Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18411-9

An unrestricted Arnold's cat map transformation

Mehmet Turan[1] · **Erhan Gökçay**[2] · **Hakan Tora**[3,4]

Received: 2 March 2023 / Revised: 20 September 2023 / Accepted: 22 January 2024

Abstract
The Arnold's Cat Map (ACM) is one of the chaotic transformations, which is utilized by numerous scrambling and encryption algorithms in Information Security. Traditionally, the ACM is used in image scrambling whereby repeated application of the ACM matrix, any image can be scrambled. The transformation obtained by the ACM matrix is periodic; therefore, the original image can be reconstructed using the scrambled image whenever the elements of the matrix, hence the key, is known. The transformation matrices in all the chaotic maps employing ACM has limitations on the choice of the free parameters which generally require the area-preserving property of the matrix used in transformation, that is, the determinant of the transformation matrix to be ± 1. This reduces the number of possible set of keys which leads to discovering the ACM matrix in encryption algorithms using the brute-force method. Additionally, the period obtained is small which also causes the faster discovery of the original image by repeated application of the matrix. These two parameters are important in a brute-force attack to find out the original image from a scrambled one. The objective of the present study is to increase the key space of the ACM matrix, hence increase the security of the scrambling process and make a brute-force attack more difficult. It is proved mathematically that area-preserving property of the traditional matrix is not required for the matrix to be used in scrambling process. Removing the restriction enlarges the maximum possible key space and, in many cases, increases the period as well. Additionally, it is supplied experimentally that, in scrambling images, the new ACM matrix is equivalent or better compared to the traditional one with longer periods. Consequently, the encryption techniques with ACM become more robust compared to the traditional ones. The new ACM matrix is compatible with all algorithms that utilized the original matrix. In this novel contribution, we proved that the traditional enforcement of the determinant of the ACM matrix to be one is redundant and can be removed.

Keywords Image scrambling · Arnold's cat map · Information security · Transformation matrix · Chaotic maps

✉ Mehmet Turan
mehmet.turan@atilim.edu.tr

Extended author information available on the last page of the article

1 Introduction

Information security is becoming the most important issue where the systems are increasing in terms of capacity and the size of information they produce and exchange. One of the common information exchange is done through images. Therefore, image security during data transmission is very important. One of the widely used methods to secure and encrypt images is chaotic transformations.

There has been many studies on chaotic maps in literature. Zia et al. presented a useful survey including the recently published studies on chaos based image encryption techniques. The algorithms are categorized into spatial, temporal, and spatiotemporal domains and each is discussed in detail [26]. Some chaotic maps for image encryption are named as Arnold's Cat map [8, 24], Henon map [21], Tinkerbell map [7], Logistic maps [6, 13], Tent map [15] and a 5D Hyper-chaotic map [5]. For example, in [18], a Lorenz Chaotic system is used. In that paper, each bit plane is encrypted separately. In [20], Wavelet and Cosine transformations are used to protect medical images. In conjunction with the discrete cosine transform and singular value decomposition, the ACM matrix is used. In [18], Fibonacci series are utilized digital images using an ACM matrix.

In classical ACM, the location of each pixel is multiplied by a matrix and a new location is obtained for that pixel. The calculations are done in modular arithmetic modulo N where N is the image size. In these methods, the ACM matrix is taken in such a way that its determinant is ± 1 and this transformation is periodic so that the original image can be recovered after repeated application of the same transformation. During the scrambling process, the one with lowest correlation is taken as the encrypted image.

Arnold's Cat Map [2] is one of the chaotic transformations used to encrypt images successfully. The transformation is periodic and reversible, therefore, it is suitable for encryption purposes. The transform simply uses matrix multiplications, therefore, application of the map is simple and effective. There are many applications and uses of the transformation. In [17], ACM is used together with the Henon map successfully. An important combination of ACM is implemented with AES encryption in [14]. The period of ACM transformation is analyzed in [3].

In [9], the Hartley transform is combined with the ACM matrix in its fundamental form (2.1). In [11], Turing machines are used with a three-dimensional map. As an encryption algorithm, the ACM matrix is combined with a Gaussian logistic map in [10, 12]. In the method, dynamic substitution and permutation are utilized. In [4, 22], the encryption contains embedded logistic maps. In [23, 25], each bit plane is encrypted differently. Combining an ACM matrix with the RC4 encryption method is demonstrated in [1]. All proposed algorithms that employ the ACM matrix employ the formulation in (2.1), (2.2) or (2.3) where the number of parameters is constrained.

The main contribution of this study is to present a novel transform matrix for the Arnold's Cat Map. Unlike the traditional ACM matrices, the proposed method removes the restriction that the transformation matrix has a unity determinant. Also, an algorithm is presented that produces all possible matrices to be used in chaotic mapping applications. As a consequence of this, the pool of matrices used for that purpose will be widened dramatically.

The paper is organized as follows. The preliminaries on the standard and generalized ACM transformation are presented in Section 2. Section 3 is devoted to the construction of new transform matrices. There it is proved that the area-preserving property is not compulsory. Besides, an algorithm is presented to generate all possible ACM matrices. Section 4 is dedicated to experimental works. Finally, the discussion and conclusion part is given in Section 5.

2 Preliminaries

The ACM transformation is based on several assumptions and the form of the matrices is presented in equations (2.1), (2.2) and (2.3). In all forms, the determinant of the transform matrix is 1 by design. The first parameter is always 1, and the free parameters a and b can be selected freely. The fourth parameter is calculated so that the determinant is always 1. The calculation is based on area-preservation. The sequence is both periodic, and hence, the original data can be recovered. Because of these features, the ACM transformation is used in encryption applications widely.

For an $N \times N$ image, the standard ACM is defined by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \tag{2.1}$$

where $x, y \in \{0, 1, \ldots, N-1\}$, (x, y) is the pixel of the original image and (x', y') is the position of the mapped pixel. Note that the determinant of the transformation matrix is 1, which guarantees that the mapping is one-to-one for all values of N.

Besides the traditional ACM, several modifications have been introduced by other researchers. See, [16, 23] and the references therein. These modified ACMs differ from the traditional method in terms of the matrix elements. Two of them are

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ i & i+1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \tag{2.2}$$

where $i \in \{0, 1, \ldots, N-1\}$, and

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \tag{2.3}$$

where $a, b \in \{0, 1, \ldots, N-1\}$. Notice that for $i = 1$, (2.2) becomes (2.1). Also, in (2.3), taking $a = b = 1$ reveals (2.1) and $a = 1$, $b = i$ results in (2.2). Therefore, (2.3) is the most general one with two free parameters a and b. In all above methods, the ACM can be described as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = M \cdot \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \tag{2.4}$$

where M is a specific 2×2 matrix whose determinant is 1.

In this paper, it will be shown that the unity determinant restriction is not a required assumption and we will maximize the number of choices for each parameter without the determinant requirement. Consequently, the key space becomes considerably large.

3 Construction of a new transform matrix

In this part, a new method to construct the transform matrix will be presented. First, we shall need the following well known auxiliary result which is easily derived from the Bézout's identity [19].

Lemma 3.1 *The number a has a multiplicative inverse modulo N if and only if a and N are relatively prime, i.e.,* $\gcd(a, N) = 1$.

In other words, $\gcd(a, N) = 1$ if and only if there exists an integer a' such that $aa' \equiv 1 \pmod N$. Here, the number a' is called the multiplicative inverse of a modulo N and is denoted by a^{-1}.

This result is also generalized for matrices and the fact is given below.

Lemma 3.2 *A matrix M is invertible modulo N if and only if* $\gcd(\det M, N) = 1$.

Denote by $\mathbb{Z}_N^{2\times 2}$ the set of all 2×2 matrices whose elements are in $\mathbb{Z}_N := \{0, 1, \ldots, N-1\}$. The set of invertible matrices in $\mathbb{Z}_N^{2\times 2}$ with ordinary matrix multiplication is called the general linear group of degree 2 and is denoted by $GL(2, \mathbb{Z}_N)$. The subgroup of $GL(2, \mathbb{Z}_N)$ consisting of matrices with determinant 1 is called the special linear group of degree 2 and denoted by $SL(2, \mathbb{Z}_N)$.

In almost all studies, starting with Arnold's cat map, the transform matrix is assumed to be in $SL(2, \mathbb{Z}_N)$. The main reason for this is that shuffling the image a certain finite number of times should result in the original one. That is, starting from an image, for the matrix M, there is a number of steps, say P, such that applying the transformation (2.4) P times should give the original image. This, indeed, means that $M^P \equiv I \pmod N$ where I stands for the identity matrix. However, for such a purpose, one does not need to have $\det M \equiv 1 \pmod N$ as the next theorem states.

Theorem 3.3 *Given an image of size $N \times N$. Any matrix M with* $\gcd(\det(M), N) = 1$ *can serve as an ACM matrix.*

Proof Take any matrix M such that $\det(M)$ and N are relatively prime, that is, $M \in GL(2, \mathbb{Z}_N)$, and consider the sequence of matrices

$$M, M^2, M^3, \ldots, M^{N^4+1} \pmod N.$$

Since there are N^4 different 2×2 matrices whose entries are in $\mathbb{Z}_N$ and $N^4 + 1$ matrices in this list, the matrices above cannot all be distinct. In particular, there are distinct integers i and j such that $M^i \equiv M^j \pmod N$. Without loss of generality, assume that $i < j$. Now, multiplying both sides of this congruence by M^{-i} leads to

$$M^{j-i} \equiv I \pmod N.$$

In other words,

$$M^{j-i} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \quad \text{for all} \quad x, y \in \{0, 1, \ldots, N-1\}.$$

This means that any image can be recovered after applying the transformation $j - i$ times repeatedly. Hence, M can be taken as an ACM matrix. □

Theorem 3.3 states that any matrix in $GL(2, \mathbb{Z}_N)$ can be taken as the transform matrix not necessarily those who preserve area. Indeed, any invertible matrix modulo N, i.e., $\gcd(\det(M), N) = 1$, can be taken as the shuffling matrix. In the proof above, the number $P = j - i$ is the *period* of M modulo N.

To count the number of invertible matrices in $\mathbb{Z}_N^{2\times 2}$, i.e., number of possible ACM matrices for a given N, we shall need the following auxiliary results.

Lemma 3.4 *Let $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i are distinct primes and $k_i \geq 1$ are integers. Then $|GL(2, \mathbb{Z}_N)| = |GL(2, \mathbb{Z}_{p_1^{k_1}})| \cdot |GL(2, \mathbb{Z}_{p_2^{k_2}})| \cdots |GL(2, \mathbb{Z}_{p_r^{k_r}})|$.*

Proof Let $M \in GL(2, \mathbb{Z}_N)$. The result follows from the Chinese Remainder Theorem since $\gcd(\det M, N) \equiv 1$ if and only if $\gcd(\det M, p_i^{k_i}) \equiv 1$ for every $i = 1, 2, \ldots, r$. □

The following result gives the number of matrices in $GL(2, \mathbb{Z}_{p^k})$ for a prime number p and positive integer k.

Lemma 3.5 *For any prime number p and positive integer k, there are $p^{3k-2}(p^2-1)$ matrices in $SL(2, \mathbb{Z}_{p^k})$. Moreover, the number of matrices in $GL(2, \mathbb{Z}_{p^k})$ is $p^{4k-3}(p-1)(p^2-1)$.*

Proof Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{Z}_{p^k}^{2\times 2}$ and $m = \det M \pmod{p^k}$. By Lemma 3.2, M is invertible modulo p^k if and only if $p \nmid m$. That is, $M \in GL(2, \mathbb{Z}_{p^k})$ if and only if $p \nmid m$. We shall consider two cases:

Case 1 If p does not divide a, then a is invertible modulo p^k. Let a^{-1} be the inverse of a modulo p^k, and for any $b, c \in \mathbb{Z}_{p^k}$, take $d = a^{-1}(bc+1) \pmod{p^k}$. In this setting, $\det M \equiv 1 \pmod{p^k}$. Since there are $(p^k - p^{k-1})$ ways to choose a, p^k ways to choose each of b and c, and only one way to choose d, the number of such matrices is $(p^k - p^{k-1}) \cdot p^k \cdot p^k \cdot 1 = p^{3k-1}(p-1)$.

Case 2 If p divides a, then a is not invertible modulo p^k. In that case, p should divide none of b and c. That is, both b and c should be invertible. Now, for $b, d \in \mathbb{Z}_{p^k}$ with $p \nmid b$, take $c = b^{-1}(ad-1) \pmod{p^k}$. Then, $\det M \equiv 1 \pmod{p^k}$. Since a, b, c and d can be chosen in p^{k-1}, $p^k - p^{k-1}$, 1 and p^k ways, respectively, the number of such matrices is $p^{k-1} \cdot (p^k - p^{k-1}) \cdot 1 \cdot p^k = p^{3k-2}(p-1)$.

Thus, adding the results in both cases gives us $p^{3k-1}(p-1) + p^{3k-2}(p-1) = p^{3k-2}(p^2 - 1)$ matrices in $SL(2, \mathbb{Z}_{p^k})$.

Finally, since there are $p^k - p^{k-1}$ invertible m's modulo p^k, the number of invertible matrices in $GL(2, \mathbb{Z}_{p^k})$ is $(p^k - p^{k-1})p^{3k-2}(p^2-1) = p^{4k-3}(p-1)(p^2-1)$ as claimed. □

Now, combining the results of Lemmas 3.4 and 3.5, one derives the following outcome which in fact gives the number of transform matrices.

Theorem 3.6 *Let $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i are distinct primes and $k_i \geq 1$ are integers. Then,*

$$|GL(2, \mathbb{Z}_N)| = \prod_{i=1}^{r} p_i^{4k_i-3}(p_i - 1)(p_i^2 - 1). \tag{3.1}$$

It is worth mentioning that for an image of size N, the number of possible matrices that can be used as ACM transformation is given by (3.1). As an example, for an image of size 200×200, one has $N = 200 = 2^3 \cdot 5^2$. That is, $p_1 = 2$, $k_1 = 3$, $p_2 = 5$, $k_2 = 2$. Therefore, the number of transform matrices is

$$2^9 \cdot (2-1) \cdot (2^2-1) \cdot 5^5 \cdot (5-1) \cdot (5^2-1) = 4.608 \cdot 10^8.$$

For the same N, the number of transform matrices in (2.2) is 200, and in (2.3) it is $4 \cdot 10^4$. One can easily see that the number of keys provided in the present paper is much more than the ones in the literature.

The proof of the next assertion gives a method to construct all possible transform matrices which gets its main idea from the Chinese Remainder Theorem [19, 16.1.G.8].

Theorem 3.7 *Let $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i are distinct primes and $k_i \geq 1$ are integers. For each $i = 1, 2, \ldots, r$, take an arbitrary matrix $A_i \in GL(2, \mathbb{Z}_{p_i^{k_i}})$. Then, there exists a unique matrix $M \in GL(2, \mathbb{Z}_N)$ such that*

$$M \equiv A_i \pmod{p_i^{k_i}} \quad \text{for all} \quad i = 1, 2, \ldots, r. \tag{3.2}$$

Proof For each $i = 1, 2, \ldots, r$, let $n_i = N/p_i^{k_i}$. Clearly, $\gcd(n_i, p_i^{k_i}) = 1$, and hence, by Lemma 3.1, n_i has a multiplicative inverse, say $\overline{n}_i$, modulo $p_i^{k_i}$. Set

$$M = n_1\overline{n}_1 A_1 + n_2\overline{n}_2 A_2 + \cdots + n_r\overline{n}_r A_r \pmod{N}.$$

It is evident that the matrix M satisfies (3.2) since, by the definition of n_i one has that $p_i^{k_i} | n_j$ whenever $j \neq i$ meaning that $n_j\overline{n}_j \equiv 0 \pmod{p_i^{k_i}}$ and by the definition of $\overline{n}_i$ that $n_i\overline{n}_i \equiv 1 \pmod{p_i^{k_i}}$.

To see why M is invertible in $\mathbb{Z}_N^{2\times 2}$, simply note that

$$\det M \equiv \det A_i \pmod{p_i^{k_i}}.$$

As $A_i \in GL(2, \mathbb{Z}_{p_i^{k_i}})$, one gets $\gcd(\det M, p_i^{k_i}) = 1$ for all $i = 1, 2, \ldots, r$ which leads to $\gcd(\det M, N) = 1$. Therefore, $M \in GL(2, \mathbb{Z}_N)$. □

The proof implies that one can construct the matrix M alternatively as follows. For each $i = 1, 2, \ldots, r$, take an arbitrary matrix

$$A_i = \begin{bmatrix} a_i & b_i \\ c_i & d_i \end{bmatrix} \in GL(2, \mathbb{Z}_{p_i^{k_i}}).$$

Then, by the Chinese Remainder theorem, there is a unique number $a \in \mathbb{Z}_N$ such that $a \equiv a_i \pmod{p_i^{k_i}}$ for all $i = 1, 2, \ldots, r$. Similarly, one can find the numbers b, c and d satisfying

$$b \equiv b_i \pmod{p_i^{k_i}}, \quad c \equiv c_i \pmod{p_i^{k_i}}, \quad d \equiv d_i \pmod{p_i^{k_i}}, \quad i = 1, 2, \ldots r,$$

respectively. Finally, one has

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{Z}_N).$$

Remark 3.1 When the image size N is a prime number, say $N = p$ for a prime number p, the matrix can be taken as any invertible matrix in $\mathbb{Z}_p^{2\times 2}$. In that case the number of possible ACM matrices is $N(N-1)(N^2-1)$. It is important to mention that if N is not a prime number, then by adding sufficiently many null rows and columns to the image, one can enlarge the image so that its size becomes a prime number. This leads to even much larger key space.

The following Algorithm 1 produces an invertible matrix modulo p^k for a prime number p and a positive integer k which is provided by Lemma 3.5, and Algorithm 2 returns a matrix that can be used as ACM matrix.

As an example, let us construct a transform matrix for an image of size 200×200. According to Algorithm 2, first, one factorizes N. Since $N = 200 = 2^3 \cdot 5^2$, one has $p_1 = 2$, $k_1 = 3$, $p_2 = 5$ and $k_2 = 2$. Following the notations as in Theorem 3.7, one writes $n_1 = N/p_1^{k_1} = 25$ and $n_2 = N/p_2^{k_2} = 8$. Then, since $n_1 \cdot 1 \equiv 1 \pmod{8}$ and $n_2 \cdot 22 \equiv 1 \pmod{25}$, one finds $\overline{n}_1 = 1$ and $\overline{n}_2 = 22$. Now, select arbitrary matrices $A_1 \in GL(2, \mathbb{Z}_8)$ and $A_2 \in GL(2, \mathbb{Z}_{25})$. To generate A_1, one runs Algorithm 1 with $p_1 = 2$ and $k_1 = 3$. First,

Algorithm 1 Generate an invertible matrix modulo p^k.

function *generate_matrix_A*
Input: p (a prime number), k
Output: A_{2x2} with $\det(A) = m$ such that $\gcd(m, p^k) = 1$.
Do
Select $m \in \{1, 2, \dots, p^k - 1\}$ such that $m\%p \neq 0$.
Select $a \in \{0, 1, \dots, p^k - 1\}$.
If $a\%p \neq 0$
find $\overline{a} \in \{1, 2, \dots, p^k - 1\}$ such that $a \cdot \overline{a} \equiv 1 \pmod{p^k}$.
select $b \in \{0, 1, \dots, p^k - 1\}$.
select $c \in \{0, 1, \dots, p^k - 1\}$.
define $d = \overline{a}(bc + m) \pmod{p^k}$.
else
select $b \in \{0, 1, \dots, p^k - 1\}$ such that $b\%p \neq 0$.
find $\overline{b} \in \{1, 2, \dots, p^k - 1\}$ such that $b \cdot \overline{b} \equiv 1 \pmod{p^k}$.
select $d \in \{0, 1, \dots, p^k - 1\}$.
define $c = \overline{b}(ad - m) \pmod{p^k}$.
end If
End
return $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

select $m \in \{1, 2, \dots, 7\}$ such that $m\%2 \neq 0$. Take, for example, $m = 5$. Then, select any $a \in \{0, 1, \dots, 7\}$, say $a = 4$. Since $4\%2 = 0$, one has to select b such that it is not a multiple of 2, say, $b = 1$. As $b \cdot 1 \equiv 1 \pmod 8$, we have $\overline{b} = 1$. Then d can be taken as any number in $\{0, 1, \dots, 7\}$, say $d = 3$. Finally, $c = \overline{b}(ad - m) \pmod 8$ gives us $c = 7$. Therefore, Algorithm 1 returns

$$A_1 = \begin{bmatrix} 4 & 1 \\ 7 & 3 \end{bmatrix}.$$

Now, Algorithm 1 is run again, but this time with $p_2 = 5$ and $k_2 = 2$. First, select $m \in \{1, 2, \dots, 24\}$ such that m is not a multiple of 5, say $m = 6$. Then, take $a \in 0, 1, \dots, 24$, say $a = 2$. Since $a\%5 \neq 0$, we find $\overline{a} \in \{1, 2, \dots, 24\}$ such that $2\overline{a} \equiv 1 \pmod{25}$. Obviously, $\overline{a} = 13$. Next, b and c can be any numbers in $\{0, 1, \dots, 24\}$, say $b = 5$ and $c = 8$. Finally, $d = \overline{a}(bc + m) \pmod{25} = 13 \cdot (5 \cdot 8 + 6) \pmod{25} = 23$. Thefore, Algorithm 1 returns

$$A_2 = \begin{bmatrix} 2 & 5 \\ 8 & 23 \end{bmatrix}.$$

Algorithm 2 Generate a new ACM matrix.

function *generate_new_ACM*
Input: N (image size)
Output: M_{2x2} such that $\gcd(\det(M), N) = 1$.
Do
Write $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i are distinct primes and $k_i \geq 1$ are integers.
For each $i \in \{1, 2, \dots, r\}$
define $n_i = N/p_i^{k_i}$.
find $\overline{n}_i \in \{1, 2, \dots, p_i^{k_i} - 1\}$ such that $n_i \cdot \overline{n}_i \equiv 1 \pmod{p_i^{k_i}}$.
A_i=Algorithm 1(p_i, k_i).
End
return $M = n_1\overline{n}_1 A_1 + n_2\overline{n}_2 A_2 + \cdots + n_r\overline{n}_r A_r \pmod N$

Finally, according to Algoritm 2, since

$$n_1\overline{n}_1A_1 + n_2\overline{n}_2A_2 = 25\begin{bmatrix}4 & 1\\7 & 3\end{bmatrix} + 176\begin{bmatrix}2 & 5\\8 & 23\end{bmatrix} = \begin{bmatrix}452 & 905\\1583 & 4123\end{bmatrix},$$

one obtains

$$M = n_1\overline{n}_1A_1 + n_2\overline{n}_2A_2 \pmod{200} = \begin{bmatrix}52 & 105\\183 & 123\end{bmatrix}$$

as an ACM matrix to shuffle and image of size 200×200.

4 Experimental work

One of the applications of the Arnold's Cat Map is to reshuffle the pixel positions of an image to hide the content. During this process, the pixel positions are moved by multiplying with the ACM matrix as given in (2.4). Since the process is periodic, when repeatedly applied, the original image is recovered. The best shuffled image obtained during the iterations with the lowest self-correlation is taken as the encrypted image. In this procedure, a long period is important since this will make it more difficult to discover the original data and guessing the ACM matrix will be difficult. Moreover, a low self-correlation is important so that the content of the image is better encrypted. It should be noted that there are many different contexts where an ACM matrix is used and the one proposed in this paper is compatible with any application.

The mathematical proof to the extension of the ACM matrix given above is also tested experimentally. The reshuffling process is implemented with the old ACM matrix where the determinant is one, and with the new ACM matrix where the determinant does not need to be one. The period and self-correlation values are measured and original and reshuffled images are given as well.

With the new ACM matrix, in most cases, we obtained longer periods and lower self-correlation values. The classical ACM matrix has a period which never exceeds three times the size of the image [3]. This limitation makes the encryption process very difficult. The new ACM matrix will have a longer period especially when the size of the image is a prime number. The period of some examples are similar to classical ACM matrices. The reason is that the classical ACM matrices form a subset of the new ACM matrix set. Some examples are given in Tables 1 and 2. The determinant of the matrices generated by the proposed method may not be equal to 1. In Table 2, sample matrices are given along with the period obtained when applied to an image. The determinant of each matrix has a non-unity value with longer periods. In Table 1, the same images as in Table 2 are used with randomly selected old ACM matrices.

For the purpose of comparison with the results known in the literature, five random figures of size 347×347 are selected. Then, corresponding to each figure a random old ACM, $M_{\text{old}} = \begin{bmatrix}1 & 5\\6 & 31\end{bmatrix}$, and a random new ACM, $M_{\text{new}} = \begin{bmatrix}334 & 54\\336 & 207\end{bmatrix}$, has been selected. The period of M_{old} is $P_{\text{old}} = 173$ and the period of M_{new} is $P_{\text{new}} = 30102$. Clearly, the period of newly generated matrix is larger than that of the old one. In both cases, during the scrambling process, the figure with the lowest correlation number is taken as the encrypted image and the correlation of both images are calculated. The results are given in Table 3 where it is clearly seen that the new ACM works better.

For further comparison, in different N values, 100 matrices are randomly selected both from old ACM pool and the newly introduced pool. For each values of N, the average period

Table 1 Some old ACM matrices together with their periods for various image size and lowest correlation when applied to a specific image of that size

N	Old ACM matrix, its period (P) and lowest correlation (C)				
79	$\begin{bmatrix}1&1\\1&2\end{bmatrix}$ $P=39$ $C=0.0503$	$\begin{bmatrix}1&1\\2&3\end{bmatrix}$ $P=80$ $C=0.0214$	$\begin{bmatrix}1&2\\1&3\end{bmatrix}$ $P=80$ $C=0.0276$	$\begin{bmatrix}1&2\\2&5\end{bmatrix}$ $P=13$ $C=0.0408$	$\begin{bmatrix}1&2\\3&7\end{bmatrix}$ $P=40$ $C=0.0253$
128	$\begin{bmatrix}1&1\\5&6\end{bmatrix}$ $P=48$ $C=0.0042$	$\begin{bmatrix}1&1\\6&7\end{bmatrix}$ $P=32$ $C=0.0298$	$\begin{bmatrix}1&2\\5&11\end{bmatrix}$ $P=64$ $C=0.0121$	$\begin{bmatrix}1&2\\6&13\end{bmatrix}$ $P=64$ $C=0.0052$	$\begin{bmatrix}1&2\\10&21\end{bmatrix}$ $P=64$ $C=0.0117$
139	$\begin{bmatrix}1&3\\4&13\end{bmatrix}$ $P=35$ $C=0.0192$	$\begin{bmatrix}1&3\\6&19\end{bmatrix}$ $P=138$ $C=0.0078$	$\begin{bmatrix}1&3\\8&25\end{bmatrix}$ $P=69$ $C=0.016$	$\begin{bmatrix}1&3\\9&28\end{bmatrix}$ $P=14$ $C=0.0574$	$\begin{bmatrix}1&4\\1&5\end{bmatrix}$ $P=140$ $C=0.0042$
166	$\begin{bmatrix}1&4\\2&9\end{bmatrix}$ $P=7$ $C=0.0279$	$\begin{bmatrix}1&4\\3&13\end{bmatrix}$ $P=82$ $C=0.002$	$\begin{bmatrix}1&4\\4&17\end{bmatrix}$ $P=28$ $C=0.0086$	$\begin{bmatrix}1&5\\5&26\end{bmatrix}$ $P=123$ $C=0.0117$	$\begin{bmatrix}1&5\\6&31\end{bmatrix}$ $P=28$ $C=0.0325$
173	$\begin{bmatrix}1&5\\7&36\end{bmatrix}$ $P=174$ $C=0.0097$	$\begin{bmatrix}1&2\\7&15\end{bmatrix}$ $P=43$ $C=0.0051$	$\begin{bmatrix}1&6\\1&7\end{bmatrix}$ $P=87$ $C=0.019$	$\begin{bmatrix}1&6\\2&13\end{bmatrix}$ $P=87$ $C=0.0054$	$\begin{bmatrix}1&6\\5&31\end{bmatrix}$ $P=227$ $C=0.012$
227	$\begin{bmatrix}1&2\\4&9\end{bmatrix}$ $P=57$ $C=0.0066$	$\begin{bmatrix}1&2\\8&17\end{bmatrix}$ $P=76$ $C=0.0057$	$\begin{bmatrix}1&8\\3&25\end{bmatrix}$ $P=57$ $C=0.0026$	$\begin{bmatrix}1&8\\4&33\end{bmatrix}$ $P=38$ $C=0.002$	$\begin{bmatrix}1&9\\2&19\end{bmatrix}$ $P=226$ $C=0.002$
256	$\begin{bmatrix}1&2\\3&7\end{bmatrix}$ $P=64$ $C=0.0065$	$\begin{bmatrix}1&2\\8&17\end{bmatrix}$ $P=128$ $C=0.0032$	$\begin{bmatrix}1&4\\5&21\end{bmatrix}$ $P=256$ $C=0.0039$	$\begin{bmatrix}1&7\\9&64\end{bmatrix}$ $P=12$ $C=0.0207$	$\begin{bmatrix}1&6\\2&13\end{bmatrix}$ $P=128$ $C=0.0027$
347	$\begin{bmatrix}1&9\\2&19\end{bmatrix}$ $P=346$ $C=0.001$	$\begin{bmatrix}1&6\\7&43\end{bmatrix}$ $P=173$ $C=0.0025$	$\begin{bmatrix}1&1\\1&2\end{bmatrix}$ $P=116$ $C=0.0045$	$\begin{bmatrix}1&7\\3&22\end{bmatrix}$ $P=174$ $C=0.0058$	$\begin{bmatrix}1&8\\8&65\end{bmatrix}$ $P=348$ $C=0.0029$
512	$\begin{bmatrix}1&8\\5&41\end{bmatrix}$ $P=512$ $C=0.0036$	$\begin{bmatrix}1&3\\2&7\end{bmatrix}$ $P=128$ $C=0.0046$	$\begin{bmatrix}1&7\\2&15\end{bmatrix}$ $P=64$ $C=0.0322$	$\begin{bmatrix}1&1\\1&2\end{bmatrix}$ $P=384$ $C=0.0058$	$\begin{bmatrix}1&8\\7&57\end{bmatrix}$ $P=512$ $C=0.0039$

of those randomly selected matrices and the lowest correlation when applied to specific figures are calculated. The results are presented in Table 4. It is easily seen that, in the new pool, average period is drastically larger than the traditional ones. Considering the size of the new pool, the results of Table 4 makes more sense. Since the number given in Theorem 3.7 is incomparable larger than the number of traditional matrices, selecting only 100 random matrices and obtaining a very large average period shows the novelty on the current research.

Table 2 Some new ACM matrices together with their periods for various image size and lowest correlation when applied to a specific image of that size

N	New ACM matrix, its period (P) and lowest correlation (C)				
79	$\begin{bmatrix}63 & 42\\24 & 14\end{bmatrix}$	$\begin{bmatrix}38 & 27\\0 & 13\end{bmatrix}$	$\begin{bmatrix}7 & 21\\31 & 64\end{bmatrix}$	$\begin{bmatrix}44 & 68\\11 & 50\end{bmatrix}$	$\begin{bmatrix}28 & 32\\40 & 7\end{bmatrix}$
	$P = 3120$	$P = 39$	$P = 6240$	$P = 78$	$P = 39$
	$C = 0.001685$	$C = 0.0307$	$C = 0.0021$	$C = 0.0268$	$C = 0.0251$
128	$\begin{bmatrix}105 & 124\\91 & 69\end{bmatrix}$	$\begin{bmatrix}79 & 55\\99 & 12\end{bmatrix}$	$\begin{bmatrix}59 & 67\\112 & 121\end{bmatrix}$	$\begin{bmatrix}45 & 87\\99 & 78\end{bmatrix}$	$\begin{bmatrix}107 & 79\\32 & 75\end{bmatrix}$
	$P = 128$	$P = 192$	$P = 64$	$P = 96$	$P = 128$
	$C = 0.0117$	$C = 0.0094$	$C = 0.0317$	$C = 0.0268$	$C = 0.0081$
139	$\begin{bmatrix}69 & 47\\68 & 126\end{bmatrix}$	$\begin{bmatrix}33 & 115\\49 & 3\end{bmatrix}$	$\begin{bmatrix}91 & 77\\62 & 42\end{bmatrix}$	$\begin{bmatrix}122 & 87\\76 & 82\end{bmatrix}$	$\begin{bmatrix}118 & 32\\27 & 24\end{bmatrix}$
	$P = 460$	$P = 9660$	$P = 138$	$P = 19320$	$P = 2760$
	$C = 0.0024$	$C = 0.0017$	$C = 0.0064$	$C = 0.00099$	$C = 0.0039$
166	$\begin{bmatrix}73 & 154\\51 & 31\end{bmatrix}$	$\begin{bmatrix}151 & 73\\162 & 19\end{bmatrix}$	$\begin{bmatrix}77 & 91\\159 & 82\end{bmatrix}$	$\begin{bmatrix}163 & 84\\118 & 79\end{bmatrix}$	$\begin{bmatrix}33 & 57\\81 & 158\end{bmatrix}$
	$P = 82$	$P = 1722$	$P = 6888$	$P = 6888$	$P = 123$
	$C = 0.0155$	$C = 0.0017$	$C = 0.0012$	$C = 0.0025$	$C = 0.0038$
173	$\begin{bmatrix}74 & 164\\94 & 73\end{bmatrix}$	$\begin{bmatrix}23 & 30\\172 & 6\end{bmatrix}$	$\begin{bmatrix}98 & 116\\152 & 33\end{bmatrix}$	$\begin{bmatrix}149 & 66\\111 & 34\end{bmatrix}$	$\begin{bmatrix}75 & 21\\83 & 102\end{bmatrix}$
	$P = 172$	$P = 172$	$P = 29928$	$P = 172$	$P = 86$
	$C = 0.0062$	$C = 0.0047$	$C = 0.00075$	$C = 0.00062$	$C = 0.0072$
227	$\begin{bmatrix}52 & 133\\87 & 58\end{bmatrix}$	$\begin{bmatrix}66 & 61\\140 & 188\end{bmatrix}$	$\begin{bmatrix}224 & 79\\165 & 133\end{bmatrix}$	$\begin{bmatrix}25 & 200\\205 & 186\end{bmatrix}$	$\begin{bmatrix}71 & 41\\36 & 96\end{bmatrix}$
	$P = 226$	$P = 113$	$P = 25764$	$P = 2712$	$P = 226$
	$C = 0.0025$	$C = 0.0034$	$C = 0.00022$	$C = 0.00006$	$C = 0.0014$
256	$\begin{bmatrix}48 & 125\\249 & 114\end{bmatrix}$	$\begin{bmatrix}181 & 193\\70 & 159\end{bmatrix}$	$\begin{bmatrix}128 & 245\\61 & 87\end{bmatrix}$	$\begin{bmatrix}228 & 245\\233 & 140\end{bmatrix}$	$\begin{bmatrix}66 & 215\\221 & 65\end{bmatrix}$
	$P = 256$	$P = 128$	$P = 384$	$P = 128$	$P = 384$
	$C = 0.0016$	$C = 0.0041$	$C = 0.0018$	$C = 0.0038$	$C = 0.00046$
347	$\begin{bmatrix}317 & 274\\332 & 109\end{bmatrix}$	$\begin{bmatrix}13 & 294\\324 & 218\end{bmatrix}$	$\begin{bmatrix}263 & 257\\136 & 114\end{bmatrix}$	$\begin{bmatrix}60 & 244\\11 & 89\end{bmatrix}$	$\begin{bmatrix}16 & 33\\285 & 95\end{bmatrix}$
	$P = 346$	$P = 346$	$P = 15051$	$P = 346$	$P = 120408$
	$C = 0.0029$	$C = 0.00099$	$C = 0.0.00021$	$C = 0.0026$	$C = 0.00004$
512	$\begin{bmatrix}333 & 456\\440 & 317\end{bmatrix}$	$\begin{bmatrix}317 & 84\\423 & 343\end{bmatrix}$	$\begin{bmatrix}21 & 119\\184 & 293\end{bmatrix}$	$\begin{bmatrix}453 & 241\\81 & 244\end{bmatrix}$	$\begin{bmatrix}244 & 325\\401 & 49\end{bmatrix}$
	$P = 128$	$P = 256$	$P = 512$	$P = 768$	$P = 768$
	$C = 0.0.0142$	$C = 0.0.0018$	$C = 0.00032$	$C = 0.01$	$C = 0.0011$

5 Conclusions

In the literature, it is commonly known that the ACM matrix should be area-preserving, that is, the determinant should be either $+1$ or -1. Actually, this is only a mathematical fact observed for the original ACM matrix introduced by Arnold. After that, all newly introduced matrices are assumed to obey this restriction. For the discrete image scrambling processes

Table 3 Some figures with lowest correlation when scrambled with a random old ACM matrix M_{old} and a random new ACM matrix M_{new}

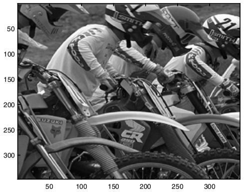
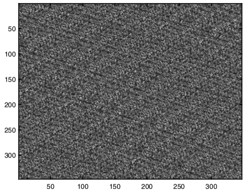
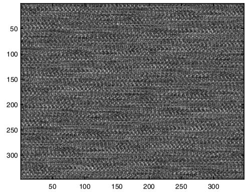
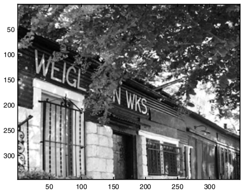
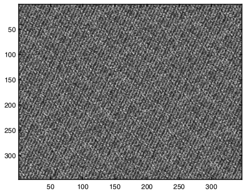
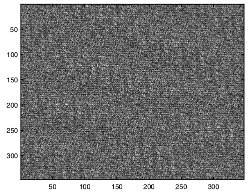
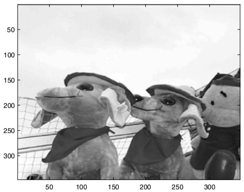
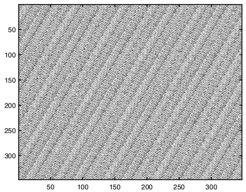
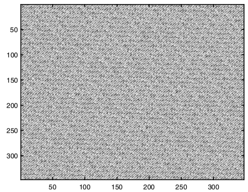
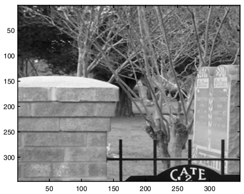
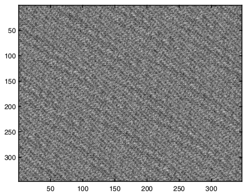
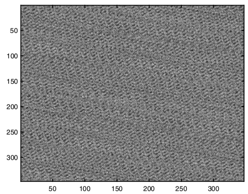
Original image	M_{old}	Correlation	M_{new}	Correlation
		0.0028		0.00001
		0.0085		0.00006
		0.0063		0.0011
		0.0064		0.00002

Table 3 continued

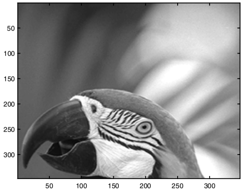
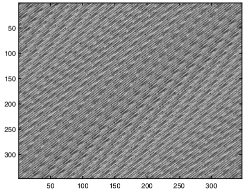
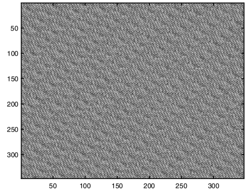
Original image	M_{old}	Correlation	M_{new}	Correlation
		0.0125		0.0014

Table 4 Average period and correlation values using 100 random old and new ACM matrices

N	Average P_{old}	Average P_{new}	Average C_{old}	Average C_{new}
173	100.46	8557	0.0064	0.0038
227	135.57	14424	0.0037	0.0015
256	140.08	193.08	0.0023	0.0027
347	210.25	32739	0.0021	0.0010
512	280.16	385.6	0.0051	0.0068

area-preserving property is not needed at all. The main objective of the current study is to remove that restriction and fill the gap in the direction to increase the number of possible matrices that can be used as an ACM matrix. It is proved mathematically that the ACM matrix may not possess the area-preserving property. Besides, removing this restriction makes the possible key space comparably large.

What is more, an algorithm is presented to generate all possible matrices that can be used in image scrambling. Experiments are provided to support the justified results. Comparison with the classical methods are given and they also show the novelty of the current research. In many new cases, the period is longer which makes it more robust against brute-force attacks.

The proposed method maximizes the number of parameters that can be used in an ACM matrix by removing the unity determinant requirement. In many cases the period of the newly proposed matrix is much longer than the period obtained with the classical ACM matrix. These two new features decrease the possibility of any brute-force attack in encryption algorithms where ACM is used. The usage of the new ACM matrix is not limited to encryption. All methods that use ACM matrix will benefit from the increased parameter space and longer periods.

Acknowledgements The authors would like to express their immense gratitude to the anonymous referees for their through reading of the manuscript and beneficial comments all of which improved the paper significantly.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data availability statement Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Competing Interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Abood NH (2017) An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. Paper presented at the 2017 annual conference on new trends in information & communications technology applications (NTICT), IEEE
2. Arnold VI, Avez A (1968) Ergodic problems of classical mechanics. Benjamin, New York, NY, USA
3. Dyson F, Falk H (1992) Period of a Discrete Cat mapping. Ame Math Monthly 99(7):603–614
4. Es-Sabry M, El Akkad N, Merras M, Saaidi A, Satori K (2022) A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method. Sci African 16:e01217. https://doi.org/10.1016/j.sciaf.2022.e01217
5. Fang D, Sun S (2020) A new secure image encryption algorithm based on a 5d hyper chaotic map. PLoS ONE 15(11):e0242
6. Hua Z, Jin F, Xu B, Huang H (2018) 2d logistic-sine-coupling map for image encryption. Signal Process 149:148–161
7. Krishna PR, Teja CVS, Thanikaiselvan V et al (2018) A chaos based image encryption using tinkerbell map functions. Paper presented at the 2018 second international conference on electronics, Communication and Aerospace Technology (ICECA), IEEE, pp 578–582
8. Li CL, Li HM, Li FD, Wei DQ, Yang XB, Zhang J (2018) Multiple-image encryption by using robust chaotic map in wavelet transform domain. Optik 171:277–286
9. Lin KT (2013) Image encryption using arnold transform technique and hartley transform domain. Paper presented at the inth international conference on intelligent information hiding and multimedia signal processing, pp 84–87
10. Masood F, Boulila W, Alsaeedi A, Khan JS, Ahmad J, Khan MA, Ur Rehman S (2022) A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map. Multimed Tools Appl 81:30931–30959. https://doi.org/10.1007/s11042-022-12844-w
11. Mohamed NA, El-Azeim MA, Zaghloul A (2016) Improving image encryption using 3D cat map and turing machine. Int J Adv Comput Sci Appl 7(1). https://doi.org/10.14569/IJACSA.2016.070129
12. Musanna F, Rani A, Kumar S (2018) Image encryption using chaotic 3-D Arnold's cat map and logistic map. In: Proceedings of 2nd international conference on computer vision & image processing, Springer, Singapore, pp 365–378
13. Pak C, Huang L (2017) A new color image encryption using combination of the 1d chaotic map. Signal Process 138:129–137
14. Shalaby MAW, Salel MT, Elmahdy HN (2020) Enhanced Arnold's cat map-AES encryption technique for medical images. Paper presented at the 2020 2nd novel intelligent and leading emerging sciences conference (NILES), IEEE
15. Shan L, Qiang H, Li J, Zq Wang (2005) Chaotic optimization algorithm based on tent map. Control Decis 20(2):179–182
16. Shang Z, Ren H, Zhang J (2008) A block location scrambling algorithm of digital image based on Arnold transformation. Paper presented at the 9th international conference for young computer scientists, pp 2942–2947
17. Sinha RK, San N, Asha B, Prasad S, Sahu SS (2018) Chaotic image encryption scheme based on modified Arnold cat map and Henon map. Paper presented at the 2018 international conference on current trends towards converging technologies (ICCTCT)
18. Souza CEC, Chaves DPB, Pimentel C (2021) One-dimensional pseudo-chaotic sequences based on the discrete Arnold's cat map over $\mathbb{Z}_{3^m}$. IEEE Trans Circuits Syst II: Expr Briefs 68(1):491–495. https://doi.org/10.1109/TCSII.2020.3010477
19. Stewart BM (1964) Theory of numbers, 2nd edn. The MacMilman Company, New York, NY
20. Thakur S, Singh AK, Ghrera SP, Elhoseny M (2019) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimed Tools Appl 78(3):3457–3470. https://doi.org/10.1007/s11042-018-6263-3
21. Wei-Bin C, Xin Z (2009) Image encryption algorithm based on Henon chaotic system. Paper presented at the 2009 international conference on image analysis and signal processing, IEEE, pp 94–97
22. Zareai D, Balafar M, Derakhshi MRF (2021) A new Grayscale image encryption algorithm composed of logistic mapping, Arnold cat, and image blocking. Multimed Tools Appl 80:18317–18344. https://doi.org/10.1007/s11042-021-10576-x
23. Zhang H, Cai R (2010) Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination. Paper presented at the international conference on intelligent computing and integrated systems, pp 113–117
24. Zhang H, Wang X, Xie H, Wang C, Wang X (2020) An efficient and secure image encryption algorithm based on non-adjacent coupled maps. IEEE Access 8:104–122

25. Zhang L, Zhang X (2020) Multiple-image encryption algorithm based on bit planes and chaos. Multimed Tools Appl 79(29):20753–20771
26. Zia U, McCartney M, Scotney B, Martinez J, AbuTair M, Memon J, Sajjad A (2022) A Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. Int J Inf Secur 21:917–935. https://doi.org/10.1007/s10207-022-00588-5

Authors and Affiliations

Mehmet Turan[1] · **Erhan Gökçay**[2] · **Hakan Tora**[3,4]

Erhan Gökçay
erhan.gokcay@atilim.edu.tr

Hakan Tora
hakan.tora@atilim.edu.tr

1 Department of Mathematics, Atilim University, Ankara, Turkey

2 Department of Software Engineering, Atilim University, Ankara, Turkey

3 Department of Electrical-Electronics Engineering, Atilim University, Ankara, Turkey

4 Department of Electrical-Electronics Engineering, Biruni University, İstanbul, Turkey