Técnica de Substituição Homofônica Perfeita Símbolo-a-Símbolo

Danielle P. B. de A. Camara e Valdemar C. da Rocha Jr.

***Resumo*— Este artigo apresenta uma nova técnica de substituição homofônica perfeita, pertencente a uma classe denominada Substituição Homofônica Símbolo-a-Símbolo (SH-SAS). A técnica SH-SAS tem apresentado desempenho semelhante à técnica JKM modificada, alcançando a mesma eficiência, e possui a vantagem prática de utilizar sempre um único símbolo mudo.**

***Palavras-Chave*— Teoria da informação, substituição homofônica, criptografia.**

***Abstract*— This article presents a new perfect homophonic substitution scheme which belongs to a class named *Letter by Letter (LBL) homophonic substitution*. This technique has shown a performance similar to that of the modified JKM homophonic substitution scheme, reaching the same efficiency, and has the practical advantage of always employing a single dummy symbol.**

***Keywords*— Information theory, homophonic substitution, cryptography.**

I. INTRODUÇÃO

Historicamente alguns sistemas criptográficos de chave secreta foram quebrados [1] explorando o fato da estatística do texto claro desviar-se daquela de uma seqüência de símbolos estatisticamente independentes e uniformemente distribuídos, usualmente chamada de seqüência verdadeiramente aleatória. A **substituição** (ou **codificação**) **homofônica** é uma técnica antiga utilizada para converter o texto claro em uma seqüência de símbolos (mais) aleatória. Esta técnica consiste na substituição (*one-to-many*) de cada letra da mensagem original por um substituto ou **homofonema** pertencente a um alfabeto maior, com o intuito de formar o *novo* texto claro que é então cifrado. Cada homofonema é então codificado de forma a produzir símbolos uniformemente distribuídos e estatisticamente independentes. Tal técnica torna um criptosistema simétrico não-expansível [1] mais seguro, uma vez que aumenta a distância de unicidade da cifra [2], porém isso tem um custo: a expansão do texto claro. Em 1988, Günther [3] fez uma importante contribuição na área introduzindo o que foi denominado **substituição homofônica de comprimento variável**. Tanto a substituição homofônica clássica como a de comprimento variável foram abordadas em [1] em termos de teoria da informação.

Este artigo aborda uma técnica de substituição homofônica padrão pertencente a uma nova classe denominada **Substituição Homofônica Símbolo-a-Símbolo (SH-SAS)**. Esta técnica mostrou desempenho semelhante à técnica **JKM modificada** [4], ao se considerar a eficiência η, com o diferencial de sempre utilizar apenas um símbolo mudo, o que nem sempre ocorre quando se utiliza a técnica JKM modificada.

Na Seção II são apresentados alguns conceitos básicos, assim como algumas definições que se mostram úteis na comparação de técnicas de substituição homofônica, facilitando assim o entendimento das seções seguintes, e conseqüentemente do trabalho aqui apresentado.

Na Seção III é introduzida uma nova técnica de substituição homofônica denominada **Substituição Homofônica Símbolo-a-Símbolo (SH-SAS)**. Como será visto, tal técnica apresenta eficiência (η) igual ou, em alguns casos, maior que a obtida com a técnica Rocha-Massey (RM) [7] e desempenho semelhante à técnica JKM modificada [4]. A técnica SH-SAS possui um diferencial positivo em relação à técnica JKM modificada, pelo fato de sempre usar um único símbolo mudo, enquanto que esta última necessita, em alguns casos, de mais de um símbolo mudo. A utilização de um único símbolo mudo na técnica SH-SAS é garantida pela construção descrita na Seção III. A Seção IV ilustra o uso da técnica aqui introduzida a partir de um exemplo. Por fim a Seção V encerra o artigo com algumas conclusões.

II. ALGUNS CONCEITOS BÁSICOS

Seja U uma fonte K-ária discreta sem memória (DMS) com alfabeto $\{u_1, u_2, \ldots, u_K\}$ e entropia

$$H(U) = -\sum_{i=1}^{K} P_U(u_i) \log P_U(u_i). \qquad (1)$$

Os símbolos que saem da fonte $U_1, U_2, \ldots$, são codificados numa seqüência de símbolos D-ários, $X_1, X_2, \ldots$. Assume-se neste artigo, para simplificação do tratamento, a codificação homofônica binária de uma seqüência $U_1, U_2, \ldots$ K-ária, com símbolos estatisticamente independentes e identicamente distribuídos, reduzindo assim o problema de codificação da fonte de mensagem ao problema de codificação de uma única variável aleatória $U = U_1$. Lembrando que a teoria descrita é passível de modificação para que sejam consideradas fontes discretas com memória, bastando para isso substituir a distribuição de probabilidade de U_i pela distribuição de probabilidade condicional de U_i dados os valores observados $U_1, U_2, \ldots, U_{i-1}$. Além disso, admite-se que U tem uma distribuição de probabilidade racional na qual $P_U(u_i) = m_i/n_i$, $1 \leq i \leq K$, em que m_i e n_i são números inteiros positivos e primos entre si.

O **canal homofônico** é um canal sem memória cujo alfabeto de entrada $\{u_1, u_2, ..., u_K\}$ coincide com o conjunto de possíveis valores de U, o alfabeto de saída V pode ser finito ou

Danielle P. B. de A. Camara e Valdemar C. da Rocha Jr., Grupo de Pesquisa em Comunicações - CODEC, Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, Caixa Postal 7800, 50711-970, Recife, PE, Brasil, Emails: dpbac@ieee.org, vcr@ufpe.br.

infinito contável, e as probabilidades de transição $P_{V|U}(v_{ij}|u_i)$ têm a propriedade que para cada j existe exatamente um i tal que $P_{V|U}(v_{ij}|u_i) \neq 0$, observa-se desta forma que $H(U|V) = 0$. Em geral, os v_{ij} para os quais $P_{V|U}(v_{ij}|u_i) > 0$ serão considerados homofonemas de u_i.

Um **codificador D-ário livre de prefixo** é um mecanismo que associa uma seqüência D-ária a cada v_{ij}, de modo que a palavra-código associada seja distinta das outras palavras-código e também não seja prefixo de outra palavra-código mais longa, o que garante que em uma seqüência de palavras-código o fim de cada palavra-código possa ser identificado imediatamente sem que seja necessária a verificação de quaisquer outros símbolos na seqüência. O **comprimento médio** de uma variável aleatória W é denotada por $E(W)$ na qual W é o comprimento do palavra-código que representa o símbolo. Dado que l_j é o comprimento médio da palavra-código associada ao símbolo homofonema v_{ij},

$$E(W) = \sum_j l_j P_V(v_{ij}). \tag{2}$$

A expansão de texto claro foi definida anteriormente [1] como o comprimento médio do homofonema menos a entropia da fonte, i.e., $E(W) - H(U)$, sendo assumido implicitamente que $H(U|V) = 0$. Esta definição de expansão de texto claro é útil ao se comparar dois sistemas de codificação homofônica que produzem o mesmo número de *bits* por símbolo na saída do canal homofônico e possivelmente possuem valores distintos para $E(W)$.

No contexto de codificação de fonte, para uma dada fonte sem memória U e um código unicamente decodificável associado a ela, a eficiência do código η é definida [5, p.86] como a razão entre a entropia da fonte $H(U)$ e o comprimento médio da palavra-código $E(W)$, i.e., $\eta = H(U)/E(W)$ e como conseqüência, a redundância ρ é definida como $\rho = 1 - \eta$, i.e. $\rho = [E(W) - H(U)]/E(W)$. A seguir são revistas as definições de **redundância** e de **eficiência** em sistemas de substituição homofônica, introduzidas em [6], denotando por R a **taxa de transmissão de informação** do referido sistema, i.e., denotando por R o número de *bits* por símbolo na saída de um canal homofônico.

Definição 1: A redundância ρ de uma técnica de codificação homofônica é definida como a razão entre a expansão do texto claro $E(W) - R$ e o comprimento médio de um homofonema $E(W)$, i.e.,

$$\rho = [E(W) - R]/E(W) = 1 - R/E(W). \tag{3}$$

Definição 2: A eficiência η de uma técnica de codificação homofônica é definida como

$$\eta = 1 - \rho = R/E(W). \tag{4}$$

Jendal-Kuhn-Massey (JKM) [1] definiram codificação homofônica como **perfeita** se a nova seqüência de texto claro é não-redundante e como **ótima** se ela além de perfeita minimizar a expansão de texto claro. Ao se comparar uma codificação homofônica para fontes distintas nota-se que uma menor expansão de texto claro não resulta necessariamente numa redundância menor, o que será ilustrado no exemplo a seguir.

Exemplo 1: Uma técnica de codificação homofônica com taxa $R_1 = 8$ e comprimento médio $E(W_1) = 10$ tem uma expansão de texto claro $E(W_1) - R_1 = 2$ e uma redundância $[E(W_1) - R_1]/E(W_1) = 0,2$, enquanto que uma técnica de codificação homofônica com taxa $R_2 = 3$ e comprimento médio $E(W_2) = 4$ tem uma expansão de texto claro $E(W_2) - R_2 = 1$ e uma redundância $[E(W_2) - R_2]/E(W_2) = 0,25$.

Uma redundância menor significa mais *bits* de entropia por homofonema (dígito de código homofônico binário) enquanto que uma expansão de texto claro menor por se só não fornece uma interpretação objetiva. Este fato ilustra a relevância da nova definição de redundância (Definição 1) na comparação de técnicas de codificação homofônica para fontes distintas [6].

À luz destas definições de redundância e eficiência, em [6] foi também introduzida uma nova definição de uma técnica de codificação homofônica ótima.

Definição 3: Uma técnica de substituição (codificação) homofônica é definida como ótima se ela é perfeita e sua redundância é a menor possível.

III. Técnica de Substituição Homofônica Símbolo-a-Símbolo

Considere mais uma vez, uma fonte U discreta sem memória tal que sua distribuição de probabilidade é formada por números racionais $P_U(u_i) = m_i/n_i, 1 \leq i \leq K$, em que m_i e n_i são números inteiros positivos e primos entre si. Se n_i for uma potência D-ária, i.e., $n_i = D^{l_i}$, a técnica JKM [1], opera com cota superior finita requerendo um número finito de experimentos a fim de selecionar um homofonema associado ao elemento u_i da fonte U, o que não ocorre no caso em que $n_i \neq D^{l_i}$. Caso este de interesse, já tendo sido abordado anteriormente, como por exemplo em [7], [8].

O objetivo desta seção é introduzir uma nova técnica de substituição homofônica padrão que mostra desempenho equivalente ao obtido utilizando a técnica JKM [1], considerando a eficiência η (Definição 2) como parâmetro de comparação.

De modo similar à técnica JKM modificada [4], na técnica SH-SAS, cada palavra-código homofônica é construída como a concatenação de palavras-código mais curtas derivadas a partir das probabilidades da fonte, resolvendo desta forma o problema de ter que armazenar um número infinito contável de palavras-código homofônicas, no caso em que n_i não é uma potência de D.

Observa-se que diferentemente da técnica JKM modificada, na técnica SH-SAS sempre se utiliza apenas um símbolo, i.e., independente da expansão do símbolo da fonte apenas uma palavra-código será associada ao símbolo mudo, o que é garantido pela construção descrita a seguir, sendo ilustrado no Exemplo 2 da Seção IV.

Na técnica SH-SAS, a fonte é requisitada a emitir um símbolo u_i e a partir daí um procedimento é feito a fim de determinar o homofonema associado a este símbolo. Tal procedimento é descrito a seguir.

1) Descrição da técnica SH-SAS: Com a finalidade de simplificar a descrição, é considerado o caso binário, i.e., $D = 2$.

a) Para cada símbolo da fonte $U = u_i$, $1 \leq i \leq K$, com probabilidade $P_U(u_i) = m_i/2^{s_i}$, i.e., para o qual $n_i = 2^{s_i}$, em que s_i é um inteiro positivo, escreve-se m_i na base 2 e a cada termo desta decomposição em base 2 associa-se um homofonema, tal que $P_V(v_{ij}) = 2^{-l_j}$.

b) Para cada símbolo da fonte $U = u_i$, $1 \leq i \leq K$, com probabilidade $P_U(u_i) = m_i/n_i$, para o qual $n_i \neq 2^{s_i}$, associam-se dois tipos de símbolos chamados, respectivamente, **símbolo homofonema** e **homofonema mudo**.
Considere que n é o menor denominador comum dessas probabilidades. Sendo $n = 2^r n'$ em que n' é o produto dos fatores ímpares de n e r um inteiro positivo, escolha o menor inteiro positivo s tal que $n'|(2^s-1)$. A probabilidade do homofonema mudo, Δ, é dada por $1/2^s$.

1. A decomposição da probabilidade de um ou mais símbolos u_i da fonte possui apenas termos periódicos. Dado que a fonte U seleciona um desses símbolos, um experimento é feito em que o símbolo mudo tem probabilidade $P(\Delta) = P(\Delta|u_i) = 1/2^s$, e desta forma o j-ésimo homofonema, denotado por v_{ij}, associado a u_i é selecionado com probabilidade

$$P_{V|U}(v_{ij}|u_i) = P_V(v_{ij})/P_U(u_i), \tag{5}$$

observando que $P_V(v_{ij})$ é o j-ésimo termo da decomposição em potências negativas de 2 de $\dfrac{m_i \cdot d}{2^s}$, em que d é um número inteiro positivo e

$$P_U(u_i)(1-2^{-s}) = \left(\frac{2^s-1}{2^s}\right)\left(\frac{m_i}{n_i}\right) = \frac{m_i \cdot d}{2^s}. \tag{6}$$

Assim V é uma fonte discreta sem memória tendo como símbolos os símbolos homofonemas de U com probabilidade

$$P_V(v_{ij}) = P_U(u_i)P_{V|U}(v_{ij}|u_i) \tag{7}$$

e um homofonema mudo com probabilidade $P(\Delta) = P(\Delta|u_i) = 1/2^s$.

2. A decomposição da probabilidade de um ou mais símbolos da fonte possui termos não-periódicos, em que a probabilidade do j-ésimo termo não-periódico associado ao símbolo u_i é

$$P_V(v_{ij}) = 2^{-l_j}, \tag{8}$$

na qual l_j é um número inteiro positivo. A probabilidade de seleção deste termo é

$$P_{V|U}(v_{ij}|u_i) = 2^{-l_j}/P_U(u_i) \tag{9}$$

e caso este termo seja selecionado, seu respectivo homofonema será gerado, sem necessidade de considerar o símbolo mudo. A soma das probabilidades dos homofonemas associados aos termos não-periódicos é portanto $\sum_t 2^{-l_t}$. Então os homofonemas v_{ij} associados aos termos periódicos são selecionados com probabilidade

$$P_{V|U}(v_{ij}|u_i') = \frac{P_V(v_{ij})}{P_U(u_i) - \sum_t 2^{-l_t}}, \tag{10}$$

na qual fizemos uso de um símbolo virtual u_i', ocorrendo com probabilidade $P_U(u_i) - \sum_t 2^{-l_t}$ e observando que $P_V(v_{ij})$ é o j-ésimo termo da decomposição em potências negativas de 2 de

$$\left[P_U(u_i) - \sum_t 2^{-l_t}\right] \cdot [1-2^{-s}], \tag{11}$$

lembrando que o símbolo mudo possui probabilidade 2^{-s}.
Se o termo não-periódico não for tratado desta forma, i.e., um termo que ao ser selecionado é imediatamente relacionado a um homofonema, aparecerão termos repetidos na representação do símbolo da fonte, e como é mostrado em [1], ao se considerar a mesma fonte, se a técnica de substituição homofônica é ótima então a decomposição de $P_U(u_i)$ para cada u_i deve consistir de potências negativas de 2 distintas, ou seja, considerando a expansão em termos distintos, $E(W)$ é minimizado e portanto η é maximizada para tal fonte. Tal situação é ilustrada na forma de exemplo (Exemplo 2).

c) A codificação binária nesta técnica é feita da seguinte forma.

1. Inicia-se uma árvore binária associando-se às folhas distantes da raiz l_j ramos os homofonemas cuja probabilidade é igual a $P_V(v_{ij}) = P_U(u_i)P_{V|U}(v_{ij}|u_i) = 2^{-l_j}$. Note que a probabilidade do símbolo mudo é a probabilidade de transição $P(\Delta|u_i)$ e, portanto nesta técnica poderá estar associada a uma palavra-código terminada num nó intermediário da árvore.
2. As palavras-código são construídas associando aos ramos superiores "0" e inferiores "1", seguindo então, o caminho da raiz à folha associada ao homofonema.
3. A construção da palavra-código associada ao símbolo mudo é feita de forma similar à construção da palavra-código do homofonema, seguindo na árvore um percurso que vai até o nó ou folha associada ao Δ.
Para evitar ambigüidade na decodificação deve-se observar que a palavra-código formada pela concatenação do símbolo mudo e de um homofonema não deve ser igual a outra palavra-código homofônica, nem prefixo de uma outra palavra-código homofônica mais longa. Com exceção das palavras-código associadas a homofonemas que não fazem uso do símbolo mudo, uma vez que nesse caso o símbolo mudo nunca precederá tal palavra-código homofônica.
Desta forma tal código é um código unicamente decodificável, tornando a decodificação trivial como será visto mais adiante, no item e).

d) Quando um homofonema mudo Δ é produzido no passo b), um símbolo mudo Δ é produzido por V e o experimento de seleção é repetido quantas vezes forem necessárias até que o correspondente símbolo homofonema v_{ij}, seja selecionado, tendo como resultado uma seqüência do tipo $\Delta\Delta\Delta\Delta \ldots \Delta v_{ij}$. A fonte U é então requisitada a selecionar o próximo símbolo a ser codificado e assim por diante.

e) A decodificação é imediata, bastando apenas apagar as

palavras-código que representam os símbolos mudos e, em seguida, mapear as palavras-código restantes aos correspondentes símbolos de U.

A seguir a técnica aqui introduzida é ilustrada e comentada por meio de um exemplo.

IV. Exemplo Ilustrativo

Nesta seção é apresentado um exemplo onde são aplicadas as técnicas de substituição homofônica SH-SAS, JKM modificada [4] e Rocha-Massey (RM) [7].

Exemplo 2: Considere uma fonte discreta binária sem memória com $K = 3$ e obedecendo à seguinte distribuição de probabilidade $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$.

Segundo o passo b) da descrição da técnica SH-SAS, $n = 2^2 \cdot 3 \cdot 5 = 60$, logo, $n' = 3 \cdot 5 = 15$ e $s = 4$, portanto $P(\Delta) = P(\Delta|u_i) = 1/16$.

Procedendo a decomposição das probabilidades dos símbolos da fonte, usando a técnica em [9] obtém-se,

$$P_U(u_1) = \frac{3}{10} = \left(\frac{1}{4}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i, \tag{12}$$

$$P_U(u_2) = \frac{5}{12} = \frac{1}{4} + \left(\frac{1}{8}\right)\sum_{i=0}^{\infty}\left(\frac{1}{4}\right)^i, \tag{13}$$

$$P_U(u_3) = \frac{17}{60} = \frac{1}{4} + \left(\frac{1}{32}\right)\sum_{i=0}^{\infty}\left(\frac{1}{16}\right)^i. \tag{14}$$

A decomposição de $P_U(u_1)$ possui apenas termos periódicos e, portanto, pelo procedimento descrito em 1. de b) da Seção III-.1 resulta

$$P_U(u_1) \cdot (1 - 1/16) = (3/10) \cdot (15/16) = 1/4 + 1/32.$$

Usando (5), as probabilidades de escolha dos homofonemas v_{11} e v_{12} associados ao símbolo u_1 são:

$$P_{V|U}(v_{11}|u_1) = (1/4) \,/\, (3/10) = 5/6$$

e

$$P_{V|U}(v_{12}|u_1) = (1/32) \,/\, (3/10) = 5/48.$$

As probabilidades dos homofonemas v_{11} e v_{12} são, respectivamente, $P_V(v_{11}) = 1/4$ e $P_V(v_{12}) = 1/32$ (Vide Equação (7)).

Já as probabilidades dos símbolos u_2 e u_3, $P_U(u_2) = \frac{5}{12}$ e $P_U(u_3) = \frac{17}{60}$, respectivamente, apresentam em suas decomposições termos não-periódicos, desta forma é seguido o procedimento descrito em 2. de b) da Seção III-.1.

De (9) observa-se que os termos não-periódicos associados a u_2 e u_3, são selecionados com probabilidades,

$$P_{V|U}(v_{21}|u_2) = (1/4) \,/\, (5/12) = 3/5$$

e

$$P_{V|U}(v_{31}|u_3) = (1/4) \,/\, (17/60) = 15/17,$$

respectivamente. Observe que aqui não há necessidade de escolha entre símbolo homofonema e homofonema mudo.

Os demais homofonemas associados ao símbolo u_2 são selecionados com probabilidades (Vide Equação (10)),

$$P_{V|U}(v_{22}|u_2') = 3/4$$

e

$$P_{V|U}(v_{23}|u_2') = 3/16,$$

uma vez que por (11) tem-se $[5/12 - 1/4] \cdot [1 - 1/16] = \frac{5}{32} = \frac{1}{8} + \frac{1}{32}$ e, portanto, as probabilidades dos homofonemas v_{22} e v_{23} associados a u_2 são, respectivamente, $P_V(v_{22}) = 1/8$ e $P_V(v_{23}) = 1/32$.

De modo similar, o homofonema v_{32} associado ao símbolo u_3 é selecionado com probabilidade (Vide Equação 9),

$$P_{V|U}(v_{32}|u_3') = 15/16,$$

uma vez que por (11), tem-se $[17/60 - 1/4] \cdot [1 - 1/16] = 1/32$, e desta forma a probabilidade do homofonema v_{32} associado ao símbolo u_3 é $P_V(v_{32}) = 1/32$. O resultado é ilustrado na Figura 1.

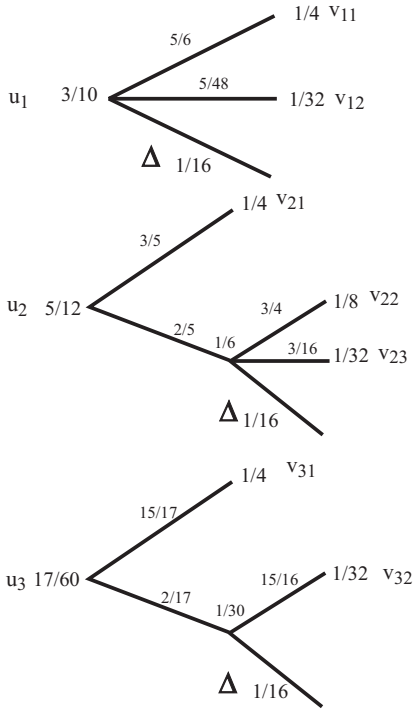

Fig. 1. Nova técnica de substituição homofônica símbolo-a-símbolo para a fonte U com distribuição de probabilidade $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$.

Segundo o procedimento de codificação para a técnica SH-SAS descrito na Seção III-.1 a árvore ilustrada na Figura 2 é obtida. Observa-se, portanto, que as palavras-código associadas aos homofonemas e ao símbolo mudo são $v_{11} \rightarrow 00, v_{12} \rightarrow 11100, v_{21} \rightarrow 01, v_{22} \rightarrow 110, v_{23} \rightarrow 11101, v_{31} \rightarrow 10, v_{32} \rightarrow 11110$ e $\Delta \rightarrow 1111$.

Os homofonemas correspondentes ao símbolo u_1 são escolhidos dentre os elementos pertencentes

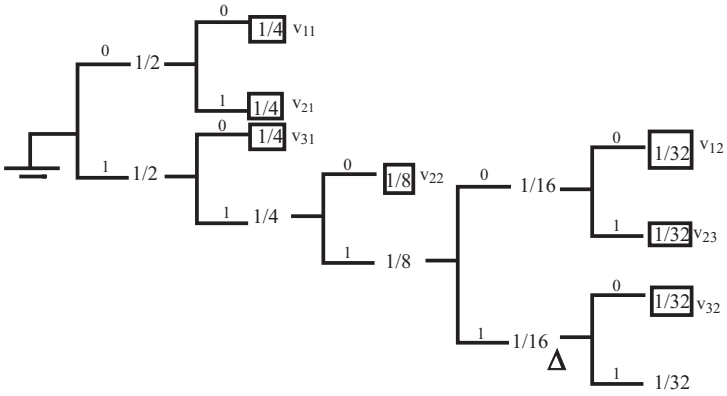

Fig. 2. Árvore obtida para a fonte U com distribuição de probabilidade $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$ ao se utilizar a técnica de substituição homofônica símbolo-a-símbolo.

aos subconjuntos $V_{11} = \{v_{11}, \Delta v_{11}, \Delta\Delta v_{11}, \ldots\}$ e $V_{12} = \{v_{12}, \Delta v_{12}, \Delta\Delta v_{12}, \ldots\}$, os homofonemas correspondentes a u_2 são selecionados nos subconjuntos $V_{21} = \{v_{21}\}$, $V_{22} = \{v_{22}, \Delta v_{22}, \Delta\Delta v_{22}, \ldots\}$ e $V_{23} = \{v_{23}, \Delta v_{23}, \Delta\Delta v_{23}, \ldots\}$, enquanto que os homofonemas relacionados a u_3 são selecionados nos subconjuntos, $V_{31} = \{v_{31}\}$, $V_{32} = \{v_{32}, \Delta v_{32}, \Delta\Delta v_{32}, \ldots\}$. Logo, o código resultante para a fonte V é representado por $\{(1111)^i 00, (1111)^i 11100, 01, (1111)^i 110, (1111)^i 11101, 10, (1111)^i 11110\}$ e o comprimento médio, calculado a partir de (2), é dado por,

$$\begin{aligned} E_{SAS}(W) = & \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+4r)\left(\frac{1}{16}\right)^r \\ & + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\ & + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+4r)\left(\frac{1}{16}\right)^r \\ & + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\ & + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\ & = 2,5667. \end{aligned}$$

Como, a entropia da fonte deste exemplo é $H(U) = (3/10)\log(10/3) + (5/12)\log(12/5) + (17/60)\log(60/17) = 1,5629$, então pela Definição 2, observa-se que a eficiência obtida pela técnica SH-SAS neste exemplo é $\eta_{SAS} = 0,6089$.

Abordando as técnicas JKM modificada e RM para a mesma fonte.

- JKM modificada
  Como visto anteriormente as decomposições das probabilidades dos símbolos u_1, u_2 e u_3, são dadas por (12), (13) e (14), respectivamente.
  De um modo geral, na técnica JKM modificada [4], após a decomposição das probabilidades dos símbolos da fonte são identificados os componentes periódicos e não-periódicos das decomposições das probabilidades dos símbolos da fonte. Os termos não-periódicos e os primeiros termos fornecem as probabilidades dos símbolos homofonemas, enquanto que as razões fornecem as probabilidades dos símbolos mudos. A partir daí é construído um código D-ário livre de prefixo.
  Se todas as razões são iguais, um único símbolo mudo é usado. Note, que neste exemplo, a decomposição de u_1 e a decomposição de u_3 tem mesma razão, $1/16$, no entanto, a decomposição de u_2 apresenta razão distinta, $1/4$. Logo, para esta fonte ao se utilizar a técnica JKM modificada são usados dois símbolos mudo, Δ_1 e Δ_2, com probabilidades, $P(\Delta_1) = 1/16$ e $P(\Delta_2) = 1/4$, respectivamente.
  Cada termo não-periódico corresponde a um subconjunto com um único homofonema e cada elemento periódico corresponde a um subconjunto com número infinito contável de homofonemas.
  Desta forma, nota-se que o símbolo u_1 tem seus homofonemas nos subconjuntos $V_{11} = \{v_{11}, \Delta_1 v_{11}, \Delta_1\Delta_1 v_{11}, \ldots\}$ e $V_{12} = \{v_{12}, \Delta v_{12}, \Delta_1\Delta_1 v_{12}, \ldots\}$, u_2 nos subconjuntos $V_{21} = \{v_{21}\}$ e $V_{22} = \{v_{22}, \Delta_2 v_{22}, \Delta_2\Delta_2 v_{22}, \ldots\}$ e u_3 nos subconjuntos, $V_{31} = \{v_{31}\}$ e $V_{32} = \{v_{32}, \Delta_2 v_{32}, \Delta_2\Delta_2 v_{32}, \ldots\}$ onde $v_{11} \rightarrow 10, v_{12} \rightarrow 11110, v_{21} \rightarrow 00, v_{22} \rightarrow 110, v_{31} \rightarrow 01, v_{32} \rightarrow 11111, \Delta_1 \rightarrow 1110$ e $\Delta_2 \rightarrow 11$. Logo, o código resultante para a fonte V é representado por $\{(1110)^i 10, (1110)^i 11110, 00, (11)^i 110, 01, (1110)^i 11111\}$ e o comprimento médio,

$$\begin{aligned} E_{JKM}(W) = & \left(\frac{1}{4}\right)\sum_{r=0}^{\infty}(2+4r)\left(\frac{1}{16}\right)^r \\ & + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\ & + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\sum_{r=0}^{\infty}(3+2r)\left(\frac{1}{4}\right)^r \\ & + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\sum_{r=0}^{\infty}(5+4r)\left(\frac{1}{16}\right)^r \\ & = 2,5667, \end{aligned}$$

e portanto, a eficiência, $\eta_{JKM} = \dfrac{H(U)}{E_{JKM}(W)} = \dfrac{1,5629}{2,5667} \Rightarrow \eta_{JKM} = 0,6089$.

- RM
  Pela técnica RM [7] o símbolo mudo é selecionado com probabilidade $P(\Delta) = 1/16$ e a fonte U é selecionada com probabilidade $15/16$, desta forma a fonte expandida tem distribuição de probabilidade dada por $\{1/4, 1/32, 1/4, 1/8, 1/64, 1/4, 1/64, 1/16\}$ (Figura 3). Assim, o comprimento médio é dado por

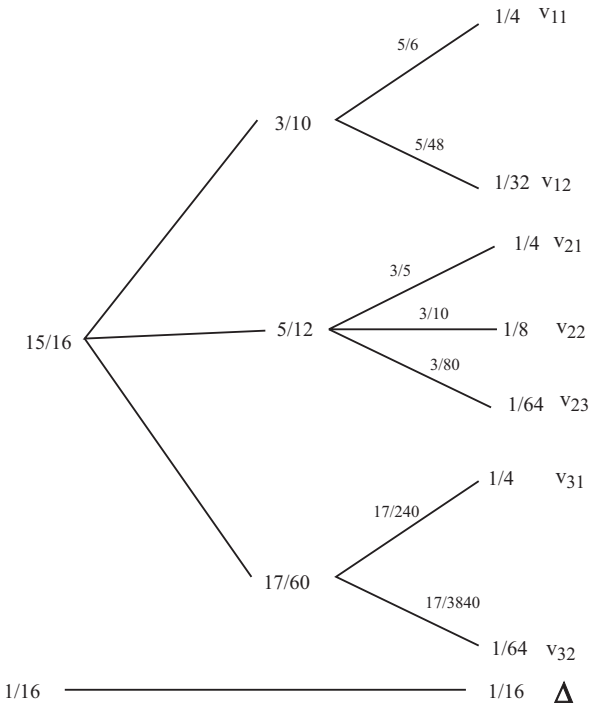

Fig. 3. Técnica RM para a fonte U com distribuição de probabilidade $P_U(u_1) = 3/10$, $P_U(u_2) = 5/12$ e $P_U(u_3) = 17/60$.

$$E_{RM}(W) = \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{32}\right)\cdot 5 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{8}\right)\cdot 3 + \left(\frac{1}{64}\right)\cdot 6 + \left(\frac{1}{4}\right)\cdot 2 + \left(\frac{1}{64}\right)\cdot 6 + \left(\frac{1}{16}\right)\cdot 4 = 2,4688,$$

sendo a eficiência dada por $\eta_{RM} = \dfrac{(1-P(\Delta))H(U)}{E_{RM}(W)} = \dfrac{\left(\frac{15}{16}\right)1,5629}{2,4688} \Rightarrow \eta_{RM} = 0,5935.$

V. Conclusões

A técnica SH-SAS apresenta a mesma eficiência que é obtida pela técnica JKM modificada. Em particular, quando a decomposição das probabilidades dos símbolos da fonte apresenta a mesma razão, comum a todos os símbolos, as probabilidades dos homofonemas coincidem nos dois casos, assim como também coincidem as probabilidades dos símbolos mudos. Neste caso, as técnicas JKM modificada e SH-SAS apresentam mesmo conjunto de homofonemas, uma vez que ambas as técnicas constroem cada palavra-código homofônica como a concatenação de palavras-código mais curtas derivadas a partir das probabilidades da fonte.

Na técnica JKM modificada [4], a razão de cada série geométrica infinita, produzida pela decomposição das probabilidades de determinados símbolos da fonte, é associada a um símbolo mudo, sendo as razões iguais mapeadas para um mesmo símbolo mudo. Portanto, caso haja razões distintas, haverá símbolos mudos distintos. A técnica SH-SAS utiliza apenas um único símbolo mudo, ao qual corresponde uma única palavra-código, que precisará ser detectada e apagada durante a decodificação (vide exemplo 2).

Ao se analisar a técnica RM percebe-se que, caso a decomposição das probabilidades dos símbolos da fonte apresente apenas termos periódicos, a eficiência obtida é a mesma para as três técnicas (RM, JKM e SH-SAS). Porém, quando a decomposição das probabilidades dos símbolos da fonte apresenta termos não-periódicos, a técnica RM apresenta uma eficiência menor que as demais.

Agradecimentos

Este trabalho recebeu apoio parcial do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, através dos projetos 141215/2002-0 e 305226/2003-7.

Referências

[1] H. N. Jendal, Y. J. B. Kuhn and J. L. Massey, "An Information-Theoretic Approach to Homophonic Substitution", *Advances in Cryptology-Eurocrypt'89* (Eds. J.-J. Quisquater and J. Vandewalle), LNCS No. 434. Springer, pp. 382-394, 1990.

[2] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Tech. J.*, vol.28, pp. 656-715, Oct. 1949.

[3] Ch. G. Günther, "A Universal Algorithm for Homophonic Coding", *Advances in Cryptology- Eurocrypt'88*, Lecture Notes in Computer Science, No.330. Heidelberg and New York: Springer, pp. 405-414, 1988.

[4] V. C. da Rocha, "Perfect homophonic substitution with finite memory", *Proc. IEEE International Symposium on Information Theory*, 30 June - 05 July 2002, Lausanne, Switzerland, p. 409.

[5] N. Abramson, *Information Theory and Coding*. McGraw-Hill, 1963.

[6] V. C. da Rocha Jr., C. Pimentel and D. P. B. A. Camara, "Redundancy in homophonic coding and a new homophonic coding technique", *Proceedings of the International Symposium on Information Theory - ISIT 2006*, Seattle, Washington, pp. 1253-1257, 9-14 July 2006.

[7] V. C. da Rocha and J. L. Massey, "Better than "optimum" homophonic substitution", *Proc. IEEE International Symposium on Information Theory*, 25-30 June 2000, Sorrento, Italy, p. 241.

[8] V. C. da Rocha, "On the minimum redundancy of homophonic coding", *International Telecomunications Symposium - ITS2002*, 30 June - 05 July 2002, Natal-RN, Brasil, pp.310-314.

[9] V. C. da Rocha and M.M. Vasconcelos, "Nova geração da representação D-ária de um número racional", *XXII Simpósio Brasileiro de Telecomunicações*, 2005, Campinas. Anais do XXIII Simpósio Brasileiro de Telecomunicações, 2005, pp. 573-575.