A Novel Image Encryption Algorithm Based On Latin And Magic Square

Seyyed Ali Mohammadiyeh [1*], Pooria Lajevardy [2]

[1] Department of Pure Mathematics, Faculty of Mathematical Sciences,

University of Kashan, Kashan, I. R. Iran

alim@kashanu.ac.ir

[2] Department of Computer Science, Faculty of Math and Computer Science

Allameh Tabataba'i University, Tehran, Iran

lajevardy@atu.ac.ir

ABSTRACT

This paper presents a new algorithm for encrypting digital images based on Latin and magic squares with preprocessing, permutation, and substitution structures. At first, a 256-bit secret key is generated by applying the hash function to the original image information; Then the Latin square is generated by the secret key and the logistics chaos function in the preprocessing, permutation, and replacement stages. In the preprocessing step, the statistical distribution of image pixels is changed by embedding random integers in the image via the XOR operation between the original image and the Latin square. In the permutation phase, first, a magic square is generated by the Latin square and its transpose, then the location of the image pixels is changed with its help. In the replacement phase, using the Latin square generated, the brightness level of each pixel changes, and the encrypted image is obtained. The simulation results show that the correlation coefficient for the encrypted image is about zero. The proposed image encryption algorithm also has high security against known attacks and high speed for real-time encryption applications.

KEYWORDS

Combinatorics, Image Encryption, Latin square, Magic square

INTRODUCTION

Digital images are one of the most widely used types of multimedia data in the recent century that may contain confidential medical, commercial, military, and so on. Thus the security of images combined with the rapid development of technology computers and the Internet have become increasingly important. Image Encryption is one of the efficient methods to protect image information by changing the image pixels, to prevent unauthorized access to the image data. [1]

To increase the security of image encryption, researchers used combinatorics applications such as latin and magic squares in image encryption. [2, 4]

A Latin square of order N is an N × N matrix, filled with elements from the set {1, . . . , N}, assuming in each row and column each element appears exactly once. The Latin square is a specific type of square matrix with uniformity. The number of Latin squares is huge. For example, the number of Latin squares for N=10 is about 10^36.9. When the order increases, the number of Latin squares will rise sharply.

METHODOLOGY

Since a large number of latin squares in the same order can be generated, so using latin squares in image encryption algorithms can increase security. [3]

Order	Number of latin squares
1	1
2	2
3	12
4	576
5	161280
6	812851200
7	61479419904000
8	108776032459082956800
9	5524751496156892842531225600
10	9982437658213039871725064756920320000
11	776966836171770144107444346734230682311065600000

Figure 1. Number of latin squares in the same orders

In the following, diagram of the presented algorithm is shown.

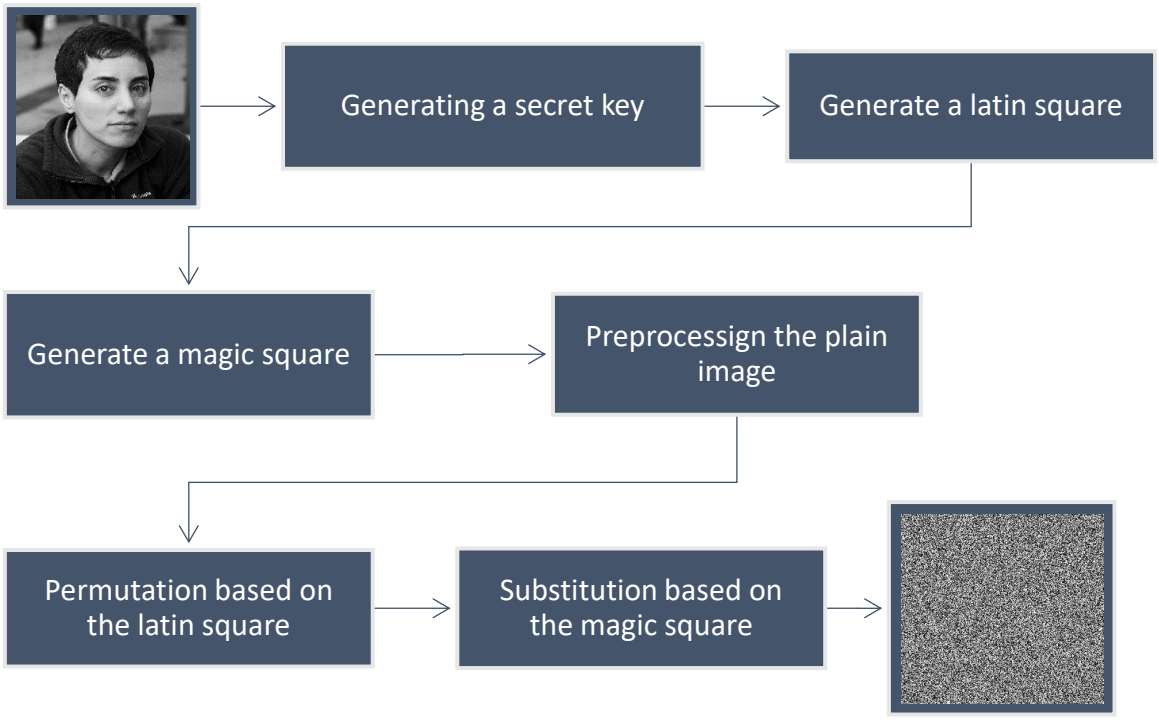

Figure 2. The diagram of the proposed algorithm

RESULT

The results of comparing the proposed image encryption algorithm showed that using Latin square in image encryption has higher resistance against noise and cut-off than other algorithms and has a high speed for real-time encryption applications.

REFERENCES

1. Khan, M., Shah, T., “A novel image encryption technique based on Hénon chaotic map and S8 symmetric group”, Neural Computing and Applications, Vol. 25, pp. 1717- 1722, 2014.

2. Xu, M., Tian, Z., “A flexible image cipher based on orthogonal arrays”, Information Sciences, Vol. 551, pp. 39-53, 2021.

3. Wilk, Martin B., and Oscar Kempthorne. "Non-additivities in a Latin square design." Journal of the American Statistical Association 52.278 (1957): 218-236.

4. Hua, Z., Li, J., Chen, Y., Yi, S., “Design and application of an S-box using complete Latin square”, Nonlinear Dynamics, Vol. 104, pp. 807-825, 2021.