Abstract: How to ensure the security of digital image is a difficult and hot problem. In the proposed system we are going to use a new image encryption algorithm which is based on Multi-Dimensional Chaotic System and Pixel Location. The multi-dimensional chaotic function called Rossler Attractor [2], [5] is used to improve the encryption process, to increase the complexity of the encryption keys and to decrease the computational complexity of the cipher image. Rossler attractor is the attractor with the three nonlinear ordinary differential equations. The three encryption keys are used as input for the Rossler attractor. The algorithm used here consists of two scrambling methods and two replacement methods, in which value of each image pixel is replaced by using XORing operation [3] with the help of row and column indices. The position of each image pixel is changed by using shuffling approaches. 3-planes chaotic function is used to scramble the pixels position. In first method X, Y planes of the Rossler Attractor is used and in the second method X, Y, and Z planes are used. Analysis of the algorithms shows that the key space is equal to $10^6$ as the key space is equal to $10^{15}$ for each of the three encryption keys. The algorithm used has a high security against different types of attacks with the large space of the encryption keys. The decryption is done in the reverse order.

Keywords: Image Encryption, Pixel Replacement, Position Scrambling, Rossler Attractor.

1. INTRODUCTION

Information Security means Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity. Information security is one of the important issues in the internet. Hence, every user needs to send the information in a secure way. Because of this, the data encryption becomes very important in the internet. Researchers had proposed many methods to encrypt the data such as: RSA, DES, IDEA etc to send the information on a garbage way so the sniffing to these data is unreadable. On another hand, securing the data is not like securing the images since it needs special methods and special rules.

One of the most important theories is Chaos theory that is used in the new image encryption systems. The chaos was used in the encryption system because of its characteristics, like sensitivity to the initial conditions and unpredictability to chaos sequences.

The rest of the paper is organized as follows: Section 2 provides an overview of the related work. Section 3 gives the details of the domain analysis. Section 4 elaborates the need of the proposed system. Section 5 deals with the system features and gives the details for each. Section 6 gives the details of the working principle of the system. The experimental results are shown in Section 7. Finally, we give concluding remarks in Section 8.

2. RELATED WORK

There are many suggested models to represent the chaos by using the mathematical models such as:

Henon Map:

The Henon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. For the canonical map, an initial point of the plane will either approach a set of points known as the Henon strange attractor, or diverge to infinity. The Hénon attractor is a fractal, smooth in one direction and a Cantor set in another. Numerical estimates yield a correlation dimension of $1.25 \pm 0.02$ and a Hausdorff dimension of $1.261 \pm 0.003$ for the attractor of the canonical map.

Lorenz Attractor:

A Lorenz attractor is a strange attractor in the form of a two-lobed figure formed by a trajectory that spirals around the two lobes, passing randomly between them. The Lorenz attractor, named for Edward N. Lorenz, is a fractal structure corresponding to the long-term behavior of the Lorenz oscillator. The Lorenz oscillator is a 3-dimensional dynamical system that exhibits chaotic flow, noted for its lemniscates shape.

It is a butterfly-shaped strange attractor. It came from a meteorological model developed by Edward Lorenz with three equations and three variables. It was one of the first strange attractors studied.
Logistic Map:

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. Logistic Map [2] the simplest chaotic system that works in discrete time and is defined by the map \( x(t) = 4r x(t) (1-x(t)) \).

3. Domain Analysis

3.1 Object-oriented programming (OOP):

Object-oriented programming (OOP) is a programming paradigm using "objects" – data structures consisting of data field and methods together with their interactions – to design applications and computer programs. Programming techniques may include features such as data structure, encapsulation, messaging, modularity, polymorphism and inheritance. Many modern programming languages now support OOP, at least as an option.

We can use exceptions to improve error handling. These allow us to separate errors from what the main intent of the program is. When you write code to list objects in an array, checking for null or invalid numbers may not be its primary purpose. With exception handling, we can separate the error handling from the really important thrust of the program. Clearer code makes maintenance, and future improvements, easier.

3.2 Image Processing (IP):

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them.

It is among rapidly growing technologies today, with its applications in various aspects of a business. Image Processing forms core research area within engineering and computer science disciplines too.

Image processing basically includes the following three steps:

- Importing the image with optical scanner or by digital photography.
- Analyzing and manipulating the image which includes data compression and image enhancement and spotting patterns that are not to human eyes like satellite photographs.
- Output is the last stage in which result can be altered image or report that is based on image analysis.

The purpose of image processing is divided into following 5 groups:

- Visualization: Observe the objects that are not visible.
- Image sharpening and restoration: To create a better image.
- Image retrieval: Seek for the image of interest.
- Measurement of pattern: Measures various objects in an image.
- Image Recognition: Distinguish the objects in an image.

4. Need Of System

Information security is one of the important issues. Hence every user needs to send the information in secure way. Securing the data is not like securing the images since it needs special methods and special rules. It provides high security against different types of attacks such as brute force attack with large space of keys. Algorithm reduces computational time and enhances encryption rate.

By using Rossler Chaotic function we have encrypted as well as decrypted the image by increasing the key space. It uses two shuffling methods and two replacement methods. The key space of our algorithm is equal to 10^{45}. Our algorithm is strong against different types of attacks and it is sensitive to initial conditions.

5. System Features

The system provides a wide variety of features focusing on the security aspect via Encryption and Decryption of Digital image.

5.1 Resistance to brute force attacks:

In cryptography, a brute-force attack, or exhaustive key search, is a cryptanalytic attack that can, in theory, be used against any encrypted data. Such an attack might be utilized when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier. It consists of systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space.

5.2 Resistance to Entropy attacks:

In computing, entropy is the randomness collected by an operating system or application for use in cryptography or other uses that require random data. This randomness is often collected from hardware sources, either pre-existing ones such as mouse movements or specially provided randomness generators.
5.3 Increased Key Space Value:

In cryptography, an algorithm’s key space refers to the set of all possible keys that can be used to initialize it. To avoid adversaries from guessing the key using a brute-force attack, the key space is usually designed to be extremely large. Another desirable attribute is that the key space be flat, having no or very few weak keys. If the key was selected randomly from all possible keys, on average half the key space must be searched to find the solution.

5.4 Sensitive to Initial conditions:

Small differences in initial conditions (such as those due to rounding errors in numerical computation) yield widely diverging outcomes for such dynamical systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable.

6. WORKING PRINCIPLE

Any image encryption system is mainly divided into two methods: pixel replacement and pixel scrambling method [1]. In this system a new image encryption algorithm is used. This algorithm is based on multidimensional chaotic system and Pixel location. The multidimensional chaotic function used is Rossler Attractor.

The algorithm consists of two scrambling methods and two replacement methods. In which each value in the image will be replaced by using a XORing operation [3] with its location and change its location by using two shuffling approaches. 3-palnes chaotic function is used to scramble the pixel positions. Following diagram fig. 6.1 shows flow of algorithm.

To change the pixel value i, j indices are used, where, the columns indices are used first then rows indices are used. In scrambling approach the X-plane and Y-plane were used; to change the location of the pixels, after the first replacement method. Then, the second scrambling approach that depends on Z, Y, X from the Rossler equation will be used after the second replacement method from the Rossler function (as shown in diagram.).

However, the decryption process is done in the reverse order. Decryption is done in reverse order. We have used same methods to perform decryption process in the following order:

- Second Scrambling.
- Row Replacement.
- First Scrambling.
- Column replacement.

Input for decryption process is an encrypted image generated by the system. For decrypting any of the encrypted images, we have used same keys that were used previously during encryption process. On selected input image, firstly we have applied second scrambling approach where image pixels will change their positions. The values of the pixels of this resultant shuffled image will be changed in row replacement method. After that first scrambling approach is applied on this once shuffled and replaced image. The resultant image after the first replacement will then go through column replacement method. We have used symmetric keys for this whole process. Thus the algorithm is sensitive to initial conditions and is strong against different types of attacks.

The key space for the algorithm is equal to $10^{45}$. 

![Figure 1: Encryption Algorithm Diagram](image1)

![Figure 2: Decryption Algorithm Diagram](image2)
7. EXPERIMENTAL ANALYSIS

7.1 PSNR Calculation:

Peak Signal-to-Noise Ratio is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression.

PSNR for Gray scale images is calculated as:

\[
PSNR = 20(\log_{10}(MAX)) - 10(\log_{10}(MSE))
\]

(1)

Where,

\( MAX \) is the maximum possible pixel value of the image. MSE (MEAN SQUARED ERROR) is defined as:

\[
MSE = \frac{1}{m\times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (I(i,j) - K(i,j))^2
\]

(2)

Where, \( I \) is a given noise-free original image of size \( m \times n \) and \( K \) is its noisy approximation. \( I(i,j) \) represents the \( (i,j) \)th pixel of the Original Image \( I \). For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. The PSNR for colored images is defined as:

\[
PSNR = 10 \left( \log_{10} \left( \frac{MAX}{3} \right) \right)
\]

(3)

7.2 Processing time for Encryption:

We have calculated the processing time for Encryption of the input image (Original Image). This includes the processing time required by Rossler chaotic function, Pre-processor, two replacement methods and two scrambling methods.

7.3 Processing time for Decryption:

We have calculated the processing time for Decryption of the Encrypted Image. This includes the processing time required by Rossler chaotic function, Pre-processor, two replacement methods and two scrambling methods.

7.4 Results:

The figures below show some experimental results:

![Figure 3: Analysis for Chrysanthemum Image](image)

![Figure 4: Analysis for Desert Image](image)

![Figure 5: Analysis for Jellyfish Image](image)

We have calculated PSNR values, Encryption and Decryption time required for the above images. These analysis results are shown in table below:

<table>
<thead>
<tr>
<th>Image</th>
<th>Encryption Time</th>
<th>Decryption Time</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrysanthemum</td>
<td>19.56sec</td>
<td>18.2sec</td>
<td>28.12</td>
</tr>
<tr>
<td>Desert</td>
<td>15.32sec</td>
<td>16.23sec</td>
<td>27.33</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>14.92sec</td>
<td>15.99sec</td>
<td>25.59</td>
</tr>
</tbody>
</table>

8. CONCLUSION

A new approach to encrypt the image by using a Rossler chaotic function and the row and column indices is used, in which the algorithm used consists of two replacement methods and two scrambling methods. In the first replacement method column index values are used and in the second replacement method row index values are used. The order to encrypt the image by using our algorithm is as follows: first replacement method, first shuffling method, second replacement method and second shuffling method. Our system provides high security against different types of attacks with the large space of the encryption keys.

9. REFERENCES


AUTHORS

Ashwini Shirish Shinkar, COMPUTER Department, K. K. Wagh Institute of Engineering and Education Research, Amrutdham, Panchavti, Nashik, Maharashtra, India.

Kshanika Hukumchandra Dashore, COMPUTER Department, K. K. Wagh Institute of Engineering and Education Research, Amrutdham, Panchavti, Nashik, Maharashtra, India.

Shweta Ajay Majgaonkar, COMPUTER Department, K. K. Wagh Institute of Engineering and Education Research, Amrutdham, Panchavti, Nashik, Maharashtra, India.

Smita Devkisn Fokane COMPUTER Department, K. K. Wagh Institute of Engineering and Education Research, Amrutdham, Panchavti, Nashik, Maharashtra, India.