

Finally, we examine the spectral properties of the functional k -potent matrix as follows,

$$A^k = \alpha I + \beta A^r, \quad \alpha\beta \neq 0, \quad k > r \geq 1 \quad (13)$$

It can be verified that the eigenvalues of a functional k -potent matrix (13) are solutions of the following equation

$$\lambda^k - \beta\lambda^r - \alpha = 0 \quad (14)$$

Since $\alpha \neq 0$, all the eigenvalues are nonzero. Therefore, the matrix is nonsingular.

Proposition 2.14 Functional k -potent matrices (13) are diagonalizable.

Proof: Assume the matrix is not diagonalizable. With the spectral decomposition of A , $A = P\Lambda P^{-1}$, where Λ is given by (5). The Jordan block in Λ is given by (7). Therefore, this Jordan block must satisfy (13). Given that $\lambda_s \neq 0$ because the eigenvalues are nonzero. One has, according to (8),

$$J_{m_s}^k = (\Lambda_s + N_s)^k = \sum_{n=0}^k C_k^n \Lambda_s^{k-n} N_s^n = \sum_{n=0}^{\min\{k, m_s\}} C_k^n \Lambda_s^{k-n} N_s^n$$

$$= \begin{bmatrix} \lambda_s^k & C_k^1 \lambda_s^{k-1} & C_k^2 \lambda_s^{k-2} & \dots & C_k^{m_s-1} \lambda_s^{k-m_s+1} \\ & \lambda_s^k & C_k^1 \lambda_s^{k-1} & C_k^2 \lambda_s^{k-2} \dots & C_k^{m_s-2} \lambda_s^{k-m_s+2} \\ & & \ddots & & \\ & & & \ddots & C_k^2 \lambda_s^{k-2} \\ & & & & \lambda_s^k \end{bmatrix}$$

and

$$\alpha I + \beta A^r = \alpha I + \beta (\Lambda_s + N_s)^r = \alpha I + \beta \sum_{n=0}^r C_r^n \Lambda_s^{r-n} N_s^n$$

$$= \alpha I + \beta \sum_{n=0}^{\min\{r, m_s\}} C_r^n \Lambda_s^{r-n} N_s^n$$

$$= \begin{bmatrix} \alpha + \beta \lambda_s^r & C_r^1 \beta \lambda_s^{r-1} & C_r^2 \beta \lambda_s^{r-2} & \dots & C_r^{m_s-1} \beta \lambda_s^{r-m_s+1} \\ & \alpha + \beta \lambda_s^r & C_r^1 \beta \lambda_s^{r-1} & C_r^2 \beta \lambda_s^{r-2} \dots & C_r^{m_s-2} \beta \lambda_s^{r-m_s+2} \\ & & \ddots & & \\ & & & \ddots & C_r^2 \beta \lambda_s^{r-2} \\ & & & & \alpha + \beta \lambda_s^k \end{bmatrix}$$

Comparing the two matrices, the off-diagonal entries are mismatched because $k > r$. Therefore, the functional k -potent matrices (13) are diagonalizable.

In summary, we categorize four groups of k -potent matrices: (i) nilpotent matrices, (ii) periodic and unipotent matrices, (iii) skew-periodic and skew-unipotent matrices, and (iv) the functional k -potent matrices. The classification is based on the characteristics of the eigenvalue/eigen-space of the matrices. The results presented above will be used to manufacture such matrices symbolically, i.e. all k -potent matrices are constructed over the integer field.

Our objective in this work is to develop an algorithm for constructing integral k -potent matrices. In particular, (skew-) periodic and (skew-) unipotent matrices are useful in digital signal encryption. Instructors who teach Linear Algebra and Numerical Analysis may find the proposed algorithm useful as they may want to come up with a number of such k -potent matrices for students to practice with the related concepts in matrix theory.

The idea is simple. A power-induced matrix can be easily constructed via the spectral decomposition formula, i.e.

$$A = P\Lambda P^{-1} \quad (15)$$

where P is an invertible matrix and Λ is either a diagonal matrix or a block diagonal matrix in Jordan form. It is easy to see that, as long as Λ is k -potent, the matrix A is k -potent of the same type. In what follows, we introduce different ways for constructing the Λ -matrix so that it is a power-induced matrix satisfying a predetermined index number.

Case (i): Nilpotent matrices

According to Proposition 2.4, the Λ -matrix in (15) is guaranteed nilpotent with certain index number if Λ consists of nilpotent Jordan blocks, and the size of the largest nilpotent Jordan block equals the index number. The following matrix, for example, is a nilpotent matrix with index 4, i.e. $\Lambda^4 = 0$.

$$\Lambda = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (16)$$

Case (ii): Periodic matrices

Proposition 2.7 and equation (9) are the keys for constructing periodic Λ -matrix. For the sake of argument, let ν be the period of Λ and let

$\Gamma_\nu = \{0\} \cup \{e^{i2m\pi/\nu}, m = 0, 1, \dots, \nu - 1\}$ be the set of eigenvalues of the periodic matrix. It is sufficient that

$$\Lambda = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_s), \tag{17}$$

where $\lambda_i \in \Gamma_\nu, i = 1, 2, \dots, s$, which guarantees that the Λ -matrix (12) is a periodic matrix with period ν . The Λ -matrix can also be written as a block diagonal matrix as follows

$$\Lambda = \text{diag}(B_1, B_2, \dots, B_m) \tag{18}$$

as long as the eigenvalues of each block $B_i, i = 1, 2, \dots, m$, belong to Γ_ν . This setting gives us some flexibility for constructing periodic matrices. One can also mix the eigenvalues of the Λ -matrix in (17) or (18) to construct periodic matrices with a higher index number. To this end, let the eigenvalues of Λ be chosen from the following set

$$\Gamma = \Gamma_{\nu_1} \cup \Gamma_{\nu_2} \cup \dots \cup \Gamma_{\nu_t}, \tag{19}$$

and let

$$\nu^* = \text{LCM}(\nu_1, \nu_2, \dots, \nu_t), \tag{20}$$

where LCM stands for least common multiple, then, it can be verified that the period of Λ is ν^* . For example, the following matrix is a periodic matrix with period 12,

$$\Lambda = \begin{bmatrix} 1 & 3 & 0 & 0 \\ -1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \tag{21}$$

because the eigenvalues of the first block are $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, which are solutions of (9) with $\nu = 3$, and the eigenvalues of the second block in (21) are solutions of (9) with $\nu = 4$.

The treatment for constructing the other Λ -matrices, i.e. unipotent, skew-periodic, and skew-unipotent matrices, is essentially the same as that for periodic matrices because the eigen-structures among those matrices are similar. When constructing such matrices, one should realize that the equations (9), (10), and (11)

must be satisfied for the corresponding matrices.

For mathematics instructors, it is preferred to work with integral matrices, i.e. the elements of a matrix are all integers, mainly because the arithmetic is symbolic as far as additions and multiplications are concerned, which also implies that there are no roundoff errors. We are able to achieve this when constructing the Λ -matrix, see (21), for instance.

Instead of constructing the Λ -matrix, one can take advantage of the companion matrix for the characteristic polynomial [3]. In general, the companion matrix of an n th degree characteristic polynomial

$$P(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_1\lambda + a_0$$

is given by

$$\Lambda_p = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ & & \ddots & & \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix} \tag{22}$$

The characteristic polynomials of various kinds of k -potent matrices are given by equations (9)-(12) and (14). Formula (15) can be used if one wants to construct a dense integral k -potent matrix, where both P and P^{-1} in (15) have to be integral matrices. In what follows, let $Z^{n \times n}$ represent the set of n by n integral matrices. The following proposition gives the necessary and sufficient condition for $A^{-1} \in Z^{n \times n}$ if $A \in Z^{n \times n}$.

Proposition 2.15 Suppose $A \in Z^{n \times n}$ and A is a nonsingular matrix, then $A^{-1} \in Z^{n \times n}$ if and only if $\det(A) = \pm 1$.

Proposition 2.15 gives us a guideline for constructing such an integral P -matrix. We can simply use the following formula for P ,

$$P = UL, \tag{23}$$

where U is an upper triangular integral matrix with 1's on the main diagonal and L is a lower triangular integral matrix with 1's on the main diagonal. It is obvious that $|P| = 1$, according to Proposition 2.15, P^{-1} is an integral matrix. With an integral P -matrix from (23), we obtain a dense integral nilpotent matrix calculate from (16),

$$A = \begin{bmatrix} 22 & 44 & 114 & 183 & 2 & -317 \\ -13 & -26 & -68 & -110 & -4 & 188 \\ 20 & 40 & 104 & 167 & 2 & -289 \\ 9 & 18 & 48 & 77 & 3 & -133 \\ -14 & -28 & -74 & -118 & -2 & 206 \\ 12 & 24 & 63 & 101 & 2 & -175 \end{bmatrix}$$

It is verified in MatLab that $A^4 = 0$, which has the same index of nilpotency as that of (11). A more sophisticated algorithm for constructing integral similarity transformation matrices can be found in [25].

We also constructed an integral periodic matrix from (21) as follows

$$A = \begin{bmatrix} -8 & -1 & 2 & 4 \\ 22 & 4 & -5 & -12 \\ -42 & -8 & 9 & 21 \\ 11 & 3 & -2 & -6 \end{bmatrix}$$

It is hard to tell that the matrix above is a periodic matrix with period 12 unless one literally calculates the power matrix A^{13} without peeking at the eigenvalues of A .

For more general k -potent matrices, the eigenvalues are usually non-integers. However, it is always feasible to make use of the companion matrix (22) for the characteristic polynomials of the k -potent matrices, such as (9)-(12) and (14), combined with the integral similarity transformation matrix P in (23). The following matrix satisfies matrix equation $A^4 = 3I - A^2$,

$$A = \begin{bmatrix} -9 & -16 & -7 & 24 \\ 7 & 12 & 6 & -17 \\ -2 & -3 & -1 & 5 \\ 1 & 2 & 2 & -2 \end{bmatrix}$$

3 Applications to image encryption

An image is formed from MN samples arranged in a two-dimensional array of M rows and N columns such as a photo, an image formed of the temperature of a integrated circuit, x-ray emission from a distant galaxy, a satellite map from Google Earth.

In imaging terminology, each sample of the image is called a pixel. Each pixel is attributed a value called grayscale ranging from 0 to 255, where 0 is black, 255 is white, and the intermediate values are shades of gray. For the purpose of image encryption, we apply a series of encryption key matrices to mask an image via matrix multiplications. This will alter the gray level of each

pixel so that the original image is no longer recognizable. This masking process is in essence a filtering process because each row (column) in the encryption key matrix is treated as a digital filter with finite impulse response. Due to the randomness and magnitude of the filter coefficients, the original image is transformed into a rather different image by way of a filter banks.

We adopt the previously studied k -potent matrices for the encryption key matrix, particularly the unipotent or periodic matrices. The nilpotent matrix can also be used for image encryption with some special treatment such as diagonal perturbation, but we will not elaborate here.

The cryptosystem proposed in this paper consists of associate keys and primary keys. The function of the associate key T_1 is to divide the original image into sub-images, not necessarily the same sizes, followed by another associate key T_2 to permute the pixels of the sub-image for pre-scrambling. The permutation key is nothing but a product of elementary matrices. The mathematical setting is given as following for the pre-encryption stage:

$$T_{1i} : Z^{M \times N} \rightarrow Z^{m_i \times n_i}, m_i < M, n_i < N, i = 1, 2, \dots, k \quad (24)$$

$$\sum m_i = M, \sum n_i = N.$$

$$T_{2i} : Z^{m_i \times n_i} \rightarrow Z^{m_i \times n_i}, i = 1, 2, \dots, k. \quad (25)$$

$$T_{2i} = E_{i1} E_{i2} \dots E_{is}$$

where E_{ij} is an elementary matrix that exchange the rows of a matrix if left-multiplied or columns of the matrix if right-multiplied.

The primary key can be formulated via a product of unipotent and/or skew-unipotent matrices as follows

$$T_M = A_1^{k_1} A_2^{k_2} \dots A_t^{k_t} \quad (26)$$

Let X_i be a sub-image from (24) to be scrambled, with matching dimensions to assure multiplicability between T_M and X_i , the encrypted image is obtained as $Y_i = T_M X_i$. The decryption key is given by

$$T_M^{-1} = (-1)^p A_t^{n_t - k_t} A_{t-1}^{n_{t-1} - k_{t-1}} \dots A_1^{n_1 - k_1} \quad (27)$$

where n_i is such that $A_i^{n_i} = \pm I, i = 1, 2, \dots, t$ and p represents the number of skew-unipotent matrices applied in (26). With (27), the original image is recovered from Y_i via $X_i = T_M^{-1} Y_i$. It is also ready to be seen that the decryption process only involves matrix

multiplication with additions and multiplications between integers. Therefore, lossless image encryption/decryption is guaranteed, see Fig. 1 for an example. The encryption key consists of three 5 by 5 unipotent matrices.

Interestingly enough, functional k -potent matrix can add more complexity to the encryption scheme, proposed as follows. Consider the functional k -potent matrix, which is also an extension of (13),

$$A^k = I + \sum_{i=1}^m \beta_i A^i \tag{28}$$

where $0 < m < k$. Let X be a sub-image as a result of the pre-encryption stage (24) and (25). Let Y be the scrambled image encrypted by the functional k -potent matrix (28), i.e. $Y = AX$. Now, the decryption process is carried out as follows:

Step 1. Pre-multiply Y by A^{i-1} , respectively, to get $Z_i = A^i X$, $i = 1, 2, \dots, m$, with $A^0 = I$.

Step 2. Pre-multiply Z_m by A^{k-m} to get $W = A^k X$.

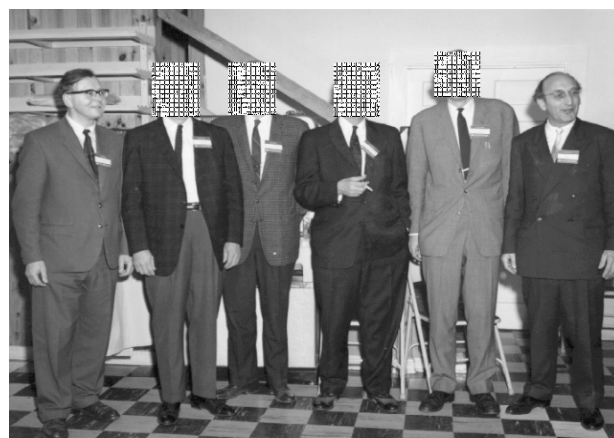
Step 3. $X = W - \sum_{i=1}^m \beta_i Z_i$ due to (28).

Another image encryption with the above proposed method is shown in Fig.2.

In this paper, we studied the eigen-spaces of various k -potent matrices, including Nilpotent, periodic, involutory, and skew-periodic matrices. Extensions are made to more general functional k -potent matrices. An immediate application of the results is seen in digital image encryption. The methodology proposed in this paper can also be extended to other functional matrices satisfying special constraints, similar to the ones for the k -potent matrices, and such constraints have imprints on the eigen-space structures of the matrices.



(a)

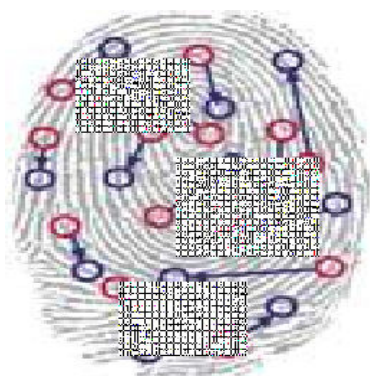


(b)

Figure 1. (a) original picture of mathematicians; (b) encrypted image of selected faces (courtesy of MatLab image processing toolbox)



(a)



(b)

Figure 2. (a) original fingerprint image; (b) scrambled image of selected areas of the fingerprint (courtesy of MatLab image processing toolbox)

References:

- [1] S. H. Friedberg, A. J. Insel, L.E. Spence, *Linear Algebra*, 4th Ed., Prentice Hall, Upper Saddle River, NJ, 2002.
- [2] G. Strang, *Introduction to Linear Algebra*, 3rd Ed., Wellesley-Cambridge Press, MA, 2003.
- [3] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 2nd Ed., The Johns Hopkins University Press, Baltimore, Maryland, 1989.
- [4] G. W. Stewart, *Matrix Algorithms, Volume II: Eigensystems*, SIAM, Philadelphia, PA, 2001.
- [5] J. H. Wilkinson, *The Algebraic Eigenvalue Problem*, Oxford Science Publications, NY, 1965.
- [6] J. Rimas, Computing of Positive Integer Powers for a Special Kind of Matrices, *WSEAS Trans. Math.*, v. 6, no.2, 289-295, 2007.
- [7] S. L. Steinberg, J. P. Zingano, and P. R. Zingano, On nilpotent singular systems, *J. Comput. Appl. Math.* 137, 97-107, 2001.
- [8] J. K. Baksalary and O. M. Baksalary, Idempotency of linear combinations of two idempotent matrices, *Linear Algebra Appl.* 321, 3-7, 2000.
- [9] J. K. Baksalary, O. M. Baksalary, and G. P. H. Styan, Idempotency of linear combinations of an idempotent matrix and a tripotent matrix, *Linear Algebra Appl.* 354, 21-34, 2002.
- [10] O. M. Baksalary, Idempotency of linear combinations of three idempotent matrices, two of which are disjoint, *Linear Algebra Appl.* 388, 67-78, 2004.
- [11] J. K. Baksalary, O. M. Baksalary, and H. Özdemir, A note on linear combinations of commuting tripotent matrices, *Linear Algebra Appl.* 388, 45-51, 2004.
- [12] L. Tang, Methods for encrypting and decrypting MPEG video data efficiently, *Proc. ACM Multimedia*, 219-229, 1996.
- [13] S. U. Shin, K.S. Kim, and K. H. Rhee, A secrete scheme for MPEG video data using the joint of compression and encryption, *Proc. Inform. Security Workshop (ISW '99)*, v. 1729 (*lecture notes on computer science*), 191-201, 1999.
- [14] Wenjun Zeng and Shawmin Lei, Efficient frequency domain selective scrambling of digital video, *IEEE Trans. Multimedia*, v. 5, no.1, 118-129, 2003.
- [15] P. P. Dang and P. M. Chau, Image encryption for secure internet multimedia applications, *IEEE Trans. Consum. Electron.*, v. 46, no.3, 395-403, 2000.
- [16] R. P. Elias, O. V. Villegas, M. L. Sanchez, and V. G. C. Sanchez, Automatic Inspection Using Edge Preserving Wavelet Lossy Image Coding by Means of Modified SPIHT, *WSEAS Trans. Signal Process.*, v. 2, no. 11, 1515-1522, 2006.
- [17] B. Ontiveros, I. Soto, and R. Carrasco, A New Cryptography Algorithm Using Cab Curves and LDPC for Wireless Communication Systems, *WSEAS Trans. Math.*, v. 6, no.2, 422-424, 2007.
- [18] J. Scharinger, Fast encryption of image data using chaotic Kolmogorov flows, *Journal of Electron. Imaging*, v. 7, no. 2, 318-325, 1998.
- [19] J.C. Yen and J. I. Guo, A new chaotic key-based design for image encryption and decryption, *Proc. IEEE Int. Conference Circuits and Systems*, v.4, 49-52, 2000.
- [20] H. Zhang, X. F. Wang, Z. H. Li, D. H. Liu, and Y. C. Lin, A new image encryption algorithm based on chaos system, *Proc. IEEE Intern. Conference Robotics, IS and Signal Process*, 778-782, 2003.
- [21] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. Journal Bifurcation & Chaos*, v. 8, no.6, 1259-1284, 1998.
- [22] G. Jakimoski and L. Kocarev, Analysis of some recently proposed chaos-based encryption algorithms, *Physics Letters A*, v. 291, no. 6, 381-384, 2001.
- [23] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision, *Computer Physics Communications*, v. 153, no. 1, 52-58, 2003.
- [24] A. Kulkarni and S. Mccaslin, Knowledge Discovery from Satellite Images, *WSEAS Trans. Signal Process.*, v. 2, no. 11, 1523-1530, 2006.
- [25] Y. Wu and A. C. Vosler, An Anti-Symmetric Key Algorithm for Signal Encryption, *Proceedings of the WSEAS Inter. Conf. on Signal Process.*, pp 140-145, 2007.