Image Processing by Key based random Permutation and Dual Encryption

MSc Internship
Cyber Security

Krithika Ilanchezhian
Student ID: X18101551

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Krithika Ilanchezhian

Student ID: X18101551

Programme: MSc Cyber Security **Year:** 2018 -2019

Module: Academic Internship

Supervisor: Imran Khan

Submission Due Date: 12/08/2019

Project Title: Image Processing by Key based random Permutation and Dual Encryption

Word Count: 4492 **Page Count:** 14

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 required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ………

Date: ………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

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):	

Image Processing by Key Based Random Permutation and Dual Encryption

Krithika Ilanchezhian
X18101551

Abstract

The development of data transfer in internet technology are highly enhanced. The enhanced features as both security development and vice versa data theft. The data theft causes a greater disaster to the data privacy. This research deals with securing of multimedia data like images. The proposed work is about secure processing of image using permutation and image encryption. The permutation of image is performed using the algorithm key based random permutation and further encrypted with blowfish and mapped by chaotic encryption. The dual patter provides a higher security to the proposed model.

Keywords: *Permutation, Blowfish encryption, Pixel, Chaotic Mapping, Decrypted image*

1 Introduction

The growth of technology development as increased the security features as well as the threat. The threat is dual time higher than the security growth. The threat is main concerned for the data stealing or information stealing of an organization or individual. The data are the asset for the attacker this data can be either text or multimedia. The recent survey provides a view that the multimedia-based attacker is highly increased, and image plays a vital role in it. The multimedia files are used for hiding the confidential text or message known as steganography, which makes the attacker more curious to steal the data.

The image-based encryption and security uses different forms of algorithm to provide a secured transmission. The encryption algorithm used from older format like additive cipher or other less secure encryption algorithm can be easily decrypted by the attacker. The newer technique of encryption provides a higher security to image processing and reduce the attacks performed to steal the data.

The research proposed is to build a more stronger image processing way to prevent the data stealing of image. The proposed method is based on the image permutation and image encryption. The method is used for providing secure image processing. The structure of the method used is divided into two parts. The first part is to permute the image and second phase to encrypt the image.

The permutation of the image is performed using Key based random permutation. KBRP takes place based on the pixel position and scrambles the image into to unreadable form like a puzzle and generates a unique value for decryption. The scrambling of image based on the pixel makes it difficult to descramble the original form without the proper decryption key or value.

The scrambled image is further secured by encryption. Encryption in proposed system is based on blow fish and chaotic encryption. The blow fish and chaotic encryption are powerful and unbreakable algorithm which increases security of the model. Blow fish algorithm is based on natural language processing and chaotic uses mapping technique to encrypt. This algorithm combined with each other makes the model efficient and protect the data with confidentiality and integrity.

The research is to analyse the security provided by the permutation and encryption. The encryption algorithm is not only enough to provide security to image. Image consist of large-scale data which makes it harder to rest on single algorithm or the commonly used algorithm. Which makes the process to rely on a newer and stronger pattern encryption algorithm. The model with higher manipulation and encryption of image are required.

2 Literature Review

The recent studies about the image encryption and security are highly increasing to develop a stronger and fastest encryption algorithm for image security. The methods and technologies implemented by different researchers provides the knowledge to develop a stronger and robust version of the image processing algorithm and permutation strategies. Each researcher uses a different strategy to implement and evaluate the system which can be used for analyzing the proposed model strength.

The previous work for image encryption using advance encryption standard by Zhan et al provides an image processing environment using MATLAB. The AES is encryption is executed with a key size of 128bit. The MATLAB provides an efficient environment develop the algorithm using the advanced numerical calculation and tools. The system uses a stronger encryption algorithm the key size a further increased to make more secured and if the key size less the algorithm can be easily broken, and the data can loot by the intruder (Zhang and Ding, 2015).

The research by Kankonkar et al using image encryption and stitching provides a secure pattern and idea for developing a secure system. The rescuer uses the portioning method to divide the data into portion based on the initialized portioning value. This method uses a portioning value of 4 and the image divided into 4 parts. The portioned images are encrypted using chaotic logistic mapping and transferred. The data cannot be decrypted without the 4 divided parts stitched together. The data stealing is harder as the attacker cannot reverse image with single part of the data. According to the research the stitching algorithm is used by the receiver to decrypt the image. The chaotic logistic mapping uses the shift register and feedback registers to generate the key for encryption. In this case if a part of the image is failed to be transferred to the receiver leads to failure of decryption and data loss is possible (Kankonkar and Naik, 2017).

2.1 Permutation

The scrambling of image or interchanging the pixels values to create unreadable image is performed using the permutation method. The research using permutation is performed by Pallavi et al, for image encryption using the random pixel values with scenario to sustain the quality of the image. The permutation of the images is performed with key value of 64 bit. The research is about providing the confidentiality to the data. The lower key value can be easily attacked by the intruder (Pallavi Indrakanti and Avadhani, 2011).

The research by Dixit states the way to enhance the key length. The researcher uses a key length of 43-digit to eliminate the flaws of 8-bit key based permutation. The permutation is performed in addition with XOR operation for scrambling the values. The permuted image is XORed with 48 bits key to produce a stronger encrypted image. The research to produce a stronger key by increasing the key length (Dixit, 2012).

The researchers Dewangan et al provides a technique to increase the security of the key by random permutation and enhance the key sequence. The research converts the image into stand two-dimensional array for easy permutation's arrayed image is permuted based on the pixel value. The researcher uses a long key value to avoid brute force attack and also explains the difficult to attack a longer key value. The outcomes of the permutation with single combination leads to a weak output rather than using multiple permutational combination like pixels and bits (Dewangan, Kamargaonkar and Shankaracharya, 2015). The pixel combined with bits provides a stronger key and faster encryption then the pixel with pixel combination. This research provides stronger way to build the permutation in the proposed by avoiding the security flaws.

The paper by Essaid et al deals with permutation in dual pattern. The chaotic mapping is used for creating a random number for permutation to scrambles the rows of the picture and generates a second value of sequence to swap the columns of the image which provides higher diffusion to the image (Essaid et al., 2019). The paper provides a stronger and advanced encryption pattern and key for the permutation.

The research on key based permutation in medical by Bhopi et al states the process of permutation by interchanging the position in three direction of the image by row, column wise and diagonal wise with binary key value. Further the image encrypted by using chaotic logistic mapping and used for generation the random number for pixel encryption. This model provides a stronger permutation system by scrambling the image in all the three direction (Bhopi, Dongre and Gulwani, 2016).

2.2 Encryption

The researcher Kanagalakshm et al uses the improvised version blow fish algorithm for encryption by improving the security of the key and evaluates the system based on the space and time complexity values. The system is developed using java platform and evaluated. The system as a weaker password sharing environment. The blowfish is based on the symmetric encryption standard and uses the same key for encryption and decryption. If the key value is less and key strength is weak the algorithm can be easily broken. The blow fish algorithm is stronger algorithm when used with a larger key size (Kanagalakshm and Mekala, 2016).

The research by Francois et al states the methodology of chaotic encryption using the model iterative encryption using chaotic standards. The image is encrypted by converting into binary format to perform diffusion. The key with larger size is used for avoiding the brute force combinational attacks. The encryption is sensitive to the key length. The model provides a storage space to store the binary value image to map the key values. The key with large value will provide a stronger encryption if the key value is altered or modified to lower key size the model can easily attacked by the attackers (François et al., 2012).

The Chaotic image encryption by frequency domain by Jonathan et al states the encryption by multiple block scrambling and encrypted using the chaotic mapping. The researcher uses the frequency-based domain scrambling to avoid flaws of spatial domain. The overlapping blocks are removed in each level of scrambling and permuted using the random parameter. This model resists all forms of plaintext attacks as the permutation dependents on the plain image. This model is also sensitive to key stream. The survey provides the idea to develop a secure algorithm based on the resistivity to the key size and overcome the attacks to steal the data (Jonathan, Musheer and Omar, 2017).

3 Research Methodology

The research based on the efficiency and the security of the algorithm used for secure image processing. The model is design using permutation and encryption algorithm to enhance the security. The research methodology is designed into two phases and data is collected from the user further verified using the noise ration and encryption performed. The process follows in order from collecting the input from user further permuting it using key based random permutation and encrypted by blow fish and mapped using chaotic mapping. The detailed architecture of the model is discussed in the design and implementation.

The scrambling of image using key based random permutation is based on computing the pixel value of the image capacity as P out of P! (factorial). The permutation manipulates the matrix of the image based on the pixel values in the row and columns and generates the output. The permutation stores the value in single dimensional array equal to capacity of the permutation value P.

The permuted output is taken as the input for encryption. The encryption is a symmetric encryption standard and use a key size of 36 to 448 bits. Same key value is used encrypting and decrypting the data. The encryption values are mapped using chaotic mapping and cannot be decrypted without a proper key this allows the user to transfer or send the information in secure platform (Singh, Kr. Singla and S. Sandha, 2012).

The data set used for the input are image data of all formats. The image are visual data made of numerous minute pixels. Pixels consist of there own values based on the visual combination of colours. The image is of two patterns coloured and black and white or grayscale images. The images with two colour combination black and white as repeated order of pixels value then trio combination. The clarity image is based the value 24 and 224 for coloured image.

The image representation in binary format for grayscale are 0 and 1. Whereas the RGB images as a higher binary value. The image for manipulation can be taken in two form either by spatial or frequency domain. The spatial domain uses the matrix format to manipulate the image. The spatial is easier to analyse and decrypt rather than the frequency domain. The proposed system uses the frequency domain for image manipulation.

The data for the experimental purpose is created using the drawing tools and personal library. The real time experimental data set are obtained from google image database. The proposed system developed using MATLAB and analysed for the efficiency and work flow. The permutation and encryption provide a secure image manipulation.

The permutation using KBRP increases the scrambling based on the key or permutation factor P which makes it harder to descramble. Further the encryption using Blow fish which is considered as the most secured and hardest breaking algorithm by crypto community is used for encrypting. The dual encryption and permutation enhance the security of the image data stronger.

4 Design Specification

4.1 Architecture Design

The architecture of the implementation explains the flow of process by getting user input data image in different file format. The process is followed by permuting the image and encrypting the image with the key and the secured image is obtained as the output.

The design also provides the phases of encryption flow and decryption as shown in the figure 1. The decryption process is same as the encryption but performed in reverse order by getting the input as secure image which is obtained as the output of the encryption process and provide the original image. The framework developed using MATLAB and evaluated based on the noise and output of the design.

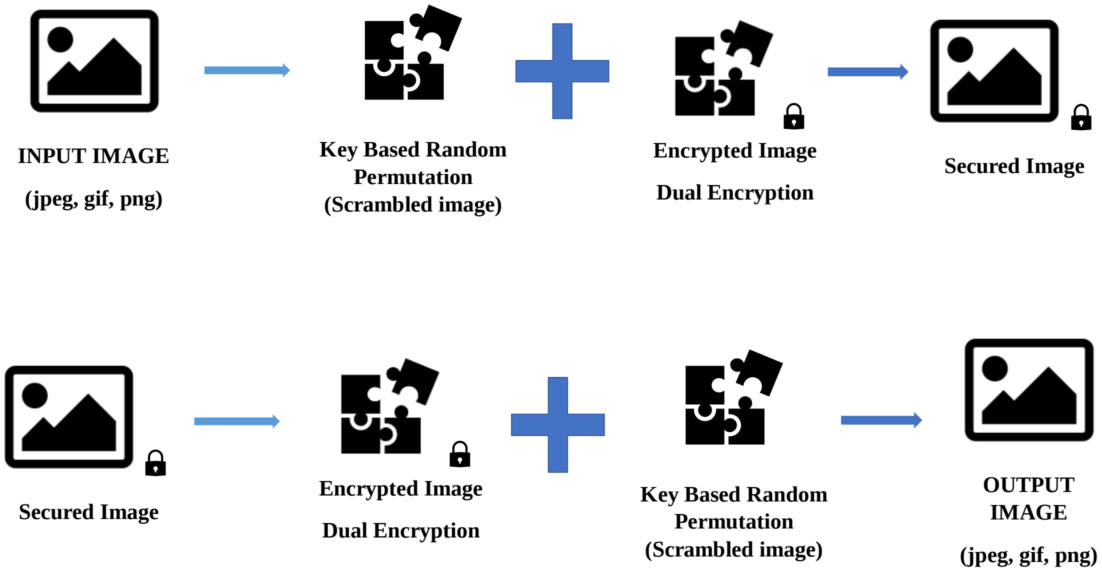

Figure 1: Process Design

4.2 Process Flow

The process flow of the system is explained using the flow chart in figure 2. The input image is taken, and the value are calculated and initialized. The initialized values are permuted using the key based random permutation and the pixel are altered based on the key. The output of the permutation is used for encryption. The encryption processes use the symmetric key too encrypt the output and map the values using chaotic mapping and obtain the final output of the encryption process. The decryption process is vise versa of the encryption.

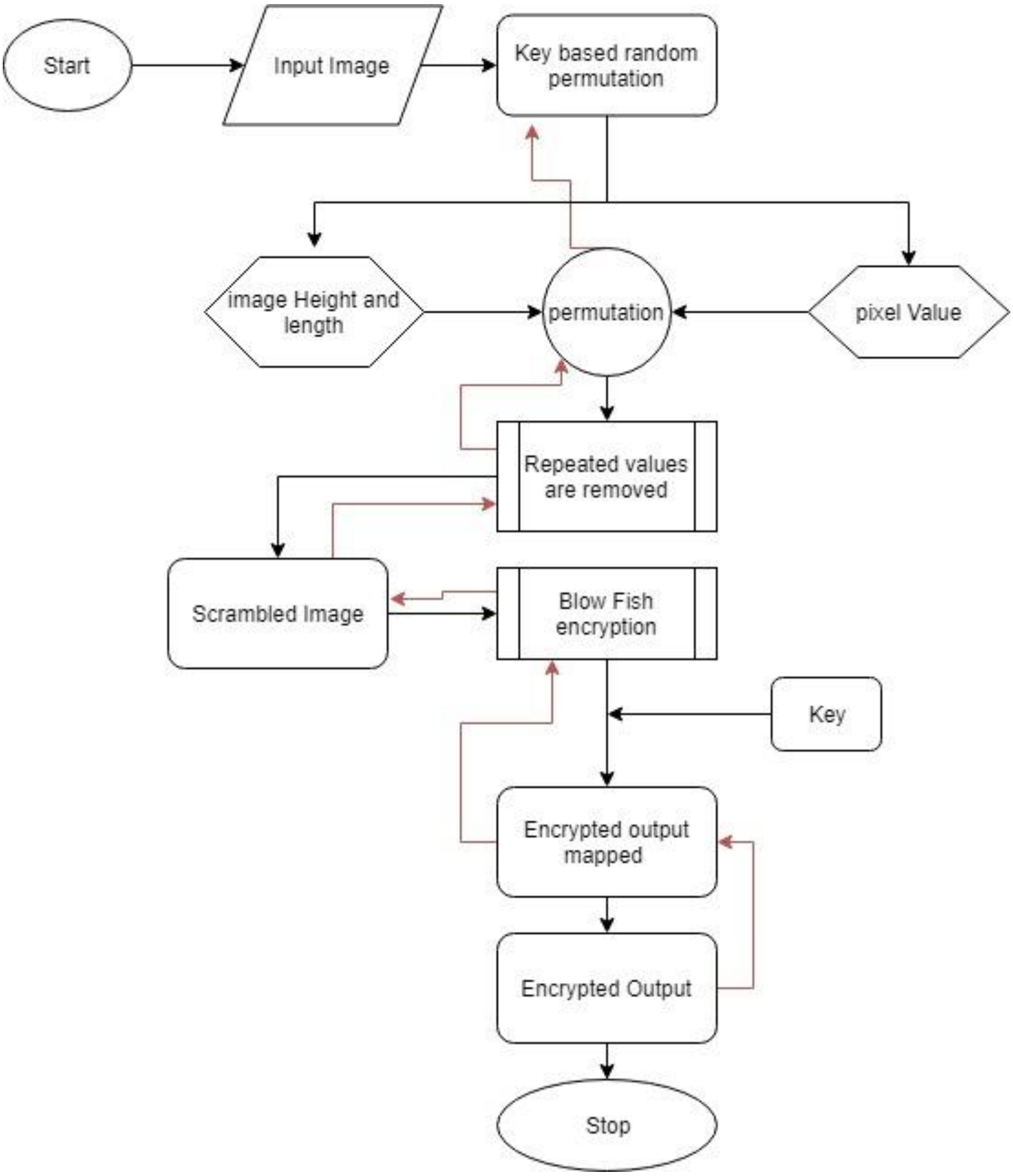

Figure 2: Encryption and Decryption Flow Chart

4.3 Algorithm

Key based random permutation is based on mathematical swapping process. The swapping or substitution is performed by setting value for the permutation constant P and the total value in the set. The total value in set will be rearranged based on the P!. Set will be permuted based on the value of P factorial and the output will produced. Permutation key vales will set based on the pixel. The higher permutation can be performed when the pixel values are higher.

Pseudocode - Key Based Permutation

```
Step 1 : The key value K is assigned based on the image height and width.
Step 2 : Pixel of the image are assigned from 0 to J.
Step 3 : The Pixel and Key value combined and permuted.
Step 4 : The permuted set is analyzed for recursive values.
Step 5 : If recursion is present the repeated values are removed, and unique values are kept.
Step 6 : The permuted output is obtained.
```

The algorithm strength is analyzed by the correlation coefficient value. When the correlation factor $|\rho|$ is less than 0.5 the image is considered to be secure.

The Blow fish algorithm is a symmetric encryption which is considered as stronger algorithm and used in most of the internet security payment and transfers. The blow fish algorithm uses a block cipher of 64-bit and key extent of 32 to 448-bit. The encryption is performed in 16 rounds to obtain the cipher block. The key extent is chosen based on the volume of the S-box or substitution box. Substitution box uses an input 8 bit and reproduces a 32-bit output (Howard and Keshav, n.d.). The encrypted value is mapped to key using chaotic mapping the creates the image to further encrypted and stronger encryption output. The chaotic mapping combines the key with permuted parameter to create a stronger key.

Pseudocode - Blow Fish and Chaotic Mapping

```
Step 1 : The scrambled image is taken as the input for blow fish encryption.
Step 2 : The image is divided into blocks.
Step 3 : Substitution box is used for initializing the key size.
Step 4 : The blocks are assigned with key K of size 32 to 448.
Step 5 : The Blow fish out is encrypted by Chaotic mapping.
Step 6 : The output of dual encryption is obtained.
```

5 Implementation

The propose system is implemented and evaluated using the MATLAB. The MATLAB provides computational tools to work with multimedia files. The tools provided in this environment helps to analyse the system and build more feasible system with maintenance.

The image is processed using frequency domain. Frequency domain process the image by mathematical representation. The frequency-based image processing is based on Fourier series and faster to compute. The pixel is converted into mathematical representation and converted back to original format.

The wiener filter process based on the frequency domain and degrades the image. The MATLAB provides the wiener filter to filter the coloured image into proper scaling and converting into grayscale image. The filter converts the image by using the Fourier series and the output is used for further process.

The image is scaled based on the most significance bit and least significance bit. The image pixel is scrambled in blocks based on the MSB and LSB values. This value helps to permute the image more precisely. The encryption is executed by adding a key to the blow fish code and executed by adding the noise to the image. The output of the implementation is evaluated using peak noise ratio of the encrypted image.

6 Evaluation

The evaluation of the proposed system is analysed based on encryption value and peak noise. The research is proposed to verify the strength of the algorithm. The strength of the algorithm is compared with existing work and propose work evaluation. The work is also evaluated based on the timing consumed for encryption and the coefficient factor of the encrypted image.

6.1 Image Evaluation

The figure shows the original image and the encrypted image. The original image is not secure when compared to the encrypted image. The encrypted image value is not able to be identified. The original and encrypted values of different images are evaluated in the figure 3.

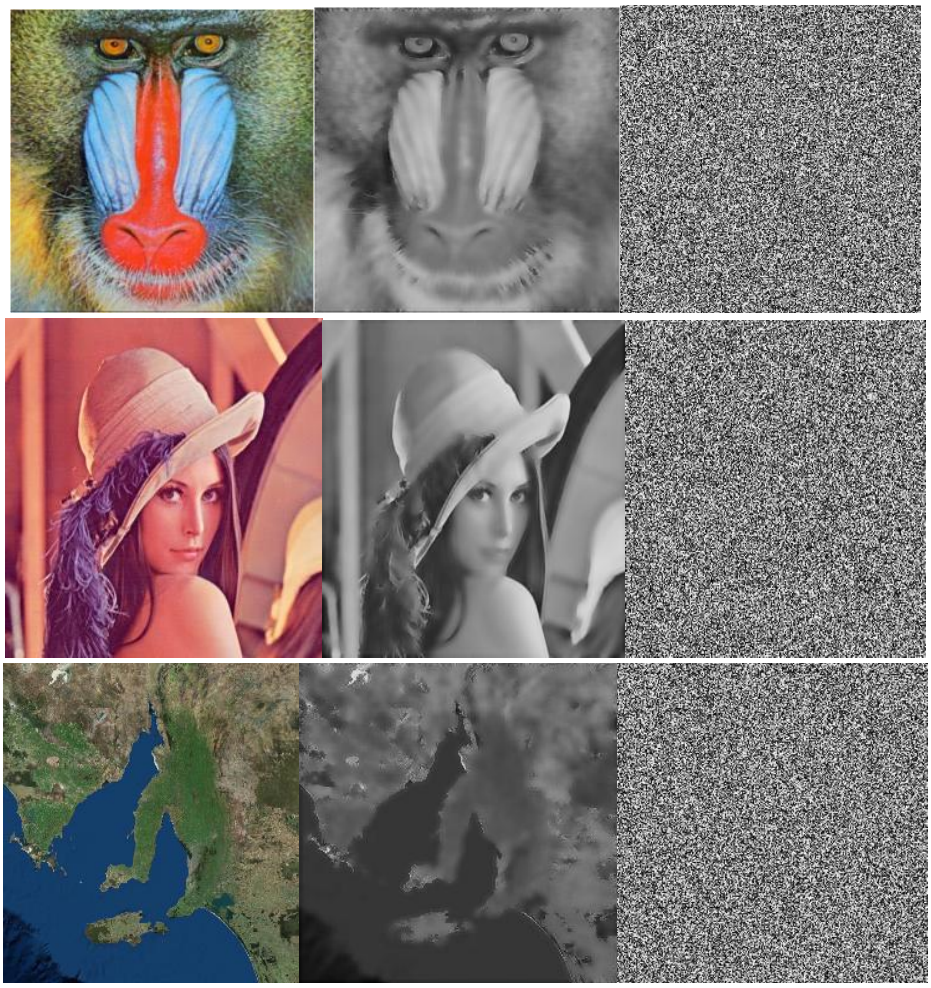

Figure 3: Original image, Filtered and Encrypted Output Image

The scrambled image shows in the figure 4 explains the process of image division by blocks and permutation process on the divided value. The wiener filtering degrades the image by adding noise and scaling the image size based on the frequency domain of the image pixels.

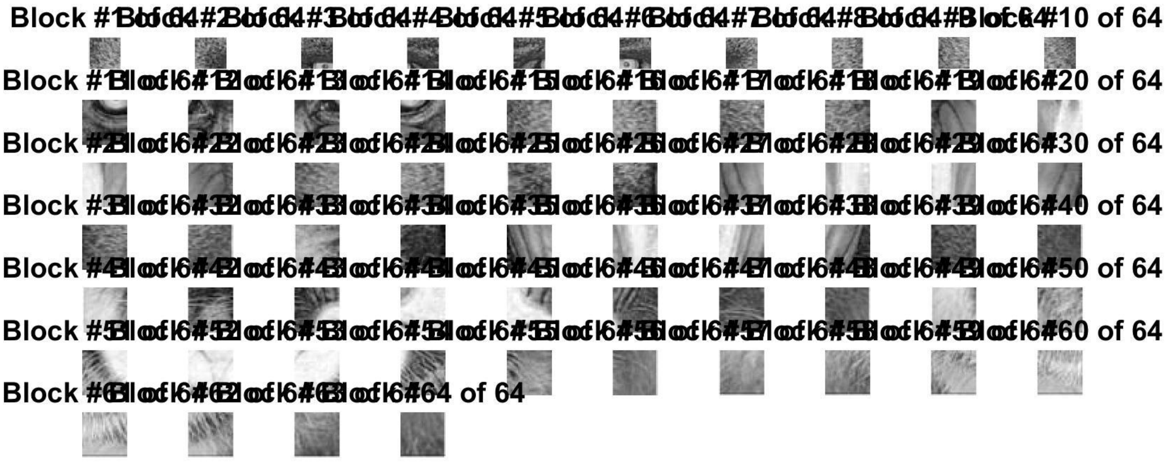

Figure 4: Scrambled Image

6.2 Peak Signal Noise Ration

The Peak signal noise ratio is computed between two images and expressed in decibels. It is used for scaling the quality of the image based on the initial and reconstructed image. If the peak signal value is higher for an image it considered as an image with better compressed quality. The design which computes or decrypts the image which matches the initial output is considered as the strongest encryption algorithm.

The peak signal noise ration and mean error for the images are calculated using the MATLAB tools. The calculation used for computing the mean and peak signal ration is (Rastislav, 2017):

$$\text{Mean }^{\wedge}2\text{ error} = \Sigma M, N\ [I1(m, n) - I2(m, n)]\ ^{\wedge}2/M*N$$

$$\text{Peak signal} = 10\log_{10}\ (\text{Imax}^{\wedge}2/\text{Mean}^{\wedge}2\text{ error})$$

The higher the peak noise value shows that the image is reconstructed properly. The table 1 provides the value of peak noise ratio in encrypted image for evaluating the model. The peak noise value of the retrieved images is 36.97 and for original image is 23.05 which shows that the peak noise value is higher and the retrieved image as better compressed quality.

Images	Encrypted	Retrieved
Image 1	36.97	23.05
Image 2	37.08	23.07
Image 3	36.92	23.06

Table 1: PSNR of Description

6.3 Graphical Evaluation

The encryption and decryption of the image is evaluated using the statistical analysis as shown in figure 5. The statistical attack will be taken place when the correlation value of the pixel adjacent to each other are higher. The higher the confuse and diffuse character makes the statistical attack impossible.

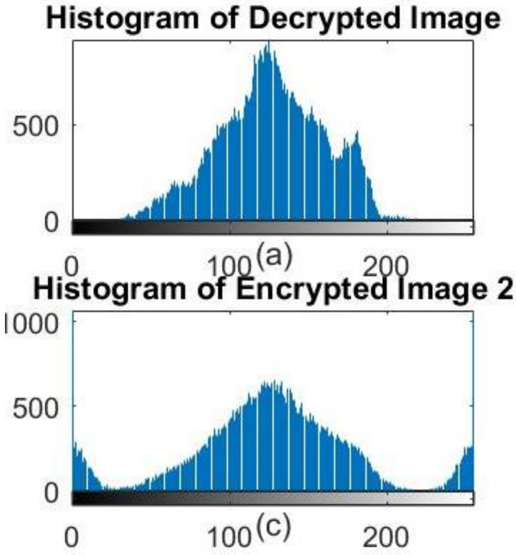

Figure 5: Graphical representation of encrypted and decrypted image

The encryption graph in figure 5 shows that the pixel values are equally distributed and does not provide any data to the attacker. In case of second encryption with a less noise contains lot of information which can be easily attacked. The decrypted image is the identical image of the input which as higher correlation value to the adjacent pixel. The encryption algorithm is stronger and provides a secured output.

6.4 Performance

The performance is evaluated based on the time taken for encryption and decryption processes. The time is calculated using tools in MATLAB and the time taken for execution is 20.60 which makes the algorithm faster processing.

The entropy examination of encrypted image provides the way to analyse the information in the image predictable or not. The entropy is calculated based on the probability of the grayscale distribution. The entropy probability for an 8-bit image over a set of 256. Then the overall entropy can be represented as 8. If the entropy value of the encrypted image should be lower than the original image value. The entropy of evaluated system is 7.99 whish is higher then the entropy value 8 (Tsai, Lee and Matsuyama, 2007).

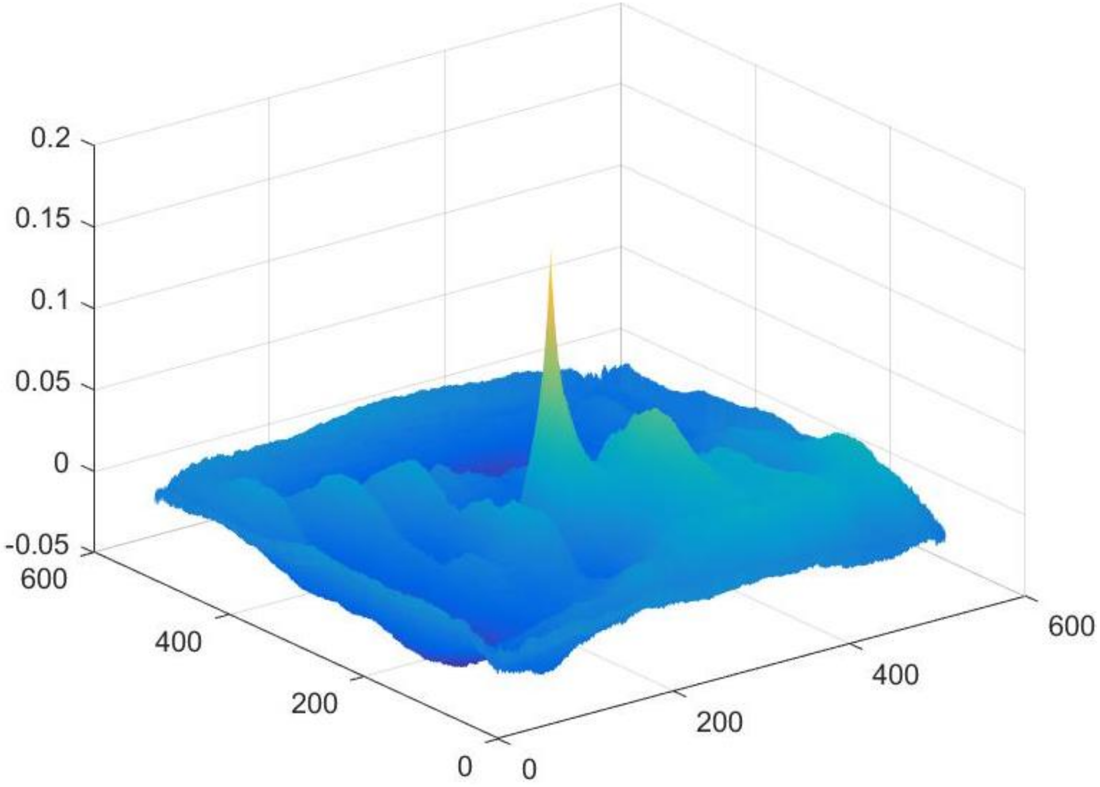

Figure 6: Peak value of the correlation factor for encrypted and decrypted image

The correlation coefficient of the images is compared in the figure 6 to evaluate the encrypted image quality. The correlation is known as the operation for extracting the data from the image. the correlation value less then 0.5 is considered as the strongest algorithm. The correlation of the input image and the encrypted image is compared. The value of encrypted image is 0.28 which is less than the correlation value 0.5. the original image had a correlation value of 0.94. based on the correlation evaluation the algorithm is considered as strongest then existing work (David, n.d.).

The number of pixel change is calculated by NPCR and the unified intensity is evaluated using UACI which analysis the image encryption security differential plain text attacks. The value obtained for NPCR is 99.62 and UACI of 31.3 which implies the algorithm is resistant to attacks (Wu, Noonan and Agaian, 2011).

Image Processing Systems	Pixel Change Ratio (NPCR)	Average od Unidentified Intensity (UACI)
Proposed System	99.62,99.66,99.61	31.3,32.34,33.4
Ref (Essaid et al., 2019)	99.61	33.41
Ref (Bhopi, Dongre and Gulwani, 2016).	99.42,99.06	30.11,31.37

Table 2: Proposed Model is Evaluated with Reference Models

The proposed system values are also compared with the output of reference models in table 2 which shows that the values are similar with each other and provides the security to overcome differential attacks.

6.5 Discussion

The existing work was developed using the single algorithm for image cyphering using asymmetric encryption standard of key size 128 bit. When compared to the existing system the proposed system as strong encryption pattern. Based on values and output of the design evaluation provides an outcome that the proposed system executes faster and encrypts the image more securely. The modern developing structure need a faster and robust with highly secured encryption pattern for multimedia processing which can provided by the proposed model.

7 Conclusion and Future Work

The research was based on implementing a stronger algorithm for image processing. The proposed method was developed with combination permutation and encryption with stronger algorithm. The recent work in image encryption need a faster and robust model for image computation. This proposed model uses dual encryption pattern to increase the security of data and also computes in given period of time. The developed outcomes provide a secured output and decrypts the image as identical to input image with filtering. The future work of this model can be used for developing security for various multimedia data like video files etc., and also create the key in real time with user interaction makes this design more feasible and advanced.

References

Zhang, Q. and Ding, Q. (2015). Digital Image Encryption Based on Advanced Encryption Standard (AES). *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*. [online] Available at: https://ieeexplore.ieee.org/document/7406040

Kankonkar, J. and Naik, N. (2017). Image security using image encryption and image stitching. *2017 International Conference on Computing Methodologies and Communication (ICCMC)*.

Pallavi Indrakanti, S. and Avadhani, P. (2011). Permutation based Image Encryption Technique. *International Journal of Computer Applications*, 28(8), pp.45-47.

Dixit, A. (2012). Image Encryption Using Permutation and Rotational XOR Technique. *Computer Science & Information Technology (CS & IT)*.

Dewangan, R., Kamargaonkar, C. and Shankaracharya, S. (2015). *Image Encryption using Random Permutation by Different Key Size*. [online] Semanticscholar.org. Available at: https://www.semanticscholar.org/paper/Image-Encryption-using-Random-Permutation-by-Key-Dewangan-Kamargaonkar/6ea332bf2d78e75b00cb5384fca85ce31108d002#citing-papers

Essaid, M., Akharraz, I., Saaidi, A. and Mouhib, A. (2019). A novel image encryption scheme based on permutation/diffusion process using an improved 2D chaotic system. *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*. [online] Available at: https://ieeexplore.ieee.org/document/8723717.

Bhopi, S., Dongre, N. and Gulwani, R. (2016). Binary key-based permutation for medical image encryption. *2016 International Conference on Inventive Computation Technologies (ICICT)*.

Kanagalakshm, K. and Mekala, M. (2016). Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key. *International Journal of Computer Applications*, 146(5), pp.41-52.

François, M., Grosges, T., Barchiesi, D. and Erra, R. (2012). Image Encryption Algorithm Based on a Chaotic Iterative Process. *Applied Mathematics*, 03(12), pp.1910-1920.

Jonathan, B., Musheer, A. and Omar, F. (2017). *Chaotic Image Encryption Algorithm Based on Frequency Domain Scrambling*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/254584474_Chaotic_Image_Encryption_Algorithm_Based_on_Frequency_Domain_Scrambling.

Singh, G., Kr. Singla, A. and S. Sandha, K. (2012). Superiority of Blowfish Algorithm in Wireless Networks. *International Journal of Computer Applications*, 44(11), pp.23-26.

Howard, P. and Keshav, D. (n.d.). *Blowfish: The first well-known encryption algorithm in public domain | CommonLounge*. [online] Commonlounge.com. Available at:https://www.commonlounge.com/discussion/d95616beecc148daaa23f35178691c35.

Rastislav, L. (2017). *Perceptual Digital Imaging*. [online] O'Reilly | Safari. Available at: https://learning.oreilly.com/library/view/perceptual-digital-imaging/9781439868935/xhtml/C012_chapter3.xhtml#chapter3

Tsai, D., Lee, Y. and Matsuyama, E. (2007). Information Entropy Measure for Evaluation of Image Quality. *Journal of Digital Imaging*, 21(3), pp.338-347.

David, J. (n.d.). *Correlation and Convolution*. [online] Cs.umd.edu. Available at: http://www.cs.umd.edu/~djacobs/CMSC426/Convolution.pdf

Wu, Y., Noonan, J.P. and Agaian, S., 2011. NPCR and UACI randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, *1*(2), pp.31-38.