CHAOTIC BASED IMAGE ENCRYPTION

Mukta Pujar
M.Tech II SEM (CSE)
Computer Science Department of Engineering
University B.D.T. College of Engineering, Davanagere, Karnataka, India
(A Constituent College of Visvesvaraya Technological University, Belagavi)

Mohammed Rafi
Professor
Computer Science Department of Engineering
University B.D.T. College of Engineering, Davanagere, Karnataka, India
(A Constituent College of Visvesvaraya Technological University, Belagavi)

Abstract: In recent years chaos and Cryptography have suggested some new and efficient way to develop secure image encryption techniques.chaotic based image encryption is developedwith an objective was to provide an Image Encryption mechanism which provides high security level, less computational time and power in reliable and efficient way to deal with balky, difficult and intractable data. Chaotic based image encryption scheme are easy to implement, faster encryption speed and strong against attacks. Non-repudiation and Encrypt the message with the private key of the sender.To analyze the confidentiality, integrity of the transmitting video or image data.

Key-words: Encryption,Cryptography, Chaotic System, Logistic map.

I. INTRODUCTION

Huge amounts of digital multimedia data such as text,image, video etc are exchanged over various sorts of networksnowadays. These multimedia data contain private orconfidential information which may cause high risk. Thesecurity techniques play a significant role in maintainingprivacy, integrity or authentication of multimedia data fromunauthorized users. From past few decades encryptiontechniques are used to protect the multimedia data fromunauthorized users by transforming into other form usingsuitable key. The chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryptiontechniques. In this communication,we propose a newapproach for image encryption based on chaotic logistic maps in order tomeet the requirements ofthe secure image transfer. In the proposed image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. Theinitial conditions for the both logistic maps are derived using the external secret key by providing different weight age to all its bits. Further, in theproposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for aparticular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified afterencrypting each block of sixteen pixels of the image. The results of several experimental, statistical analysis and key sensitivity tests show

that theproposed image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

II. LITERATURE SURVEY

"Image encryption using chaotic logistic map," Image Vision Compute, Vol. 24, pp. 926-34, Sept. 2006. N. K. Pareek, V. Patidar, and K. K. Sud [1]:says new approach for image encryption based on chaotic logistic maps in order to meet the requirements of the secure image transfer. proposed image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weightage to all its bits. Further, in the proposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map.

"A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons and Fractals, Vol. 32, pp. 1518-29, Apr. 2007.

"A new image encryption algorithm based on hyper-chaos," Phys. Lett. A, Vol. 372, pp. 394-400, Apr. 2008.T. Gao, Q. Gu, and Z. Chen, [2][3]: says

new image encryption scheme, which employs an image total shuffling matrix to shuffle the positions of image pixels and then uses a hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image. The experimental results demonstrate that the suggested encryption algorithm of image has the advantages of large key space and high security, and moreover, the distribution of grey values of the encrypted y image has a random-like behaviour.

"Multi chaoticsystemsbased pixel shuffle for image encryption," Optical communications, Vol. 282, pp. 2123-7, Feb. 2009.C. K. Huang, and H. H. Nien,[4]: says encrypting colour images using multiple chaotic systems like the Henon, the Lorenz, the Chua, and the Rossler systems. All of which have great encryption performance. The authors claimed that their pixel-chaotic-shuffle (PCS) encryption method has high confidential security. However, the security analysis of the PCS method against the chosen-plaintext attack (CPA) and known-plaintext attack (KPA) performed by Solaket .successfully breaks the PCS encryption scheme without knowing the secret key. In this paper we present an improved shuffling pattern for the plaintext image bits to make the cryptosystem proposed by Huang et al. resistant to chosen-plaintext attack and known-plaintext attack.

"A chaotic block cipher algorithm for image cryptosystems" Commun Nonlinear Sci NumerSimulat, Vol. 15, pp. 3484-97, 2010.M. Amin, O. S. Faragallah, and A. A. El-Latif,[5]: says new chaotic block cipherscheme for image cryptosystems that encrypts block of bits rather than block of pixelsIt encrypts 256-bits of plainimage to 256-bits of cipherimage within eight 32-bit registers.The scheme employs the cryptographic primitive operations and a non-linear transformation function within encryption operation, and adopts round keys for encryption using achaotic system. The new scheme is able to encrypt large size of images with superior performance speed than other schemes. The security analysis of the new scheme confirms ahigh security level and fairly uniform distribution.

"Logistic chaotic maps for binary numbers generations," Chaos, Solitons and Fractals, Vol. 40, pp. 2557-68, 2009.

A. Kanso, and N. Smaoui[5]: says Two pseudorandom binary sequence generators, based on logistic chaotic maps intended for stream cipher applications, are proposed. The first is based on a single one-dimensional logistic map which exhibits random, noise-like properties at given certain parameter values, and the second is based on a combination of two logistic maps. The encryption step proposed in

both algorithms consists of a simple bitwise XOR operation of the plaintext binary sequence with the keystream binary sequence to produce the ciphertext binary sequence.

III. METHODOLOGY

Cryptography

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions making such algorithms hard to break in practice by any adversary. Therefore to prevent multimedia information from none authorized users, cryptography gives an important role for digital content's Security.

Chaotic System

A chaotic system has a noise like behaviour while is exactly deterministic so if we have its parameters and initial values, we can reproduce it. These signals are extremely sensitive to initial conditions. One of the most famous chaotic systems is logistic map. Chaos theory is a field of mathematics and used in several emerging application areas like neurology for EEG analysis, cardiology for embryonic chick heart cells, weather prediction, communication, control and theory of circuits, Direct sequence Code Division Multiple Access system. 'Chaos' means a state of disorder and they are highly sensitive to initial conditions. A small difference in initial conditions yields entirely uncorrelated sequence. Many researchers have shown chaos sequences can be used for encryption of images.

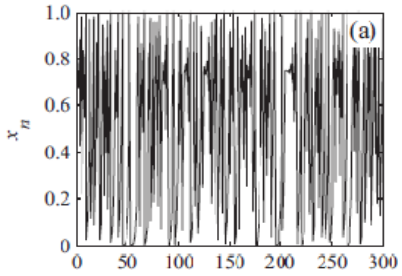
Logistic Map

This method uses the key to enhance security. Two keys say M and N are generated using a logistic map. Then XOR operation is applied to each other and the result is then XOR-ed again with the original image. Logistic map is a function given by equation-2.1 that generates one dimensional non periodic chaotic sequence $\{X_n\}$ where X_n lies between 0 and 1 which are random in nature.Recently, one very simple chaotic map has been studied for cryptography applications is logistic map.Logistic map shown in (2.1) is a discrete chaotic system when the parameter r satisfies $3.57 \leq r \leq 4$. Here, the initial value X_0 and the parameter r are regarded as the secret key.

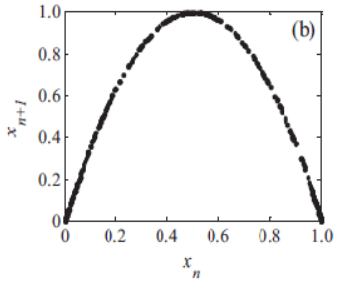
Mathematically, the logistic map is written as

$$X_{n+1}=rX_n(1-X_n) \quad (2.1)$$

Where $X_n$represents the chaoticsequence which liesbetween zero and one as shown in the Figure. Theparameter r is a positive number in the range 0 to 4.As for the initial value X_0 =0.9 and the parameter r=3.86, the 300-point time series and phase portrait areshown in Fig. 2.2, in which the 100 transient points are discarded. From Fig. 2.2, we can see the time sequencegenerated by logistic map has good stochastic property.



(a)



(b)

Fig. 2.2. Logistic map. Frame (a) shows the 300-point time series of logistic map with X_0=0.9 and r=3.86 and Frame, (b) represents the phase portrait of Frame (a)

IV. SYSTEM ARCHITECTURE

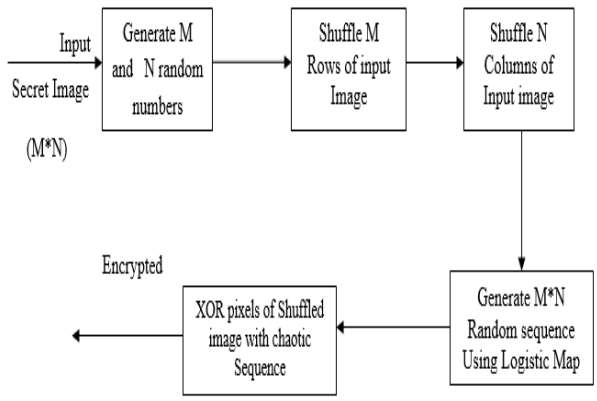
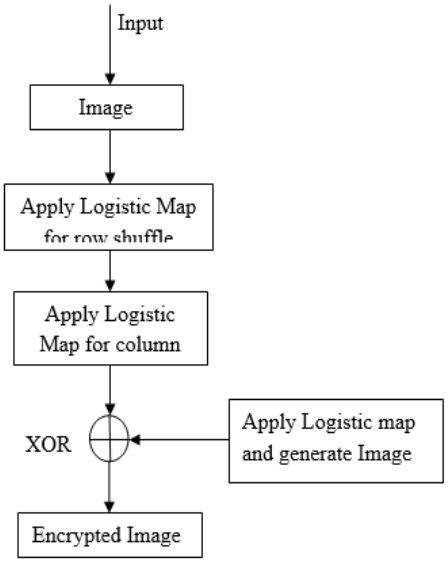


Fig: Block diagram for Chaotic Image Encryption.

In this work, combined approach of key sequences generated by logistic map and with Chaotic sequence is propose .Secrete image can be given as an input of size M*N. Where, M can be considered as Number of rows and N as number of columns. Here, we are going to generate some random numbers to M and N.
Shuffle the input image of rows M and column N using the generated random numbers. After shuffling the input image of rows and column, once again it is going to generate the random sequence number of M*N using Logistic Map. The shuffled input image pixels are XORed with chaotic sequence to get the Encrypted image.
Finally to get the decrypted image all the stages are reversed.

V.ALGORITHM AND FLOW DIAGRAMS

a. Flow Diagram for Encryption Process



Taken input as secret image. First we are Reading an input image and it is going to generate some random values as M for rows and N for column. And we are applying Logistic Map for M generated random values for row shuffle. Similarly, applying logistic map for Column shuffle. Performing an XOR operation between the row and column shuffled image and generated random image for the Encrypted Image.

b. Algorithm for Encryption Process

Steps for Encryption Process:

Input: A Secret or original image**. Output:** Encrypted Image.

Step 1: Read an Input image.

Step 2: Applying Logistic Map to generated random numbers M for row shuffle.

Step 3: Applying Logistic Map to generated random numbers N for column shuffle.

Step 4: Applying Logistic Map to generate random Image and it is XORed with shuffled Image.

Step 5: Output as Encrypted Image.

C. Flow Diagram for Decryption Process

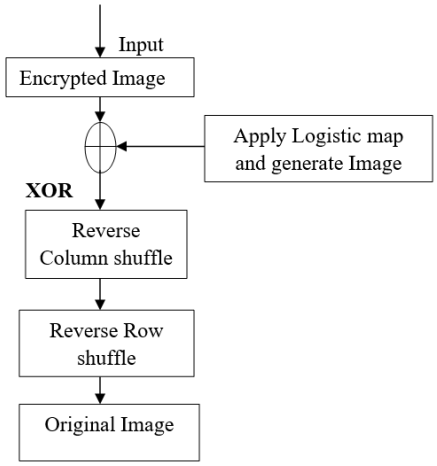


diagram shows the flow chart of Decryption Process. Here, it is exactly reverse order of Encryption process. Taking Encrypted Image as input, we are performing an XOR operation between the Random image and row and column shuffled image. Apply Logistic map for anti-column shuffle and similarly apply logistic map for anti-row shuffle to get an original Image.

d. Algorithm for Decryption Process

Steps for Decryption Process:
Input: An Encrypted image.
Output: An Original Image.
Step 1: Take Encrypted image as Input.
Step 2: Applying Logistic Map to generate random Image and it is XORed with shuffled Image.
Step 3: Reverse Method of encryption, so do anti-column shuffle.
Step 4: Anti-row shuffle.
Step 5: Output as Original Image.

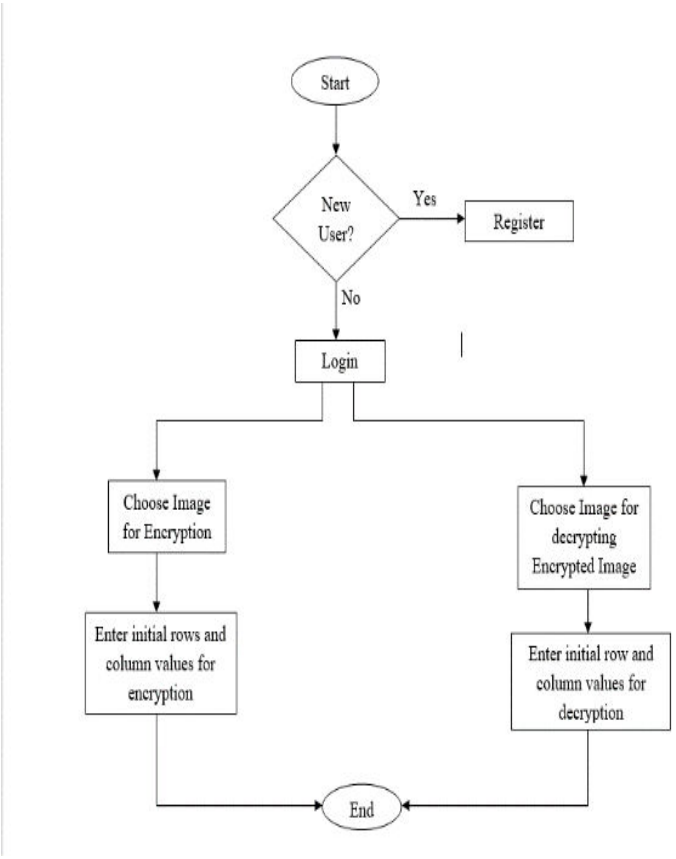
VI IMPLEMENTATION

Algorithm and Flow Diagram for Overall Implementation

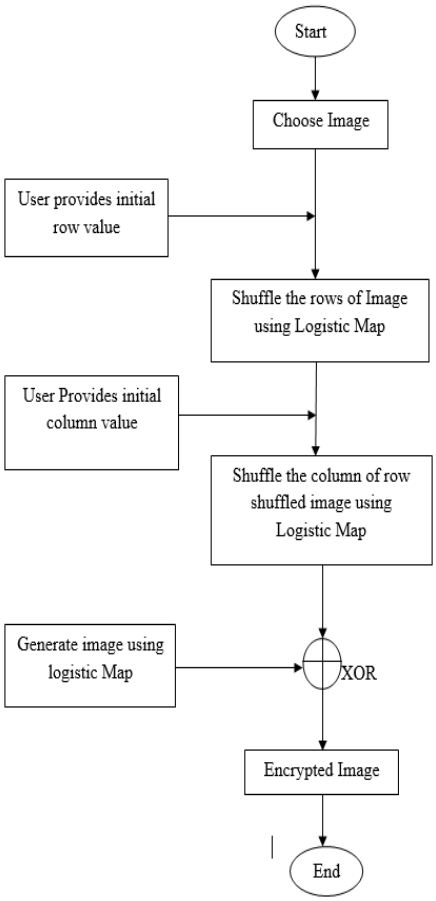
Steps for overall Implementation
Step 1: Start.
Step 2: Asks for New user. If yes, then User must go for Registration. Else if, User has already registered user then can Login directly.
Step 3: User have to choose the Image for the Encryption.
Step 4: After choosing an image, user should enter initial values for row and column for the encryption.
Step 5: Once after done with the encryption, go back and choose the Encrypted image for the decryption.
Step 6: Enter initial values for row and column for decryption.
Step 7: End.

Flow Diagram for Overall Implementation

At first, any new user must register then only he/she can login. If user is new then he must register first. If the user has already registered then he can directly Login. Once after the successful registration and login process, he has to select the image for the Encryption.



. Flow Diagram for Encryption Implementation



Algorithm and Flow Diagram for Encryption Implementation

Steps for EncryptioImplementationStep 1: Start.
Step 2: Select Original Image.
Step 3: User provides initial row value.
Step 4: Shuffle the rows of Image using Logistic Map.
Step 5: User provides initial column value.
Step 6: Shuffle the column of row shuffled Image using Logistic map.
Step 7: Generate random image using logistic map
Step 8: Perform XOR operation Between Random image and original image.
Step 9: End

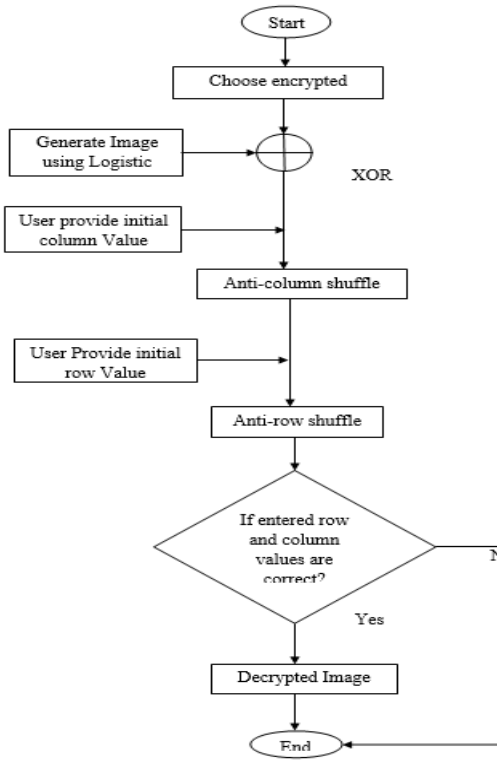
Here, user have choose image first and provide initial values for row and then shuffle the rows of Image using logistic map. And then user has to provide initial values for column shuffle. Shuffle the column of row shuffled image using logistic map and generate the image using Logistic map. Perform the XOR operation between Random Image and Shuffled Image then it gives output as Encrypted Image.

Algorithm and Flow Diagram for Decryption Implementation

Steps for Decryption Implementation:

Step 1: Start.
Step 2: Select the Encrypted Image.
Step 3: Generate random image using logistic map.
Step 4: Perform XOR operation between random image and Encrypted image.
Step 5: User has to provide initial value for column.
Step 6: Reverse column shuffle of reverse XORed image using Logistic map.
Step 7: User has to provide initial value for row.
Step 8: Reverse row shuffle of reverse column shuffle image using Logistic map.
Step 9: If entered row and column values are matches then will get Decrypted Image as output. Else we cannot find the original image.
Step 10: End.

Flow Diagram for Decryption Implementation



Here, first select the Encrypted image and generate Random image using Logistic map and perform XOR operation between random image and shuffled image. User has to provide initial column value for anti-column shuffle and also provide initial row value for anti-row shuffle. If the given initial value of row and column matches then we will get a Decrypted image s Original image. Else if initial values do not match then we cannot find an original image.

VI.RESULTS AND ANALYSIS

Snapshots

Fig. 6.1 Main screen of the project.

- The Fig. 6.1 illustrates the first page which contains the introduction about the project. This page contains the Name of college, Department name, title of the project, the member of the project, project coordinator and the project guide details. It has Login button for the login by user, Register button is for the new

user for their registration and Exit button to exit from the screen.

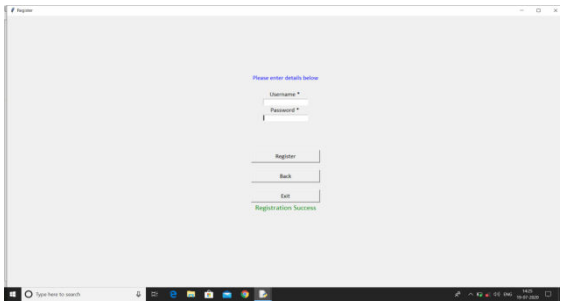


Fig. 6.2 Registration Success.

- This figure 6.2 shows the successful registration by the new user.User can register by giving username and password, and click on the register button. Here, it shows that Registration is success.

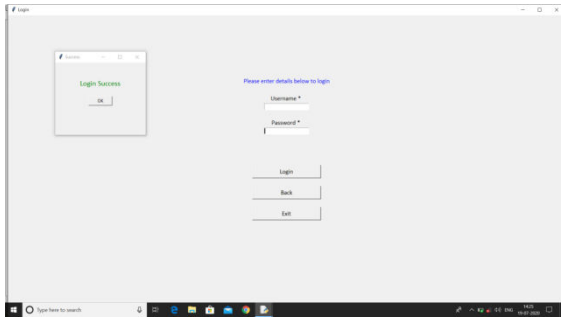


Fig. 6.3 Login success.

- The figure 6.3 shows snapshot of successful Login by the user. Once after the registration done by the user he can directly login by giving their username and password. If the both username and password matches then it shows that login is success.

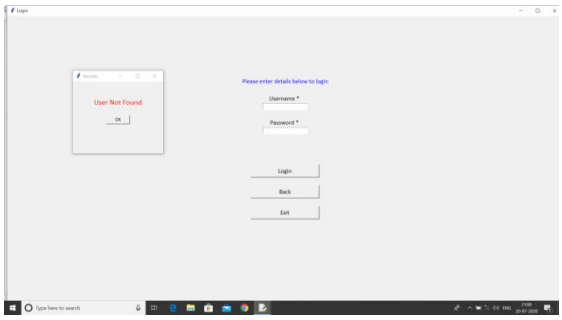


Fig. 6.4 User not found.

- The figure 3.4 shows snapshot of undefined user name. If the given username does not match with the given password then it shows that user is not found

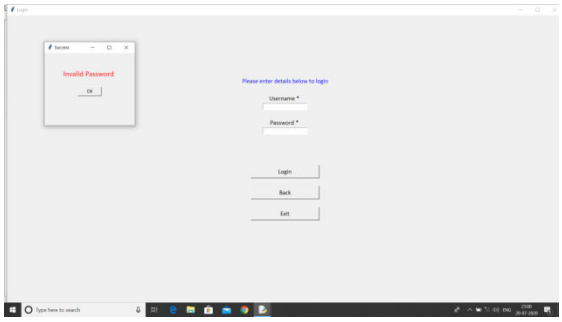


Fig. 6.5 Invalid Password.

- The figure 6.5 shows the snapshot of wrong password given by the user. Password entered by the user does not match with the username then it shows the Invalid Password.

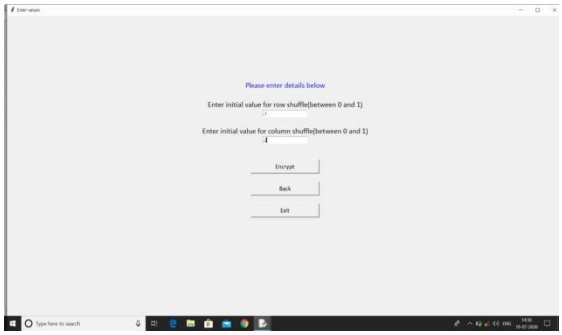


Fig. 6.6 To enter the Values for the Encryption Process.

- The figure 6.6 shows the snapshot for the details to be given for the encryption Process. Enter the initial value for row shuffle and also to enter the initial value for Column shuffle. Encrypt button is used for the further to select the image; Back button is used to go back to screen. And Exit button is to exit from the screen.

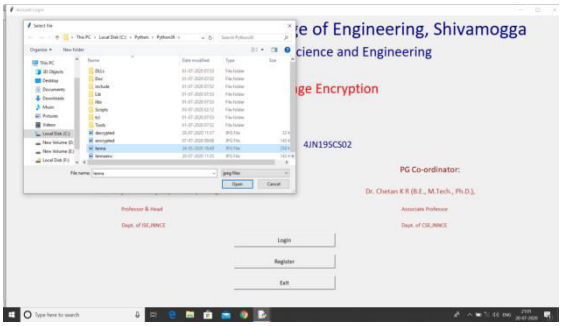


Fig. 6.7 Selection of an Original Image.

- The figure 6.7 shows the snapshot of Selection of the original image for the encryption Process. Here, we are going to select the .jpg or .bmp images for the encryption.

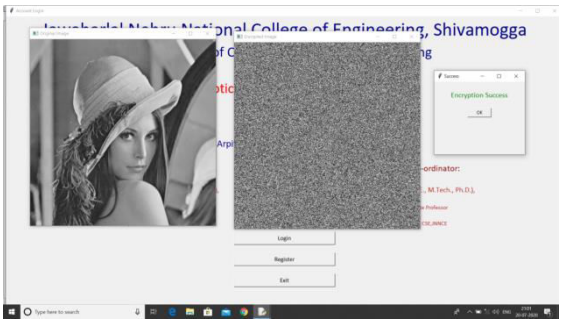


Fig. 6.8 Encryption Success.

- The figure 3.8 shows the snapshot of original image as well Encrypted image with the Encryption success message. If you get both the original and encrypted image then it shows Encryption is success.

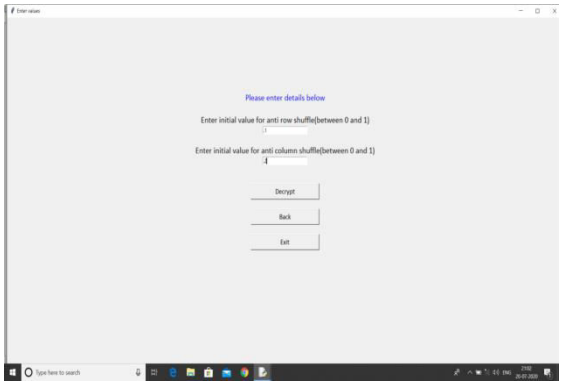


Fig. 6.9 Enter Values for Decryption Process.

- This figure 6.9 shows snapshot to enter details for the Decryption. Here, we have to give the same initial value that is given for the Encryption. Enter the initial value for anti-row shuffle and for the anti-column shuffle, Click on the Decrypt button for the Decryption. And again Back button is to come back to the screen and Exit button to exit from the screen.

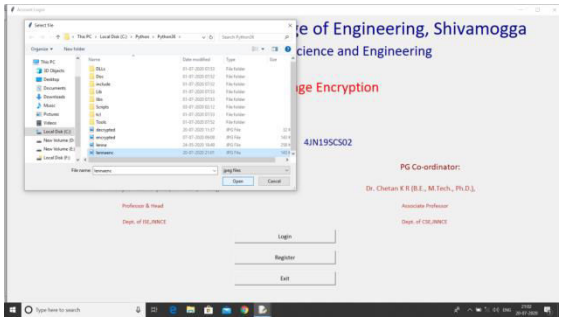


Fig. 6.10 Choose Encrypted Image.

- The figure 6.10 shows that selection of the Encrypted image for the Decryption Process.

Fig. 6.11 For Decryption success.

- The Figure 6.11 shows the snapshot of Decryption Success. If both the Encryption and Decryption initial values matches, then we are getting an Original Image and it show Decryption is success.

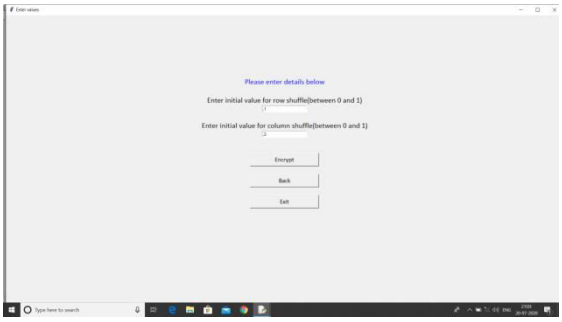


Fig. 6.12 Entered value is wrong.

- Figure 6.12 shows snapshot of Wrong entered value by the user either in encryption or in decryption. But in the given figure shows for decryption, initial value entered for anti-column shuffle is mismatching here.

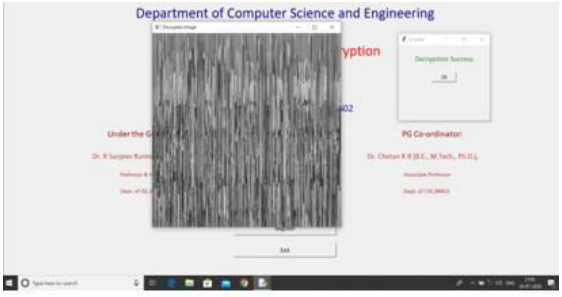


Fig. 6.13 Decrypted Error Image

- The figure 6.13 shows the error decrypted Image. The initial value entered by the user for both Encryption and Decryption should be the same, either of them mismatches then we are not getting an original image as output instead will get the error image as shown in the figure.

Histogram Analysis

The histogram represents the distribution of pixel values in an image. An encrypted image is expected to have a uniform distribution of the histogram values, making for the attacker difficult to learn something about the image. Thus, the suitability of the proposed encryption method is shown by the uniform distribution of pixel values in a coded image. Image histogram describes how the image pixels are distributed by plotting the number of pixels (along the y -axis) at each intensity level (along the x -axis). A good image encryption system should provide uniform image histogram for all encrypted images irrespective the nature of the original plane image. The histogram of four different plane images like- Lena.

These histograms show not uniform and large spikes, which correspond to the grayvalues that appear more often in the plain-images.

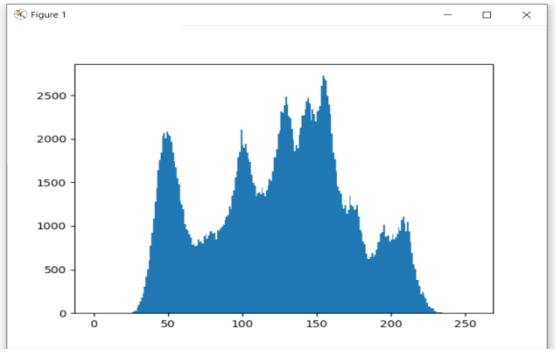


Fig. Histogram for Original Image.

The histograms of their encrypted images are shown in Figures respectively. Here all the spikes are almost uniformlydistributed and significantly different from those of the original images. A histogram of the encrypted image bears no statistical similarity to the plain image and hence do not provide any clue to employ any statistical attack on the proposed image encryption technique.

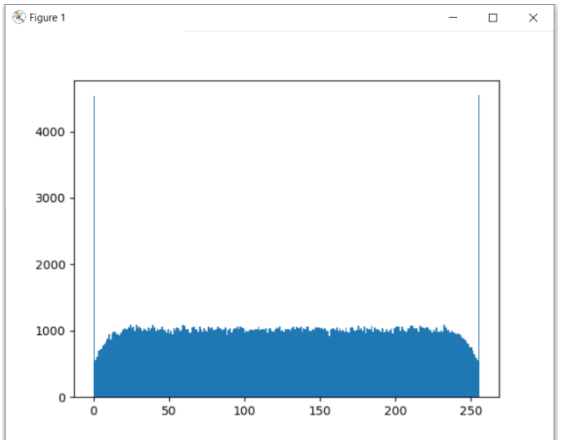


Fig. Histogram for Encrypted Image.

VII. CONCLUSIONAND FUTURE SCOPE

CONCLUSION

In this thesis, efficient chaos-based image encryption schemes are designed and analyzed,In order to improve the key space, new chaotic maps have been used. The experimental results show Image encryption and decryption using keysequence generated from sequence of logistic map. Two 8-bit gray scale images were chosenfor performance analysis of the algorithm. Proposed scheme iscompared with image encryption scheme using logistic mapmethod. The results shows original and encrypted image ishighly un correlated and perceptually different. The histogramplot of encrypted image is fairly uniform compared toencryption using only logistic map. It is also shown thatdecryption with wrong key (small change in initial value of'X_0' of the Key sequence) results completely different image.Correlation, Entropy, Mean Square Error between original andencrypted image computed for both proposed and logistic mapmethod. The XOR operations and pixel shuffling ofthe image are used to confuse and defuse the pixel valueand pixel position. The key in the chaotic system generatesthe initial condition, so the security of the chaoticsequences totally dependent on the secrete key.

FUTURE SCOPE

Further developments of the work presented in this thesis are described in the following directions.

a) Efficient chaotic cipher

Many digital chaotic ciphers are broken because of their carelessdesign and not because of the essential defects in digital chaotic systems. Thisfact highlights the need of the principles of designing a strong chaotic cipher.

b) Pure pseudo random generator

The pseudo random sequences generated by digital chaos are thecore parts in many chaotic ciphers. How to measure the unpredictability of thepseudorandom sequences is an unsolved problem. In the continuous chaostheory, information entropy can be used to depict the rate of information lossas chaotic iterations.

c) Combined compression to reduce cipher size

In image storage or transmission, lossless or loss compression isusually applied, so as to reduce the information to be stored or transmitted.Similarly, it is also expected that a reduction of the cipher image size bycombined compression encryption techniques should increase the encryptionefficiency. In general, the compression part should consume a considerablylesser time in the whole process.

d) Extension to chaos based video encryption

In future, this study can be extended to videoencryption/decryption. In general, video data exist more often in acompressed format, which involves intra frame compression and motioncompensation. The extended cipher could be designed to operate on theI(ntra) frames, P(redicted) frames, and B(i-predictive) frames of thecompressed video. Besides, selective encryption techniques on video havelong been considered as an attractive research direction. Its basic concept is to115encrypt only a portion of the entire plain video to protect it from illegalattempts to reconstruct the video.

e) Theoretical aspects of cipher

The chaos theory consistently plays an active role in moderncryptography. In future, the work can be extended, by applying thetheoretical aspects of cipher design, to Integrated Circuit (IC) chip basedimplementation, and make an effort to better the performance of chaoticimage encryption.

f) Cryptanalysis of digital chaotic cipher

Cryptanalysis is fundamental for the progress and improvement ofimage encryption.

REFERENCES

1. N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryption usingchaotic logistic map,” Image Vision Compute, Vol. 24, pp. 926-34,Sept. 2006.
2. T. Gao, Q. Gu, and Z. Chen, “A new image encryption algorithm based on hyper-chaos,” Phys. Lett. A, Vol. 372, pp. 394-400, Apr. 2008.
3. T. Gao, and Z. Chen, “Image encryption based on a new total shuffling algorithm,” Chaos, Solitons and Fractals, Vol. 38, pp. 213- 20, Jan. 2008.
4. C. K. Huang, and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” Optical communications, Vol. 282, pp. 2123-7, Feb. 2009.
5. C. K. Huang, and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” Optical communications, Vol. 282, pp. 2123-7, Feb. 2009.
6. A. Kanso, and N. Smaoui, “Logistic chaotic maps for binary numbers generations,” Chaos, Solitons and Fractals, Vol. 40, pp. 2557-68, 2009.

7. G. Alvarez, and S. Li, "Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption," Commun Nonlinear Sci NumerSimulat, Vol. 14, pp. 3743-9, Nov. 2009.
8. H. S. Kwok, K. Wallace, and S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons and Fractals, Vol. 32, pp. 1518-29, Apr. 2007.
9. X. Y. Wang, and Q. Yu, "A block encryption algorithm based on dynamic sequences of multiple chaotic systems," CommunsNonlinear Sci NumerSimulat, Vol. 14, pp. 574-81, 2009.
10. Z. Lin, and H. Wang, "Efficient image encryption using a chaosbased PWL meristor," IETE Technical Review, Vol. 27, pp. 318-25, Jul-Aug 2010.
11. D. Chattopadhyay, M. K. Mandal, and D. Nandi, "Robust chaotic image encryption based on perturbation technique," ICGST- GVIP, Vol. 11, pp. 41-50, Apr. 2011.
12. L. Zhang, X. Liao, and X. Wang, "An Image Encryption Approach Based on Chaotic Maps," Chaos, Solitons & Fractals, Vol. 24, pp. 759-65, 2005.
13. R. Rhouma, and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper chaos," Phys Lett A, Vol. 372, pp. 5973-8, 2008.