# A robust encryption scheme using RC4 And Arnold's Chaotic Map

Aneesh Kumar[1], Abhishek Kumar[2], Siddharth Singh[3], Monu Singh[2*]

[1,2,3,4] Deptt. of CSE, Galgotias University, Greater Noida

aneesh.20scse1010469@galgotiasuniversity.edu.in; abhishek.20scse1010468@galgotiasuniversity.edu.in; siddharth.20scse1010385@galgotiasuniversity.edu.in; monu.singh@galgotiasuniversity.edu.in

**ABSTRACT** Recently, the internet becomes a worldwide source for transmission of information from one end to the other, whether it is video, audio, image, text, etc. Transferring images over the network is very risky, as any unauthorized person can do modifications to these images and may lead to big trouble. For secure transmission of these images over the internet with high security and confidentiality, it is necessary to convert the image into an unreadable format. To do this, there are various encryption techniques used for securing images. Amongst all the image encryption technique which is extensively used by researchers for secure and safe transmission of the image on the reliable network, RC4 and Arnold's chaotic map are the techniques used for encryption of image. Our proposed paper aim is to represent a new encryption technique that combines RC4 algorithm and Arnold Chaotic map which is a chaotic map to propose a new algorithm and encrypt an image. The aim of using Rivest Cipher 4 algorithm is to enhance the confidentiality to encryption by generating key and Arnold Chaotic Map is used for confusion to change the image's pixels. The efficiency of our proposed algorithm is evaluated using a Histogram analysis, Coefficient Analysis, and key Space Analysis. The achieved result of histogram analysis shows the same distribution trend of pixels before and after the encryption of an image. Further the proposed scheme is evaluated against various parameters (like NPCR, and entropy values) to check its resistance over differential attacks and the result shows values near to the ideal values.

**KEYWORDS:** Image Encryption, RC4, Arnold's Cat Map, Chaotic Map.

## I. INTRODUCTION

In this decade there is a lot of uses for the internet, computer, and multimedia device. Only the text is not sent but also the information is conveyed via the internet in a form of an electronic signal. In this form, the information is not secured on a widespread network. public demand for some technique which will hinder their message from unauthorized access and deliver to the person of destination source. To protect images, files, and videos, we need digital encryption techniques. Various applications are developing, and they all require secure security of their text, audio, video, and files.

To enhance the security many researchers have put their legs to form a new technique for the safer transmission of the information. They mainly change the pixel size or degrade the quality of the image to make it encrypted but anyhow the existence of the encrypted image is still visible.

In this paper we will take encryption techniques like the RC4 algorithm for key generation and then by Arnold Cat Map, we will encrypt the image by a modal of confusion.

Next section shows how the algorithms are being working for securing the images.

### A. RON RIVEST CIPHER 4 ALGORITHM (RC4)

RC4 is a symmetric-key algorithm. The encryption is performed using RC4 by combining the plain text with the pseudo-random bits using exclusive-or and decryption is also achieved in the similar manner. The state table S is initialized by the permutation of the variable length key ranges up to 256 bits. After this is completed the state table s is used for generating a sequence of bits using PRGA. RC4 algorithm has two stages: The first stage includes the initialization of the state table S, and the other is the operation. The first stage is used to mix the state table and the key.

“In the RC4 encryption algorithm, the encryption process is done by using two Algorithms, first the **Key Scheduling Algorithm (KSA)** and the other is the **Pseudo-Random Generation Algorithm (PRGA)** which results in a stream of bits (keystream).” [2]

#### a: “Key-Scheduling Algorithm (KSA).”

Step1: Initialize and declare a=0

Step2: Initialize state array S, and assign values from 0 to 255

Step3: Initialize and declare b=0

Step4: Run a loop ranges up to 255

## II. THE PROPOSED METHOD

Step4.1: b = (b + S[a]+K [a % L]) % 256

Step5: Swap the values of S[a] with S[b]

Step6: Return state array

#### b: “Pseudo-Random Generation Algorithm (PRGA)”

I/P: “State array”, O/P: “Key sequence $K_{seq}$”

Step1: Initialize a and b with 0

Step2: Run a loop until sequence ends

Step2.1: a = (a+1) % 256

Step2.2: b = (b + S[b]) % 256

Step2.3: swap the values of S[a] with S[b]

Step2.4: Kseq = S[(S[a]+ S[b]) % 256]

Step3: Return $K_{seq}$

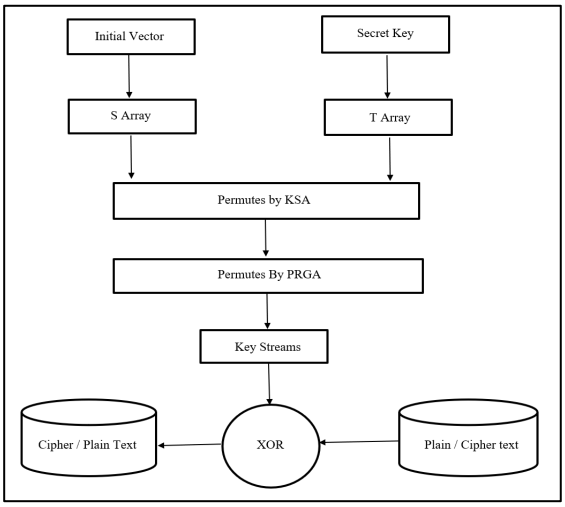


**FIGURE1**

## B. ARNOLD’S CHAOTIC MAP

“ACM is one of the chaotic map models that is used to randomize the pixel positions in an image. Mathematically, this concept works by stretching and distorting a square shape and then reassembling it into the same shape. Since it was introduced, ACM has been used to randomize the pixel position of an image so that it does not look the same, which is the same as the confusion technique. ACM does this by scrambling the pixel’s position without changing the value of the pixel itself.” [5]

“Although ACM is a chaotic map, if iterations are repeated many times, the original image may be rearranged because the ACM concept relies on position randomization only. According to researchers, up to 3N iterations may be needed to return to the original image, where N is the dimension of the image Arnold’s cat map is commonly used for image encryption by shuffling the image pixels but, it can be used to encrypt another form of multimedia data.” [5]

## EQUATION USED:

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} X+Y \\ X+2Y \end{bmatrix} \ \% \ n$$

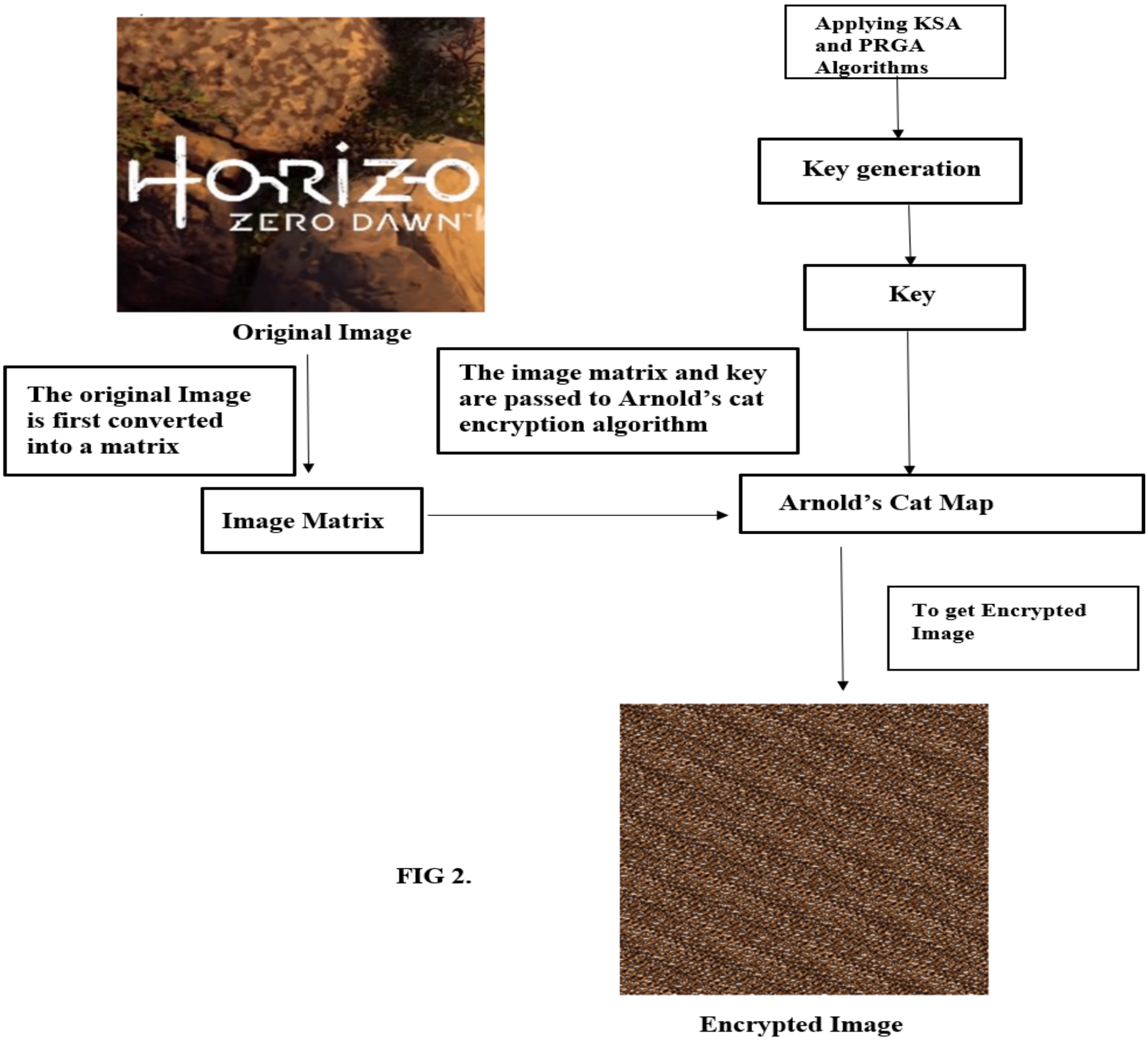

Applying KSA and PRGA Algorithms
Key generation
Key
Original Image
The original Image is first converted into a matrix
The image matrix and key are passed to Arnold’s cat encryption algorithm
Image Matrix
Arnold’s Cat Map
To get Encrypted Image
Encrypted Image

FIG 2.

## III. SIMULTION RESULT

### 1) VISUAL ASSESSMENT

The visual assessment obtained from the proposed scheme for the encrypted images is shown in table 1. Below is the assessment of three images. The three test images are encrypted in such a way that they are not recognizable at all.

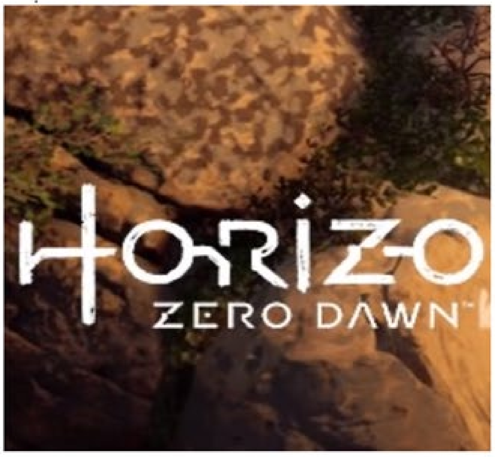
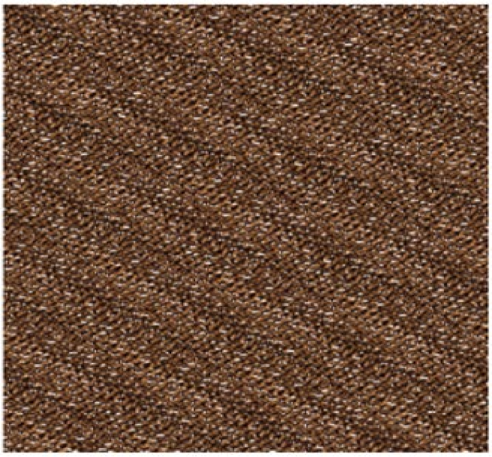
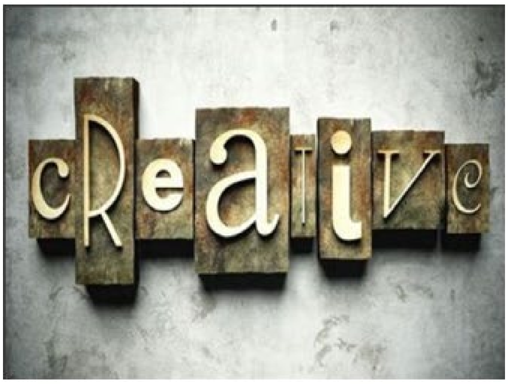
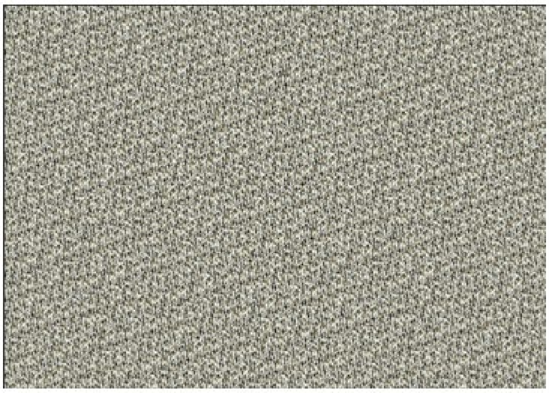
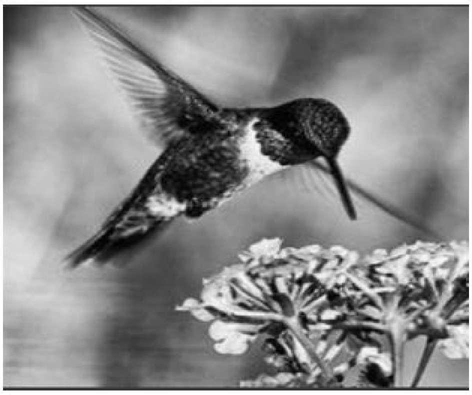
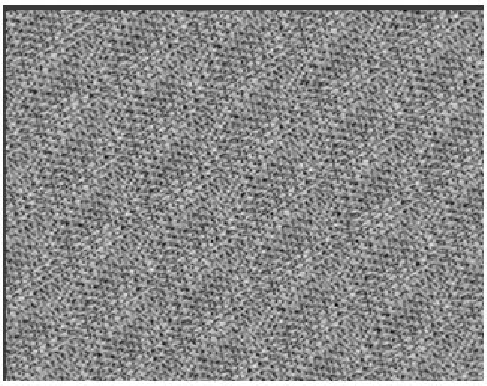
| IMAGE | ORIGINAL IMAGE | ENCRYPTED IMAGE |
|---|---|---|
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |

**TABLE 1**

The text or pictures in the test images are so scrambled that they can't be seen by the naked eye.

Hence, our image's pixel values are distorted which provides high visual security.

## 2) HISTOGRAM ANALYSIS

The graphical depiction of how the image pixels is distributed is called its Histogram.

In the test, encryption is performed with confusion, using Arnold's Chaotic Map. The outcomes can be seen in Table1.

In this Histogram analysis, the histograms of the three test images have been shown in Table 2 with their respective histograms of the encrypted images.

From the test results, we can see that the encrypted images do not exhibit any properties related to the original image as the positions of the pixel have been shuffled. To convert the images into square new pixel values has been combined and the colour before and after the encryption is same because there is no variation in the pixel value of image.

In terms of pixel distribution, the image before and after the encryption is showing same distribution trends.

Table 2 demonstrates the comparison between histograms of the ciphered images and the original images. It should be noted that they have same distribution trend, but the values of pixels are not same.

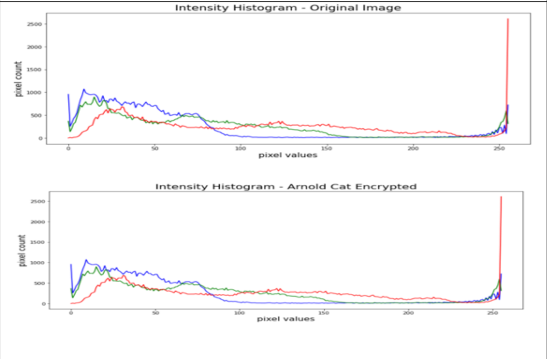
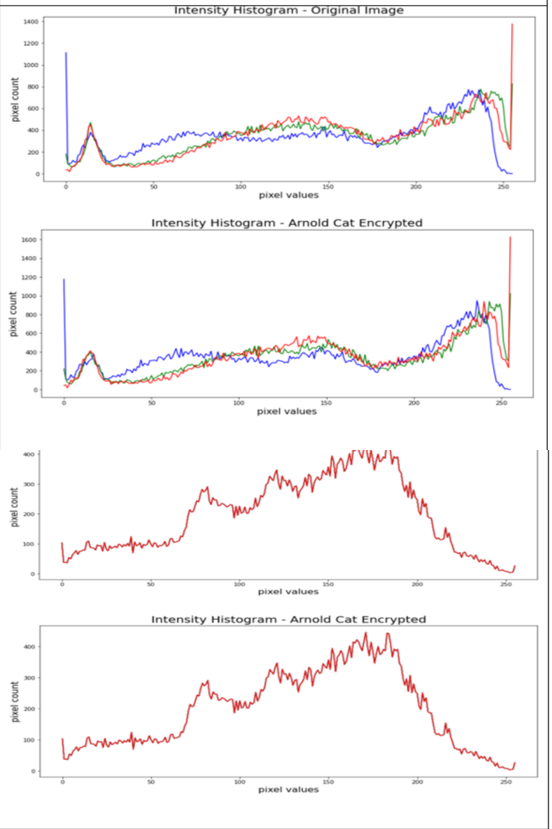
| IMAGE | HISTOGRAM ANALYSIS |
|---|---|
| 1. |  |
| 2. |  |

**TABLE 2: Histogram Analysis**

## 3) CORRELATION COEFFICIENT

A digital image in general has a prominent level of redundancy, and to break this redundancy we have proposed an encryption algorithm. The adjacent pixels of a ciphered image should not have any correlation so to protect against unauthorized attacks. There are horizontal, vertical, and diagonal correlation but we have chosen only horizontal correlation which is shown in table 3.

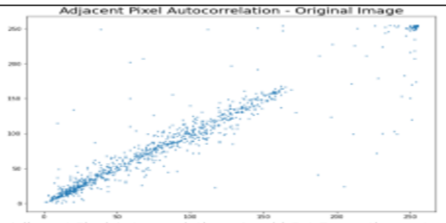
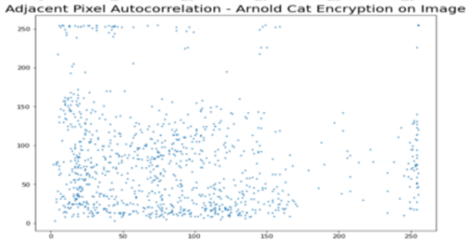
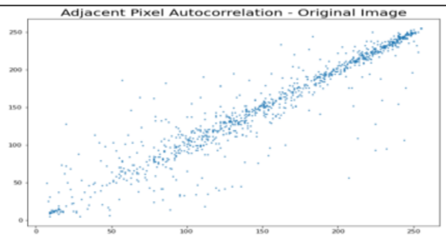
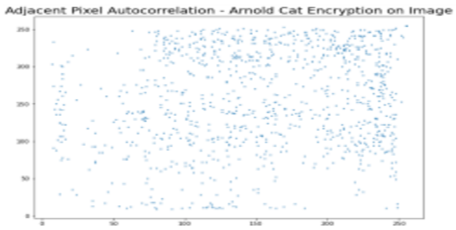
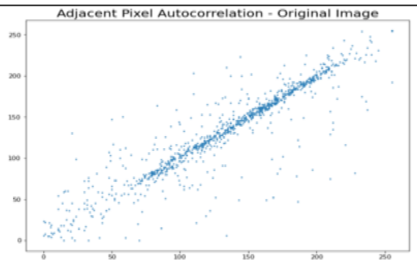
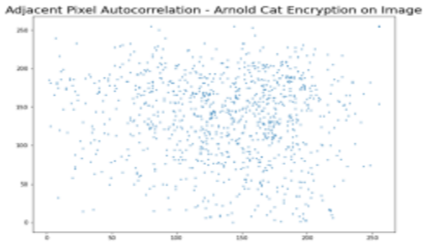
| IMAGE | CORRELATION COEFFICIENT OF ORIGINAL AND ENCRYPTED IMAGE |
|---|---|
| 1. | <br> <br><br> |
| 2. | <br> <br><br> |
| 3. | <br> <br><br> |

**TABLE 3: Correlation Coefficient**

As we can see from table 3 the correlation coefficient of the three test encryption images is so scattered that they are not showing any prominent level of correlation, and nothing can be extracted from the images.

## 4) KEYSPACE ANALYSIS

In our proposed algorithm we have used RC4 to generate the key. RC4 uses two algorithms to produce a keystream that is highly permuted and cannot be easily decrypted. Hence, an unauthorized person cannot detect the key easily.

## 5) ENTROPY ANALYSIS

Entropy analysis measures the degree of even distribution of images before and after the encryption. If degree close to the value 8 then it is more challenging to predict.

**Mathematical Equation:**

$$H(S) = \sum_{i=0}^{N} P(s_i)\log_2 \frac{1}{P(s_i)}$$

Our proposed scheme has entropy value of 7.678 (average) which is remarkably close to the ideal value.

## 6) NPCR (NUMBER OF PIXEL CHANGE RATE)

To test how strong an algorithm is against various differential attacks we use NPCR. It is to be noted that if the value lies above 99% then it said to be a strong algorithm which can withstand any differential attack.

**It is given as:**

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

**where,**

$$D(i,j) = \begin{cases} 0, & A(i,j) = B(i,j) \\ 1, & A(i,j) \neq B(i,j) \end{cases}$$

**and**

**W** and **H** are width and height respectively

We have compared the average NPCR values of different algorithms with our proposed algorithm which is shown in Table 4.

| **Encryption Method** | **NPCR** |
|---|---|
| Proposed | 99.15% |
| “Fractional DCT with chaotic function” [9] | 99.04316% |
| “Dagadu” [8] | 93.12% |
| “Hybrid Chaotic DNA Diffusion” [10] | 99.00129% |
| “fourth order chaotic system” [11] | 99.05127% |

**TABLE 4: Average NPCR values**

It can be seen from the Table 4 that are proposed method is stronger and more stable than the other algorithms.

## III. CONCLUSION:

This report, a cryptography and chaos-based algorithm are used for generating algorithm which can increase the security and authentication of images shared over a network environment. Cryptography technique RC4 has been implemented to generate the keystream for Arnold’s cat map. For Key generation, RC4 is used as it creates a sequence of the pseudo-random 128-bit encryption keys. Here, a chaotic map is used as it provides a good of speed, high-secure complexity, and low computational overheads.

We have performed various statistical analyses for our proposed algorithm, and it is concluded from the results that our encrypted images do not show any closeness to their original images.

The proposed algorithm is further evaluated by various parameters like NCPR and Information entropy analysis which have the average values of 7.678 and 99.15% respectively which is close to their ideal values.

Hence our system provides high security against various attacks also.

## REFERENCES

[1]. Manish Mishra, Shraddha Pandit “Image Encryption Technique Based on Chaotic System and Hash Function” 2014 IEEE International Conference (ICCCS '14), Feb 20-21, 2014, Chennai, INDIA.

[2]. Assist. Let. May H. Abood “An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms” Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017) 7 - 9 March 2017.

[3]. Sara Sajasi, Amir-Masoud Eftekhari-Moghadam “A high-quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method”

[4]. Geetanjali N. Narhare, Savita R. Bhosale “DATA HIDING USING RC4 ALGORITHM IN IMAGE FORM”.

[5]. Anak Agung Putri Ratna, *, Frenzel Timothy Surya, Diyanatul Husna, I Ketut

Eddy Purnama, Ingrid Nurtanio, Afif Nurul Hidayati, Mauridhi Hery Purnomo, Supeno Mardi Susiki Nugroho, Reza Fuad Rachmadi "Chaos-Based Image Encryption Using Arnold's Cat Map Confusion and Henon Map Diffusion"

[6]. S. Fadhel Hamood, M.S. Mohd Rahim, O. Farook Mohammad, "Chaos image encryption methods: A survey study,"

[7]. L. Kocarev, "Chaos-based cryptography: A brief overview," 6–21, 2001, doi:10.1109/7384.963463.

[8]. J. C. Dagadu, J. Li, E. O. Aboagye and X. Ge, "Chaotic Medical Image Encryption Based on Arnold Transformation and Pseudorandomly Enhanced Logistic Map.

[9]. KUMAR, Sumit; PANNA, Bhaskar; JHA, Rajib Kumar. "Medical image encryption using fractional discrete cosine transform with chaotic function.

[10]. DAGADU, Joshua C.; LI, Jian-Ping; ABOAGYE, Emelia O. "Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion.

[11]. LIU, Jizhao, et al. "A novel fourth-order chaotic system and its algorithm for medical image encryption.