Abstract - Secure communication is one of the most important tasks of any communication system. In order to provide security to the information which can be in the form of text, image, audio or video, encryption is used. In this paper an image encryption algorithm is proposed which is based on chaos theory. Two chaotic maps, Arnold’s cat map and modified logistic map, are used in this proposed algorithm. Arnold cat map is used for image scrambling and linear logistic map is first modified and then is used for key generation. This key is then used for image encryption. This algorithm provides uniform histogram and also reduces the correlation coefficients of encrypted image.

Keywords: Chaos theory, Arnold’s cat map, logistic map etc.

I. INTRODUCTION

Today is the age of information technology in which information can be treated as an asset that has a worth like any other asset. So information needs to be secured from unauthorized access. In order to provide security, information should be hidden from unauthorized user (confidentiality), protected from unauthorized change (integrity), and available to authorized users (availability). Text encryption algorithms such as AES cannot be used for image encryption because of large size of image. So number of image encryption algorithms is proposed in last two decades.

Chaos theory has an application in the field of image encryption, in which pixels of image are rearranged randomly with the help of chaotic maps like Arnold’s cat map etc. In this proposed work, logistic map is first modified and then used in combination with Arnold’s cat map.

Logistic map: 1-D logistic map was proposed by RM May. This map is simplest non-linear chaotic system which is defined as:

\[ x_{n+1} = r x_n (1-x_n) \]

where \( x_n \) \( (0, 1) \), \( a \) \( (0, 1.4] \), \( b \) \( [5, 43] \), or \( x_n \) \( (0, 1) \), \( a \) \( (1.4, 1.5] \), \( b \) \( [9, 38] \), or \( x_n \) \( (0, 1) \), \( a \) \( (1.5, 1.57] \), \( b \) \( [3, 15] \). The ranges of \( a \) and \( b \) are obtained by iteration experimental analysis.

Arnold cat map: it was demonstrated by Vladimir Arnold in 1960s by using an image of a cat. Arnold cat map uses the concept of linear algebra to change the position of pixels of original image. Original image is divided into blocks and then Arnold transformation is done.

II. PROPOSED WORK AND RESULTS

Three images of different size (200*200, 300*300 and 512*512) are selected. The proposed algorithm is implemented in six steps. Fig 1 shows the flow chart of algorithm.

Steps for image encryption algorithm are:

1. Original image is loaded.
2. Gray scale conversion of original image.
3. Image is scrambled using Arnold’s cat map.
4. Key is generated using modified logistic map.
5. Using generated key Image is encrypted.
6. Encrypted image is checked on different parameters like histogram etc.
Fig. 1 flow chart of algorithm
Fig. 2(a) : Original image

Fig 2(b) : Gray Scale image

Fig. 2(c) : Scrambled image

Fig. 2(d): Encrypted image
Fig 2 shows the result of an image encryption algorithm. Fig. 2(a) shows original image of size 300*300, Fig. 2(b) is gray scale conversion of original image. Fig 2(c) shows image after ACM scrambling and Fig 2(d) shows encrypted image. Fig 2(e) gives the comparison between histograms of original image and encrypted image. This algorithm reduces the correlation coefficients of encrypted image. Table 1 shows horizontal and vertical correlation coefficients.

Table 1: correlation coefficients

<table>
<thead>
<tr>
<th>Image Size</th>
<th>Horizontal Correlation coefficient</th>
<th>Vertical Correlation coefficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>200*200</td>
<td>-0.1007</td>
<td>-0.5500</td>
</tr>
<tr>
<td>300*300</td>
<td>-0.2590</td>
<td>-0.7157</td>
</tr>
<tr>
<td>512*512</td>
<td>-0.3310</td>
<td>-0.7530</td>
</tr>
</tbody>
</table>

III CONCLUSION AND FUTURE SCOPE

In this work encryption based on Arnold’s cat map have been enhanced. The encryption key used for encryption requires security and unpredictability. This work is done with help of logistic map which is first modified. This proposed work provides uniform histogram and reduction in correlation coefficients of encrypted image. For future work mathematical analysis of the chaos of the higher dimensional Arnold’s maps is yet to be explored and the encryption of image after higher order scrambling by Arnold’s cat map is yet to be observed.

REFERENCES

[1] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li,” A new chaotic algorithm for image encryption” ©2005 Published by Elsevier Ltd.