Data Hiding in Image Encryption by using Logistic Mapping Algorithm
Aiswaryapradeep¹, D Vinotha²
B.Tech Scholar, Assistant Professor²
Department of CSE
PRIST University, Tamilnadu, India

Abstract:
System is dependent on system sites or internet for sharing data from one user to another, from one place to another. It is very effective and easy for transferring information but it is very complex in terms of providing security. There are many algorithms which are being used to provide security in text and images. In this paper system study many cryptographic algorithms which are based on different parameters, like public key, private key cryptography and different images. But all existing algorithms have some advantage and disadvantage. On the basis of existing methods system will develop a strong cryptography technique that will be very effective in terms of time and security. A new cryptographic approach for images is proposed here in this paper. Here logistic function one of the methods of logistic mapping is used for encryption and decryption along with XOR function. Here system uses 4 steps of encryption and decryption process.

1. INTRODUCTION

The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging, telemedicine and military communication, etc. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information. Encryption will be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read. Encryption of data has become an important way to protect data resources especially on the internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources. In last couple of years, the concept of chaos system has blew the researcher’s mind in the direction of cryptography. Cryptography is a technique of protecting confidential data by converting original data into an unreadable format known as cipher text and then recovering it back in its original form. In this process original message is transformed into garbage message. So that there is a restriction for unauthorized people. Many researchers have projected a number of different encryption techniques to provide the discretion of the message which can be text, data, and image. Nowadays the need grows to securely outsource data to an entrusted system think for instance of a remote database server administrator by somebody else if you want your data to be secret you have to encrypt it. It is desirable to store data on data storage service and file service in encrypted form to reduce security and privacy risks. But it is usually implies that one has to sacrifice functionality for security. For example if a client wishes to retrieve only documents containing certain words it was not previously data storage server from the search and system the query without loss of data confidentiality.

2. PROPOSED SYSTEM

2.1. RETRIVAL INFORMATION

There are two secret keys are used for encryption and decryption of information which we input it to. One for cover image and other for data. At first the image is input and then it is encrypted the image we input it by using a secret key. For encrypting image we used 2 processes by using different variables. Values in the image get shuffled within itself in a row wise and column wise manner. Therefore there will be no loss of image confidentiality. So in this way the image is highly secure. After process 1 and process 2 completes the main operational image will be displayed with grains in encrypted format. For embedding the data the password is also entered in a specified length. This password length and details are as per the sender’s choice. Now the data to be hidden is specified in a bit wise format. For embedding the image get shuffled in a row wise and column wise manner. Therefore the data get shuffled within the image itself and as a result there will be no loss of data. After the embedded process, data will embed to the encrypted image with all the specified queries. Then for decryption process, first we need to decrypt the data from the image so by optional queries the receiver gets the idea for decrypting. For decrypt the data, when the receiver enters the password the system checks if it matches with the predefined password which is already entered by the sender. Now only if the password format and length matches it approves the authentication. Once the password that the user entered is confirmed then the data can be viewed by the
user. This data in the already encrypted image is displayed in the separate window or dialogue box. Therefore, after decryption the receiver gets the original image without any loss of data and without any compromising quality. This method of encryption and decryption helps in to handle the transfer of data with high security and confidentiality. Then for decrypting image same process need to do. When the receiver enters the password the system checks if it matches with the predefined password which is already entered by the sender. Now only if the password format and length matches it approves the authentication. Once the password that the user entered is confirm then the image can be viewed by the user. So the final image that they view is of high quality and without any loss of data. This is because the psnr and rmse value of high quality. The image that appears is in the original size. The encryption the original image is 128 pixel and we resized to double size that is 256 pixel. After the decryption process the original image that we view is of 128 bits which is reshuffled from the previous 256 pixel. Final decrypt image is of high psnr and rmse value and hence which of high quality and original image is restored. Because of this high quality process we receive the original image without any loss packets and can assure is of good quality.

**ALGORITHM**

- The algorithm procedure of performing image encryption is given as follows

**Step 1**
We defines PMT as a table that contains Pixel values from 0-255 in the shuffled order with the size 256x1

**Step 2**
One dimensional logistic system with x output and i/p variable and two initial conditions x0 and λ

\[ X_{n+1} = \lambda X_n(1 - X_n) \] ..........1

\[ \lambda \in [0,4] \text{ , } x \in [0,1] \text{ when } \lambda \in [357,4] \]

**Step 3**
We replace the Pixel value by using PMTI. So the current Pixel is the same after and before the replacement.

\[ \text{Index} = \text{mod}((\text{pixel}(i,j) + \text{shift}), \text{pixel} \_\text{level}) \] ..........2

\[ \text{Pixel}(i,j) = \text{PMTI}(\text{index}) \] ..........3

\[ \text{Shift} = C \ast \text{random(} \logistic \) \] ..........4

**Step 4**
To increase the in certainty of the cipher image the column replacement and the replacement are used.

\[ \text{Column} = \text{XOR} (\text{PMT2 ; column}) \] ..........5

\[ \text{Row} = \text{XOR} (\text{PMT2 ; ROW}) \] ..........6

2.2. GOALS OF PROPOSED SYSTEM

**a. Authentication:** This process provides the assurance that the communicating entity is the one that it claims to be. It means that, a message has not been modified while in transit (data integrity) and that the receiving party can verify the source of the message.

**b. Secrecy or Confidentiality:** Confidentiality refers to the relationship between two or more persons in which the information communicated between them is to be kept in confidence. It means that, the authenticated users are able to interpret the message content and no one else

d. **Non-Repudiation:** It is a process of guaranteeing message transmission that provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

e. **Availability and Service Reliability:** Availability refers to the ability of a user to access information or resources

**Image Preprocessing**

At first input the data which consist of images and data on which the further activities are done. The system first reads the image. Suppose the image is in colour then it need to convert it into grey scale for to obtain security and then convert it into bitwise order. The data length must be greater than 8 bit only then it is easy to process the data as part of this the original data is in 128x128 pixel. If we encrypt it in this way some of the images will be missing. That’s why the image should be resize to double f If we do in this manner it is helpful in further processing
2.3 Encrypting image

Process of converting information or data into a code, especially to prevent unauthorized access

This encryption method is used only to encrypt the images. Here we are using logistic algorithm. The logistic map is one dimensional chaotic system, with X output and input variable and two initial conditions X0 and λ as follows:

\[ X_{n+1} = \lambda X_n (1 - X_n) \]

There are two processes used here for encrypting the image from the input.

**PROCESS 1**

In this step, the system asks the sender to enter the password for encrypting the image. The sender can use any valid password to set it for encryption. If the user enters an incorrect input as password then an error message appears. Two variables are declared as a0 and x0. In these variables the values are to be entered. These values define the length of image to be encrypted. Further the image is resized. Which means that the original image which is in size f is resized into double f? The image is saved into variable name f1 which can be used for further purpose. Along with f image a0 and xo values are also entered. Due to the resizing of the image, the receiver gets the exact image which was sent without any loss of values in the image. Thus the image quality and confidentiality can be maintained. After the first process the operational image is shown with the title. This image appears with some grains that signifies beginning of encryption process.

**PROCESS 2**

In process 2 the same procedure as in step 1 is followed but with some changes occurs. Here two variables are declared as a1 and x1 instead of a0 and x0 which was used in process 1. In the previous process a0 and x0 values and images are saved in f1. Now in process two the f1 in which a1 and x1 are entered are then saved into f2 variable. Values in the image get shuffled within the image itself and as a result there will be no loss of data. Final data that will be received is highly secure and confidentiality will be maintained. If the length of the data is greater than the image size, that means if the image size is greater than the predefined length of the data and the error appears according to the data length. If everything is entered correctly then the process continues. Then the next process is embedded data is placed into the image that we already encrypted. There are some queries that appears on the screen before embedding the data into then encrypted image.
At first it asks for the password to embed the data we can use any length or pattern of password as per our choice. The optional query is whether we need to extract the data or not, this is how the process will work. If it is yes, it request for the password to carry out the encryption. Once the password is entered it then checks it is of the predefined length. If we opt no from the option then it ask for the next step. After the embedded process, data will embedded to the encrypted image With all the specified queries

**DATA FLOW:**

![Data Flow Diagram](image)

2.5 **DECRYPTING DATA**

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys. Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a decryption passcode or key is not available, special software may be needed to decrypt the data using algorithms to crack the decryption and make the data readable. Before decrypting the data the following queries are asked. On the basis of this only the decryption process can be carried out. The first query is asked is whether to decrypt the data or decrypt the image. If the user answer is yes then the data is decrypted or else image is decrypted. The next query is asked to enter the predefined password data extraction which the already specified by the sender. Which the sender informs the receiver through mails or any other sources. When the receiver enters the password the system checks if it matches with the predefined password which is already entered by the sender. Now only if the password format and length matches it approves the authentication. Once the password that the user entered is confirm then the data can be viewed by the user. This data in the already encrypted image is displayed the separate window or dialogue box. Along with this the details of the data can be shown or displayed at the bottom of the working screen. Details are such as how many bits were taken to hidden the data in the image, space availability; characters are shown in the screen. Therefore, after decryption the receiver gets the original image without any loss of data and without any compromising quality. This method of encryption and decryption helps in to handle the transfer of data with high security and confidentiality.
2.6 IMAGE DECRYPTION

As announced in the problem outline, the subject of this year's problem is to compute the original from a given encrypted digital image. More specifically, you are given image data, consisting of $256 \times 256$ black(0)/white(1) pixels encrypted one by one, and your task is to decode this to get its original image. For example, given a figure of the left one below, you are asked to obtain the right one, by decrypting at each pixel.

Since the decryption is extremely difficult, we will provide some additional information to help decryption after the data decryption next is to do image decryption. The image decryption process is starts with asking a query to enter the predefined password for image extraction which the already specified by the sender. Which the sender informs the receiver through mails or any other sources. When the receiver enters the password the system checks if it matches with the predefined password which is already entered by the sender. Now only if the password format and length matches it approves the authentication. Once the password that the user entered is confirmed then the image can be viewed by the user. If the password is wrong then error message is appears. From this the user has to understand that the user enter the password with something wrong in it. So user can able correct it out. If entered password is correct then the receiver can view the image. So the final image that they views is of high quality and without any loss of data. This is because the psnr and rmse value of high quality. The psnr Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The root-mean-square deviation (RMSD) or root-mean-square error (RMSE) is a frequently used measure of the differences between values (sample and population values) predicted by a model or an estimator and the values actually observed. The image that appears is in the original size. The encryption the original image is 128 pixel and we resized to double size that is 256 pixel. After the decryption process the original image that we view is of 128 bits which is reshuffled from the previous 256 pixel. Final decrypt image is of high psnr and rmse value and hence which of high quality and original image is restored. Because of this high quality process we receive the original image without any loss packets and can assure is of good quality.

Since the decryption is extremely difficult, we will provide some additional information to help decryption after the data decryption next is to do image decryption. The image decryption process is starts with asking a query to enter the predefined password for image extraction which the already specified by the sender. Which the sender informs the receiver through mails or any other sources. When the receiver enters the password the system checks if it matches with the predefined password which is already entered by the sender. Now only if the password format and length matches it approves the authentication. Once the password that the user entered is confirmed then the image can be viewed by the user. If the password is wrong then error message is appears. From this the user has to understand that the user enter the password with something wrong in it. So user can able correct it out. If entered password is correct then the receiver can view the image. So the final image that they views is of high quality and without any loss of data. This is because the psnr and rmse value of high quality. The psnr Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. The root-mean-square deviation (RMSD) or root-mean-square error (RMSE) is a frequently used measure of the differences between values (sample and population values) predicted by a model or an estimator and the values actually observed. The image that appears is in the original size. The encryption the original image is 128 pixel and we resized to double size that is 256 pixel. After the decryption process the original image that we view is of 128 bits which is reshuffled from the previous 256 pixel. Final decrypt image is of high psnr and rmse value and hence which of high quality and original image is restored. Because of this high quality process we receive the original image without any loss packets and can assure is of good quality.

3. RESULT AND DISCUSSION

In this proposed work the Logistic map has been used. To demonstrate the efficiency of the algorithm, the results of various tested images is shown below. It is found that this new scheme has a satisfactory security level with low computational complexity, and hence fast, which proves to be a good candidate for secure image transmission.

Key Sensitivity: A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decryption process may results into a completely different output image. Our proposed encryption algorithm is sensitive to a very small change in the secret keys. If we change a little in any of the initial conditions then the decrypted image is completely different and in un-understandable form.

Key Space: Key space is the total number of different keys that can be used in the cryptographic system. A cryptographic system should be sensitive to all secret keys. There are total four initial conditions logistic map used in the algorithm. All these four initial conditions are used as secret keys of encryption and decryption. In this situation, the precision of each key , the key space size is which is extensively large enough to resist the exhaustive attack. Many attacks can be done which are based on the statistical analysis. Statistical analysis has been performed on the test images to demonstrate the bad correlation among the
pixels of the encrypted images. The following test have been performed like PSNR, RMSE Information entropy and Correlation coefficient. The results shown below shows that there is negligible correlation between pixels of the encrypted image in comparison to original image. Root Mean Squared Error is the average squared difference between original input image and a encrypted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total number of pixel. Peak Signal-to-Noise Ratio is the ratio between the original image and the encrypted image. PSNR is. The higher the PSNR, the closer the encrypted image is to the original. In general, a higher PSNR value should correlate to a higher quality image. For good encryption scheme the PSNR should be as low as possible. An ideal image encryption procedure should be sensitive with respect to secret key. The change of a single bit in the secret key should produce a completely different encrypted image. High key sensitivity is required by secure image, which means the cipher image cannot be decrypted correctly even if there is only a small difference between the encryption and decryption keys.

4. CONCLUSION

In order to provide security to the image, Logistic mapping is used which converts an image into another form (non readable form). This has many applications in image processing such as image and data encryption. This proposed system which two secret key and high quality result may provide security of high level.

The proposed algorithm has following merits:
  o The algorithm has a large enough key space to resist all kinds of brute force attack.
  o The cipher-image has a good statistical property
  o The encryption algorithm is very sensitive to the secret keys.
  o provides high security level
  o less computational time
  o Both reliable and efficient way to deal with balky, difficult and intractable data
  o Main merit is that in the proposed system the final image is of high quality this is because the psnr and rmse values used in encryption.

The experimental results show that our algorithm is with high security, and can be competitive with some other proposed image encryption algorithms.

5. FUTURE ENHANCEMENT

The future of encryption is brighter than ever before. The demand for more control and protection of corporation information assets and third-party information is increasing dramatically. The amount of information being communicated and stored electronically is vastly greater than even five years ago. As a result, the need for more effective information security products is growing at a higher rate than any other aspect of IT technology within the enterprise today. The Internet and the mobility of its users have removed the perimeters of communication. Encryption is the last line of defense for the modern day enterprise.