Trabalho apresentado no XXXVIII CNMAC, Campinas - SP, 2018.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Transformadas Digitais e Códigos de Bloco: Uma via de Mão Dupla

Arquimedes J. A. Paschoal[1]
Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco, IFPE, Caruaru, PE
Ricardo M. Campello de Souza[2]
Departamento de Eletrônica e Sistemas, UFPE, Recife, PE
Hélio M. de Oliveira[3]
Departamento de Estatística, UFPE, Recife, PE

Resumo. A construção de novos códigos de bloco lineares pode ser feita a partir de transformadas digitais. Aqui, mostramos que novas transformadas digitais podem ser derivadas a partir de códigos corretores de erros. Primeiro, apresentamos a construção de códigos de Pascal, baseados na Transformada Numérica de Pascal (TNP), e então as transformadas de Hamming e Golay baseadas, respectivamente, nos códigos de mesmo nome. Um Algoritmo para a decodificação de códigos de Pascal é apresentado. Uma aplicação das transformadas numéricas de Pascal, Hamming e Golay, como uma ferramenta de pré-processamento para cifragem de imagens, é sugerida.

Palavras-chave. TNP, Triângulo de Pascal, Transformadas Numéricas, Transformada de Hamming, Transformada de Golay, Cifragem de Imagens.

1 Introdução

Códigos corretores de erros são a ferramenta usual para proteger a integridade da informação que transita em um canal ruidoso [10]. Dentre os códigos corretores de erros mais conhecidos estão os códigos de Hamming, por terem sido os primeiros códigos desenvolvidos [5]. Existem inúmeras técnicas para a construção de códigos corretores de erros e conforme mostrado em [1, 2] este códigos também podem ser obtidos a partir de transformadas digitais. Neste cenário, propriedades verificadas pela matriz de transformação de tais transformadas podem ser exploradas no sentido de se produzir algoritmos eficientes para decodificação dos mesmos. Neste artigo apresentamos os códigos de Pascal, obtidos a partir da recém introduzida Transformada Numérica de Pascal [7]. Um algoritmo eficiente, baseado nas propriedades do triângulo de Pascal, para sua decodificação é apresentado. De forma algo similar, é possível criar novas transformadas digitais a partir de códigos corretores de erros existentes. Neste artigo introduzimos as transformadas de Hamming

[1]arquimedes.paschoal@caruaru.ifpe.edu.br
[2]ricardo@ufpe.br
[3]hmo@de.ufpe.br

DOI: 10.5540/03.2018.006.02.0332

e de Golay. Uma aplicação da TNP e destas transformadas como ferramentas de pré-processamento na cifragem de imagens é apresentada. Sua avaliação é feita por meio dos indicadores: histograma, NPCR, UACI e correlações horizontal, vertical e diagonal. Um teste de aderência nos histogramas das imagens transformadas fornece uma indicação da aproximação de tais histogramas por distribuições uniformes. *Scripts* em Matlab® para transformação das imagens, obtenção das métricas de interesse na área de processamento de imagens e sua reconstrução foram desenvolvidos. Foram utilizadas 10 imagens nos testes, obtidas da base de dados `http://sipi.usc.edu/database/` e convertidas para tons de cinza.

2 Códigos de Pascal

Sabe-se que a matriz de verificação de paridade H de um código de bloco linear satisfaz à relação $vH^T = 0$, em que v é uma palavra do código [10]. Para qualquer transformação linear T, tem-se que seus autovetores satisfazem à relação $[T - \lambda I]v = 0$, em que λ é o autovalor associado ao autovetor v. Identificando-se a matriz de verificação de paridade H com a forma escalonada padrão da matriz $[T-\lambda I]$, percebe-se que, a partir de qualquer transformada digital, é possível definir um código de bloco linear [4]. Especificamente, esta técnica foi usada para construir as famílias dos códigos de Fourier e de Hartley [1, 2]. Neste artigo, uma nova família de códigos de bloco lineares, denominada de Códigos de Pascal, é construída. Usando a matriz de Pascal sobre $GF(p)$, P_N [8], como matriz de transformação, podemos construir os códigos de Pascal, denotados $CP^{(\lambda)}(n, k, d)$. Determinando os autovalores da matriz P_N, a matriz $[P_N - \lambda I]$ é encontrada. Esta matriz, reduzida à forma escalonada, resulta na matriz de verificação de paridade, $H_p^{(\lambda)}$, do código. A existência de um código de Pascal sobre $GF(p)$ requer que o polinômio característico da matriz P_N possua, pelo menos, um autovalor neste corpo.

Exemplo 2.1. *Construção do código de Pascal de comprimento $N = 13$ sobre $GF(3)$. Considere a matriz de Pascal, sobre GF(3), cujo polinômio característico é $p(x) = 1 + 2x + x^3 + 2x^4 + x^9 + 2x^{10} + x^{12} + 2x^{13} = 2(1 + x)^{12}(2 + x)$,*

$$P_{13} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 2 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 1 \end{bmatrix}.$$

Os autovalores de P_{13} são $\lambda_1 = 2$, com multiplicidade algébrica $m = 12$, e $\lambda_2 = 1$, com multiplicidade algébrica $m = 1$.

DOI: 10.5540/03.2018.006.02.0332

A matriz $[P_{13} - \lambda_1 I]$*, reduzida à forma escalonada, é*

$$H_{13}^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

O código de Pascal gerado é o código $CP^{(2)}(13, 4, 4)$ *e sua matriz geradora é*

$$G_{13}^{(2)} = \begin{bmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Para o autovalor $\lambda_2 = 1$*, obtém-se o código* $CP^{(1)}(7, 1, 7)$*. Isto ilustra o fato de que é possível se obter códigos de comprimentos diferentes do comprimento da transformada.* ■

2.1 Decodificação dos códigos de Pascal

Os códigos de Pascal, sendo códigos lineares de bloco, podem ser decodificados via técnicas usuais [10]. Todavia, uma forma alternativa de decodificação pode ser concebida explorando-se características específicas da matriz de transformação de Pascal, P_N. Considere que a palavra recebida seja escrita como $r = v + e$, em que v é a palavra-código transmitida e e é o vetor erro possivelmente introduzido pelo canal. Como as palavras-código do código de Pascal são autovetores associados à matriz de transformação, resulta que a aplicação da TNP à palavra recebida r produz: $TNP(r) = \lambda v + TNP(e)$. Sem perda de generalidade, seja $\lambda = 1$. Assim, caso a palavra recebida não contenha erros, $TNP(r) = r = v$. Caso contrário, a palavra recebida contém erros. Assim, a síndrome da palavra recebida r corresponde ao cálculo da TNP de r. Considere inicialmente a ocorrência de um único erro na posição i, $0 \leq i \leq (p-1)$. Então $TNP(e) = l_i$, em que l_i é a i-ésima linha da matriz de transformação da TNP. Desta forma, podemos escrever $TNP(r) = v + l_i$. Denotando $TNP(r)$ por $R = [R_0\ R_1\ \cdots\ R_{p-1}]$ e $v = [v_0\ v_1\ \cdots\ v_{p-1}]$, resulta

$$TNP(r) = \begin{bmatrix} R_0 \\ R_1 \\ \vdots \\ R_{p-1} \end{bmatrix} = \begin{bmatrix} \textit{Matriz Geradora} \\ \textit{de Autovetores} \\ \textit{(MGA)} \end{bmatrix} + \begin{bmatrix} l_i^{(0)} = 1 \\ l_i^{(1)} \\ \vdots \\ l_i^{(p-1)} \end{bmatrix},$$

em que $l_i^{(j)}$ corresponde à j-ésima componente da i-ésima linha da matriz de Pascal. A matriz geradora de autovetores (MGA) é obtida como solução do sistema $v = P_N^{-1} v$. Note que como as linhas da matriz de Pascal sempre iniciam por 1 e são todas distintas, basta saber o segundo elemento do vetor que representa a i-ésima linha da matriz de Pascal, que todo o vetor estará determinado. A seguir, apresentamos o pseudocódigo para decodificação em caso de erro único.

DOI: 10.5540/03.2018.006.02.0332

Algorithm 1 Decodificação dos Códigos de Pascal para um único erro

procedure DECODEPASCAL(R)
  if $(R = r)$ **then**
    Não houve erro ou erro não detectável.
  else if $(R^{(0)} = R^{(p-1)})$ **then**
    Erro na posição zero
    k é solução do sistema $R = MGA + kl_0$
  else
    $k \leftarrow R^{(0)} - R^{(p-1)}$
    $l_i^{(p-1)} \leftarrow 0$
    $v_{p-1} \leftarrow R^{(p-1)}$
    $j \leftarrow 2$
    repeat
      l_i^{p-j} é solução do sistema $R = MGA + kl_i$
      $j \leftarrow j + 1$
    until $(l_i^{p-j-1} \neq 0)$
    A linha está determinada
  end if
end procedure

3 As Transformadas de Hamming e de Golay

Na Seção 2 construiu-se a matriz de verificação de paridade, H, de um código de bloco linear, escalonando-se a matriz quadrada singular $[T - \lambda I]$. Aqui, segue-se o "sentido oposto", i.e., partindo da matriz de paridade de um código de bloco linear $C(n, k, d)$, acrescentamos, à mesma, k linhas de modo a obter uma matriz quadrada (singular) de ordem n, H_e, correspondente à matriz $[T - \lambda I]$. Este procedimento leva à construção de uma nova matriz de transformação $T = H_e + \lambda I$. Tal transformada recebe o nome do código de bloco linear usado na sua construção. Assim, se $C(n, k, d)$ representa o código de Hamming sobre $GF(p)$, então T representa a matriz de transformação da Transformada Numérica de Hamming (TNH) sobre $GF(p)$. Uma forma de representar algebricamente a TNH é considerar a matriz de verificação de paridade H no formato

$$H = \begin{bmatrix} h(x) \\ xh(x) \\ \vdots \\ x^{n-k-1}h(x) \end{bmatrix},$$

em que $h(x)$ é o polinômio de paridade do código de Hamming cíclico sobre $GF(p)$ [6]. As k linhas necessárias para compor a matriz H_e são obtidas deslocando-se ciclicamente o polinômio $h(x)$.

Exemplo 3.1. *Considere o código de Hamming cíclico binário $C(7, 4, 3)$ com polinômio de verificação de paridade dado por $h(x) = x^4 + x^2 + x + 1$. A matriz de verificação de*

paridade H é dada por

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

A matriz de transformação da transformada numérica de Hamming, neste caso, é

$$T_H^{(1)} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

De forma similar, definimos a Transformada Numérica de Golay usando o polinômio de paridade do código de Golay escolhido.

3.1 Propriedades das transformadas numéricas de Hamming e Golay

Além da linearidade, as propriedades listadas a seguir são satisfeitas pelas Transformadas de Hamming e de Golay [9], além da linearidade.

i) **Deslocamento no domínio do tempo**: Considere a sequência $\widehat{v} = (\widehat{v}_0, \cdots, \widehat{v}_{N-1})$ em que $\widehat{v}_i = v_{i-m}$. Então, $\widehat{v} \leftrightarrow \widehat{V}$, em que $\widehat{V} = x^m V$.

ii) **Deslocamento no domínio da frequência:** Considere a sequência $\widehat{V} = (\widehat{V}_0, \cdots, \widehat{V}_{N-1})$ em que $\widehat{V}_k = V_{k-l}$. Então, $\widehat{v} = x^l v$.

iii) **Transformada da sequência constante:** A transformada da sequência $v = (r, r, \cdots, r)$ é a sequência de componentes $V_k = r \cdot peso(h(x)) \pmod p$, $\forall k$.

iv) **Transformada da sequência impulso:** A transformada da sequência $\delta = (1, 0, \cdots, 0)$, corresponde à primeira coluna da matriz $T_H^{(\lambda)}$, isto é, aos coeficientes do polinômio $x[h(x) + \lambda(x)]$, em que $\lambda(x)$ é o polinômio constante.

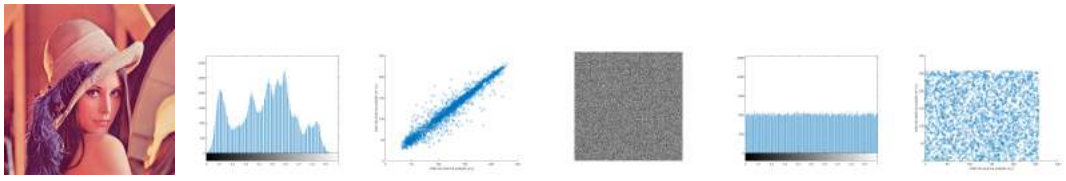
4 Aplicações em Processamento de Imagens

Uma possível aplicação inicial das transformadas numéricas de Pascal, Hamming e Golay é como uma ferramenta de pré-processamento na cifragem de imagens. Neste cenário, a correlação entre pixels adjacentes é uma medida indicativa da capacidade da transformada em dispersar (difundir) informação; outras medidas desta capacidade são o histograma, a entropia e os valores do NPCR *(Number of Changing Pixel Rate)* e UACI *(Unified Averaged Changed Intensity)* [3, 11]. Todas estas medidas foram implementadas usando-se o Matlab como ferramenta de programação. As imagens utilizadas nos testes foram obtidas da base de dados `http://sipi.usc.edu/database/` e convertidas para tons de cinza. Para efeito de processamento de imagens, a imagem original (512×512 pixels) foi dividida em 4096 blocos de 8×8 pixels. Como a imagem é convertida em tons de cinza, os valores dos pixels variam de 0 até 255. Portanto, usou-se o corpo finito $GF(257)$.

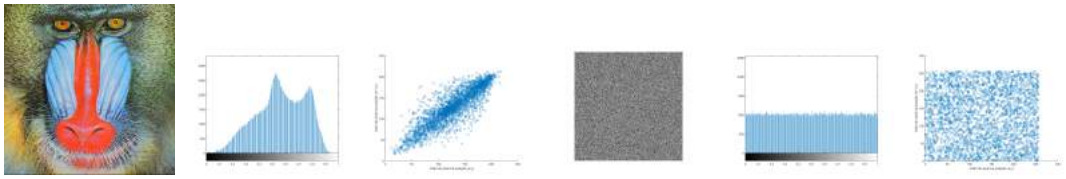
DOI: 10.5540/03.2018.006.02.0332

4.1 Avaliação de desempenho das transformadas

As transformadas numéricas de Pascal, Hamming e Golay são avaliadas por meio dos seguintes indicadores: histogramas, NPCR, UACI, r_{xx} (correlação horizontal entre pixels vizinhos), r_{yy} (correlação vertical entre pixels vizinhos), r_{xy} (correlação diagonal entre pixels vizinhos) e Entropia de Shannon $H(S)$. A Figura 1 mostra duas das 10 imagens



(1) Lena



(2) Mandril

Figura 1: Imagens utilizadas, seus histogramas e correlações verticais, TNP das imagens, histogramas das transformadas e correlação vertical das transformadas.

utilizadas nos testes, juntamente com os indicadores mencionados. Note que a aplicação da TNP produz uma imagem difusa, apresentando um histograma que se *aproxima* de uma distribuição uniforme. A Tabela 1 resume os valores obtidos para as transformadas apresentadas aqui. Em termos de correlação entre pixels, percebe-se que as transformadas de Pascal e de Hamming apresentam resultados similares, enquanto que a transformada de Golay apresenta resultados inferiores, o que é confirmado visualmente nas imagens das transformadas [9].

Tabela 1: Coeficientes de correlação das imagens antes e depois da aplicação da TNP, TNH e TNG.

	TNP		**TNH**		**TNG**	
Métrica	Lena	Mandril	Lena	Mandril	Lena	Mandril
$\mathrm{r}_{xy}(h)$	0,9848	0,7580	0,9849	0,7602	0,9865	0,7879
$\widehat{r}_{xy}(h)$	0,0037	-0,0015	0,0068	0,0027	0,2150	0,0282
$\mathrm{r}_{xy}(v)$	0,9712	0,8641	0,9722	0,8650	0,9740	0,8786
$\widehat{r}_{xy}(v)$	0,0039	0,0039	-0,0043	0,0011	0,1398	0,0300
$\mathrm{r}_{xy}(d)$	0,9586	0,7251	0,9594	0,7283	0,9609	0,7493
$\widehat{r}_{xy}(d)$	0,0034	-0,0011	0,0004	-0,0030	0,0064	0,0090

5 Conclusões

A transformada numérica de Pascal foi usada na construção de novos códigos de bloco multiníveis, os códigos de Pascal. A introdução das transformadas numéricas de Hamming

(TNH) e de Golay (TNG) representa uma importante aplicação da teoria introduzida em [1, 2], e delineia a existência de um *isomorfismo* entre códigos de bloco lineares e transformadas digitais. Umas das propriedades marcantes destas novas transformadas é que a transformada de um vetor constante (propriedade iii) resulta em um vetor no domínio da transformada também constante. Isto contrasta fortemente com as transformadas usuais. Os resultados obtidos para as transformadas digitais TNP, TNH e TNG como ferramentas para o pré-processamento de cifragem de imagens são apresentados.

Referências

[1] R. M. Campello de Souza, E. S. V. Freire and H. M. de Oliveira, Fourier codes. In *10th International Symposium on Communication Theory and Applications*, Ambleside, UK, 2009. Also available in the repository arXiv:1503.03293 [cs.IT]

[2] R. M. Campello de Souza, R. M. C. Britto e H. M. de Oliveira, Códigos de Hartley em corpos finitos. In *Anais do XXIX Simpósio Brasileiro de Telecomunicações*, Curitiba, 2011.

[3] S. Das, S. N. Mondal and N. Ghoshal, An Innovative Approach in Image Encryption. *Proc. of Int. Conf. on Recent Trends in Information, Telecommunication and Computing*, 158-166, 2014. DOI: 02.ITC.2014.5.96

[4] E. S. V. Freire, *Construção de Códigos de Bloco Lineares via Transformadas Digitais*. Dissertação de Mestrado, Programa de Pós-Graduação em Engenharia Elétrica, UFPE, 2009.

[5] R. W. Hamming, Error detecting and error correcting codes, *Bell Labs Technical Journal*, v.29, 147-160, 1950.

[6] T. K. Moon. *Error Correction Coding: Mathematical Methods and Algorithms*. John Wiley and Sons, 2005.

[7] A. J. A. Paschoal, R. M. Campello de Souza, H. M. de Oliveira, A Transformada numérica de Pascal. In *Anais do XXXIII Simpósio Brasileiro de Telecomunicações*, Juiz de Fora, Brasil, 2015.

[8] A. J. A. Paschoal, R. M. Campello de Souza e H. M. de Oliveira, Novas relações na matriz de transformação da transformada numérica de Pascal. *Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, v.6, 2018.

[9] A. J. A. Paschoal, *Novas Transformadas em Corpos Finitos: Definições e Cenários de Aplicação*. Tese de Doutorado, Programa de Pós-Graduação em Engenharia Elétrica da UFPE, 2018.

[10] S. Lin and D. J. Costelo. *Error Control Coding*. Englewood Cliffs, Prentice Hall, 2004.

[11] Y. Wu, J. P. Noonan and S. Agaian. NPCR and UACI randomness tests for image encryption. *Journal of Selected Areas in Telecommunications*, 31–38, 2011.

