

Dual image encryption using Modified Fisher-Yates and Cipher Stream Chaining

MSc Research Project
MSc in Cloud Computing

Mukul Gopinath
Student ID: x17123739

School of Computing
National College of Ireland

Supervisor: Dr. Sachin Sharma

**National College of Ireland
MSc Project Submission Sheet
School of Computing**



Student Name:	Mukul Gopinath
Student ID:	x17123739
Programme:	MSc in Cloud Computing
Year:	2017/18
Module:	MSc Research Project
Lecturer:	Dr. Sachin Sharma
Submission Due Date:	18/04/2019
Project Title:	Dual image encryption using modified Fisher-Yates and Cipher Stream Chaining
Word Count:	5,548

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:	
Date:	18 th April 2019

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. You must ensure that you retain a **HARD COPY** of **ALL** projects, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
3. Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.


Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	



Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

Submission Author	Mukul Gopinath
Turnitin Paper ID (Ref. ID)	1114613321
Submission Title	x17123739_Research_Project
Assignment Title	Submit here: Research Project Report
Submission Date	18/04/19, 01:57

 [Print](#)

Dual image encryption using modified Fisher-Yates and Cipher Stream Chaining

Mukul Gopinath
X17123739

Abstract

Health-care and hospitals can cater their business in a whole new level if they adopt cloud to the fullest potential. The issue arises in terms of the privacy and security where the data accumulated should not be compromised at any point. The X-ray, reports are stored as images which needs to be secured and made meaningless with the help of encryption so that the data is not useful even if the access is compromised. Thus, the image encryption employed should be able to reconstruct the encrypted image and lossless. This research aims at implementing a dual layered approach with Fisher Yates and Cipher Stream Chaining methods to encrypt and secure the image. The experiment could achieve Net Pixel Change Ratio (NPCR) of 100%, entropy of 7.999 and Uniform Average Color Intensity (UACI) of 35.46% which have been evaluated to be close to an ideally encrypted image.

Keywords: *NPCR (Net Pixel Change Rate), UACI (Unified Average Color Intensity), Entropy, Fisher Yates algorithm, Cipher Stream Chaining.*

1 Introduction

The widespread need for organizations to adopt cloud to enhance their business and benefit has been growing rapidly. The adoption of cloud has been extended in the field of research, education, healthcare, banking and retail. The evolution of data and technology has been influenced abundantly. The issues that current technology faces besides latency and performance includes privacy, confidentiality and security. The textual data encryption has been adopted by the institutions to encrypt and secure the data at rest. The need for image encryption has been in the research for a while.

In SaaS (Software-as-a-Service), the customers or consumers are varied in their needs, thereby resulting in varied requisites. In the multi-tenancy, the level of security and privacy need differs, the data breach or data loss may affect each one differently. To overcome this, the concept of data encryption was introduced, as the data would be of no use even if access is compromised and data is stolen. The data encryption has been evolving in the textual stage and there has been lots of contribution towards them, whereas the medical field is still facing issues in adopting the cloud due to the confidentiality and security of medical images. The concept of image steganography is a step towards image distortion and securing the image by making it meaningless to the attacker (Kaur and Kaur; 2015).

The image encryption technique in this research involves randomizing, shuffling and distorting the image such that the processed image doesn't resemble the original image, also it is not easily recoverable. The main factors that are to be considered includes speed, accuracy, extent of security and reliability. The area of research in image encryption focuses on the

security aspects and less on the speed and accuracy. The Fisher Yates algorithm is used for randomizing and shuffling the image to increase chaos and distortion.

Can dual layer modified Fisher Yates algorithm improve the image encryption qualitatively and quantitatively?

The proposed method deals with modified Fisher Yates method which is used to shuffle, randomize the pixels and distorting the structure of the image, thus increasing chaos. The additional layer of Cipher Stream Chaining is used to increase the interdependency among the shuffled neighbouring pixels, to improve the entropy, also the quality of encryption.

To qualitatively analyse the extent of encryption, we utilize standard benchmarks such as NPCR (Net Pixel Change Ratio) which emphasises on the number of pixels that have been trans-positioned with comparison to the original image; UACI (Uniform Average Colour Intensity) which evaluates the composition of RGB levels of the image; Entropy examines the randomness of the image which standardises the extent of encryption.

The implementation of this proposed approach will be able to secure the image and achieving the evaluation close to ideally encrypted image will ensure the security and privacy of the image. The quick and efficient approach aims at real-time implementation in SaaS products to ease the migration of Healthcare and other business which demand high levels of security and privacy. The image encryption will satisfy the customers to not only rely on the authentication mode but also on the target data being secured in case of the access being compromised.

The latter part of the paper is structured as: Section 2 which critically reviews and summarizes the previous work in relation to privacy, security, different image encryption. Section 3 explains the different techniques or methodologies adopted towards implementing the solution. Section 4 is an illustration of the process with the pseudocode of the algorithms. Section 5 comprises of the implementation of the solution discussing the methodologies utilized in the process. Section 6 is the phase of evaluation where the various quantitative experiments are carried out to evaluate the implemented solution and provide the comparison to that of the benchmarks. Section 7 concludes the research and discusses about the future scope or extensions.

2 Related Work

2.1 Introduction

This section is a brief summarization of the past work that has been carried out with relation to encryption and security in the domain of computing. The entire section is divided into three other subsections. Subsection 2 which focuses on the various encryption approaches and critically analyses each approach. Subsection 3 helps to understand on how to quantitatively analyse the encryption methodology against the efforts of implementation. Subsection 4 concludes the related work.

2.2 Encryption Algorithms

2.2.1 Chaotic Logistic Map

The research implements Double Chaotic Logistic Map (DCLM) which compares to One step Logistic Map (OLM) but the results are uniform except for the security provided. The two keys K1, K2 are generated initially, then the keys are XORed to obtain the encrypted key. The image array is XORed with the encrypted key to produce the encrypted image array. The correlation analysis between the two methods show that the value is positive in the DCLM and negative in OLM. A positive correlation means that the decryption results with no loss of pixels/clarity and vice versa. The research is limited to correlation and MSE, doesn't provide any insight on the time for encryption/decryption, the NPCR, entropy values are not analyzed, easy to decrypt as it is a single layered encryption which lacks complexity (Safi and Maghari, 2017).

The paper proposes a Multiple stage Logistic Map (MLM) which comprises of read, pixelate and change which is a series of operations on the image. The research lacks evaluation and decryption. There is no evidence of reconstructing the image back and thus no proper evidence of the security and efficacy of encryption (Brindha, 2018).

The encryption technique adopted is improved logistic mapping which is more secure and chaotic. The entropy is ideal as it is close to 8. The encryption and decryption time are low. The evaluation in terms as number of images considered is low (Bing, 2017).

The research evaluates Stream-based and Block-based encryption where the pixel correlation is compared. The histogram shows less difference hence the technique is less efficient to the others. The pixel read is performed in a different manner known as the 'Spiral wave scan'. The entropy value differs significantly for each image; hence the method is not suitable for all images as it lacks uniformity (Singar and Bharti, 2017).

2.2.2 Confusion and Diffusion techniques

The process of encryption utilizes Two step Iterated Logistic Map (TILM) which comprises of confusion and diffusion as the main constituents. The method implements single scan and thus is faster than the iterative read operations in other methods. The NPCR and UACI values are close to ideal but the evaluation is limited to a single image, hence lacks a statistical average due to the sample size (Sharma, 2016).

The encryption method involves the use of Lorenz equation and Henon map results in better entropy and reduces the pixel correlation. The NPCR and UACI values are close to ideal. The entropy value is high compared to other benchmarks. The evaluation is performed for a few set of images and is extensive on the particular image that is encrypted, also doesn't extend towards images of different shape and sizes (Murugan and Nanjappa Gounder, 2016).

The use of pixel transposition to encrypt the image is adopted using the RGB histogram. This method employs compression of up to 65% compared to the original image. This improves the transmission speed of encrypted and compressed image when compared to that of the original image. The avalanche effect which is desirable by any cryptographic algorithm is high in this method. The proposed method although suffers from bit loss due to compression and logarithmic operation (Kumar, 2017).

The Coupled Map Lattice (CML) utilizes the process of diffusion to encrypt the image. The NPCR and UACI values are close to ideal, but not better than the benchmark methods that

is taken for reference, also the time to encrypt/decrypt is significantly high. The method is a single layered approach and thus addition of another layer could increase the time (Sharma *et al.*, 2018).

The encryption is based on Arnold transform, Fresnel domain and binary matrix techniques. The method employs usage of Arnold transform then dividing into n size QR codes which then undergo Binary Matrix using Fresnel domain. There is no quantitative evaluation, hence not comparable to that of any methods. The evaluation is substantial and limited to one image being encrypted and decrypted (Kumar and Nishchal, 2018).

This paper proposes a technique to partially encrypt and watermark medical images. The image is first sub-sampled and the processed through the quantizer as it uses Discrete Wavelet Transform (DWT). The method limits itself to X-ray and scans only, thereby not being suited for varied images. The histogram is similar in both original and encrypted images which results in low entropy and thus reducing the randomness or chaos (Abdel-nabi and Al-haj, 2017).

The image encryption process in this research is done by first extracting the RGB values and passing it to the Discrete Cosine Stockwell Transform (DCST) which transforms on time vs frequency decomposition which is then passed on to the Singular Value Decomposition (SVD) which diagonalizes the matrix. The reconstructed image after decryption is higher in quality compared to the other algorithms. Although the evaluation doesn't provide any insights on the NPCR and UACI values which are the quantitative measure in the process of encryption (Vaish, A; Kumar, 2018).

The proposed approach in this research aims at parallelly encrypt and compress the image. The approach follows an 8×8 Discrete Cosine Transform (DCT) which is carried out for four stages. The secret key is generated and then the alternating transform is applied using the key. The decryption of the image is easy hence there is no focus towards the confidentiality and security. The correlation is high when compared to other methods which is not preferable; also, doesn't provide evaluation metrics like UACI or NPCR (Li and Lo, 2015).

2.2.3 Phase Encoding

The encryption is using the Runge-Kutta algorithm which implements random phase encoding. The encryption also involves compressive sensing in various ratios. The image decrypted where the compression ratio is 2:1 is distorted whereas similar in the case of 4:3. The Peak Signal-Noise Ratio (PSNR) and Mean Squared Error (MSE) is high which make the decrypted image different from the original image. The evaluation also lacks information of NPCR and UACI (Huang and Yang, 2018).

The encryption implemented is a hybrid approach with logistic map and Arnold cat map which is a dual layered approach. The Entropy and NPCR values are close to ideal whereas the UACI value is not close enough for the ideal value (Abdullah and Abdullah, 2017).

2.2.4 Magic Rectangle

The encryption scheme employs the use of magic rectangle to use the cipher in order to encrypt the image. The method is fast and efficient as there are four sets of ciphers and one is picked at random for each portion of the image. The image compression reduces the time for encryption. The scalability with size of image is poor as the time to encrypt increases rapidly

with size. The compression doesn't reflect below 100KB. The evaluation is limited in terms of NPCR and UACI which voids the standardization of the method (Amalarethinam, 2015).

2.2.5 Fisher Yates algorithm

The research implements Fisher Yates with DWT to increase the chaos and then passed through chaotic modulation to generate the ciphered image. The evaluation of NPCR and entropy are low. There are many iterations which cause the algorithm to slow down the processing time. The time for encryption and decryption is higher for a single layered approach (Ahmad, 2014).

The approach towards data hiding in images termed as image steganography is used in this research. The process involves hiding message 'M' in a cover image 'C' with a random key 'K', after which a Triple-A algorithm is used to produce the image which contains the message embedded in the image. The approach implements a 'spiral wave scan' or 'helical traversal'. Since the approach doesn't aim towards securing the image, but to secure the message to be embedded in the image, there is no necessity to evaluate the NPCR and UACI values (Alam, Zakariya and Akhtar, 2014).

The encryption involving block-wise pixel shuffling using Fisher Yates method is performed. The implementation lacks to visually distort the image as the encrypted image has similar histogram and higher correlation. The entropy values are not ideal but are comparatively good. The evaluation is limited as there are no NPCR or UACI metrics for the images (Hazra and Bhattacharyya, 2016).

2.2.6 Cipher Block Chaining (CBC)

The encryption process adopted in this technique is to divide the image into blocks and XORed. The two inputs for the XOR are output of the previous operation and the subsequent block, for the first iteration, a key block is used as one input. The process is continued for 'n' blocks. The Entropy value is ideal and better than other implementations. The time for encryption and decryption is higher, NPCR and UACI values are low (J, Mahalakshmi; K, 2016).

2.3 Evaluation of the Encrypted Image

The evaluation of the encryption in the past research is based on the NPCR, UACI, entropy and correlation coefficient. The correlation coefficient of the adjacent pixels in the encrypted image should be as low as possible so that it doesn't resemble the original image. The entropy value should be as close as 8 to be ideal. The NPCR value should be over 99.5% and UACI value should be around 33.4% to be considered as ideal (Wu *et al.*, 2011).

Approaches	Methodology	NPCR	Entropy
(Abdullah and Abdullah; 2017)	Hybrid chaotic map	99.63	7.9975
(Oravec et al.; 2018)	Coupled Map Lattice	99.30	7.9994
(Murugan and Gounder; 2016)	Confusion and Diffusion	99.62	7.9994
(Singar et al.; 2017)	Cell shuffling	99.60	7.81
(Hazra and Bhattacharyya; 2016)	Block-wise Fisher Yates	N/A	7.46
(Sharma and Bhargava; 2016)	Two step logistic map	99.61	N/A
(Saeed et al.; 2014)	Fisher Yates in Wavelet Domain	95.86	6.40

Table 1: NPCR and Entropy values achieved in the past work

2.4 Conclusion

The study of the past approaches suggests the need for the image encryption in domain like healthcare and SaaS solutions which emphasize on the importance of the image security. Although the concept of image steganography has been around for a while, the need to encrypt faster and efficiently with layered approach is most expected. The summary of Evaluation metrics in the past work are represented in *Table 1* above. Hence it would be better if a faster and efficient algorithm can achieve the same or better results (NPCR, UACI, Entropy).

3 Methodology

The strength of the encryption lies in the level of randomness that is introduced, also the ability to withstand attacks. The efficacy of the encryption would be based on the NPCR, UACI and entropy values as they are the standard metrics to test the encryption. In this solution, we have employed a technique which can provide performance, security, privacy and confidentiality, using Java programming to encrypt and store efficiently. The main methodologies that have been incorporated in the process is as follows:

1. Fast image extraction – obtain 2-Dimensional array from 1-Dimensional RGB array.
2. Diffie-Hellman Key Exchange – key exchange to improve authentication.
3. Modified Fisher Yates – randomly shuffling the pixels using Diffie-Hellman key.
4. Cipher Stream Chaining – increase interdependency and randomness.

3.1 Fast Image Extraction

The process of reading the pixels of the image can consume most of the time compared to the actual encryption process as the image is buffered as a stream and then the RGB values are translated into a 2-Dimensional array. The extraction of colour using the inbuilt Color class reduces the performance and speed of extraction. To overcome this, the bitwise operand is utilised to get the RGB values. The image is imported using IOImage class provided by Java. The object of ImageIO is converted to BufferedImage object and then parsed from the byte array to obtain the 2-D matrix.

3.2 Diffie-Hellman Key Exchange

The Diffie Hellman Key Exchange is a technique to authenticate two users to establish the access and then communicate or authenticate the process. The level of security provided by the method is directly related to the size of the key that is chosen. The process of key generation and translation is explained in the *Figure 1* below, where A and B are the communicators or the authenticators. They share a key with one another and using their own key, a common secret key is generated. The access is granted, or process continues if the Key K is same for both.

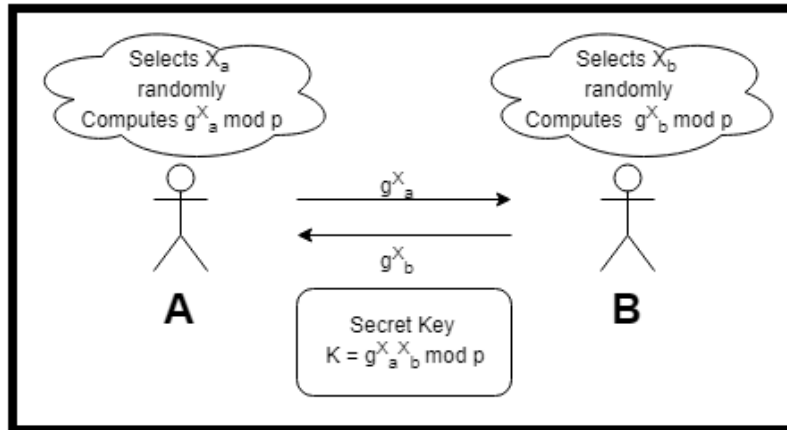


Figure 1: Diffie-Hellman Key Exchange Technique

3.3 Fisher Yates Method

The Fisher Yates Algorithm was introduced and named after Ronald Fisher and Frank Yates, which is also known as Knuth Shuffle named after Donald Knuth is an efficient and chaotic method to improve the randomness and to shuffle the image (Alam et al; 2014).

The modification in the implementation is towards key generation using a random key to select the array position from a 2-dimensional array instead of a 1-Dimensional array. The process of encryption is made efficient by swapping in-array implementation instead of creating a new array and placing the encrypted elements in a new array.

3.4 Cipher Stream Chaining

The cipher stream chaining is a technique to increase the interdependency of the shuffled pixels and the complexity of decryption. The technique involves binary operation of the neighbouring pixels where the neighbouring pixels are picked and XORed. As shown in the *Figure 2* below, output of the operation is one of the inputs to the next iteration. Through this chaining, the complexity of decryption is increased and thus makes the decryption a tougher process.

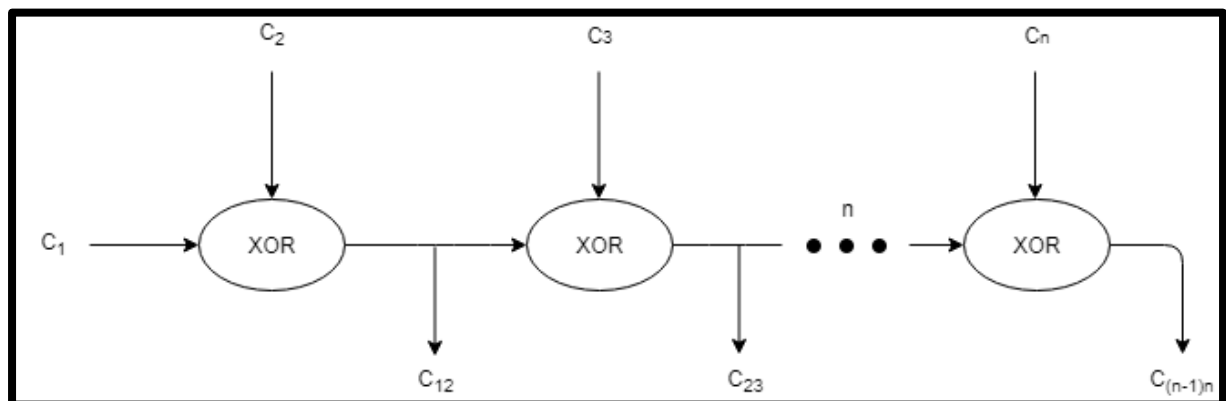


Figure 2: Cipher Stream Chaining

4 Design Specification

The *Figure 3* shows the flow of encryption from original image to encrypted image. The process is discussed in detail in the Implementation section.

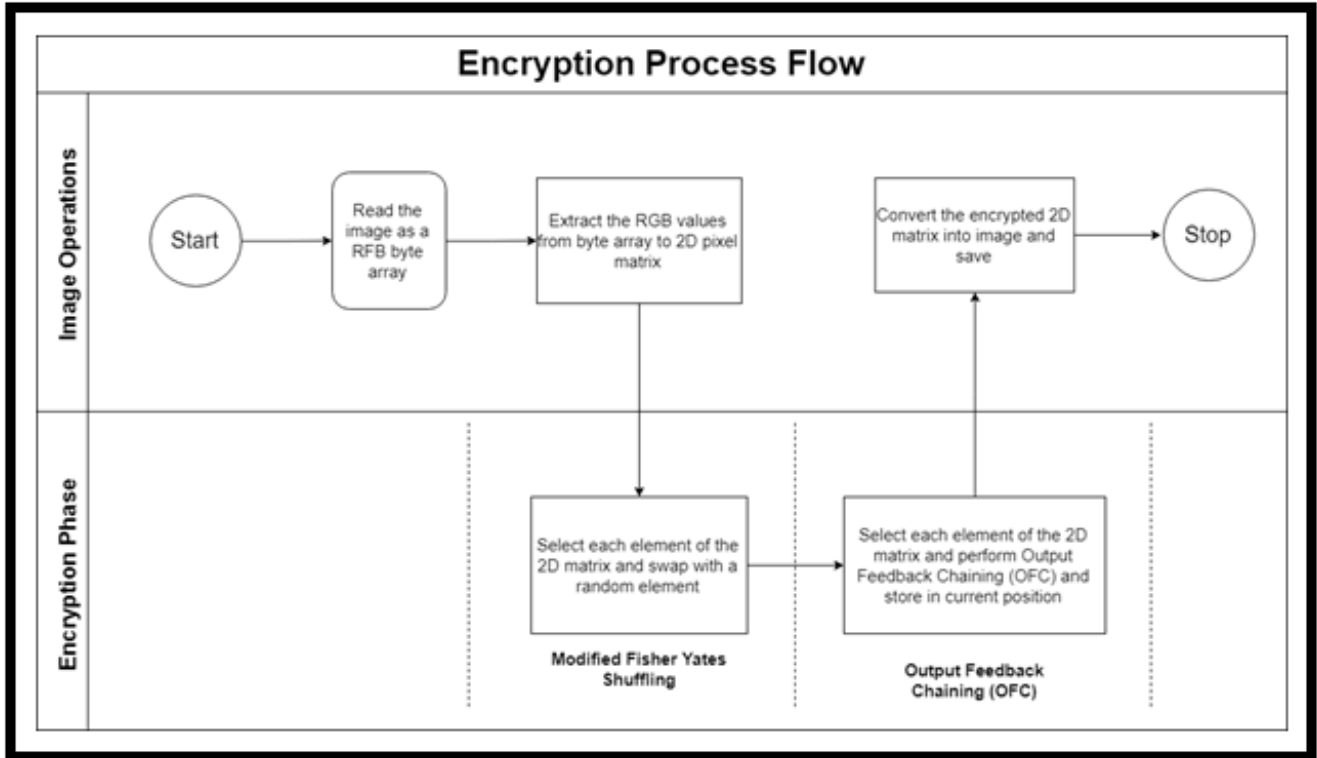


Figure 3: Process flow diagram for proposed Encryption

Algorithm 1 Pixel extraction from RGB image

Input: Original image

Output: Original image 2D matrix

```

pixelCounter ← 0
column ← 0
row ← 0
while pixelCounter < pixelCount do
  blue ← (pixel[pixelCounter] & 0xFF) << 16
  green ← (pixel[pixelCounter + 1] & 0xFF) << 8
  red ← (pixel[pixelCounter + 2] & 0xFF)
  pixelValue ← red + green + blue
  pixelCounter ← pixelCounter + 3
end while
  
```

Algorithm 2 Modified Fisher Yates Shuffle

Input: Original image 2D matrix**Output:** Stage I encrypted image 2D matrix

```
i ← 0, j ← 0
while i < 2d Matrix height do
  while j < 2d Matrix width do
    Generate and select random element position (m,n)
    temp ← array[i][j]
    array[i][j] ← array[m][n]
    array[m][n] ← temp
    j ← j + 1 {Swap elements in (i,j) with (m,n)}
  end while
  i ← i + 1
end while
```

Algorithm 3 Cipher Stream Chaining

Input: Stage I encrypted image 2D matrix**Output:** Final encrypted image 2D matrix

```
i ← 0
j ← 0
while i < arrayHeight do
  while j < arrayWidth do
    inext ← i
    jnext ← j + 1
    array[inext][jnext] ← array[inext][jnext] ⊕ array[i][j]
  if j == width then
    inext ← i + 1
    jnext ← 0
    {If last element of the row is encountered ,
     Next Element is next row and first column element}
  end if
  j ← j + 1
  end while
  i ← i + 1
end while
```

The Section 5 discusses the pseudocode algorithm and the process flow in detail.

5 Implementation

The implementation of the research is done with the help of Java programming in Eclipse IDE. The use of java is preferred here as it is scalable and provides various classes to perform the operations with ease.

The process of encryption follows a image read operation which is read as a byte stream. The pixel array (1-D) is then parsed to form a 2-Dimensional array of (**width * height**) by bit shifting the RGB values to obtain an integer pixel value as below:

- 1) Alpha (24 – 31) – 24-bit shift
- 2) Red (16 – 23) – 16-bit shift
- 3) Green (8 – 15) – 8-bit shift
- 4) Blue (0 – 7) – No bit shift

In order to obtain RGB to integer the process follows a left bit shift and integer to RGB follows a right bit shift as specified above. The pseudocode is shown in Algorithm 1.

5.1 Fisher Yates Encryption

The 2-Dimensional array is parsed using a random number for each index of the array and swapped using the Fisher Yates method. In order to improve the speed of the encryption, the swapping is done in the array instead of creating a new array and performing the swap to the new array. This improves the speed of encryption. The pseudocode is shown in Algorithm 2.

At this stage of Encryption, the NPCR value is 96.476% (average), 99.72% (highest) and the Entropy value is 7.1 (average), 7.9 (highest).

5.2 Cipher Stream Chaining Encryption

At this phase of encryption, the Cipher Stream Chaining is implemented where the neighbouring pairs of pixels are taken and XORed in order to encrypt. This approach improves the complexity as the output of the first iteration is taken as one of the inputs for the next iteration along with the subsequent pixel as another input. The pseudocode is shown in Algorithm 3.

The NPCR value is 100% and the Entropy value is 7.81 (average), 7.88 (highest). At this stage the NPCR and Entropy value have been improved compared to the Fisher Yates.

5.3 Layered Encryption

In order to improve the average entropy and NPCR values, the image encryption is layered with Fisher Yates (Stage I) and Cipher Stream Chaining (Stage II). *Figure 3* illustrates the layered approach where the image after extraction is passed through the Fisher Yates encryption, which is then given as input for Cipher Stream chaining. The output of stage II is stored as the final encrypted image.

The NPCR value is 100% and the Entropy value is 7.88 (average), 7.999(highest). The layered approach thus helps in improving the overall metrics.

5.4 Decryption phase

The decryption phase takes the Encrypted image as input in order to obtain the decrypted image. The Encrypted image undergoes reverse cipher stream chaining as reverse of XOR is itself. The image then undergoes Fisher Yates decryption where the key is essential to generate the random sequence to swap the pixel back to the original position.

6 Evaluation

This section comprises of the qualitative and quantitative metrics of the image encryption process that is followed in this research. The evaluation consists of six subsections. Subsection 1 depicts the implementation of encryption and decryption for two set of samples. Subsection 2 summarises the Time to encrypt and decrypt the images. Subsection 3 to 5 are the Evaluation metrics which are NPCR, UACI and Entropy. Subsection 6 concludes the evaluation by highlighting the improvement in the research.

6.1 Encryption process

The Encryption process takes place in a series of two steps. At the first stage, the image is encrypted using the Fisher Yates method and at second stage, the first stage image is encrypted using Cipher Stream Chaining and stored as the encrypted image. The *Figure 4 and 5* below illustrate two samples of the series of encryption along with their decrypted image.

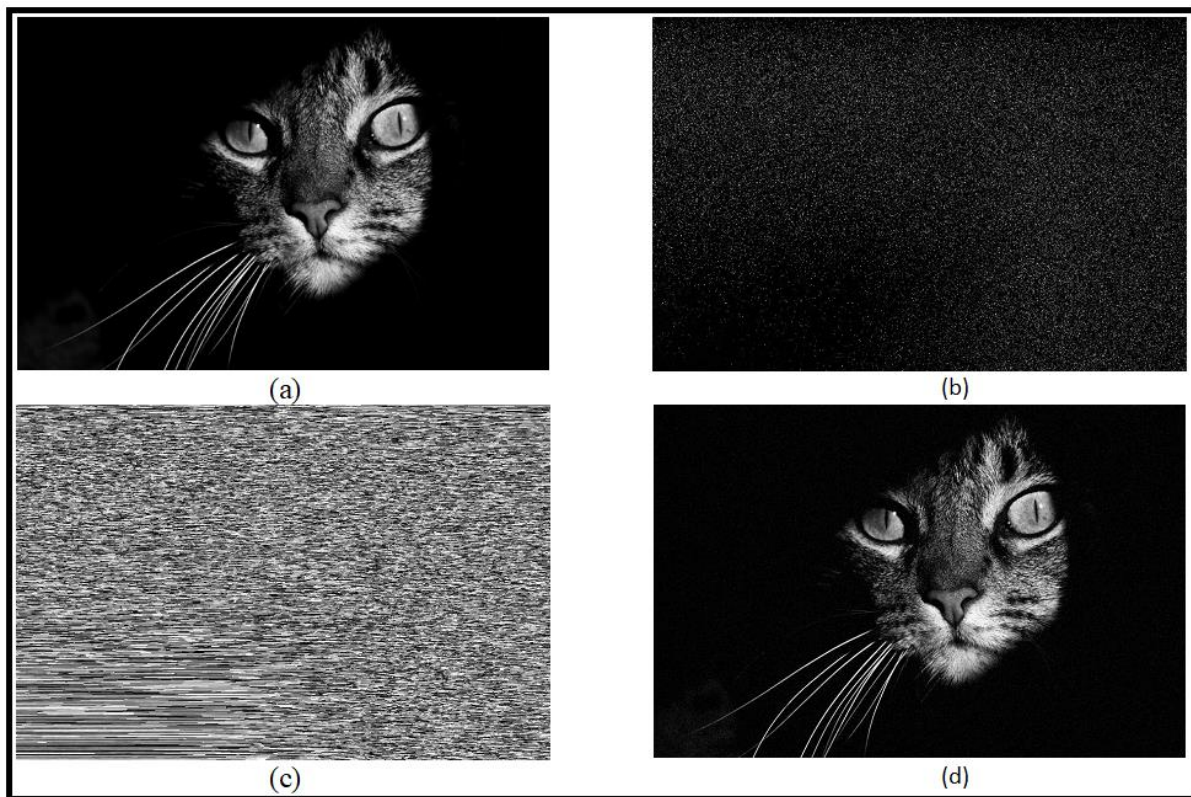


Figure 4: Cat Image
(a) Original Image (b) After Stage I Encryption (c) After Stage II Encryption (d) Decrypted Image

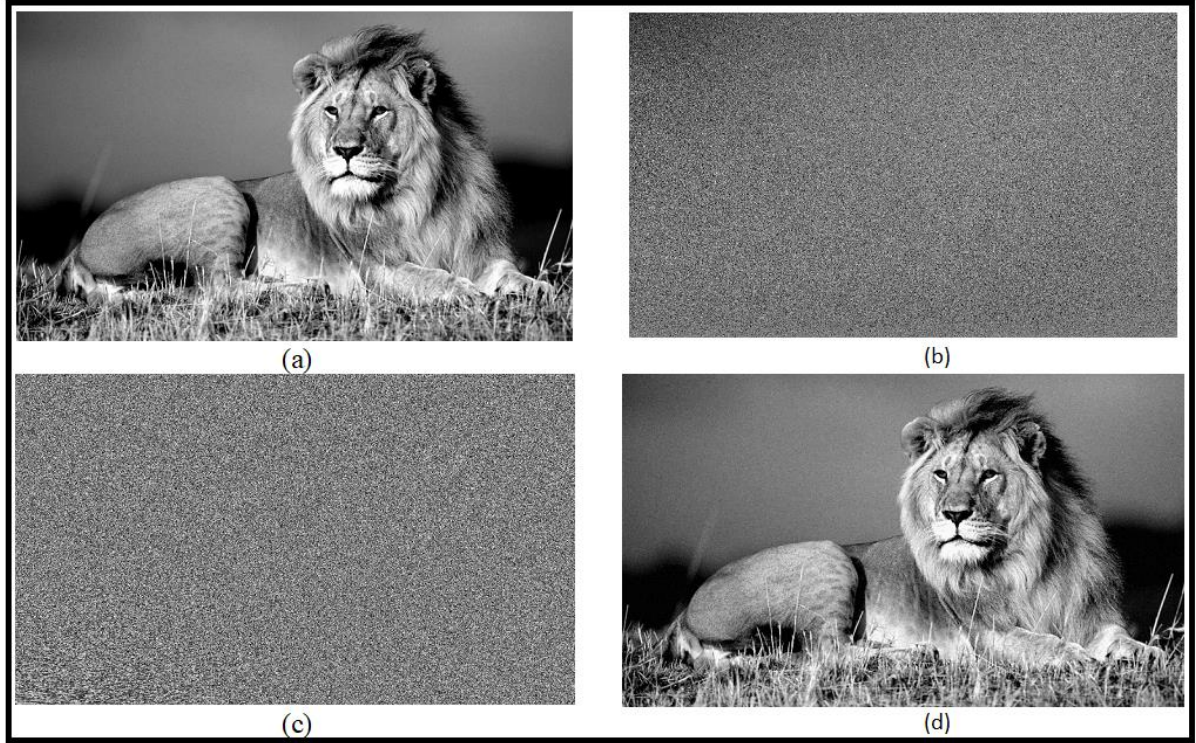


Figure 5: Lion Image
(a) Original Image (b) After Stage I Encryption (c) After Stage II Encryption (d) Decrypted Image

6.2 Net Pixel Change Ratio (NPCR)

The NPCR is a measure which evaluates the pixel transpositioned, which means it compares if the pixel value in the original image and the encrypted image is the same.

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

Where,
$$D(i,j) = \begin{cases} 0, & \text{if } original(i,j) = encrypt(i,j) \\ 1, & \text{if } original(i,j) \neq encrypt(i,j) \end{cases}$$

The ideal value is 100% which is achieved in this method. NPCR of 100% means that all pixels have been changed and doesn't resemble the image. *Table 2* shows the highest and average NPCR values in Fisher Yates, Cipher Stream Chaining and layered approach. *Figure 6* shows the NPCR plots for hundred sample images. *Figure 7* shows the Confidence Interval for Mean NPCR with 95% CI.

	Fisher Yates	Cipher Stream Chaining	Layered Approach
<i>Highest NPCR</i>	99.72%	100%	100%
<i>Average NPCR</i>	96.476%	100%	100%

Table 2: Average and Highest NPCR in each stage of Encryption

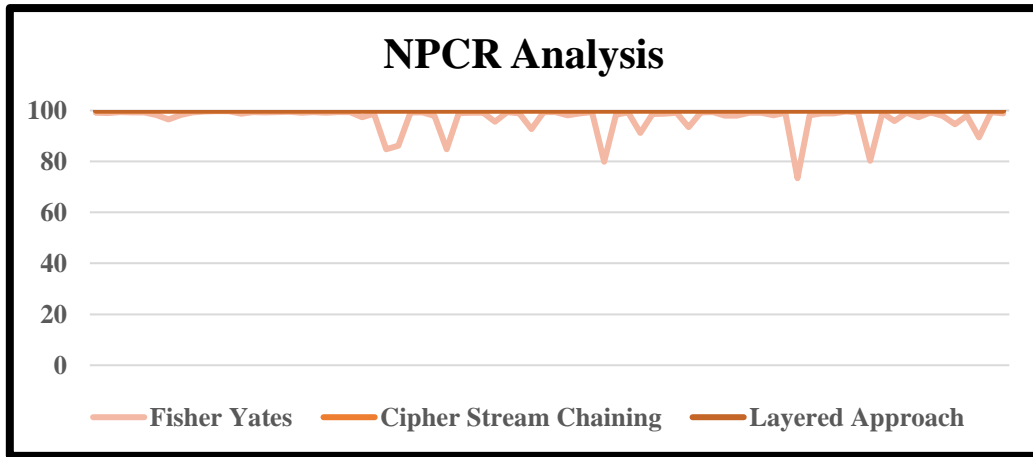


Figure 6: NPCR Comparison

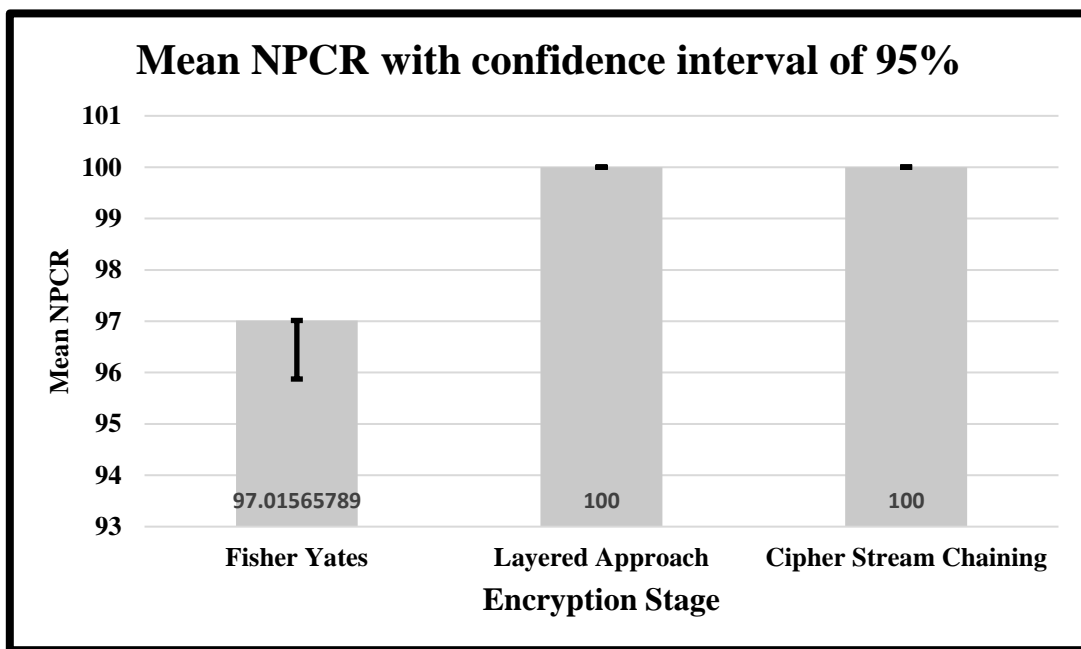


Figure 7: Confidence interval plot of NPCR

6.3 Entropy Analysis

The Entropy is the study of randomness or chaos in an image. The ideal value of an encrypted image is close to 8. In the implementation, entropy value is 7.1 in Fisher Yates, 7.81 in CSC and 7.88 in layered approach (on average of 100 images) which is summarized in *Table 3*. The maximum entropy (on average) is achieved in the layered approach.

	Fisher Yates	Cipher Stream Chaining	Layered Approach
Highest Entropy	7.904	7.88	7.9999
Average Entropy	7.1	7.81	7.88

Table 3: Average and Highest Entropy in each stage of Encryption

The *Figure 8* shows Entropy plot where images are in X-axis and the Entropy values (both stages) are in Y-axis. *Figure 9* is the Confidence plot for Mean entropy with 95% CI.

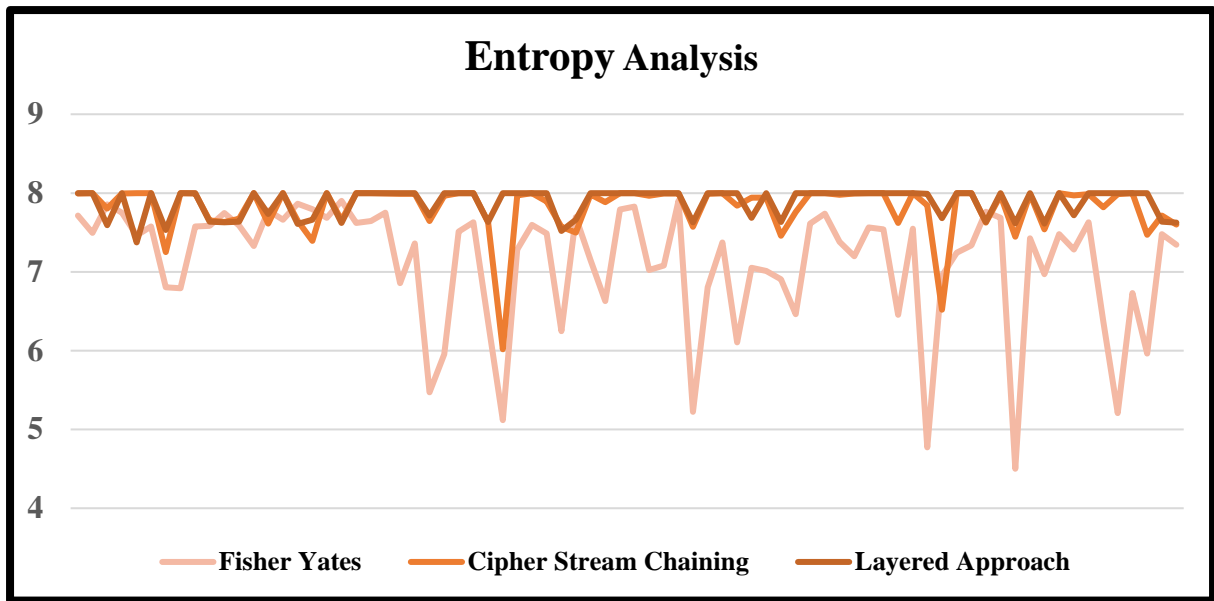


Figure 8: Entropy Analysis

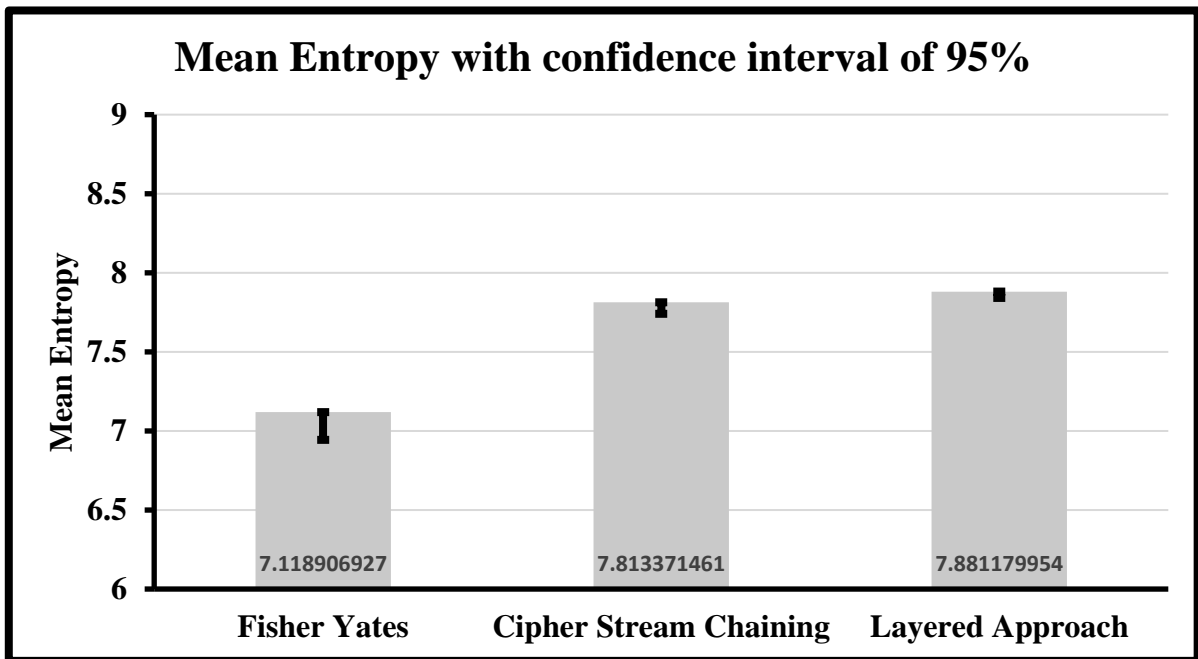


Figure 9: Confidence interval plot of Entropy

6.4 Uniform Average Colour Intensity (UACI)

The UACI defines the colour distribution in an image. The image is ideally encrypted if the value of UACI is around 33.4%.

$$UACI = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F \times T}$$

	Fisher Yates	Cipher Stream Chaining	Layered Approach
Average UACI	26.52%	34.14%	35.26%

Table 4: Average UACI in each stage of Encryption

The UACI plot is done using a sample of 100 images where each image is taken in the X-axis and UACI value of each component is stacked in the Y-axis. *Figure 10(a),(b)* shows the UACI of Fisher Yates and Cipher Stream Chaining encryption which is not uniform and thus varying, whereas in *Figure 10(c)* where the layered encryption is plotted, the RGB distribution is uniform. *Figure 11* depicts the confidence plot of mean UACI with 95% CI.

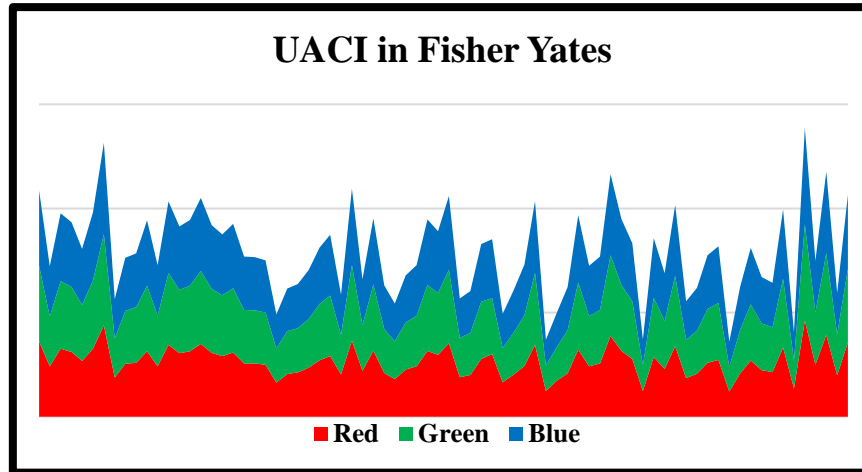


Figure 10 (a): UACI in Fisher Yates

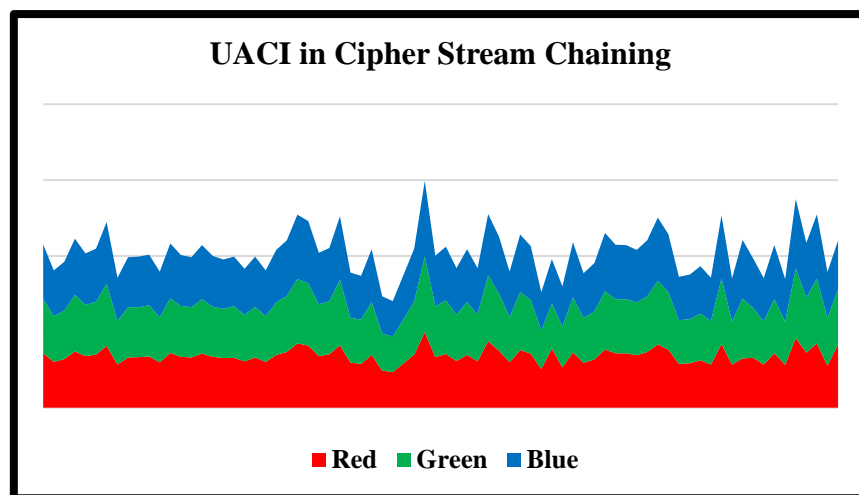


Figure 10 (b): UACI in Cipher Stream Chaining

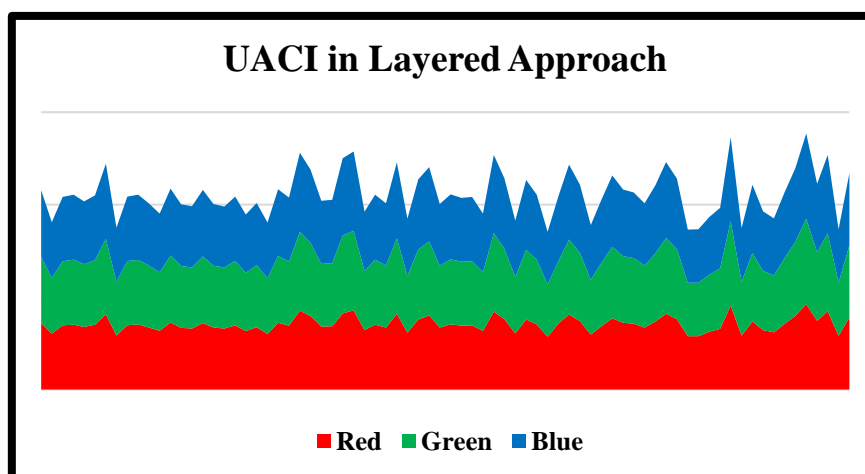


Figure 10 (c): UACI in Layered Approach

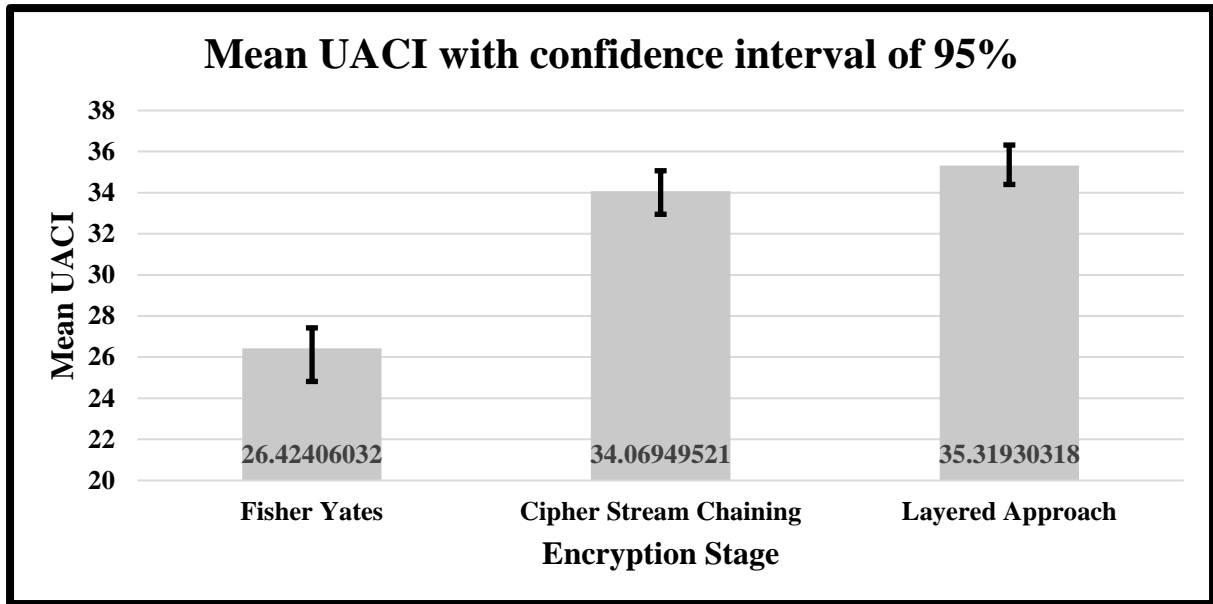


Figure 11: Confidence interval plot of UACI

6.5 Encryption and decryption time

The size of image ranges from 2398 x 2400 (largest) to 250 x 250 (smallest). The average of 100 images sizes to 678 x 895. Also, the time to encrypt a 250 x 250 image is only 0.16 seconds, whereas it is 0.26 seconds in average. The time taken for encryption and decryption is in Table 5.

	Time taken for 100 images (in seconds)	Time taken per image (in seconds)
Encryption	26.11	0.26
Decryption	23.04	0.23

Table 5: Average time for encryption and decryption

6.6 Conclusion

The Yates Fisher method with Cipher Stream Chaining is implemented in this approach yields results that are similar with ideally encrypted image. The time taken to encrypt the image is less as in the other research, the image size is less (256x256) whereas comparing to this evaluation where the image size is 678x895 (average) and following a dual layered approach, the time for encryption 0.23 seconds shows that the method is fast. The time to encrypt a (250x250) image is only 0.16 seconds. The Entropy value is 7.999 (≈ 8) and the NPCR value is 100%. The UACI values is 35.26% ($\approx 33\%$).

7 Conclusion and Future Work

Image encryption by a quick and efficient approach is the motive behind this research. The implementation helps to encrypt and secure the medical images like X-ray, reports; thus, easing the process of cloud adoption by healthcare. The evaluation metrics to quantitatively assess the extent of encryption are NPCR and Entropy, besides the time to encrypt/decrypt the image. The past works relating to the image encryption using Fisher Yates method have not achieved the NPCR and Entropy values as achieved in this research. The NPCR (100%) and Entropy

(7.999) value is ideal. Thus, the approach ensures that the method can generate an ideally encrypted image.

The future work for the research would be to improve the UACI values; also, to implement the Diffie-Hellman key exchange to authenticate the decryption using a secret key from two users or accessors to ensure privacy and security. The speed for encryption and decryption needs to be compared with other implementations to study the performance.

Acknowledgement

I am thankful to my thesis supervisor Dr. Sachin Sharma for constantly encouraging and motivating me throughout the course of the project which helped me to thrive towards the successful implementation. The critics about my approaches helped me to direct myself towards a more efficient and novelist research implementation, without which this wouldn't have been possible.

References

Abdel-nabi, H. and Al-haj, A. (2017) 'Encryption and Histogram Shifting Watermarking', pp. 802–807.

Abdullah, H. N. and Abdullah, H. A. (2017) 'Image encryption using hybrid chaotic map', *International Conference on Current Research in Computer Science and Information Technology, ICCIT 2017*, pp. 121–125. doi: 10.1109/CRCISIT.2017.7965545.

Ahmad, M. (2014) 'A gray-scale image encryption using Fisher-Yates chaotic shuffling in wavelet domain', *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*. IEEE, pp. 1–5. doi: 10.1109/ICRAIE.2014.6909175.

Alam, S., Zakariya, S. M. and Akhtar, N. (2014) 'Analysis of Modified Triple-A Steganography Technique using Fisher Yates Algorithm', *2014 14th International Conference on Hybrid Intelligent Systems*. IEEE, pp. 207–212. doi: 10.1109/HIS.2014.7086199.

Amalarethnam, D. I. G. (2015) 'Image Encryption and Decryption in Public Key Cryptography based on MR', *2015 International Conference on Computing and Communications Technologies (ICCCT)*. IEEE, pp. 133–138. doi: 10.1109/ICCCT2.2015.7292733.

Bing, L. (2017) 'An Image Encryption Algorithm of Scrambling Binary Sequences by Improved Logistic Mapping', pp. 1747–1751.

Brindha, M. (2018) 'Multiple stage image encryption using chaotic logistic map', *Proceedings of the International Conference on Intelligent Sustainable Systems, ICISS 2017*. IEEE, (Iciss), pp. 1239–1243. doi: 10.1109/ISS1.2017.8389384.

Hazra, T. K. and Bhattacharyya, S. (2016) 'Image Encryption by Blockwise Pixel Shuffling Using Modified Fisher Yates Shuffle and Pseudorandom Permutations', *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. IEEE, pp. 1–6. doi: 10.1109/IEMCON.2016.7746312.

Huang, H. and Yang, S. (2018) 'Image Encryption Technique Combining Compressive Sensing with Double Random-Phase Encoding', 2018.

J, Mahalakshmi; K, K. (2016) 'AUSTRALIAN JOURNAL OF BASIC AND An efficient Image Encryption Method based on Improved Cipher Block Chaining in Cloud Computing as a Security Service', 10(2), pp. 297–306.

Kumar, A. and Nishchal, N. K. (2018) 'An image encryption scheme employing quick response codes', *2018 3rd International Conference on Microwave and Photonics, ICMAP 2018*, 2018–January(Icmapp), pp. 1–2. doi: 10.1109/ICMAP.2018.8354586.

Kumar, R. (2017) 'Image Encryption Based on Pixel Transposition and Lehmer Pseudo Random Number Generation', pp. 1188–1193.

Li, P. and Lo, K. (2015) 'Joint Image Compression and Encryption Based on Alternating Transforms with Quality Control', *2015 Visual Communications and Image Processing (VCIP)*. IEEE, pp. 1–4. doi: 10.1109/VCIP.2015.7457867.

Murugan, B. and Nanjappa Gounder, A. G. (2016) 'Image encryption scheme based on block-based confusion and multiple levels of diffusion', *IET Computer Vision*, 10(6), pp. 593–602. doi: 10.1049/iet-cvi.2015.0344.

Nayak, A. A. *et al.* (2018) 'Security issues in cloud computing and its counter measure', *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings*, 2018–January, pp. 35–41. doi: 10.1109/RTEICT.2017.8256554.

Safi, H. W. and Maghari, A. Y. (2017) 'Image encryption using double chaotic logistic map', *Proceedings - 2017 International Conference on Promising Electronic Technologies, ICPET 2017*, pp. 66–70. doi: 10.1109/ICPET.2017.18.

Sharma, M. (2016) 'Chaos Based Image Encryption Using Two Step Iterated Logistic Map', *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*. IEEE, pp. 1–5. doi: 10.1109/ICRAIE.2016.7939535.

Sharma, M. *et al.* (2018) 'Image encryption technique with key diffused by coupled map lattice', *Optica Applicata*. IEEE, 2018–January(1), pp. 35–41. doi: 10.5277/oa180103.

Singar, C. P. and Bharti, J. (2017) 'Scanning Techniques', *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*. IEEE, pp. 257–263. doi: 10.1109/RISE.2017.8378163.

Vaish, A; Kumar, M. (2018) 'Color image encryption using singular value decomposition in discrete cosine Stockwell transform domain', XLVIII(1). doi: 10.5277/oa180103.

Wu, Y. *et al.* (2011) 'NPCR and UACI Randomness Tests for Image Encryption'.