Multiplexador e Entrelaçador.

Nesse esquema, w_i é o resultado da operação ou-exclusivo entre um *bit* z_j proveniente do gerador de símbolos aleatórios (IID) e um *bit* u_i proveniente da fonte de informação, que é suposta ser estacionária e ergódica [3]. Fazendo $i = (j-1)n + r$, em que $j = 1, 2, \ldots$ e $1 \leq r \leq n$, pode-se expressar esse resultado por $w_i = u_i \oplus z_j$. O multiplexador tem como saída sucessivos blocos de comprimento $n+1$, contendo um *bit* do gerador de símbolos aleatórios seguido de n *bits* obtidos pela operação ou-exclusivo. Dessa forma obtemos a seguinte expressão para a saída v_k do multiplexador, em que $j = 1, 2, \ldots$

$$v_k = \begin{cases} z_j, & k = j(n+1) - n \\ w_{k-1}, & k = (j-1)n + r, 2 \leq r \leq n+1, \end{cases}$$

em que $w_{k-1} = u_{k-1} \oplus z_j$. Finalmente, a saída x_k do codificador universal BDME é obtida processando a saída v_k do multiplexador utilizando um entrelaçador, sendo expressa por $x_k = v_{\pi(k)}$, em que $\pi(.)$ denota a função de permutação do entrelaçador.

Conforme é detalhado a seguir, cada entrelaçador examinado opera sobre um determinado número T de símbolos de entrada, denominado período do entrelaçador, o qual é variado podendo assumir diversos valores. Neste artigo são considerados os períodos T, $T \in \{64, 256, 1.024, 4.096, 16.384, 65.536, 262.144\}$.

O segundo codificador homofônico universal considerado é o codificador com Codificação Diferencial e Entrelaçador (CDE), cujo diagrama de blocos é ilustrado pela Figura 2.

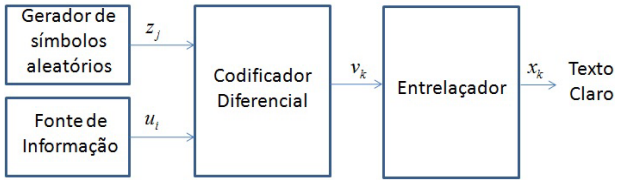

Fig. 2. Diagrama de blocos do Codificador Universal com Codificação Diferencial e Entrelaçador.

A saída do codificador diferencial é formada por blocos de $n + 1$ *bits*, em que o primeiro *bit* é oriundo da fonte de símbolos aleatórios. A Figura 3 ilustra o detalhamento do codificador diferencial, no qual as chaves S_1 e S_2 operam de modo síncrono. Com S_1 fechada e S_2 aberta o símbolo z_j é carregado no elemento de memória. Em seguida, com S_1 aberta e S_2 fechada, são carregados n símbolos da fonte de informação.

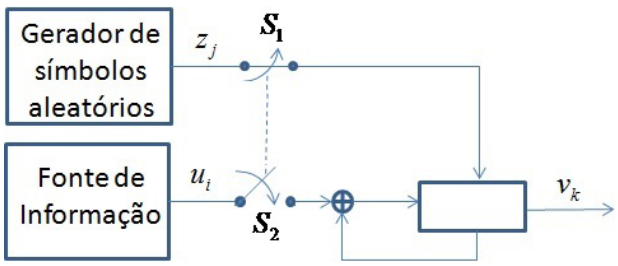

Fig. 3. Codificador diferencial.

A expressão que representa a saída v_k do codificador diferencial, considerando $j = 1, 2, \ldots$, é

$$v_k = \begin{cases} z_j, & k = j(n+1) - n, \\ u_{k-1} \oplus v_{k-1}, & k = (j-1)n + r, \end{cases}$$

em que $2 \leq r \leq n+1$. A saída x_k do codificador universal CDE é obtida processando a saída do codificador diferencial utilizando um entrelaçador, sendo expressa por $x_k = v_{\pi(k)}$, em que $\pi(.)$ denota a função de permutação do entrelaçador.

A taxa R, tanto do codificador BDME como do codificador CDE, é dada por $R = \frac{n}{n+1} = \frac{1}{1+\frac{1}{n}}$. Quando $n \to \infty$, tem-se $R \to 1$. Considerando uma fonte de informação U previamente comprimida por um codificador de fonte ideal, a taxa é dada por $R = \frac{1}{1+\frac{1}{nH(U)}}$. Quando $n = 1$, i.e., para $R = 1/2$, os codificadores universais BDME e CDE são equivalentes, conforme o esquema ilustrado na Figura 4, na qual a abertura e o fechamento das chaves S_1 e S_2 alternam a cada símbolo.

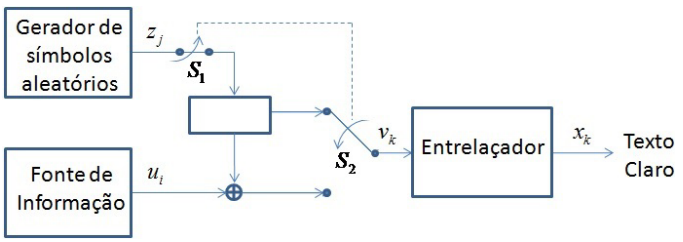

Fig. 4. Diagrama de blocos de codificador universal com $n = 1$.

Nesse caso, i.e., com $n = 1$ e $R = 1/2$, as 2-uplas na entrada do entrelaçador são os pares $(z_i, u_i \oplus z_i)$, $i = 1, 2, \ldots$. O elemento $u_i \oplus z_i$ associa-se ao texto cifrado da cifra de blocos descartáveis (*one-time pad*) [11], em que u_i representa um símbolo do texto claro e z_i representa um símbolo da chave secreta. Essa cifra possui a seguinte importante propriedade;

Propriedade 3.1 (Cifra de blocos descartáveis): Se Z for completamente aleatória, ou seja, se os valores assumidos pela variável aleatória Z obedecerem a uma distribuição de probabilidade uniforme, então a variável aleatória definida por $U \oplus Z$ também é completamente aleatória e não depende da distribuição de probabilidade de U.

Além disso, nota-se que $P(Z = z_i, V = u_i \oplus z_i) = P(Z = z_i)P(V = u_i \oplus z_i | Z = z_i)$ implica

$$P(Z = z_i, V = u_i \oplus z_i) = P(Z = z_i)P(U = u_i). \qquad (1)$$

Decorre de (1) que, em geral, Z e $U \oplus Z$ não satisfazem à condição requerida para a independência estatística, ou seja, que $P(Z = z_i, V = u_i \oplus z_i) = P(Z = z_i)P(V = u_i \oplus z_i)$, exceto para o caso em que a fonte U já é completamente aleatória, e que naturalmente não necessitaria de codificação homofônica. Assim, os pares $(z_i, u_i \oplus z_i)$ de símbolos binários em que tanto $u_i \oplus z_i$ quanto z_i são completamente aleatórios, não são necessariamente estatisticamente independentes. Para tentar ocultar esta possível eventual dependência estatística entre os pares $(z_i, u_i \oplus z_i)$ utilizamos um entrelaçador.

IV. Detalhes da Implementação do Codificador Homofônico

O codificador homofônico ilustrado pela Figura 4 foi implementando considerando o gerador pseudo-aleatório de Park-Miller-Carta como gerador de símbolos pseudo-aleatórios [12], [13]. As cinco sementes S utilizadas para o gerador foram $S \in \{12.345, 54.321, 112.358, 19.872.008, 26.011.982\}$. Como fontes de informação, são consideradas um arquivo de texto que é uma compilação de *e-books* de Agatha Christie com 27.110.784 *bytes* e quatro imagens no formato bitmap: "Platão" com 22.548.502 *bytes*, "Cana51" com 21.784.734 *bytes*, "SC06" com 23.476.598 *bytes* (Figura 5) e uma imagem toda branca (3000 × 3000 pixels) com 27.000.054 *bytes*, utilizada como referência na análise, pois possui a entropia mais baixa possível (pior caso para realizar a codificação homofônica). Por outro lado, $R = 1/2$ representa a situação mais favorável para os entrelaçadores, em comparação com taxas $1/(n+1)$, para $n > 1$.

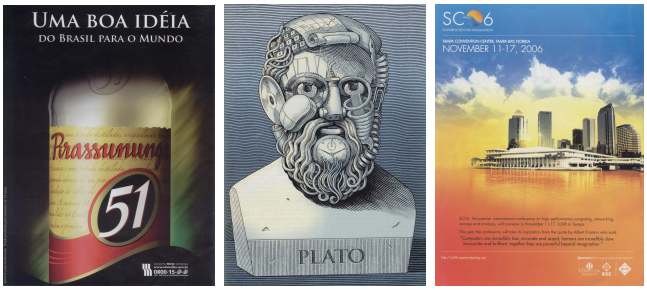

Fig. 5. Imagens de Platão (2322 × 3236 pixels), Cana 51 (2338 × 3105 pixels) e SC06 (2409 × 3248 pixels).

Os entrelaçadores considerados na análise são o entrelaçador de Berrou-Glavieux [14], [15], o Co-Primo, o JPL [16], o LRTB, o Takeshita-Costello [17] e o e Welch-Costas [18]. Detalhes sobre esses entrelaçadores podem ser encontrados em [19].

V. A Suite de Testes Estatísticos do NIST

A fim de testar a qualidade estatística da sequência produzida na saída do esquema da Figura 4, foi empregada a suite de testes estatísticos do NIST. Essa suite consiste em 188 testes estatísticos em que cada um deles verifica a hipótese de que uma sequência binária longa arbitrária é aleatória sob um determinado aspecto. A finalidade desses testes é identificar possíveis desvios estatísticos da aleatoriedade ideal que podem afetar uma dada sequência binária.

Cada um dos testes da suite verifica uma hipótese nula específica, sobre a aleatoriedade da sequência testada. É definido um nível de significância α para o teste, que é a probabilidade da sequência ser aleatória e possuir propriedades de não aleatoriedade. Tipicamente escolhe-se $0,001 \leq \alpha \leq 0,01$. Uma estatística é calculada e comparada com um valor crítico, que depende de suas distribuições de referência. Essa estatística é utilizada para calcular um valor P (denotado por *P-value*), que indica a força da evidência contra a hipótese nula. Baseado nessa estatística, aceita-se ou rejeita-se a hipótese nula. Se *P-value*$\geq \alpha$, a hipótese nula é aceita, enquanto que

se *P-value*$< \alpha$, a hipótese nula é rejeitada, ou seja, ela é aparentemente não-aleatória.

Neste trabalho, considerou-se os parâmetros padrão do próprio *software* do NIST. Além disso, considerou-se a metodologia que foi usada para testar os cripto-sistemas finalistas da competição para a escolha do algoritmo para representar o *Advanced Encryption Standard* (AES) [20]. O grau de significância α foi fixado em 0,01. Define-se como sequência de entrada ε o arquivo resultante da codificação homofônica universal a ser testado. A sequência de entrada é formada por m subsequências: $\varepsilon = \varepsilon_1\varepsilon_2 \ldots \varepsilon_m$. Considerou-se $m \geq 300$ subsequências de entrada, com comprimento $n = 2^{20} = 1.048.576$ *bits* cada uma.

Para cada teste estatístico e cada sequência testada, duas avaliações são realizadas: uma de proporção e outra de uniformidade. É calculada a proporção de subsequências aprovadas no teste estatístico. Se a proporção calculada estiver fora de um *intervalo de confiança*, então existe uma evidência de não aleatoriedade na sequência testada e a sequência consequentemente é reprovada no teste. Para avaliar a uniformidade dos *P-values* no intervalo $[0, 1]$, aplica-se um teste χ^2 para determinar um *P-value*$_T$, que representa uma conclusão geral para todas as sequências testadas. Se *P-value*$_T < 0,0001$, então os *P-values* das subsequências não são considerados uniformemente distribuídos e a sequência consequentemente é reprovada no teste. Uma sequência é considerada aprovada em um determinado teste estatístico se ela for aprovada tanto no teste de proporção quanto no teste de uniformidade dos *P-values*.

Para medir o desempenho de uma sequência nos 188 testes estatísticos do NIST, define-se como figura de mérito um índice aqui denominado *Índice NIST*.

*Definição 5.1 (**Índice NIST**):* Sejam n_a o número de testes nos quais a sequência foi aprovada na suite do NIST e n_t o número total de testes dessa suite. Definimos o índice NIST como $I_N = \dfrac{n_a}{n_t}$, em que $0 \leq I_N \leq 1$.

Obter $I_N = 1$ significa que uma sequência foi aprovada em todos os 188 testes estatísticos do NIST, enquanto que obter $I_N = 0$ significa que a sequência foi reprovada em todos os testes. Para a aplicação de codificação homofônica, definimos como satisfatória uma sequência que obtém $I_N \geq 0,95$ (limite de tolerância).

VI. Ensaios Realizados

O primeiro ensaio teve como objetivo avaliar a qualidade estatística da saída do codificador homofônico, para cada uma das fontes, variando-se o entrelaçador. Foram considerados os períodos $64, 256, 1.024, 4.096.16.384, 65.536$ e 262.144 *bits* para cada entrelaçador. No caso dos entrelaçadores Berrou-Glavieux, JPL e LRTB, considerou-se a versão quadrada. A Figura 6 ilustra dois gráficos do índice NIST médio (considerando as cinco sementes do gerador de Park-Miller-Carta) para a imagem branca, considerando em cada gráfico três entrelaçadores distintos.

Observando os dois gráficos da Figura 6, constata-se que em nenhum dos períodos considerados obteve-se $I_N \geq 0,95$ para essa fonte, quando os entrelaçadores JPL e LRTB foram

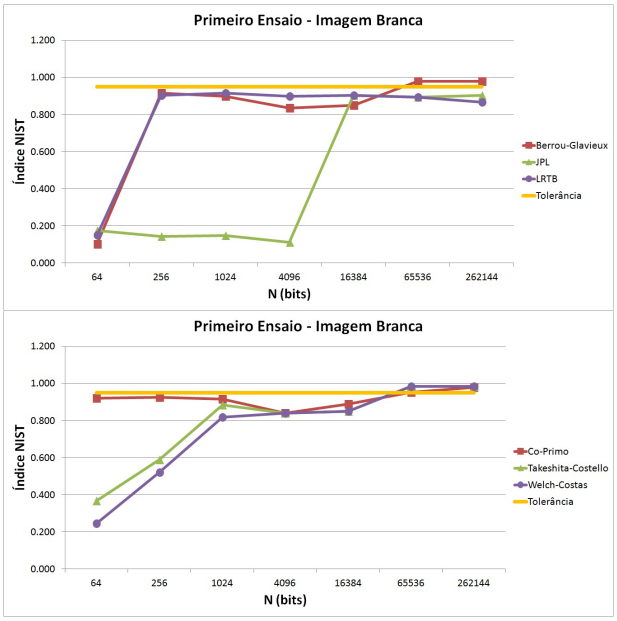

Fig. 6. Índice NIST do primeiro ensaio para a imagem branca.

utilizados. Para os demais entrelaçadores, $I_N \geq 0,95$ foi obtido para $T = 65.536$ e $T = 262.144$, o que sugere uma influência do período do entrelaçador no desempenho estatístico do sistema. Observou-se também que houve reprovações persistentes em alguns testes, para todos os períodos, especificamente no *Discrete Fourier Transform (Spectral) Test* quando o entrelaçador Co-Primo e as versões quadradas dos entrelaçadores de Berrou-Glavieux, JPL e LRTB foram utilizadas. Isso sugere uma fraqueza introduzida por esses entrelaçadores, que geram padrões repetitivos próximos entre si na sequência de saída. Não foram observadas reprovações persistentes relativas aos entrelaçadores Takeshita-Costello e Welch-Costas.

Motivado pelo mau desempenho dos entrelaçadores de Berrou-Glavieux, JPL e LRTB, que foram considerados em suas formas quadradas ($N = M$), realizou-se um segundo ensaio com valores de $N \neq M$, para os períodos considerados no primeiro ensaio. A Figura 7 mostra dois gráficos do índice NIST para a imagem branca, considerando os períodos $T = 65.536$ e $T = 262.144$ para esses entrelaçadores. O eixo das abscissas representa o parâmetro N dos entrelaçadores, que foi variado em potências de 2. Esses resultados foram obtidos considerando a semente $S = 12.345$ do gerador de Park-Miller-Carta.

Observando os gráficos da Figura 7, constata-se que em nenhum valor de N considerado obteve-se $I_N \geq 0,95$ para essa fonte quando o entrelaçador LRTB foi utilizado. No caso do entrelaçador JPL, considerando um período $T = 2^k$, $k = 16$ e $k = 18$, tem-se $I_N \geq 0,95$ quando $N \in [2, 2^{k-15}]$. Entretanto, nesse intervalo ainda ocorrem reprovações persistentes no *Discrete Fourier Transform (Spectral) Test*. Assim, conclui-se que os entrelaçadores LRTB e JPL não são adequados para utilização no esquema da Figura 4. No caso do entrelaçador de Berrou-Glavieux tem-se $I_N \geq 0,95$ quando $N \in [1, 2^{k-7}]$. Nesse intervalo, só não ocorrem reprovações persistentes no

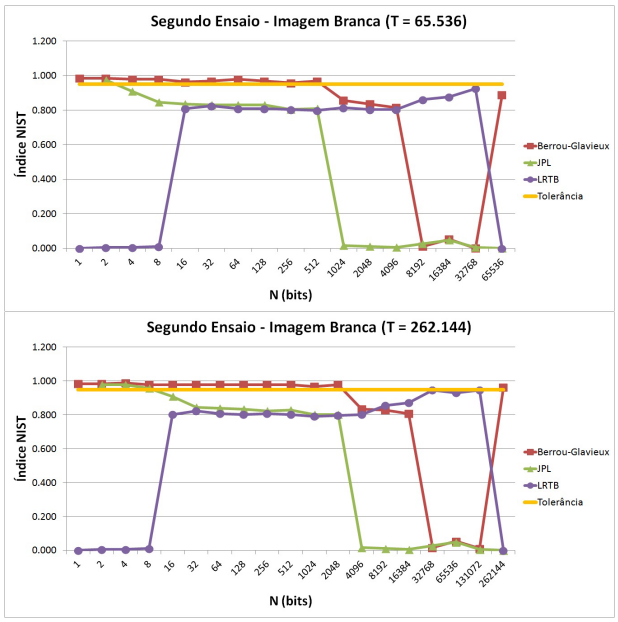

Fig. 7. Índice NIST do segundo ensaio para a imagem branca.

Discrete Fourier Transform (Spectral) Test quando $N = 1$ e $N = 2$. Assim, somente nesses casos considera-se satisfatória a utilização desse entrelaçador.

No caso dos entrelaçadores Co-Primo, Takeshita-Costello e Welch-Costas, testou-se, para cada período considerado, apenas uma configuração de parâmetros. Convém realizar mais ensaios com outras configurações para verificar se o mau desempenho do entrelaçador Co-Primo e os bons desempenhos dos entrelaçadores de Takeshita-Costello e Welch-Costas se mantêm. Resultados semelhantes foram encontrados quando as outras fontes de informação foram testadas, de modo que o caso da imagem branca pode ser considerado como uma boa representação do desempenho do sistema para todos os entrelaçadores.

VII. Comentários Finais

Neste artigo apresentamos os resultados de ensaios estatísticos envolvendo alguns entrelaçadores aplicados nos codificadores universais BDME e CDE na configuração em que a taxa é $R = 0,5$. Uma figura de mérito, denotada por índice NIST, é definida e utilizada para avaliar o desempenho estatístico desses esquemas variando-se os entrelaçadores e os seus respectivos períodos. Constatou-se a influência do período nesse desempenho: obtém-se resultados satisfatórios para períodos maiores ou iguais a $T = 65.536$. Constatou-se também fraquezas estatísticas presentes em alguns entrelaçadores, identificadas pelas reprovações persistentes em um teste específico do NIST, desqualificando-os para a aplicação. Essa metodologia pode inclusive ser adotada para medir o grau de aleatoriedade das permutações dos entrelaçadores em outras aplicações e contextos. É sugerido como trabalho futuro uma investigação de diversas configurações de parâmetros envolvendo os entrelaçadores Co-Primo, Takeshita-Costello e Welch-Costas para verificar se os seus respectivos desempenhos estatísticos, aqui encontrados, serão mantidos.

Agradecimentos

A pesquisa do segundo autor recebeu apoio parcial do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, Projeto No. 304696/2010-2.

Referências

[1] J. L. Massey, "An introduction to contemporary cryptology", *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533 - 549, May 1988.

[2] C. G. Günther, "A universal algorithm for homophonic coding", *Adv. Cryptology - Eurocypt '88*, Lect. Notes in Comp. Sci., no. 330, Springer-Verlag, 1988, pp. 405 - 414.

[3] J. L. Massey, "Some spplications of source coding in cryptography", *European Trans. Telecomm.*, vol. 5, no. 4, pp. 421 - 429, 1994.

[4] D. R. Simões e V. C. da Rocha Jr., "Um esquema de codificação homofônica universal utilizando o algoritmo LZW", *XXVI Simpósio Brasileiro de Telecomunicações*, Rio de Janeiro, RJ, 2008, pp. 1 - 6.

[5] D. R. Simões and V. C. da Rocha Jr., "A versatile universal homophonic coding scheme", *X Int. Symp. on Comm. Theory and Applications*, Ambleside, Inglaterra, 2009, pp. 1 - 4.

[6] D. R. Simões, J. Portugheis and V. C. da Rocha Jr., "Universal homophonic coding scheme using differential encoding and interleaving", *Inform. Process. Letters*, vol. 113, no. 1, pp. 628 - 633, 2013.

[7] D. R. Simões, "Uma nova proposta para a codificação homofônica universal", Dissertação de Mestrado, Depto. de Eletrônica e Sistemas, UFPE, Recife, PE, 2009.

[8] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications", NIST Special Publication 800-22, National Institute of Standards and Technology, rev. 1a, 2010.

[9] "NIST Statistical Test Suite - Version 2.1.2", Julho 2014, disponível online: *http://csrc.nist.gov/groups/ST/toolkit/documentation_software.html* (Acesso em 01 de Abril de 2016).

[10] H. N. Jendal, Y. J. B. Kuhn and J. L. Massey, "An information-theoretic approach to homophonic substitution", *Adv. Cryptology - Eurocypt '89*, Lect. Notes in Comp. Sci., no. 434, Springer-Verlag, 1990, pp. 382 - 394.

[11] C. E. Shannon, "Communication theory of secrecy systems", *Bell Sys. Tech. J.*, vol. 28, no. 4, pp. 656 - 715, Oct. 1949.

[12] K. Park and K. W. Miller, "Random number generators: good ones are hard to find", *Comm. ACM*, vol. 31, no. 10, pp. 1192 - 1201, Oct. 1988.

[13] D. G. Carta, "Two fast implementations of the "minimal standard" random number generator", *Comm. ACM*, vol. 33, no. 1, pp. 87 - 88, Jan. 1990.

[14] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo codes", *Proc. IEEE Int. Conf. on Communications*, Genebra, Suíça, 1993, pp. 1064-1070.

[15] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo-codes", *IEEE Trans. on Communications*, vol. 44, no. 10, pp. 1261-1271, Oct. 1996.

[16] S. Dolinar, D. Divsalar and F. Pollara, "Code performance as a function of block size", *JPL TMO Progress Report* 42-133, 1998.

[17] O. Y. Takeshita and D. J. Costello Jr., "New classes of algebraic interleavers for turbo-codes", *Proc. Int. Symp. Information Theory*, Cambridge, MA, 1998, p. 419.

[18] J. P. Costas, "Medium constraints on sonar design and performance", *EASCON Convention Record*, pp. 68A-68L, 1975.

[19] C. Heegard and S. B. Wicker, *Turbo Coding*. Kluwer Academic Publishers, 1999, ch. 3, sec. 3.7, pp. 53-58.

[20] J. Soto and L. Bassham, "Randomness testing of the Advanced Encryption Standard finalist candidates", NIST IR 6483, National Institute of Standards and Technology, 2000.