Generalized centro-invertible matrices with applications

Leila Lebtahi[1] Óscar Romero[2] Néstor Thome[1]

Abstract

Centro-invertible matrices were introduced by R.S. Wikramaratna in 2008. From an involutory matrix, we introduce generalized centro-invertible matrices and apply them to the modular arithmetic case. Specifically, algorithms for image blurring/deblurring are designed by means of generalized centro-invertible matrices. In addition, we establish that every pair of sets of generalized centro-invertible matrices corresponding to two fixed involutory matrices have the same number of elements.

Keywords: Involutory matrix, centro-invertible matrix, centro-symmetric matrix.

1. Introduction

An involutory matrix is a matrix that is equal to its inverse. This type of matrices appears in a wide range of different topics such as: computing elementary matrices, signature matrices, orthogonal matrices which are also symmetric, reflections against a plane, classification of finite simple groups, taking the transpose in a matrix ring, etc.

The use of an involutory matrix for encrypting was suggested by Hill [3], using the same matrix for encrypting and decrypting avoiding the computation of an inverse matrix. The Hill cipher's keyspace consists of all matrices of a given size that are invertible over the ring $\mathbb{Z}_m$ of integers modulo m. These matrices were also studied by in [5].

Let J be the square matrix with ones on the cross-diagonal and zeros elsewhere; J is often called the centro-symmetric permutation matrix. This matrix J allowed to introduce the centro-invertible matrices as those matrices X whose inverses coincide with the matrices obtained by rotation of all the elements of X through 180 degrees about the mid-point of the matrix, that is JXJ [13]. As an application, an algorithm to generate uniformly distributed pseudo-random numbers was developed in [12].

Throughout this paper, $\mathbb{Z}^{n\times n}$ will denote the set of $n \times n$ integer matrices and $\mathbb{Z}_m^{n\times n}$ the set of $n \times n$ matrices with coefficients in $\mathbb{Z}_m$. For two given matrices $A = [a_{ij}] \in \mathbb{Z}^{n\times n}$,

[1]Instituto Universitario de Matemática Multidisciplinar. Universitat Politècnica de València. E–46022 Valencia, Spain. E–mail addresses: {leilebep,njthome}@mat.upv.es. This work was partially supported by Ministry of Education (DGI Grant MTM2010-18228).

[2]Departamento de Comunicaciones. Universitat Politècnica de València. E–46022 Valencia, Spain. E–mail address: oromero@dcom.upv.es.

$B = [b_{ij}] \in \mathbb{Z}^{n\times n}$, and a positive integer m, the expression $A \equiv B(\mathrm{mod}\,(m))$ will denote the equivalence relation given by $a_{ij} \equiv b_{ij}(\mathrm{mod}\,(m))$, for all i and j. We also recall that if $M \equiv N(\mathrm{mod}\,(m))$ for $M, N \in \mathbb{Z}^{n\times n}$ then $AM \equiv BN(\mathrm{mod}\,(m))$.

On the other hand, several problems have been studied in image processing, for instance, those related to blurring and deblurring images. Sometimes, it is needed to protect totally or partially an image, for example, when it is electronically sent, shown in mass media, etc. Several methods for blurring/deblurring images have been developed [1, 2].

We will consider a special type of matrices: generalized centro-invertible matrices. They are an extension of the centro-invertible matrices using an involutory matrix R instead of the centro-symmetric permutation matrix J. Then, an integer matrix A is called generalized centro-invertible if it satisfies $RAR = A^{-1}$. Finally, applications to image blurring/deblurring of generalized centro-invertible matrices will be given.

This paper is organized as follows. In Section 2 we have stated bijections between every pair of sets of generalized centro-invertible matrices corresponding to two fixed involutory matrices. Section 3 presents algorithms for constructing generalized centro-invertible matrices, blurring and deblurring images. Finally, some examples are shown in Section 4.

2. Relationships between $\mathbf{GCI}(m, R_i)$ and $\mathbf{GCI}(m, R_j)$

It is clear that integer generalized centro-invertible matrices are nonsingular matrices with determinant ± 1. Hence, if $A \in \mathbb{Z}^{n\times n}$ is a generalized centro-invertible matrix then $A^{-1} \in \mathbb{Z}^{n\times n}$. Working with involutory matrices, a generalized centro-invertible matrix A satisfies $RAR = A^{-1} = A$, thus A is generalized centro-symmetric [6, 7, 8, 9, 10, 11, 14].

For a given involutory matrix $R \in \mathbb{Z}_m^{n\times n}$, let $\mathbf{GCI}(m, R)$ be the set of all the matrices $A \in \mathbb{Z}_m^{n\times n}$ such that A is generalized centro-invertible, that is,

$$\mathbf{GCI}(m, R) = \{A \in \mathbb{Z}_m^{n\times n} :\ RAR = A^{-1}\}.$$

Theorem 1. *For every pair of matrices $R_1, R_2 \in \mathbf{GCI}(m, I_n)$, there exists a bijective function between $\mathbf{GCI}(m, R_1)$ and $\mathbf{GCI}(m, R_2)$. In particular, this one-to-one correspondence remains valid when restricted to the diagonal matrices in $\mathbf{GCI}(m, R_1)$ and the diagonal matrices in $\mathbf{GCI}(m, R_2)$.*

Proof. First we assume that $R \in \mathbf{GCI}(m, I_n)$. It is easy to see that the function $\Psi : \mathbf{GCI}(m, R) \to \mathbf{GCI}(m, I_n)$ given by $A \mapsto RA$ is well defined since for a matrix A satisfying $RAR = A^{-1}$ we have $[\Psi(A)]^2 = I_n$. It is clear that Ψ is bijective, so the sets $\mathbf{GCI}(m, R)$ and $\mathbf{GCI}(m, I_n)$ are equipotent. Observe that, moreover, Ψ is an involution. If, in addition, R is a diagonal matrix then the restriction of Ψ to the set of diagonal matrices in $\mathbf{GCI}(m, R)$ states a bijection with the set of diagonal matrices in $\mathbf{GCI}(m, I_n)$ since $\Psi(A) = RA$ is diagonal for every diagonal $A \in \mathbf{GCI}(m, R)$.

Now, if $R_1, R_2 \in \mathbf{GCI}(m, I_n)$, the above result assures that both $\mathbf{GCI}(m, R_1) \simeq \mathbf{GCI}(m, I_n)$ and $\mathbf{GCI}(m, R_2) \simeq \mathbf{GCI}(m, I_n)$ one-to-one correspondences hold. So, the bijection between $\mathbf{GCI}(m, R_1)$ and $\mathbf{GCI}(m, R_2)$ is guaranteed as well as the second part of this theorem. Then, the result is shown. ■

3. Generalized centro-invertible matrices: applications to image blurring

A digital image is a rectangular grid of pq pixels arranged in a two-dimensional matrix of p rows and q columns. In order to blur an image, we apply a set of blurring matrices.

Let $\mathbb{Z}_{256}^{n\times n}$ be the set of $n \times n$ matrices with coefficients in $\mathbb{Z}_{256}$. The part of the image to be blurred is subdivided into $X_1, \ldots, X_t$ where X_i denotes $n \times n$ sub-images of the original one. Consider the blurring function $e_A : \mathbb{Z}_{256}^{n\times n} \to \mathbb{Z}_{256}^{n\times n}$ defined by $e_A(X_i) = AX_i (\mathrm{mod}\,(256))$ for $X_i \in \mathbb{Z}_{256}^{n\times n}$.

Next, we present an algorithm for blurring by computing previously an involutory matrix R and then a generalized centro-invertible matrix A. Thus, this matrix A will be used to blur. Our procedure consists in restricting the function e_A to the set $\mathcal{X} = \{X_1, \ldots, X_t\}$ where X_i denotes the sub-images to be blurred.

ALGORITHM 1

Inputs: Sub-image X_i, size n of A. *Outputs*: Blurred sub-image Y_i.

Step 1 Generate $n \times n$ random integer matrices T_R, T_A (lower triangular), Q_R, Q_A (upper triangular), all of them with 1's in the main diagonal.

Step 2 Compute $P_R = T_R Q_R$ and $P_A = T_A Q_A$.

Step 3 Choose an arbitrary integer $r(R)$ such that $1 \leq r(R) \leq n-1$ and set $R = P_R \ \mathrm{diag}(I_{r(R)}, -I_{n-r(R)}) P_R^{-1}$.

Step 4 Choose an arbitrary integer $r(A)$ such that $1 \leq r(A) \leq n-1$ and set $A = R\ P_A \ \mathrm{diag}(I_{r(A)}, -I_{n-r(A)}) P_A^{-1}$.

Step 5 $Y_i = AX_i (\mathrm{mod}\,(256))$.

From Steps 1 and 2, the fact that $\det(P_R) = \det(T_R)\det(Q_R) = 1$ implies $P_R^{-1} \in \mathbb{Z}^{n\times n}$. Step 3 yields $R \in \mathbb{Z}^{n\times n}$ and, moreover, $R^2 = I_n$. Steps 1 and 2 assure that $P_A^{-1} \in \mathbb{Z}^{n\times n}$, and Step 4 yields an involutory matrix $RA \in \mathbb{Z}^{n\times n}$, that is, A is generalized centro-invertible.

The inverse of the matrix A used to blur will be needed to deblur. We remark that it is not necessary to compute explicitly the inverse A^{-1} since $A^{-1} = RAR$.

In order to deblur an image we proceed as follows. Let us now consider the deblurring function $d_A : \mathbb{Z}_{256}^{n\times n} \to \mathbb{Z}_{256}^{n\times n}$ defined by $d_A(Y) = (RAR)Y (\mathrm{mod}\,(256))$ for $Y \in \mathbb{Z}_{256}^{n\times n}$. We first restrict the function d_A to the set $\mathcal{Y} = \{Y_1, \ldots, Y_t\}$ where Y_i are the blurred sub-images by means of A. Then, for every $i = 1, \ldots, t$, we get $d_A(Y_i) = (RAR)Y_i (\mathrm{mod}\,(256)) = A^{-1}Y_i (\mathrm{mod}\,(256)) = X_i$. Thus, the deblurred sub-images coincide with the matrices X_i.

Using different blurring/deblurring levels

In order to obtain different levels of blurring, say b levels, it is necessary to construct b matrices A_k, $k = 1, \ldots, b$ as in Algorithm 1 but by modifying its Step 1 as follows:

$$E_k = e_{k+1} \sum_{j=1}^{k} e_j^T \tag{1}$$

$$T_{R,1} = I_n, \quad T_{R,k} = T_{R,k-1} + \alpha_{R,k} E_k, k \in \{2, \ldots, b\} \tag{2}$$

$$Q_{R,1} = I_n, \quad Q_{R,k} = Q_{R,k-1} + \beta_{R,k} E_k, k \in \{2, \ldots, b\} \tag{3}$$

for every $k \in \{1, \ldots, b\}$ and for some $\alpha_{R,k}, \beta_{R,k} \in \mathbb{N}$ where e_k denotes the k-th canonical basis vector of $\mathbb{R}^n$. That is, for each $k \in \{2, \ldots, b\}$, the matrices $T_{R,k}$ and $Q_{R,k}$ are rank-1 updates of $T_{R,k-1}$ and $Q_{R,k-1}$, respectively.

Matrices $T_{A,k}$ and $Q_{A,k}$ can be constructed following this last procedure. Now, for a given sub-image X_i, to get the k-th level of blurring of X_i, we have to compute $Y_{i,k} = A_k X_i (\mathrm{mod}\,(256))$. In this way, we get different blurring levels from the lowest for $k = 1$ to the highest for $k = b$ (see Figure 2):

ALGORITHM 2

Inputs: Sub-image X_i, size n of A. *Outputs*: Blurred sub-image $Y_{i,k}$.

Step 1 Compute E_k as in (1).

Step 2 Compute $T_{R,k}$, $T_{A,k}$ and $Q_{R,k}$, $Q_{A,k}$ as in (2) and (3).

Step 3 Compute $P_{R,k} = T_{R,k} Q_{R,k}$ and $P_{A,k} = T_{A,k} Q_{A,k}$.

Step 4 Perform R_k and A_k as in Steps 3 and 4 of Algorithm 1.

Step 5 Compute $Y_{i,k} = A_k X_i (\mathrm{mod}\,(256))$.

The expression $d_{A_k}(Y_{i,k}) = (R_k A_k R_k) Y_{i,k} (\mathrm{mod}\,(256)) = A_k^{-1} Y_{i,k} (\mathrm{mod}\,(256)) = X_i$ allows us to deblur $Y_{i,k}$.

Progressive blurring/deblurring

To get a progressive deblurring we will use the set $A_1, A_2, \ldots, A_l$. For finding the k-th level deblurring we will need the last k matrices in previous set.

A variant of the previous algorithm is obtained considering generalized centro-invertible matrices $A_1, A_2, \ldots, A_\ell$. In this case, $e_{A_1,A_2,\ldots,A_\ell}(X) = A_\ell A_{\ell-1} \cdots A_1 X (\mathrm{mod}\,(256))$ is the blurring computation. For deblurring the image $Y \in \mathbb{Z}_{256}^{n \times n}$, we apply the expression

$$d_{A_1,A_2,\ldots,A_\ell}(Y) = A_1^{-1} \cdots A_{\ell-1}^{-1} A_\ell^{-1} Y (\mathrm{mod}\,(256)) = R A_1 \cdots A_{\ell-1} A_\ell R Y (\mathrm{mod}\,(256))$$

The construction of the matrices $A_1, \ldots, A_\ell$ can be carried out using Steps 1-4 of Algorithm 1. An alternative method to get these matrices is given in the following algorithm:

ALGORITHM 3

Inputs: Matrices P_R,A and $r(R)$. *Outputs*: Matrices $A_1, \ldots, A_\ell$.

Step 1 Generate random integer matrices with determinant 1, W_{1i} of size $r(R) \times r(R)$ and W_{2i} of size $(n - r(R)) \times (n - r(R))$.

Step 2 Compute $W_i = P_R \,\mathrm{diag}(W_{1i}, W_{2i}) P_R^{-1}$.

Step 3 Compute $A_i = W_i A W_i^{-1}$.

Algorithm 3 provides A_i from the starting matrix A. This algorithm works because the commutativity of matrices R and W_i implies that $W_iAW_i^{-1}$ is generalized centro-invertible since the starting matrix A is. Step 1 of Algorithm 3 can be carried out as in Steps 1 and 2 of Algorithm 1. As an alternative method, maintaining the same matrix R, we can repeat Step 4 in Algorithm 1 with different matrices P_A's to get matrices $A_1, \ldots, A_\ell$.

4. Examples of blurring/deblurring

In this section we present some examples. First, we compute an involutory matrix R and generalized centro-invertible matrix A using Algorithm 1. Figure 1 shows the partially blurred image and the deblurred image, that coincides with the original one.

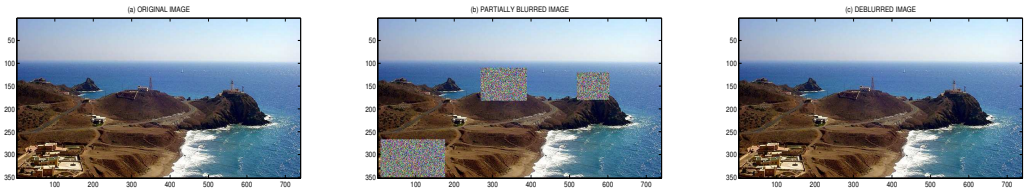

Figure 1: (a) Original image, (b) blurred image, (c) deblurred image

We remark that our blurring image algorithms do not compute inverse matrices, provide a large number of blurring matrices and multiple blurred matrices can be used to obtain progressive blurring/deblurring levels. Figure 2 shows an example of progressive blurring levels. In addition, for a given blurred level, it is possible to make a progressive deblurring to any previous blurring level.

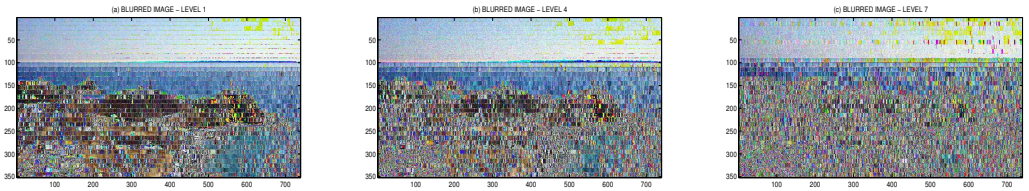

Figure 2: Image blurring levels: (a) level 1, (b) level 4, (c) level 7 (from 1 to 10)

5. Conclusions

In this paper, generalized centro-invertible matrices have been introduced as an extension of centro-invertible matrices. We have shown that two sets of generalized centro-invertible matrices determined by a fixed pair of involutory matrices have the same number of elements. Our algorithms allow to generate generalized centro-invertible matrices by simple procedures. This new class of matrices has been applied to blurring/deblurring images taking into account blurring levels and progressive blurring.

References

[1] M. Bertero, P. Boccacci. Introduction to Inverse Problems in Imaging, IOP Publications, Bristol, 1998.

[2] P.C. Hansen, J.G. Nagy, D.P. O'Leary. Deblurring images: matrices spectra and filtering, SIAM Press, Philadelphia, 2006.

[3] L.S. Hill. Cryptography in an algebraic alphabet, *American Mathematical Monthly*, 36, 3006–312, 1929.

[4] A. Ríder Moyano, R.M. Rubio Ruiz. The indicator of involution, *Boletín de Matemáticas*, Nueva Serie, X, 2, 59–67, 2003 (in Spanish).

[5] J. Overbey, W. Traves, J. Wojdylo. On the keyspace of the Hill Cipher. *Cryptologia*, 29, 1, 59–72, 2005.

[6] J.L. Stuart. In ation matrices and ZME-Matrices that commute with a permutation matrix, *SIAM Journal of Matrix Analysis Applications*, 9, 3, 408–418, 1988.

[7] J. Stuart, J. Weaver. Matrices that commute with a permutation matrix, Linear Algebra and its Applications, 150, 255–265, 1991.

[8] D. Tao, M. Yasuda. A spectral characterization of generalized real symmetric centrosymmetric and generalized real symmetric skew-centrosymmetric matrices, SIAM J. Matrix Anal. Appl. 23, 3, 885—895, 2001/02, (electronic), http://epubs.siam.org/sam–bin/dbq/article/38673.

[9] W.F. Trench. Characterization and properties of matrices with k-involutory symmetries, Linear Algebra and its Applications, 429, 2278–2290, 2008.

[10] W.F. Trench. Characterization and properties of matrices with k-involutory symmetries II, Linear Algebra and its Applications, 432, 2782–2797, 2010.

[11] J. Weaver. Centrosymmetric Matrices (cross-symmetric) matrices, their basic properties, eigenvalues and eigenvectors, American Mathematical Monthly, 2, 10, 711–717, 1985.

[12] R.S. Wikramaratna. The additive congruential random number generator - a special case of a multiple recursive generator, *Linear Algebra and its Applications*, 216, 1, 371–387, 2008.

[13] R.S. Wikramaratna. The centro-invertible matrix: A new type of matrix arising in pseudo-randon number generation, *Linear Algebra and its Applications*, 434, 1, 144–151, 2011.

[14] M. Yasuda. A spectral characterization for Hermitian centrosymmetric K matrices and Hermitian skew-centrosymmetric K matrices, *SIAM Journal of Matrix Analysis Applications*, 25, 3, 601–605, 2003.