UDC 004.032

Yu. Khanas, R.-A. Ivantsiv
Lviv Polytechnic National University, DCAD, Lviv

DETERMINATION OF COMPATIBILITY AND EFFICIENCY OF NUMERICAL MATRIX TRANSFORMATION ALGORITHMS

The article demonstrates the application of various matrix transformation algorithms with detailed analysis and commentary on the results. This is done to determine experimentally the effectiveness of their combination for further developments and experiments.

Key words: matrix reflection, matrix balancing, matrix reduction, virtual string, virtual column.

ВИЗНАЧЕННЯ СУМІСНОСТІ ТА ЕФЕКТИВНОСТІ АЛГОРИТМІВ ТРАНСФОРМАЦІЇ ЧИСЛОВИХ МАТРИЦЬ

Продемонстровано застосування різних алгоритмів трансформації матриць з детальним аналізом та коментуванням результатів з метою експериментального визначення ефективності їх комбінування для подальших розробок та експериментів.

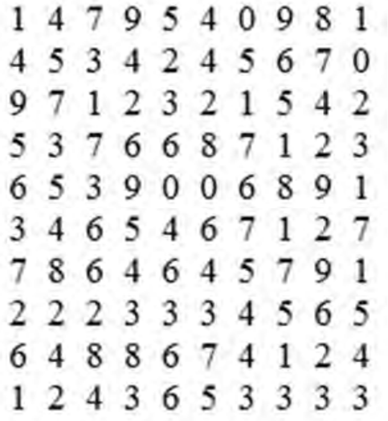
Ключові слова: віддзеркалення матриці, збалансування матриці, скорочення матриці, віртуальний рядок, віртуальний стовпець.

Introduction

Since some of the transformation algorithms are intended for matrices of a clearly defined type, it would be wise to check if they can be used for multi-type matrices, or which modifications are required for this. The article will cross the algorithms developed at the beginning of the research, as well as the already modified algorithms, all actions will be carried out on one matrix for the purpose of comparison of the results.

1. Select an object and determine its characteristics

For the experiments, a matrix of 10x10 size was selected.



1	4	7	9	5	4	0	9	8	1
4	5	3	4	2	4	5	6	7	0
9	7	1	2	3	2	1	5	4	2
5	3	7	6	6	8	7	1	2	3
6	5	3	9	0	0	6	8	9	1
3	4	6	5	4	6	7	1	2	7
7	8	6	4	6	4	5	7	9	1
2	2	2	3	3	3	4	5	6	5
6	4	8	8	6	7	4	1	2	4
1	2	4	3	6	5	3	3	3	3

Fig. 1. Input matrix

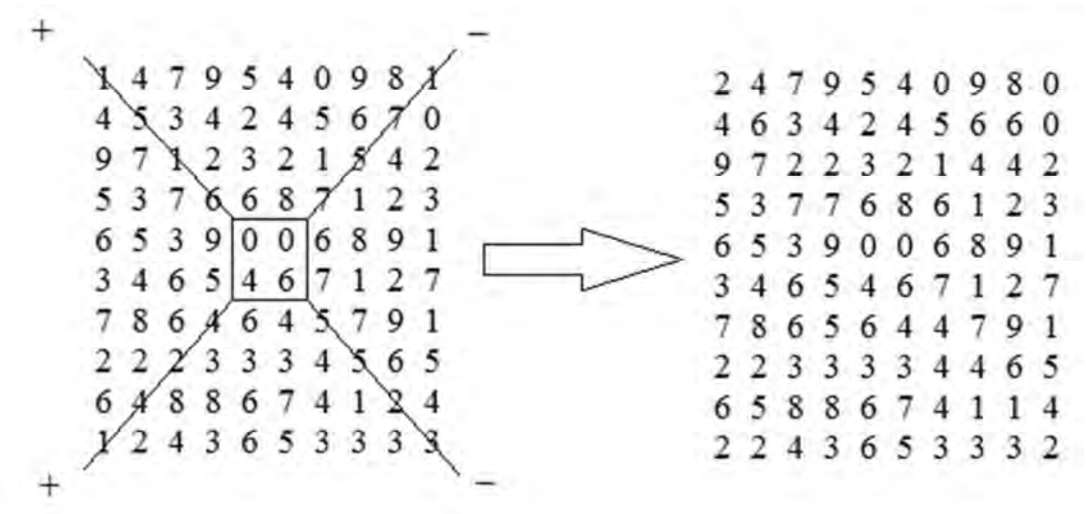
The matrix is filled with integer positive numbers with one sign, so algorithms for multivalued numbers, negative or fractional, will not be used here.

A matrix with a pair of columns and rows, and this number is the same.

In order not to complicate the demonstration of results once again, some of the actions intended to reduce the matrix will be carried out, but the reductions themselves will not be made.

2. Selection and implementation of transformation algorithms

For matrices of this type and size, the first algorithm makes sense to use diagonal balancing.

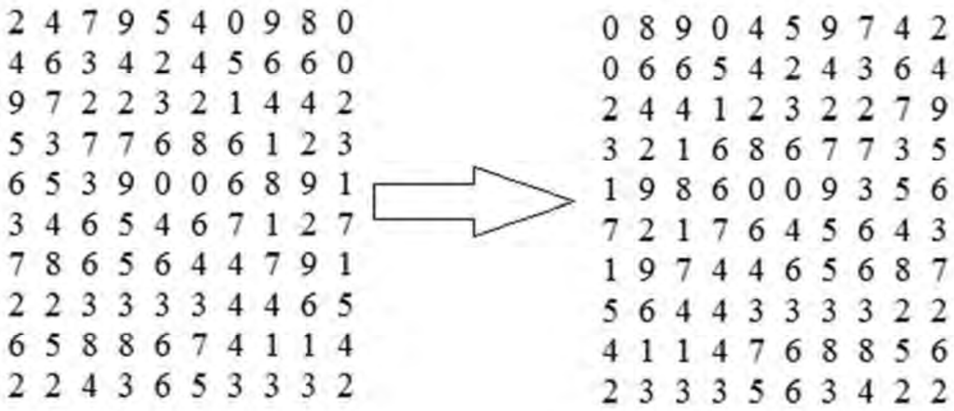


```
+                              −
  1 4 7 9 5 4 0 9 8 1        2 4 7 9 5 4 0 9 8 0
  4 5 3 4 2 4 5 6 7 0        4 6 3 4 2 4 5 6 6 0
  9 7 1 2 3 2 1 5 4 2        9 7 2 2 3 2 1 4 4 2
  5 3 7 6 6 8 7 1 2 3        5 3 7 7 6 8 6 1 2 3
  6 5 3 9 0 0 6 8 9 1        6 5 3 9 0 0 6 8 9 1
  3 4 6 5 4 6 7 1 2 7        3 4 6 5 4 6 7 1 2 7
  7 8 6 4 6 4 5 7 9 1        7 8 6 5 6 4 4 7 9 1
  2 2 2 3 3 3 4 5 6 5        2 2 3 3 3 3 4 4 6 5
  6 4 8 8 6 7 4 1 2 4        6 5 8 8 6 7 4 1 1 4
  1 2 4 3 6 5 3 3 3 3        2 2 4 3 6 5 3 3 3 2
+                              −
```

Fig. 2. Conducting one iteration of diagonal balancing

Taking into account the content of the matrix 10x10 (100 numbers), of which 4 is the central part and thus in four diagonal parts there are four numbers, which is changed and in the sum of them will be 16 out of 100, that is, only a small part of the matrix has been transformed.

For the next transformation, the reflection of the matrix was selected, which in turn would change the order of all the components in the matrix.

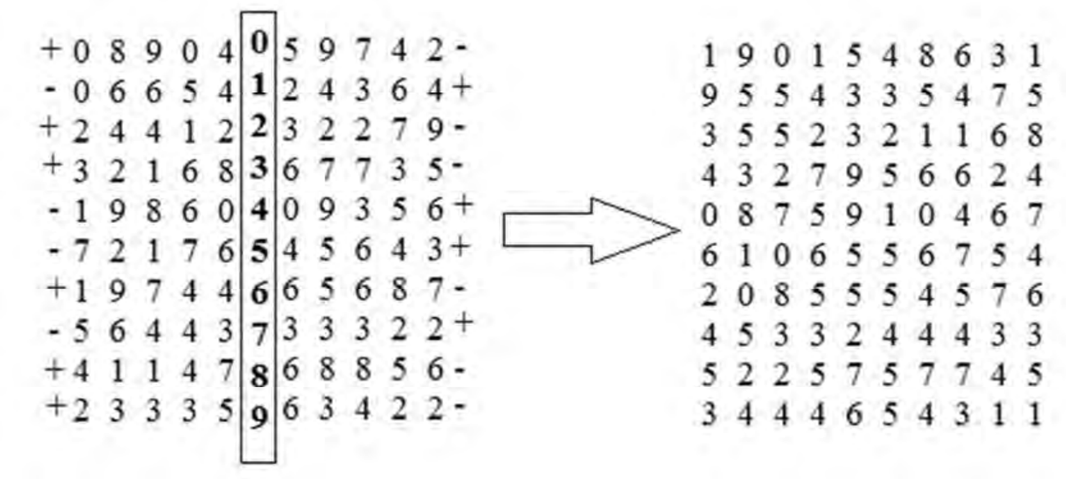


```
2 4 7 9 5 4 0 9 8 0        0 8 9 0 4 5 9 7 4 2
4 6 3 4 2 4 5 6 6 0        0 6 6 5 4 2 4 3 6 4
9 7 2 2 3 2 1 4 4 2        2 4 4 1 2 3 2 2 7 9
5 3 7 7 6 8 6 1 2 3        3 2 1 6 8 6 7 7 3 5
6 5 3 9 0 0 6 8 9 1        1 9 8 6 0 0 9 3 5 6
3 4 6 5 4 6 7 1 2 7        7 2 1 7 6 4 5 6 4 3
7 8 6 5 6 4 4 7 9 1        1 9 7 4 4 6 5 6 8 7
2 2 3 3 3 3 4 4 6 5        5 6 4 4 3 3 3 3 2 2
6 5 8 8 6 7 4 1 1 4        4 1 1 4 7 6 8 8 5 6
2 2 4 3 6 5 3 3 3 2        2 3 3 3 5 6 3 4 2 2
```

Fig. 3. One iteration of horizontal reflection

In the future, this type of transformation will not be used, since the re-reflection simply returns the matrix to its previous appearance. It is only possible to use vertical balancing, that is, the mirror image of the matrix in the vertical direction, but also no more than one iteration. Also, the simultaneous use of these two algorithms gives the third type of reflection, namely, the diagonal.

Next is the content to check the effect of adding virtual strings or columns. For example, a virtual column will be added to this matrix, it will be central and allow you to perform horizontal balancing. This column will not change, and after balancing it will be removed from the matrix. That is, the column will not be sent in the message.



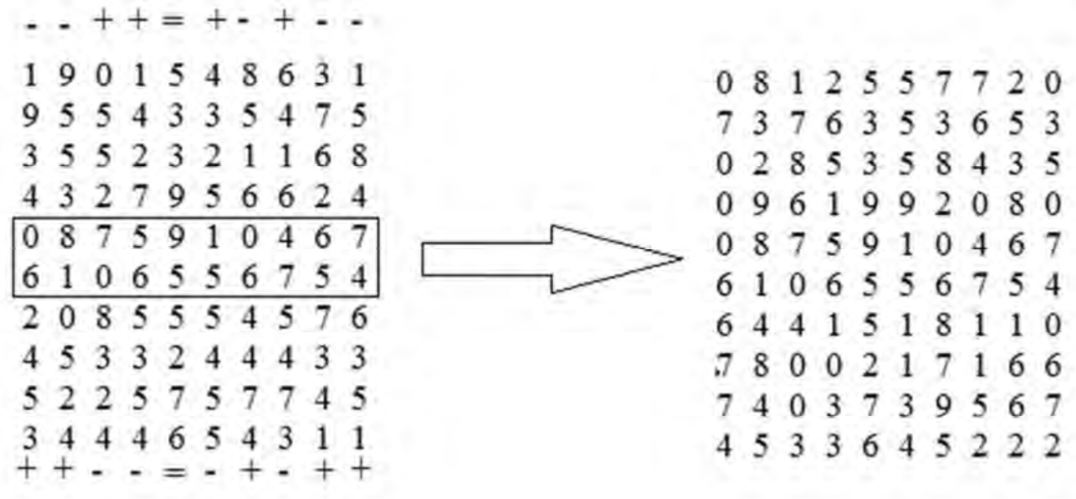
```
+0 8 9 0 4 |0| 5 9 7 4 2 -        1 9 0 1 5 4 8 6 3 1
-0 6 6 5 4 |1| 2 4 3 6 4 +        9 5 5 4 3 3 5 4 7 5
+2 4 4 1 2 |2| 3 2 2 7 9 -        3 5 5 2 3 2 1 1 6 8
+3 2 1 6 8 |3| 6 7 7 3 5 -        4 3 2 7 9 5 6 6 2 4
-1 9 8 6 0 |4| 0 9 3 5 6 +   =>   0 8 7 5 9 1 0 4 6 7
-7 2 1 7 6 |5| 4 5 6 4 3 +        6 1 0 6 5 5 6 7 5 4
+1 9 7 4 4 |6| 6 5 6 8 7 -        2 0 8 5 5 5 4 5 7 6
-5 6 4 4 3 |7| 3 3 3 2 2 +        4 5 3 3 2 4 4 4 3 3
+4 1 1 4 7 |8| 6 8 8 5 6 -        5 2 2 5 7 5 7 7 4 5
+2 3 3 3 5 |9| 6 3 4 2 2 -        3 4 4 4 6 5 4 3 1 1
```

Fig. 4. Horizontal balancing using the virtual column

The balancing was carried out in the unit range, that is, all the numbers of the matrix were varied per unit. As it is seen in the figure, all components of the matrix were transformed, and the virtual column was removed from the transformed matrix.

However, there is an option of balancing and without adding virtual components. Since the number of rows and the number of columns are even, then it is not possible to select one center, in which case it is expedient to indicate the center not one but two rows or columns.

Since the horizontal balancing with the single range already exists, then a vertical balancing with the extended center of the matrix and the centripetal range will be performed.



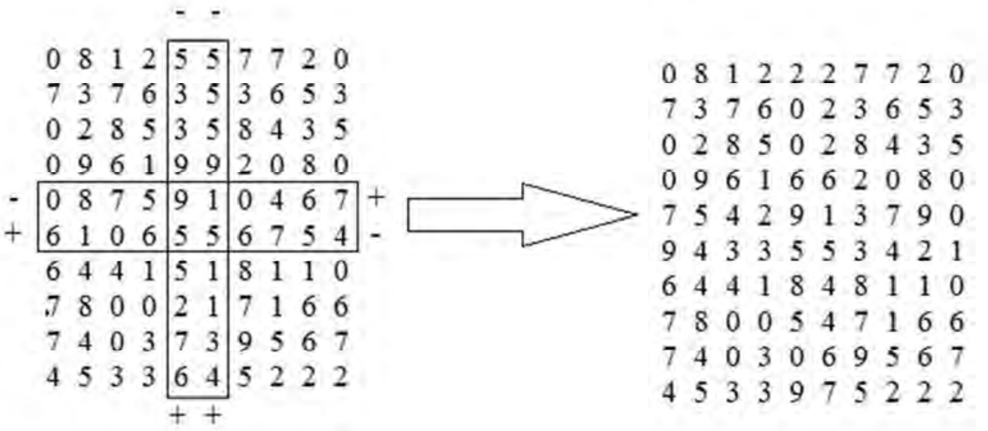
```
 - - + + = + - + - -
 1 9 0 1 5 4 8 6 3 1          0 8 1 2 5 5 7 7 2 0
 9 5 5 4 3 3 5 4 7 5          7 3 7 6 3 5 3 6 5 3
 3 5 5 2 3 2 1 1 6 8          0 2 8 5 3 5 8 4 3 5
 4 3 2 7 9 5 6 6 2 4          0 9 6 1 9 9 2 0 8 0
|0 8 7 5 9 1 0 4 6 7|         0 8 7 5 9 1 0 4 6 7
|6 1 0 6 5 5 6 7 5 4|   =>    6 1 0 6 5 5 6 7 5 4
 2 0 8 5 5 5 4 5 7 6          6 4 4 1 5 1 8 1 1 0
 4 5 3 3 2 4 4 4 3 3          7 8 0 0 2 1 7 1 6 6
 5 2 2 5 7 5 7 7 4 5          7 4 0 3 7 3 9 5 6 7
 3 4 4 4 6 5 4 3 1 1          4 5 3 3 6 4 5 2 2 2
 + + - - = - + - + +
```

Fig. 5. Centric vertical balancing

Accordingly, the range began with the edge of the matrix per unit, since in the adjacent portions of the columns there were four numbers, so the balancing range increased to “4” as it approaches the center of the matrix.

The last of the transformation algorithms is cross-matching.

Its essence is to determine the central lines and columns that form the intersection and their comparison and balancing. However, the matrix does not have only one column and the line is exactly in the center, so as in the previous example, you should expand the center of the matrix and select two rows and two columns with the centers of the matrix and balance in a certain range, taking into account the contents of the central part. The specified range means that the change of the matrix content can be made on any previously specified number, for example, “3” will be chosen, now the numbers of the matrix will increase and decrease by three instead of one.



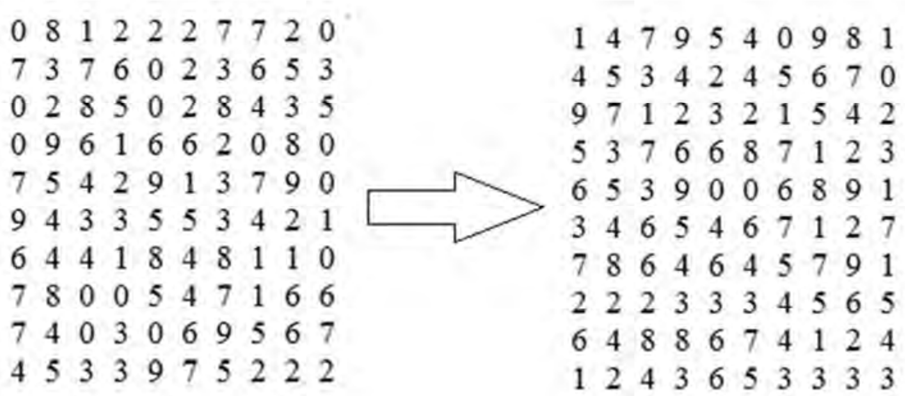
```
          - -
  0 8 1 2 5 5 7 7 2 0
  7 3 7 6 3 5 3 6 5 3
  0 2 8 5 3 5 8 4 3 5
  0 9 6 1 9 9 2 0 8 0
- 0 8 7 5 9 1 0 4 6 7 +
+ 6 1 0 6 5 5 6 7 5 4 -
  6 4 4 1 5 1 8 1 1 0
  7 8 0 0 2 1 7 1 6 6
  7 4 0 3 7 3 9 5 6 7
  4 5 3 3 6 4 5 2 2 2
          + +
```

```
0 8 1 2 2 2 7 7 2 0
7 3 7 6 0 2 3 6 5 3
0 2 8 5 0 2 8 4 3 5
0 9 6 1 6 6 2 0 8 0
7 5 4 2 9 1 3 7 9 0
9 4 3 3 5 5 3 4 2 1
6 4 4 1 8 4 8 1 1 0
7 8 0 0 5 4 7 1 6 6
7 4 0 3 0 6 9 5 6 7
4 5 3 3 9 7 5 2 2 2
```

Fig. 6. Cross-balance with extended center and defined range

Considering the central part of this rule, this rule is introduced for the case of a dilemma, when both parts of the matrix are equal and there is no reason to reduce or increase one of the parts; therefore, the numbers from the central part are taken into account, but they do not change themselves.

So you can compare the results:



```
0 8 1 2 2 2 7 7 2 0
7 3 7 6 0 2 3 6 5 3
0 2 8 5 0 2 8 4 3 5
0 9 6 1 6 6 2 0 8 0
7 5 4 2 9 1 3 7 9 0
9 4 3 3 5 5 3 4 2 1
6 4 4 1 8 4 8 1 1 0
7 8 0 0 5 4 7 1 6 6
7 4 0 3 0 6 9 5 6 7
4 5 3 3 9 7 5 2 2 2
```

```
1 4 7 9 5 4 0 9 8 1
4 5 3 4 2 4 5 6 7 0
9 7 1 2 3 2 1 5 4 2
5 3 7 6 6 8 7 1 2 3
6 5 3 9 0 0 6 8 9 1
3 4 6 5 4 6 7 1 2 7
7 8 6 4 6 4 5 7 9 1
2 2 2 3 3 3 4 5 6 5
6 4 8 8 6 7 4 1 2 4
1 2 4 3 6 5 3 3 3 3
```

Fig. 7. Comparison of the input matrix and transformed

Even visually it is similar to the fact that the input matrix was replaced by a matrix of the same size, only with a chaotic set of numbers different from the previous version. Such transformations are a convenient tool for encrypting information. The matrix reduction algorithms were designed for compression, the algorithms for encryption are given, so algorithms can be developed for other tasks.

Conclusions

In the article, only some of the main and modified algorithms were shown, because numbers 0–9 were used and too many transformations and transformations could instead replace (decrypt) the matrix radically, on the contrary, give very small results. Therefore, experiments will continue to determine the optimal number of algorithms and their iterations for one example. Also, systematization of the algorithms of those methods will be carried out in order to develop a more precise algorithm for the formation of the key.

1. Yuriy Khan, Roman-Andriy Ivantsiv. Application Mirroring of Matrices to Prevent Excessive Reduction // Perspective Technologies and Methods of Designing MEMS (MEMSTECH 2016): Materials of the XII International Scientific and Technical Conference (April 20-24, 2016, Lviv-Polyana, Ukraine). – 2016 – P. 143–145. (SciVerse SCOPUS). 2. Ivanciv R., Khan Y. Methods of information security based cryptographic transformations matrix Noiseimmunity // Experience of the development and application of CAD in microelectronics: materials of the XIII International Conference CADSM-2015, February 24–27, 2015, Polyana, Ukraine / Lviv Polytechnic National University. – L.: Tower and Co, 2015 – C. 218–220 – Paral. T.T.Ark.Eng.