PH567 Non-Linear Dynamics

A Project Report On

Image Encryption using Logistic Map

Members:

Vinit Doke 190260018
Shourish Khade 190260026
Parth Shrivastava 190260033
Tanmay Choudhary 190020121

Abstract

In this paper, we study an encryption method based on logistic chaotic map. The method of encryption involves four steps; generating a pseudo random sequence using Logistic Map, generating a sequence using Linear Feedback Shift Register; creating a key sequence for encrypting the image with the help of the sequence generated using Logistic map and the Linear Feedback Shift Register, and then using the key sequence to encrypt the image. For decryption, we use the key sequence generated during encryption along with the encrypted image to decrypt it back to the original form. The simulation results of the Test Images show that the histogram, pixel correlation, information entropy are distinct enough to be immune against an attempt to decrypt by an interceptor.

Contents

1 Introduction

In recent years, digital communication technology has become an integral part of storage and transmission of data. Along with the rise in methods of digital transmission and storage of data, there has also been a rise in the number of network security issues which have in turn plagued and restricted the development of network technology. In the security system of digital information, encryption technology is the most common method used, which is just encryption of the original data into a scrambled and unusable form from which the original data can be extracted by certain decryption algorithms. However,under current circumstances, encryption technology is mainly based on the requirements of text encryption since the more common encryption system cannot achieve better results in the compatibility and encryption quality of digital image encryption.

Although digital images can be presented as 3-dimensional sets of data systems that directly use text-encryption techniques often face problems of inefficiency in encryption and decryption, hence low security and low practical usage. We can use different methods for encryption of digital images, for e.g. Digital watermarking technology, which helps us protect the copyright of digital images, but still the visibility of digital images cannot be avoided using this method.The other method follows the principle of encrypting the digital information contained in the digital image.

This method follows the process of first encrypting the digital information of the image and obtaining a completely different image, contents of which cannot be viewed. When the digital is required for viewing or using, a decryption algorithm is used to calculate and extract the original image from the encrypted one. In an environment with high security requirements, this is an important means of image content protection.

Commonly used algorithms or techniques include digital image encryption based on pixel transformation, digital image encryption based on random sequence, digital image encryption based on image compression coding, and digital image encryption based on image key. The chaos technology is difficult to crack due to randomness, which makes the digital image encryption technology based on chaos technology become a more reliable digital image encryption technology. Many researchers have introduced the concept of chaos to improve the precision and security of chaos technology.

2 Logistic Map

Since we are using a chaotic system as a source for our pseudo-random sequence, an enquiry into the Logistic Map is warranted. It is given by the recurrence relation

$$x_{n+1} = rx_n(1 - x_n)$$

where $r \in (0, 4)$ and $x_i \in [0, 1]$.
While plotting the above when the parameter satisfies the condition $r \in (3.569, 4]$, a chaotic sequence will be generated. The characteristic of the sequence is very similar to that of white noise. It is commonly used in the chaotic encryption of digital images. From the very definition and characteristics of a chaotic system, we know that such systems are very sensitive to initial value. In a cryptographic system, if the subtle changes in the key leads to considerable changes in the encryption effect,the algorithm used for encryption has a higher sensitivity to the existence of the key and hence a better encryption effect. Hence we use such chaotic systems due to their sensitivity to the initial value.

In this paper, we use the chaotic mapping to create the pseudo-random sequence, different from the traditional method of using computer software to create pseudo-random sequences. Taking the same initial value in the data encryption technique based on a chaotic system, the sequence of pseudo-random number is exactly the same and the randomness of the sequence is better.

3 Methodology

The basic idea of encryption of digital images is to modify or rearrange each pixel of the image by a unique process so as to obtain a modified image (encrypted image) which has no resemblance to the original image. This 'unique process' should be such that there exists another unique process, which when used on the encrypted image, gives us back the original image.

3.1 Method of Encryption

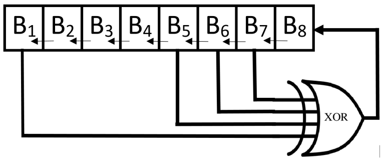
The method of encryption of image used in our project involves four steps; generating a pseudo random sequence using Logistic Map, generating a sequence using Linear Feedback Shift Register, creating a key sequence for encrypting the image, using the key sequence to encrypt the image.

We use the Logistic Map Function

$$x_{n+1} = rx_n(1 - x_n)$$

to generate a pseudo random sequence of given length. We choose a **seed value** (initial value) in $(0, 1)$ and the growth parameter value r. These values will be the 'keys' which will later be used for the decryption process. The length of the sequence should be equal to the number of pixels in the image. Hence, if the image has a resolution of $M \times N$, we will generate a pseudo random sequence having $M \times N$ terms. Then, we scale each value in the sequence up to 256, followed by rounding it off to the nearest integer. Finally, we convert each term in the sequence to an 8-bit binary number. This is our sequence K_1

We generate another sequence of the same length using an 8-bit Linear Feedback Shift Register (LFSR). A Linear Feedback Shift Register is a shift register whose input bit is a linear function of its previous state. The LFSR we use here, shifts each bit of the previous state (each state is an 8-bit binary number) to the left by one bit. It takes in the XOR of 1st, 5th, 6th and 7th bits of the previous state and feeds the output to the 8th bit of the next state. We choose a seed value and this process is followed to generate a sequence of length $M \times N$. This is our sequence K_2.



(a) LFSR

$$B_{n+1,q} = B_{n,q+1} \;\; where \;\; q \in \mathbb{Z} \cap [0, 7], \; n \in \mathbb{Z} \cap [1, M \times N - 1]$$

$$B_{n+1,8} = B_{n,1} \oplus B_{n,5} \oplus B_{n,6} \oplus B_{n,7}$$

where $\mathrm{B}_{n,q}$ is the qth bit in the nth term of the sequence.

The final key sequence to be used for encryption is generated by taking a bitwise XOR output of the corresponding elements of both K_1 and K_2. The resultant sequence is our key sequence K.

$$K = K_1 \oplus K_2$$

The 2-dimensional $M \times N$ image is then converted to a 1-dimensional sequence of pixel values ranging from 0 to 255. Each term of the sequence is then converted to an 8-bit binary number. This resultant sequence P is our image sequence. We then do a bitwise XOR operation between the corresponding elements of the key sequence K and the image sequence P to give us the resultant encrypted image sequence $\mathrm{P}^\dagger$. This 1-dimensional sequence is then again converted to a 2-dimensional $M \times N$. This will be our encrypted image.

$$P^\dagger = P \oplus K$$

3.2 Method of Decryption

The method of decryption is performed, given that we know precisely the key values (seed values of K_1, K_2 and the growth parameter $\mathbf{r}$). We follow the first three steps to generate a key sequence $K_{decryption}$. We do a bitwise XOR of corresponding elements of the encrypted image sequence $\mathrm{P}^\dagger$ and our key sequence $K_{decryption}$ to obtain the decrypted image sequence. We convert this sequence to an $M \times N$ dimensional image as done previously. If the correct key values as used in encryption process are used to generate the sequence $K_{decryption}$, the $K_{decryption}$ sequence will be identical to the sequence K and hence, the decrypted image will be identical to the original image.

$$P = P^\dagger \oplus K_{decryption}$$

An additional step of scrambling could be added to the encryption system in order to make it more robust. 'Scrambling' here is simply reshuffling of pixel locations in original image to obtain a scrambled image on which the encryption is done using already described method. This process of reshuffling is done by first obtaining a permutation matrix

$$P(i) = \lfloor (10^8 X(i) \rfloor mod(MN) + 1$$

where X(i) is an array of size $1 \times MN$ obtained using the logistic sequence, and $\lfloor x \rfloor$ represents the greatest integer function. Then scrambling is achieved by replacing the element A(i) with A(P(i)), where A(i) is the 1D array of original image. Thus, a second key could be introduced in our process which makes it more secure. However, if this additional scrambling is used, it leads to a slightly noisy image upon decryption. This noise may be attributed to the fact that the mapping of pixel positions mentioned above is not one-one.

4 Security Analysis

In order to study the security characteristics of the Encryption System various analyses can be performed, out of which Statistical, Sensitivity, and Information Analysis are discussed here.

4.1 Statistical Analysis

4.1.1 Histograms

We analyse the histograms of the Original image and the Encrypted image. The histogram of original image is quite distinct, while that of the encrpyted image is **Uniform** as compared to that of the original image.

4.1.2 Correlation Coefficient

In a meaningful image (here original image) adjacent pixels are highly co-related to each other in all directions. This co-relation is quantitatively measured through **Correlation Coefficient** for both the images (original and encrypted) according to following formulae [2]:

$$cov_{Hori}(A) = \frac{1}{M \times N} \sum_{j=1}^{M} \sum_{i=1}^{N-1} (A(i,j) - E(A))\,(A(i,j+1) - E(A))$$

$$cov_{Vert}(A) = \frac{1}{M \times N} \sum_{j=1}^{N} \sum_{i=1}^{M-1} (A(i,j) - E(A))\,(A(i+1,j) - E(A))$$

$$cov_{Diag}(A) = \frac{1}{M \times N} \sum_{j=1}^{M-1} \sum_{i=1}^{N-1} (A(i,j) - E(A))\,(A(i+1,j+1) - E(A))$$

$$r_{Hori}(A) = \frac{cov_{Hori}(A)}{D(A)}, r_{Vert}(A) = \frac{cov_{Vert}(A)}{D(A)}, r_{Diag}(A) = \frac{cov_{Diag}(A)}{D(A)}$$

where,

$$E(A) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} A(i,j)$$

$$D(A) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (A(i,j) - E(A))^2$$

(Here subscripts 'Hori','Vert' and 'Diag' stands for Horizontal, Vertical and Diagonal respectively. Also $M \times N$ represents size of the image.)
The correlation properties can also be observed through scatter plots.

4.2 Sensitivity Analysis

A good encryption should be sensitive to the slightest change in the 'key'. This ensures that a different key with small difference with the true key would not be able to decrypt the image correctly. The sensitivity analysis can also be studied through logistic map as it is highly chaotic with respect to the initial input. As demonstrated here, if we take a value of parameter **r** differing from actual key value r by 0.01, the decrypted image is incorrect and hence, does not give us back the original image.

4.3 Information Entropy

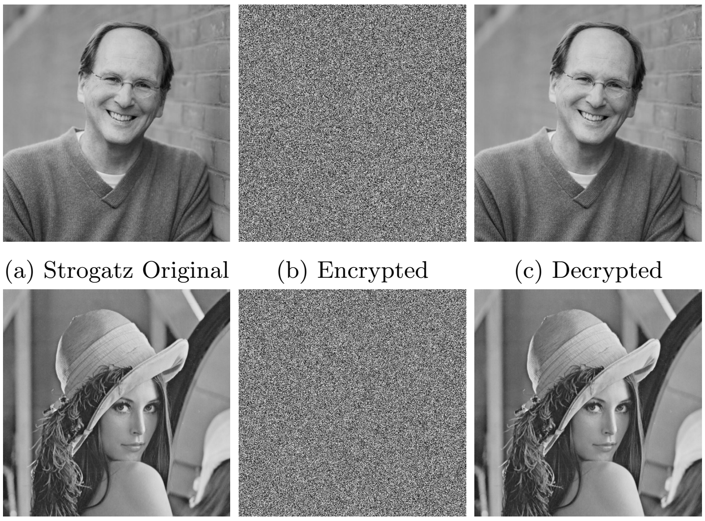
For a $256 - level$ grey scale image **A**, its information entropy $H(A)$ is defined as the following form:

$$H(\mathbf{A}) = \sum_{i=1}^{255} p(i) log_2 \left(\frac{1}{p(i)} \right) [1]$$

where $p(i)$ represents the probability of i^{th} level grey pixels, i.e. p(i) = (the number of pixels whose intensities are equal to i) / (the total number of image pixels)
Here entropy signifies the randomness in our image, more random the encrypted image more secure it is from information entropy attack. The maximum entropy for 256-level gray image is 8.

5 Results and Conclusion

We tested and analysed the Encryption-Decryption Method on two portraits: **1.** Portrait of Steven Strogatz and **2.** 'Lenna': a widely used image in the Computer Vision field. Following are the original,encrypted and decrypted versions of the test images, respectively.

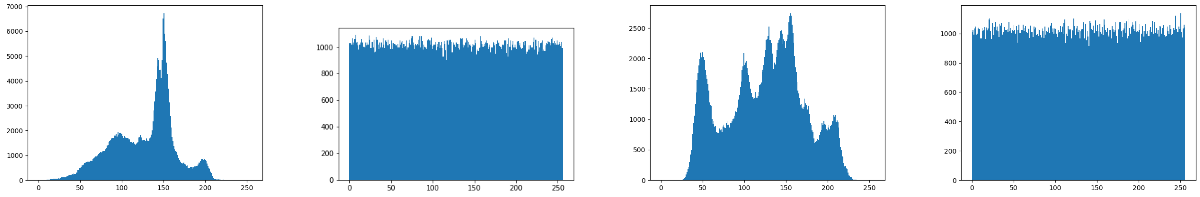


(a) Strogatz Original (b) Encrypted (c) Decrypted

(d) Lenna Original (e) Lenna Encrypted (f) Lenna Decrypted

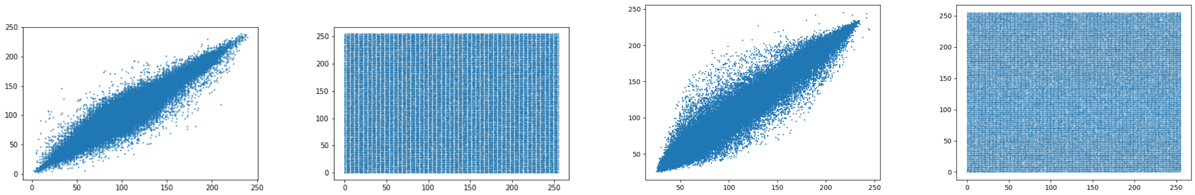
Figure 2: Test Images

5.1 Histogram and Co-variance Plots



(a) Strogatz Original (b) Strogatz Encrypted (c) Lenna Original (d) Lenna Encrypted

Figure 3: Image Histograms



(a) Strogatz Original (b) Strogatz Encrypted (c) Lenna Original (d) Lenna Encrypted

Figure 4: Horizontal Pixel Covariance

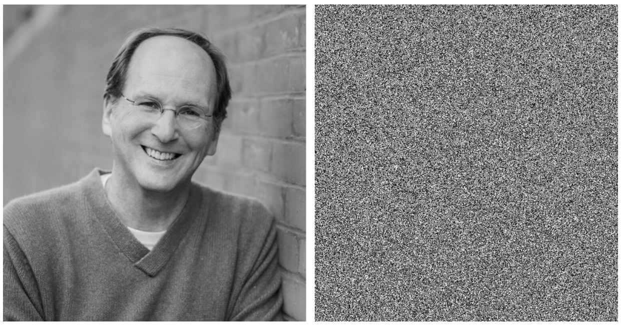
5.2 Information Entropy and Pixel Correlation Coefficients

Image	**Original**		**Encrypted**		**Decrypted**	
	Entropy	**rH** **rV** **rD**	**Entropy**	**rH** **rV** **rD**	**Entropy**	**rH** **rV** **rD**
Lena	7.44	0.96964 0.98387 0.95596	7.99	0.01732 -0.00195 -0.00141	7.44	0.96964 0.98387 0.95596
S. Strogatz	7.08	0.97497 0.9775 0.9597	7.99	0.03039 0.00268 -0.00032	7.08	0.97497 0.9775 0.9597

Here, rH stands for Pixel Correlation Coefficient in the Horizontal direction. rV stands for Pixel Correlation Coefficient in the Vertical direction. rD stands for Pixel Correlation Coefficient in the Diagonal direction

5.3 Sensitivity Analysis Results

We take $r_1 = 3.99$ and $r_2 = 3.98$ and apply the same decryption process for an image encrypted with $r = r_1$. We also assume a fixed initial value/seed value. The corresponding decrypted images are as follows:



(a) Strogatz Original (b) With Incorrect r value

Figure 5: Changed Parameter(Wrong Key)

5.4 Conclusion

In this paper we proposed a simple algorithm for digital image encryption using Logistic map and Linear Feedback Shift Register. The initial values of Linear Feedback Shift Register and Logistic map along with the growth parameter of Logistic map served as the keys in the encryption process.

Security analysis shows that the histograms of original and encrypted images are quite different and that of the latter one is uniform as compared to that of original image. Also the correlation coefficients of the original image are very close to 1 which indicates that adjacent pixels are highly correlated which is not case with the encrypted image for which the coefficients are not close to 1. This can also be verified by observing scatter plot. Information entropy for encrypted image is greater than that of original image and is close to 8. Thus the encryption system is reasonably secure and robust.

From the overall situation, the research results in the field of digital image chaos encryption are quite rich, and it has also promoted the development and application of digital image encryption technology. However, the current image chaotic encryption technology still fails to break through the category of two-dimensional integer-order chaotic systems, since there is still room for improvement in dynamic characteristics and pseudo-randomness. The chaos encryption technology based on high dimension space proposed by some scholars has the problems of poor uniformity of pixels in the process of encryption, the difficulty of confusion processing,and hence a lower efficiency of encryption and decryption process.

6 Code Repository

Link to the Code Repository on GitHub:
https://github.com/vinitdoke/PH567_Course_Project.git

References

[1] Hailan Pan, Yongmei Lei, and Chen Jian. Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, 2018(1):142, Dec 2018.

[2] Zhang Yong. Image encryption with logistic map and cheat image. *ICCRD2011 - 2011 3rd International Conference on Computer Research and Development*, 1, 03 2011.