K-Potent Matrices-Construction and Applications in Digital Image Encryption

Yan Wu
Department of Mathematical Sciences
Georgia Southern University
Statesboro, GA 30460
USA
yan@georgiasouthern.edu

Abstract: - A k-potent matrix is any matrix A, the k_{th} power of which is a linear combination of the identity matrix and A, for example, unipotent, idempotent, and involutary matrices are special k-potent matrices. Such matrices have values in applications to digital image encryption. In order to achieve lossless image decryption, all arithmetic operations are restricted over the integer field. Therefore, algorithms are sought to construct integral k-potent matrices. It turns out that the unique eigen-structure of these matrices provides the key for constructing k-potent matrices systematically. In this paper, we explore the spectral properties of k-potent matrices and applications to digital image encryption.

Key-Words: Nilpotent, Idempotent, Involutary, Unipotent, Skewed *k*-potent Matrix, Diagonalizability, Image Encryption

1 Introduction

In the past decade or so, image encryption techniques were developed to keep up with the pace of the growth of internet and multimedia communications. There are hard encryption and soft encryption approaches. Most digital images are scrambled with soft encryption, which is also the choice of encryption as a component of the proposed UAS. Most image encryption methods can be classified as the DCT-based techniques, DWT-based (Discrete Wavelet Transform) techniques, transformations, and chaotic maps. Both DCT and DWT-based techniques are known as compression oriented schemes. The well-received MPEG encryption was first proposed by Tang [Tang, 1996] and is called "zig-zag permutation algorithm". The idea is to substitute the fixed zig-zag quantized DCT coefficient scan pattern by a random permutation list. A number of improvements on MPEG encryption were developed thereafter [Shin *et. al.*, 1999; Zeng and Lei, 2003;]. The DWT-based method, [Dang and Chau, 2000], takes advantage of the efficient image compression capability of wavelet networks through multi-resolution analysis integrated with block cipher data encryption. The chaos-based encryption of images employs the principle of applying chaotic maps with strong perplexing characteristics, such as non-periodic, non-convergent, randomness, and ergodic to the visual data. The most common nonlinear chaotic maps inherit properties as discrete cryptographic systems. Such systems are hybrids between permutation and substitution ciphers with specific properties. Scharinger [Scharinger, 1998] was the first to apply a class of nonlinear maps known as Kolmogorov flows for the digital encryption purpose. More papers on chaotic encryption followed, such as the chaotic key-based algorithms [Yen and Guo, 2000], chaotic systems for permutation transformation in images [Zhang, *et. al.*, 2003], and high-dimensional Arnold and Fibonacci-Q maps [Fridrich, 1998]. However, some chaotic cryptosystems have been identified susceptible to cryptanalysis due to the design disfigurement of their part-linear characters. Some attack algorithms have been developed in [Jakimoski and Kocarev, 2001; Li, *et. al.* 2003]. A common concern of the aforementioned encryption methods arises from the decryption site, where the data is unscrambled. In many occasions, the perfect decryption is impossible due to slight disparity of the encryption/decryption keys or simply roundoff errors in and out of the transformation domain. In many applications, such as medical and military operations, the quality of the images transmitted to the receiver station is crucial during the decision making process. Therefore, perfect reconstruction of the original image from the encrypted data is imperative when selecting various encryption methods, in addition to robustness to various attacks.

Images are stored in two-dimensional arrays, which make matrices the natural candidates for the kernels of encrypting operators. Moreover, matrix multiplication is analogous to convolution/deconvolution between filters and signals. The matrix kernel leaves signatures onto the image pixels and grey levels strictly over the integer field. There will be no roundoff errors in the decrypted images; hence, perfect reconstruction of the original image is achieved. The matrix considered in this paper is called *k*-potent integral matrix. It is a generalization of nilpotent, idempotent, and involutary matrices.

Let $A \in C^{n \times n}$ be an *n* by *n* complex matrix and it is said to be idempotent if $A^2 = A$. This definition can be generalized to a higher power on *A*, if $A^k = A$ for some positive integer $k \geq 2$. With the same condition on *A*, if $A^k = 0$, a zero matrix, for some positive integer *k*, the matrix *A* is called a nilpotent matrix. Another important class of matrices is called involutary, i.e. $A^2 = I$, the identity matrix. We define the unipotent matrix as a natural extension of the involutary matrix as follows: a matrix *A* is unipotent if it satisfies $A^k = I$, for some positive integer *k*. A skew-periodic matrix satisfies $A^k = -A$, while a skew unipotent matrix is defined as $A^k = -I$. All the above mentioned special matrices can be unified by a single equation:

$$A^k = \alpha I + \beta A, \qquad (1)$$

where $\alpha\beta = 0, \alpha, \beta \in \{-1, 0, 1\}$, and $k \geq 2$. A matrix *A* is said to be *k*-potent if it satisfies (1).

2 Eigen-structure of *k*-potent matrix and construction

As discussed in the previous section, we are looking for integral matrices that satisfy (1). Some of these matrices can be adopted in image encryption as the encryption keys. One of the requirements for a robust cryptosystem is that the key space is infinite dimensional. Well, how many integral matrices are there that satisfy (1)? The answer is infinitely many. The following study will reveal a systematic approach for constructing such matrices, which turns out be closely related to the eigen-structure of the *k*-potent matrix. We will go through the case studies of some well-known matrices, and, more importantly, extend the results to higher *k*-values as in (1).

We first investigate the spectral decomposition of nilpotent matrices. A square matrix *A* is such that $A^k = 0$, the zero matrix, for some positive integer *k* known as the index number of Nilpotency if the integer is the smallest positive integer so that $A^{k-1} \neq 0$. Nilpotent matrices are useful in the design of digital FIR filter banks with unequal filter length. The eigen-structure of a nilpotent matrix is revealed in what follows. Note that most of the proofs are omitted due to limited space.

Proposition 2.1 The eigenvalues of a nilpotent matrix are all zeros.

Proposition 2.2 Suppose the square matrix A is a nonzero nilpotent matrix, then A is not diagonalizable.

Proposition 2.2 implies that the spectral decomposition of a nilpotent matrix *A* has the following form

$$A = P \Lambda P^{-1} \qquad (2)$$

where the columns of *P* consist of the generalized eigenvectors of *A* and Λ is a block diagonal matrix with nilpotent Jordan blocks on the main diagonal as follows

$$\Lambda = \begin{bmatrix} J_{m_1} & & & & \\ & J_{m_2} & \text{O} & & \\ & & \ddots & & \\ & \text{O} & & J_{m_p} & \\ & & & & \ddots & \\ & & & & & J_{m_n} \end{bmatrix} \qquad (3)$$

Proposition 2.3 Let Λ be the Jordan Canonical form (3) with nilpotent Jordan blocks along its main diagonal. If $m_p = \max\{m_1, m_2, ..., m_n\}$, then $\Lambda^{m_p - 1} \neq 0$ and $\Lambda^{m_p} = 0$.

Proposition 2.3 implies that the Jordan matrix Λ is a nilpotent matrix, and the index number of the Nilpotency for Λ equals the dimension of the largest nilpotent Jordan block in Λ.

The following result provides the key for constructing integral nilpotent matrices, which can be obtained quickly from Proposition 2.3

Proposition 2.4 The index number of a nilpotent matrix equals the size of the largest nilpotent Jordan block associated with the matrix.

Our next group of matrices is in the category of periodic matrices. A square matrix *A* such that $A^k = A$ for *k* to be a positive integer is called a periodic matrix.

If k is the least such integer, then the matrix is said to have period k-1. The well-known idempotent matrix i.e. $A^2 = A$, is obviously a special case of the periodic matrix to be studied here. Periodic matrices are useful in digital signal encryption such as image coding. We begin with exploring the spectral properties of a periodic matrix.

Proposition 2.5 Let A be a periodic matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \{0\} \cup \left\{ e^{i2m\pi/(k-1)}, m = 0,1,...,k-2 \right\}$.

Proposition 2.5 tells us that the eigenvalues of a periodic matrix are distributed around the unit circle or possibly at the origin. The next proposition addresses the diagonalizability of periodic matrices.

Proposition 2.6 Periodic matrices are diagonalizable.

Unlike nilpotent matrices, the eigen-space of a periodic matrix is non-degenerate. A periodic matrix is similar to a diagonal matrix via a similarity transformation. This result is useful for numerical formation of periodic matrices.

The index number of a periodic matrix obviously relates to the periodicity of the matrix as seen from the definition of a periodic matrix. We would like to point it out that the eigenvalue (except zero) of a periodic matrix with period ν must satisfy the following equation:

$$\lambda^{\nu} - 1 = 0. \qquad (4)$$

Condition (4) gives another criterion for identifying a periodic matrix with certain periodicity.

In what follows we look into the case of unipotent matrices. A unipotent matrix extends the involutary matrix to a higher-order power matrix. To be exact, a unipotent matrix satisfies $A^k = I, k \geq 2$. It is easily seen from the definitions that a unipotent matrix must also be a periodic matrix, but not the other way around unless the periodic matrix is also invertible. Again, we are interested in exploring the spectral properties of unipotent matrices.

Proposition 2.7 Let A be a unipotent matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \left\{ e^{i2m\pi/k}, m = 0,1,2,...,k-1 \right\}$

Proposition 2.3.1 further reveals the connection between a unipotent matrix and a periodic matrix from the circular distribution of their eigenvalues.

Proposition 2.8 Unipotent matrices are diagonalizable

Similar to (4), the eigenvalue of a unipotent matrix with index number k must satisfy the following equation:

$$\lambda^k - 1 = 0. \qquad (5)$$

Since the treatment for the skewed k-potent matrix is exactly the same as that for the previously discussed k-potent matrices, we summarize the results as follows on the skewed k-potent matrix.

A skew-periodic matrix A satisfies the constraint with index $k \geq 2, A^k = -A$. We have the following results for the spectral properties of skew-periodic matrices.

Proposition 2.9 Let A be a skew-periodic matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \{0\} \cup \left\{ e^{i(2m+1)\pi/(k-1)}, m = 0,1,...,k-2 \right\}$.

The eigenvalues (except zero) of a skew-periodic matrix are solutions of the following equation

$$\lambda^{k-1} + 1 = 0. \qquad (6)$$

Proposition 2.10 Skew-periodic matrices are diagonalizable.

A skew-unipotent matrix A satisfies the constraint $A^k = -I$. We have the following results for the spectral properties of skew-unipotent matrices.

Proposition 2.11 Let A be a skew-unipotent matrix with index number k and let λ be an eigenvalue of A, then $\lambda \in \left\{ e^{i(2m+1)\pi/k} \right\}_{m=0}^{k-1}$.

The eigenvalues of a skew-unipotent matrix with index number k satisfy the following equation:

$$\lambda^k + 1 = 0. \qquad (7)$$

Proposition 2.12 Skew-unipotent matrices are diagonalizable.

In summary, we categorize three groups of k-potent matrices: (i) nilpotent matrices, (ii) periodic and unipotent matrices, and (iii) skew-periodic and skew-unipotent 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.

$$A = P\Lambda P^{-1} \tag{8}$$

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 (8) 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. $\Lambda^4 = 0$.

$$\Lambda = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{9}$$

Case (ii): Periodic matrices

Proposition 2.5 and equation (4) are the keys for constructing periodic Λ-matrix. For the sake of argument, let ν be the period of Λ and let $\Gamma_\nu = \{0\} \cup \{e^{i2m\pi/\nu}, m = 0,1,...,\nu-1\}$ be the set of eigenvalues of the periodic matrix. It is sufficient that

$$\Lambda = \operatorname{diag}(\lambda_1, \lambda_2, ..., \lambda_s), \tag{10}$$

where $\lambda_i \in \Gamma_\nu, i = 1,2,...,s,$ which guarantees that the Λ-matrix (10) is a periodic matrix with period ν. The Λ-matrix can also be written as a block diagonal matrix as follows

$$\Lambda = \operatorname{diag}(B_1, B_2, ..., B_m) \tag{11}$$

as long as the eigenvalues of each block $B_i, i = 1,2,...,m,$ 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 (10) or (11) to construct periodic matrices with a higher index number. To this end, let the eigenvalues of Λ be chosen from the following set

$$\Gamma = \Gamma_{\nu_1} \cup \Gamma_{\nu_2} \cup ... \cup \Gamma_{\nu_t}, \tag{12}$$

and let

$$\nu^* = \operatorname{LCM}(\nu_1, \nu_2, ..., \nu_t), \tag{13}$$

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,

$$\Lambda = \begin{bmatrix} 1 & 3 & 0 & 0 \\ -1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \tag{14}$$

because the eigenvalues of the first block are $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$, which are solutions of (4) with $\nu = 3$, and the eigenvalues of the second block in (21) are solutions of (11) 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 (5), (6), and (7) 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 (14), or by taking advantage of a companion matrix for the characteristic polynomial [Golub and Van Loan, 1989], for example, those characteristic polynomials from equations (4)-(7). Formula (8) can be used if one wants to construct a dense integral *k*-potent matrix, where both P and P^{-1} in (8) have to be integral matrices. In what follows, let $Z^{n\times n}$ represent the set of *n* by *n* integral matrices.

Proposition 2.13 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 3.1 gives us a guideline for constructing such an integral *P*-matrix. We can simply use the following formula for *P*,

$$P = UL, \tag{15}$$

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 2.13, P^{-1} is an integral matrix. With an integral *P*-matrix from (15), we obtain a dense integral nilpotent matrix calculate from (9),

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

It is verified in MatLab that $A^4 = 0$, which has the same index of nilpotency as that of (9).

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:

$$\begin{array}{l} T_{1i} : Z^{M\times N} \to Z^{m_i\times n_i},\ m_i < M,\ n_i < N,\ i = 1,2,...,k \\ \sum m_i = M,\ \sum n_i = N. \end{array} \tag{16}$$

$$\begin{array}{l} T_{2i} : Z^{m_i\times n_i} \to Z^{m_i\times n_i},\ i = 1,2,...,k. \\ T_{2i} = E_{i1}E_{i2}\cdots E_{is} \end{array} \tag{17}$$

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

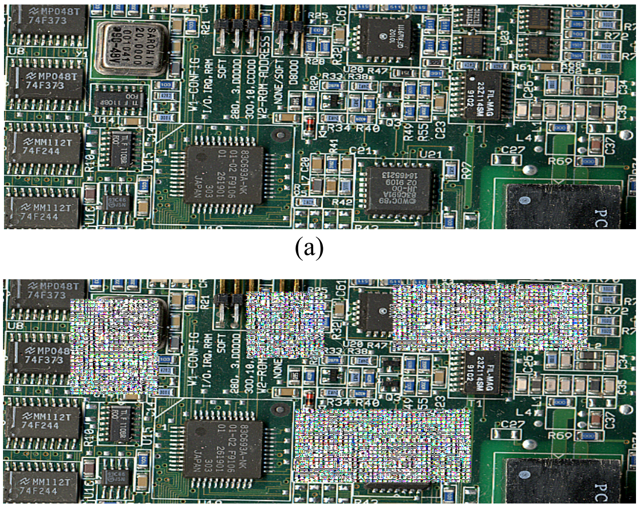
$$T_M = A_1^{k_1} A_2^{k_2} \cdots A_t^{k_t} \tag{18}$$

Let X_i be a sub-image from (16) 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

$$T_M^{-1} = (-1)^p A_t^{n_t - k_t} A_{t-1}^{n_{t-1} - k_{t-1}} \cdots A_1^{n_1 - k_1} \tag{19}$$

where n_i is such that $A_i^{n_i} = \pm I,\ i = 1,2,...,t$ and p represents the number of skew-unipotent matrices applied in (18). With (19), 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.

It seems noteworthy to point out that the methodology proposed in this paper can be applicable to other matrices satisfying special constraints, similar to the ones for the *k*-potent matrices, and such constraints are characterized by the spectral decomposition of the matrices.



(a)

(b)

Figure 1. (a) snapshot of a circuit board; (b) scrambled image of selected components of the circuit board (courtesy of MatLab image processing toolbox)

References:

[1] L. Tang, Methods for encrypting and decrypting MPEG video data efficiently, Proc. ACM Multimedia, 219-229, 1996.

[2] 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.

[3] Wenjun Zeng and Shawmin Lei, Efficient frequency domain selective scrambling of digital video, *IEEE Trans. Multimedia*, v. 5, no.1, 118-129, 2003.

[4] 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.

[5] J. Scharinger, Fast encryption of image data using chaotic Kolmogorov flows, *Journal of Electron. Imaging*, v. 7, no. 2, 318-325, 1998.

[6] 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.

[7] 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.

[8] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. Journal Bifurcation & Chaos*, v. 8, no.6, 1259-1284, 1998.

[9] G. Jakimoski and L. Kocarev, Analysis of some recently proposed chaos-based encryption algorithms, *Physics Letters A*, v. 291, no. 6, 381-384, 2001.

[10] 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.

[11] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 2nd Ed., The Johns Hopkins University Press, Baltimore, Maryland, 1989.