Selective Region Hybrid Multiple Key Authentication System for Digital Image

Internet Security and Audit Analysis (CSE3501)

Pratyush Kumar
19BCE0506
Vishnu Shetty Belanje
19BCE2116

SLOT: L39+L40

B.Tech Computer Science and Engineering

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

Vellore Institute of Technology

Vellore

Faculty Incharge:

AJU D (SCOPE)

Abstract

Security is a very important concern in the 20th century. Pictures and multimedia data have become a common part of our life, it is very important that they are encrypted and safely secured and visible only to those who have the authority to view the data . At the same time it can be noticed that all parts of the image are not sensitive, and hence does not benefit from encryption.Our project aims to overcome this extra computations by detecting the sensitive parts of the image(faces) by using Computer Vision models and encrypting only that section of the image. We also propose a hybrid encryption algorithm that uses a two step encryption mechanism to enhance the overall security. In our proposed method we first perform symmetric encryption of the image with a user-defined key using CBC followed by an asymmetric encryption performed by the RSA algorithm. These two algorithms synergise to provide a robust and secure encryption technique that performs better than existing techniques.

Motivation

In this day and age, where pictures and multimedia data have become a common part of our life, it is very important that they are encrypted and safely secured and visible only to those who have the authority to view the data. At the same time it can be observed that not all parts of the picture are sensitive. Thus, it is redundant and can be considered a waste of resources to encrypt the whole image.

Aim

In our project we aim to identify the sensitive parts of an image through computer vision models like OpenCV and only encrypt them(Eg: faces of people are considered as sensitive information). For this project we propose a hybrid image encryption algorithm that outperforms existing algorithms in terms of security.

Methodology

To show proof of concept, in this project we will be considering people captured in CCTV footage. The faces of these people can be considered as sensitive and private data, and hence, ought to be encrypted. Traditionally, the whole picture is encrypted and stored in the database.In our proposed method we will be using Computer Vision models like OpenCV to detect and isolate the face. Once the face is detected,we will use our encryption algorithm to encrypt only the bounded box. This way we would encrypt only the sensitive data, and would save unwanted computations. It is important to note that once the face is detected and encrypted, the 4 corners of the bounded box must be stored in the image as encrypted data. These 4 corners will be very important for the decryption of the face, as it will give us the location to start the decryption. We will also be proposing a hybrid encryption image encryption algorithm to increase the security and robustness of the image.

Expected Outcome:

- CCTVs are continuously recording and hence, a lot of data is being stored. Encrypting every image of the recording can add significant overhead to the storage, especially since the whole image is not sensitive. Our proposed method significantly reduces this storage overhead by encrypting only the sensitive part (face).

- Our method will save time while encrypting and decrypting the image/footage.

- Another benefit of our method is that the surroundings of the image are still visible to everyone. Thus, the details of a crime scene's surroundings can still be seen even without the decryption key.

- Through this method it is possible to collect images while solving the issue of invading a citizen's privacy. Privacy masking has been used for this purpose in the past,but the major drawback in this method is that it cannot be decrypted in case we want to identify the person. In our method, since we are encrypting the face, the identity can be revealed with the help of a key.

This method can be extended for other uses as well such as signatures, number plates, etc.

Keywords

Partial Image encryption, Bounded Box, Diffusion, Scrambling, Arnold Cat Map, RSA, Logistic Chaotic.

Introduction

In the age of the Digital Era, sharing data in the form of images has become more common and frequent. People use social media and other means to constantly share images and multimedia.Sharing images brings the challenge of security and privacy Only the authorised user should be able to view the images. With the use of encryption images can be shared freely in public but at the same time, people cannot recognise the original content as the image is distorted by the encryption technique. Thus only with the use of the correct key by the authorised user, the original image can be obtained. .

Various image encryption techniques have been proposed over the last decade to improve the security and robustness of the image. As computers become faster, Hackers can decrypt traditional encryption techniques based on complex mathematical formulas in seconds. This has led to constant innovation of new techniques, as old techniques become ineffective as the time taken for brute force decryptions reduce.One of the better examples will be the dated DES algorithm. When it was first proposed it took 84 days to decrypt by brute force. But after a short span of 3 years as the computational power of computers increased it took only 22 hours to decrypt. It was soon replaced by the AES algorithm proposed in the 2000's. Thus there is constant innovation in the space of image encryption. And each technique remains secure as long as there are constant upgrades to combat the increase in the computational speeds of computers.

It can also be noticed that in our day to day life that every image is not fully sensitive and the whole image does not really benefit from encryption. Majority of the images are filled with backgrounds etc and it is redundant to spend resources on encrypting regions of no sensitive information. For example, in CCTV footage it can be observed that only the faces of individuals are sensitive . In our paper we will be proposing a method to detect,isolate and encrypt only the sensitive regions of the image. This significantly reduces the time and space required for the encryption of the image. We can reallocate the resources saved towards increasing the security of the sensitive regions of the image.

Encryption of any image involves two very important steps. Diffusion,changing the values of the pixels and Scrambling,changing the location of the pixels. Together these two steps serve as the base for every image encryption technique. In our paper we will be proposing a hybrid encryption technique that enhances the existing RSA algorithm, making it viable for image encryption.RSA is a very popular algorithm used for secure data transmission that relies on the difficulty of factoring large prime numbers. The large complexity involved in factoring large prime numbers, increases the security of the algorithm. At the same time RSA is not widely used for image encryption, as pixels with the same value have the same encrypted value making it visually recognizable. Thus in this paper we will be proposing an effective way to combat this drawback , while improving the security of the existing algorithm and making the technique robust.

Literature Survey

[1]This article proposes a method for partially encrypting private information in images using FF1 and FF3-1. The proposed method encrypts private information without increasing the data size, solving the problem of wasted storage space.
Using the proposed method, specific sections of encrypted images can be decrypted and recognized before decryption of the entire information, which addresses the problems besetting traditional privacy masking and image encryption methods.

[2]In the proposed image encryption scheme, an external secret key of 32-bit, a chaotic logistic map and DNA encoding scheme are employed. The initial conditions for the logistic map are derived using the external secret key by applying logical operations to all its bits and further encoding them to DNA sequence.
The proposed method uses chaotic logistic mapping and DNA encoding to encrypt the image. A 32 bit ASCII private key is used to diffuse the image. The results demonstrated clearly show that

encryption algorithm based on chaotic logistic mapping and DNA encoding gives better result than encrypting only with chaotic logistic mapping

[3]There are two main types of methods in image encryption algorithms: scrambling and diffusion. Scrambling is achieved by transforming the positions of the pixels. Diffusion is performed by changing the values of the pixels.In this paper, an image encryption algorithm based on the H-fractal structure and dynamic self-invertible matrix is proposed. This algorithm combines the scrambling and diffusion encryption methods.
The algorithm enriches the means of digital image encryption. It has high security to resist brute force attacks and statistical attacks, and it has the ability to recover when the cipher data is lost. Thus, this algorithm can be used to protect the security of digital images.

[4]The proposed system has a lightweight bit-level confusion and cascade cross circular diffusion, which diffuses a small change in the plane image to the whole image with fewer rounds to enhance the security of the cryptographic system and reduce computational redundancy in the traditional architecture.
This study combined the Arnold map with the RSA public key encryption algorithm and proposed a new asymmetric image encryption scheme that considers the difficulty of large integer factorization to ensure its security. Experimental results and tests show that the proposed asymmetric image encryption scheme is secure and effective and has high key sensitivity and good anti attack capabilities.

[5]A new chaos-based random number generator (RNG) is developed and the usefulness of the designed RNG in an encryption process is shown over NIST 800-22 randomness tests. S-Box generation algorithm is designed, and the performance tests of S-Box are realized. The proposed CS-AES algorithm is more secure and effective.
It is found that encryption and decryption times of the CS-AES algorithm are better than other algorithms, after chaos-based encryption. It also became clear that memory usage values are close to the S-AES algorithm but much better than the AES algorithm.

[6]To date, many data encryption algorithms are proposed and commonly used, such as AES, Blowfish, RC5, RSA, or IDEA.It is hard to use directly in multimedia data and is ineffective to encrypt colour images due to the high correlation between pixels. Multimedia data is often high-frequency and requires real-time interactions. In order to dispel the high relation among pixels and raise the entropy value, an algorithm based on a chaotic map is used.
The proposed system is designed to take advantage of the powerful facility, which is supported by a chaotic map resulting in a much-improved security/performance trade-off. As a result, the proposed system offers good performance for image encryption.A comparative study with the previous Blowfish algorithm shows the superiority of the modified algorithm.

[7]In this paper, a novel image encryption algorithm is proposed based on the combination of the chaos sequence and the modified AES algorithm. In this method, the encryption key is generated

by the Arnold chaos sequence. Then, the original image is encrypted using the modified AES algorithm and by implementing the round keys produced by the chaos system
The proposed approach not only reduces the time complexity of the algorithm but also adds the diffusion ability to the proposed algorithm. The key space of the proposed method is large enough to resist the brute-force attacks. This method is so sensitive to the initial values and input image so that the small changes in these values can lead to significant changes in the encrypted image.

[8]In this paper, a new two dimensional modified Henon map (2D-MHM) which is derived from Henon map is proposed. The map has a broad chaotic regime over an extensive range of system parameters, maximum Lyapunov exponent and better chaotic performance when compared to existing chaotic maps.The algorithm employs confusion and diffusion operations in consecutive manner which is different from traditional chaos based cryptosystems.
Extensive experimental findings show that the proposed algorithm can encrypt different types of images with a high security level and be able to resist various kinds of attacks. Further, the proposed algorithm offers more security when compared to traditional encryption algorithms. Therefore, the proposed algorithm can be used in diverse applications for secure communication.

[9]In this paper, we survey an existing work which uses classic and modern techniques for image encryption, as the classic techniques used for text based on alphabets as basic elements while the modern techniques overcome this limitation by using mathematical algorithms for coding the information due to their digital system.
All the mentioned techniques in the current study have their own advantages and disadvantages, but hyper-chaotic technique is the most significant and the most effective one among all. The feature which puts the chaotic techniques in the first place is its uniformity of histograms.

[10]In this paper, we propose an image encryption algorithm based on random walk and two hyperchaotic systems. The random walk method is adopted to scramble the position of pixels within a block. Furthermore, the permutation operation between blocks is presented to enhance the scramble effect. Thus, high correlation among pixels of the original image is broken by permutation.
The permutation method can effectively break the high correlation between neighborhood pixels in a plain image. Additionally, the initial keys are related to the MD5 hash value of the original image. We carry out many experimental tests and analyses, the results indicate that our encryption scheme provides high security

[11]Certain chaos-based cryptosystems have been proven to exhibit various security defects because their used chaotic maps do not have complex dynamical behaviors. This paper introduces a cosine-transform-based chaotic system (CTBCS). Using two chaotic maps as seed maps, the CTBCS can produce chaotic maps with complex dynamical behaviors.
This paper firstly proposed a cosine-transform-based chaotic system known as the CTBCS, which uses the cosine transform as a nonlinear transform to produce new chaotic maps with complex chaos performance.

[12]This study aimed at comparing Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption algorithms in image encryption using MATLAB. The comparison is done in the terms of testing image encryption quality for each algorithm. In addition, analyzing the histogram and correlation results.
The results showed that the AES algorithm correlation coefficient tends to be closer to the zero, thus a stronger correlation. Also, AES algorithm has a better image encryption quality since it has more convergent columns in the histogram.

[13]In this paper, image is used as information and different types of encryption techniques are used to encrypt it and protect it from hackers. Various parameters from each image encryption technique are found and compared with one another.
In this paper a detailed study of various encryption techniques has been made. All techniques except watermarking, give an ideal decrypted image which has been verified by different parameters. Mean Square Error (MSE) for AES is obtained maximum that is it has the highest difference between original image and encrypted image providing more security. PSNR for watermarking is maximum but it has the least MSE proving it to be a less secure technique.

[14]In this paper an efficient method to develop secure image encryption –decryption techniques is proposed. In this encryption algorithm the security of the image is enhanced with the help of AES libraries. Several test images of different sizes are used to demonstrate the validity of the encryption algorithm.
The proposed method consists of three main steps; dividing plain image into two parts ,zero padding, xoring of two encrypted messages with the third generated key which were to obtain an effective cipher to achieve security against unauthorized access during data transmission through an unsecured channel. The basic idea of this work is to show the influence of using multiple keys of various sizes for the security purpose of the algorithm.

[15]In this paper, reversible information concealing encryption key is utilized; the uncompressed picture will encode the substance through the encryption key. The triple DES calculation is utilized for household and exportable utilization for picture encryption and figure content substance.
The algorithmic rule bestowed here provides sensible lead to terms of secure correspondence the Triple DES calculation can get into the wide information concealing calculation. Steganography is the procedure used to information secure cryptography is utilized to encode and decode the information as the information concealing key and information encryption key the two assume a basic job in secure correspondence.

[16]In this paper, an existing work which uses classic and modern techniques for image encryption is surveyed. The classic techniques used for text are based on alphabets as basic elements while the modern techniques overcome this limitation by using mathematical algorithms for coding the information due to their digital system.
A comparison has been conducted between several ciphers techniques (classic and modern) for images based on various parameters such as: Histogram, Correlation, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio (PSNR),

Entropy and Time complexity. An analysis of simulation results shows that chaotic encryption techniques, especially hyper-chaotic, are the most efficient among them all.

[17]In this paper a new algorithm of encrypting and decrypting images and text files is proposed. The proposed method is implemented by combining the concepts of Diffie Hellman algorithm and Blowfish algorithm.
The proposed system attempts to ensure that the data is read by only the intended user by providing a two level security system and overcoming most of the shortcomings faced by existing algorithms.

[18]In order to improve the problems of small key space and poor security when the one-dimensional logistic chaotic map is applied in image encryption, a modified Logistic chaotic map is proposed. Based on the modified Logistic chaotic map, a new image encryption algorithm is introduced.
From the experimental simulation results and analysis, it can be concluded that the algorithm has infinite key space, and the key sensitivity is relatively high, which can resist the attack of exhaustion method analysis. The pixel values of the encrypted image are evenly distributed and the correlation between adjacent pixel values is weak, which indicates that the algorithm can resist statistical analysis attacks very well.

[19]In this work, the NIST (National Institute of Standards and Technology) special publication focused on the FF1 scheme for format-preserving encryption is analysed. Using that information, an encryption model applied to image encryption is built, upon which several tests, namely histogram and analysis NPCR (Net Pixel Change Ratio) scores, and computational cost are performed.
The proposed image encryption scheme could be applied to a biometric database together with an Identity-Based model, since the size and number of images might be small enough to perform all the needed encryptions in a reasonable time.

[20]In this paper, image as information is used. An advanced approach of well-known encryption techniques like AES, Genetic Algorithm, and RSA algorithm is used to encrypt it and keep the information safe from attacks making it highly difficult and time consuming to decipher the image without using the key.
Experimental results show that the model yields high random cipher image measured by various quality measurement parameters such as MSE, AD, MD and PSNR thus making it difficult to recover the original image without the key.

Tabular Format

Article ID	Methodology	Merits	Demerits	Efficiency
1)	(a) selection of the encryption area, (b) encryption of image pixel values using format preserving encryption, and (c) storage of encrypted image pixel values	The proposed method has no padding, so there is no increase in the data size, and the information requiring privacy can be specifically set and encrypted	Algorithm is complex and implementation is costly in the current scenario	The results of NPCR and UACI show that the proposed method perform better than the encryption using AES.The value of the information entropy is as close to the optimal value as that of the AES-encoded image
2)	An external secret key of 32-bit, a chaotic logistic map and DNA encoding scheme are employed. Further,the input image and key image will be operated to give the final encrypted image.	High-level efficiency with multimedia data. Highly secure than traditional encryption algorithms	The future scope of this work can be done improve the method of generating the cipher image using key	The results show that encryption algorithm based on chaotic logistic mapping and DNA encoding gives better result than encrypting only with chaotic logistic mapping
3)	H-fractal structure and dynamic self-invertible matrix based encryption.	The security analysis shows that this algorithm is easy to implement. It has a large key space and strong key sensitivity and can effectively resist plaintext attacks.	High level of computation because of multiple steps can make this method infeasible for fast encryption	99.6% NPCR and 33.5% UACI (The maximum theoretical value of the NPCR is 100%, and the ideal value of the UACI is 33.4635%)
4)	Image encryption scheme based on a generalized Arnold map and RSA algorithm. The image is first XOR diffused. The row and column directions are confused, and then the image information is hidden again by point diffusion.	The implementation process of this algorithm is simple and efficient. The proposed asymmetric image encryption scheme is secure and effective and has high key sensitivity and good anti attack capabilities.	Can be computationally intensive to encrypt the image as larger RSA values are used to make it more secure	The calculated NPCR and UACI values were 99.60289% and 33.43695%, respectively.
5)	A chaos-based hybrid encryption algorithm which employs complex dynamic features of	Higher security than chaos, AES, and S-AES algorithms. It is found that encryption and decryption times of	Even a very small change in keys will create a very different random number series	99.6368 NPCR value and 31.6329 UACI value for the proposed CS-AES algorithm.

	chaotic systems and S-AES algorithm together. Novel RNG and S-Box generation algorithm, based on scaled Zhongtang chaotic system, is used for the algorithm.	the CS-AES algorithm are better than other algorithms.	and encrypted data will not be decrypted.	
6)	An algorithm based on a chaotic map is used as a preprocessing step. An image is shuffled their positions and divided it into blocks based on the chaotic map, then passes these blocks to the Blowfish encryption algorithm.	This technique enhances the security level of the encrypted images.	Cannot be used for non-grayscale images	MSE is zero and PSNR is infinite (no loss of data in the decrypted image). 7.9697875 is the average entropy value.
7)	Combination of the chaos sequence and the modified AES algorithm. The encryption key is built using Arnold chaos system, and then, the image is encrypted using CCAES.	The CCAES algorithm is secure against the entropy attacks. Resistant to differential attacks. Reduced time complexity than traditional encryption algorithms.	Generation of secure key can be computationally intensive	99.679775 NPCR value, 33.4808 UACI value and the CCAES algorithm takes approximately 2.895s for encryption and decryption process.
8)	New two dimensional modified Henon map (2D-MHM) which is derived from Henon map is proposed. Chaotic performance is analyzed through bifurcation diagram, Lyapunov exponent spectrum and Lyapunov dimension	Offers more security when compared to traditional encryption algorithms such as RC4, RC5 and AES with acceptable running time.	Not secured against differential attacks. Not tested in different environments and different types of internet users.	99.3255 NPCR, 21.3445 UACI and 0.92766 average correlation coefficient (plain image = = 0.9296)
9)	Comparison between several ciphers techniques for images based on various parameters such as: Histogram, Correlation, NPCR, UACI, PSNR, Entropy and Time complexity	The pixels are extremely uncorrelated. The time needed for the process of searching is enhanced in having safe measures in hyper-chaotic technique. Another feature which puts the chaotic techniques in the first place is its uniformity of histograms	Some encryption algorithms require more computational power and some have high time complexity	All the mentioned techniques in the current study have advantage and disadvantage, but hyper-chaotic technique is the most significant and the effective one among all.

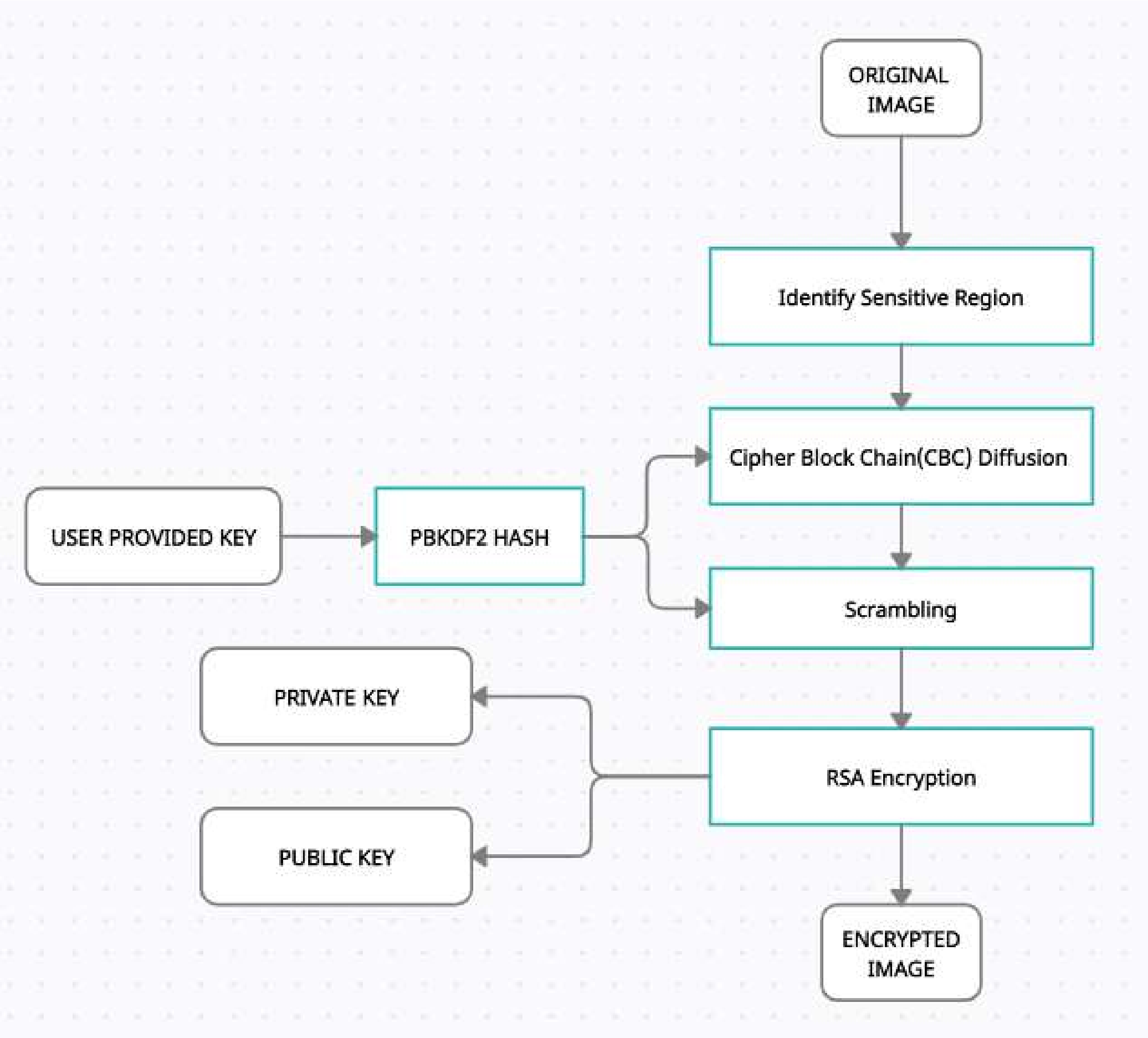
10)	The random walk method is adopted to scramble the position of pixels within a block. Furthermore, the permutation operation between blocks is presented to enhance the scramble effect	Better performance and higher security than traditional encryption methods.	Not tested with attacks other than plain-text attack	0.9961 NPCR, 0.3347 UACI, 0.425s is the execution time and the entropy value is 7.9993
11)	The LSC-IES follows the well-known diffusion-confusion concept and we simulated it using different dig- ital images	LSC-IES is quite sensitive to its secret keys, and has a higher security level than several competing image encryption algorithm	Cannot be used in real-world scenario (video encryption)	For an image of size 256 ×256, $N^{*}_{0.05}$ = 99.5693% and ($U^{*-}_{0.05}$, $U^{*+}_{0.05}$) = (33.2824% , 33.6447%);
12)	This study aims at comparing AES and RSA encryption algorithms in image encryption using MATLAB.	The study aims at comparing two different encryption algorithms and hence they are no merits stated in the paper	RSA requires more computer power supply compared to single key encryption. Slow key generation.	AES algorithm correlation coefficient tends to be closer to the zero, thus a stronger correlation. Also, AES algorithm has a better image encryption quality since it has a more convergent columns in the histogram
13)	Analyze different encryption algorithms and compare them based on various parameters to see which one is the best.	The study aims at comparing different encryption algorithms and hence they are no merits stated in the paper	Real-world implementation has not been done to test the theoretical results	No statistical data found as the paper focuses on comparing different encryption algorithms.
14)	In this encryption algorithm the security of the image is enhanced with the help of AES libraries. Several test images of different sizes are used to demonstrate the validity of the encryption algorithm.	Two fish has a large security margin, notable speed across platforms, well-suited to smart cards, and support for arbitrary key sizes, free for anyone to use without any restrictions.	It is key-dependent.	The basic idea of this work is to show the influence of using multiple keys of various size for security purpose of the algorithm
15)	The Triple DES algorithm is used to encrypt the data into cipher text. The data hiding key is generated to them as they are used to hide the data and a new key is also generated as image encryption key. One	If person doesn't have key or if they lose the key, at that point they're insufficient to play out any of the activity	Triple DES significantly increases the computational time.	DES 5.997s taken, 3DES 6.160s taken, AES 9.246s taken, Blowfish 3.975s taken for image encryption and decryption.

	key is used to hide data and another is used to update the hided info and any new updated info is required to feature or delete some unessential data			
16)	A comparison has been conducted between several ciphers techniques (classic and modern) for images based on various parameters such as: Histogram, Correlation, NPCR, UACI, PSNR, Entropy and Time complexity.	The pixels are extremely uncorrelated. The time needed for the process of searching is enhanced in having safe measures in hyper-chaotic technique. Another feature which puts the chaotic techniques in the first place is its uniformity of histograms	Some encryption algorithms require more computational power and some have high time complexity	All the mentioned techniques in the current study have advantages and disadvantages, but hyper-chaotic technique is the most significant and the most effective one among all.
17)	The proposed method is implemented by combining the concepts of Diffie Hellman algorithm and Blowfish algorithm.	Data is read by only the intended user by providing a two level security system and overcoming most of the shortcomings faced by existing algorithms. Another advantage is that the system works for multiple formats of images (.jpg, .png, .tiff etc.) and text files	Diffie Hellman and Blowfish methods when individually applied, faces a lot of security threats like man in the middle attack, data authentication etc	The file is decrypted only if the key matches. Even if the file goes in wrong hands somehow, it will remain encrypted and not readable
18)	A modified logistic chaotic map in which the range of full mapping parameters and chaotic parameters are multiplied by arbitrary β times compared to the original map	Infinite key space, and the key sensitivity is relatively high. Resist the attack of exhaustion method analysis and statistical analysis.	Requires high power of comp	The pixel values of the encrypted image are evenly distributed and the correlation between adjacent pixel values is weak

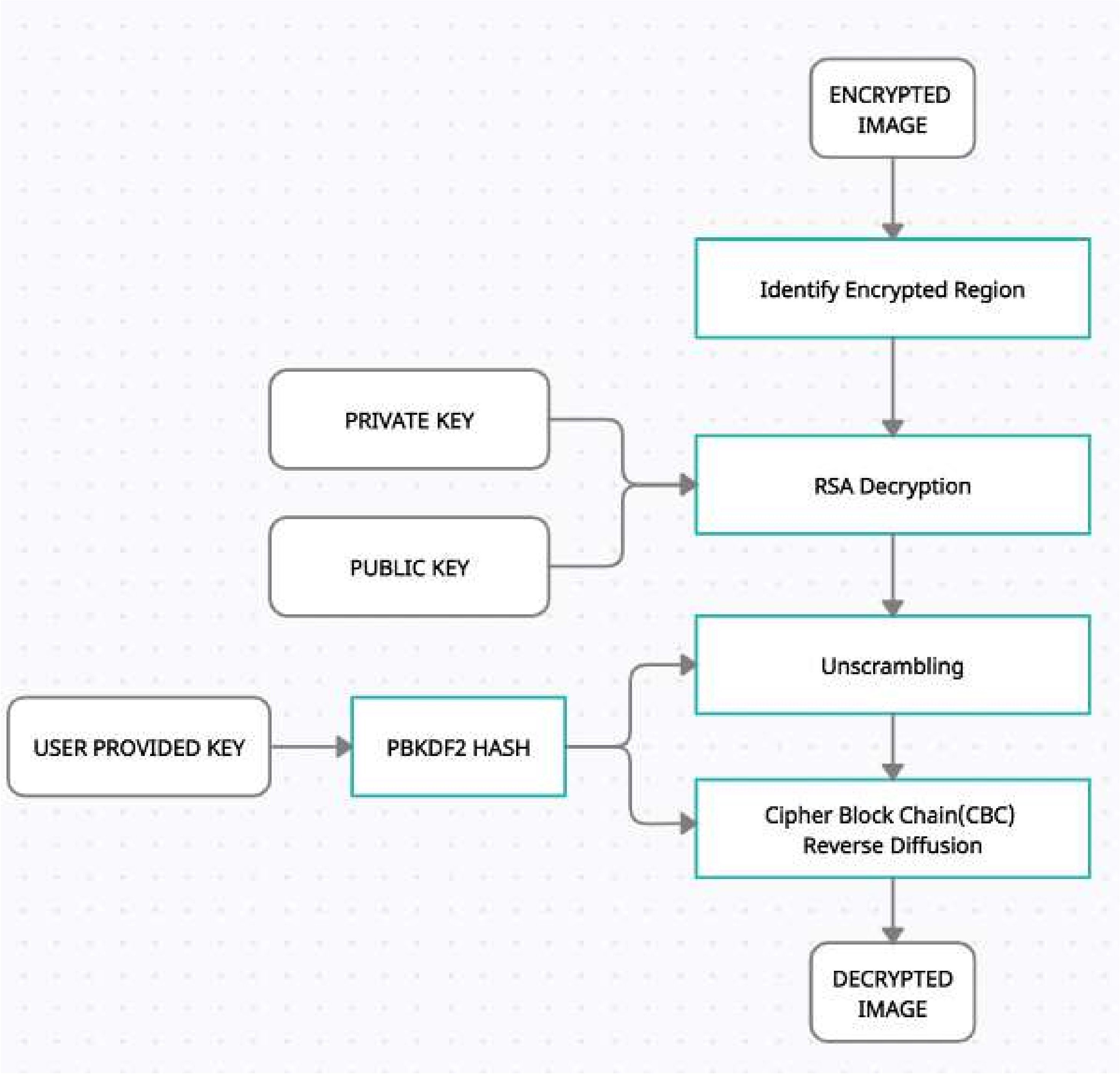
19)	An encryption model focused on FF1 scheme for format-preserving encryption based on publication by NIST.	Useful for encrypting document numbers, telephone numbers, geospatial coordinates, and potentially everything that can be stored in a database.	Huge computation time as the model uses AES encryption algorithm	NPCR values for
				R = 99.999961121,
				G = 99.999961304, and
				B = 99.999960693

20)	An image is taken as input and different encryption techniques are performed over it. A single image is encrypted with three different encryption techniques one by one in which some techniques are of symmetric algorithm and some are of asymmetric algorithm (like Genetic, AES, and RSA).	Highly encrypted image which is very difficult to decrypt without the authorization of its generator because of its dual nature i.e. symmetric and asymmetric encryption technique.	It is difficult to recover the original image without the key.	Experimental results show that the model yields a high random cipher image measured by various quality measurement parameters such as MSE, AD, MD and PSNR.

Encryption Architecture:



Decryption Architecture:



Proposed Methodology:

The first step involves the detection of the sensitive parts of the image through the computer vision model OpenCV. We make a Rectangular outline around each sensitive part by using a **bounded box**. The four corners of the bounded box are stored and the image inside the bounded box region is inputted into our hybrid algorithm.

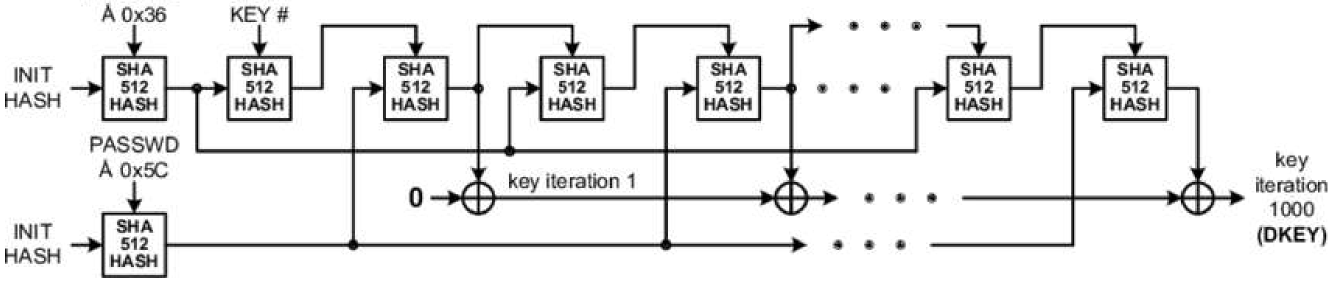
Any image encryption algorithm has two basic steps:

1) Diffusion: Changing the values of the pixels (R, G, B).
2) Scrambling: Swapping and changing the original position of the pixels.

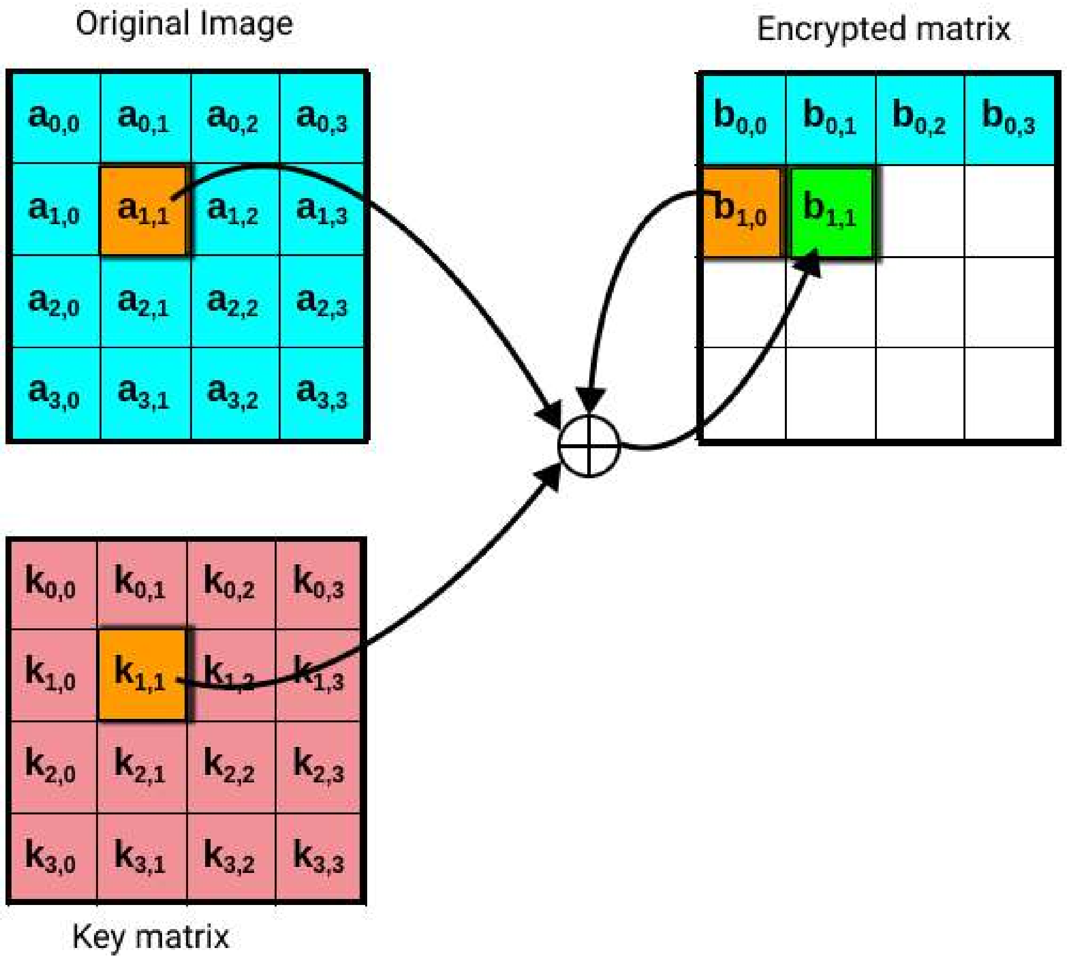
With the combination of these two techniques an image can be encrypted. The strength of the encryption highly depends on the randomness of the scrambling and diffusion.

The image encryption algorithm that we are proposing will be a combination of symmetric as well as asymmetric encryption. We will be taking a key as input from the user and performing scrambling and diffusion based on this key. We will also be performing asymmetric encryption by making use of the RSA algorithm. Thus the RSA algorithm will provide the user with the private key after the encryption.

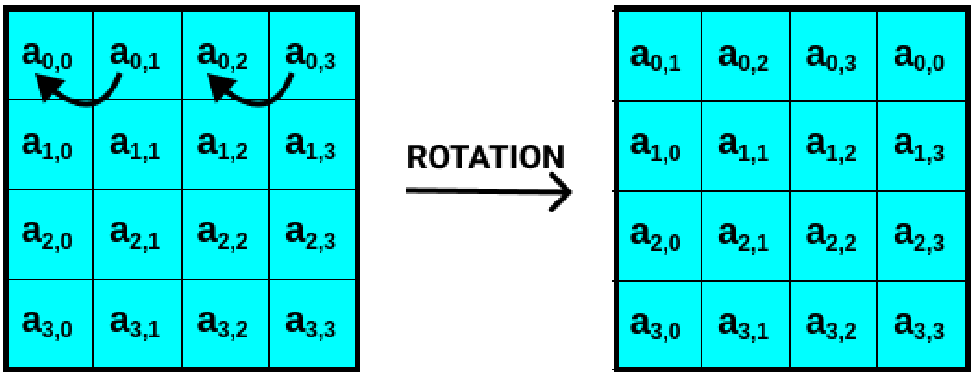
PBKDF2 Hashing: We will take the key from the user and obtain an expanded hash value, by using a key extension algorithm (PBKDF2). This algorithm is used to strengthen passwords, in our case it is used to increase the size of the key, so that its length is equal to our pixel count. This way we protect our image encryption from having a very weak key that can be decoded very easily. The values obtained from PBKDF2 are unique and will further enhance the security of the algorithm. The obtained hash value is then split into an array of N elements ranging from 0 to 256. The number of elements(N) in this array is equal to the number of pixels in the image. To further increase the randomness we add the values of 5 consecutive key values in the key array and perform modulus 256 to get the final list of key values.



Cipher Block Chaining(XOR): CBC is a very well known method and is recognised for providing message confidentiality. It is the advanced version of ECB which compromises security requirements because of the direct relationship between the original image and the key.In our algorithm we will be using the Cipher Block Chaining method to perform the diffusion on the pixels. In this method we traverse each pixel and encrypt it by performing XOR operation on each pixel with the key array as well the previous encrypted pixel.By XORing with the previous encrypted pixel before being encrypted with the key,it greatly increases the variation in the encrypted values.Thus pixels with similar r,g,b values will not have the same encrypted value,thereby making our algorithm more secure and less predictable.

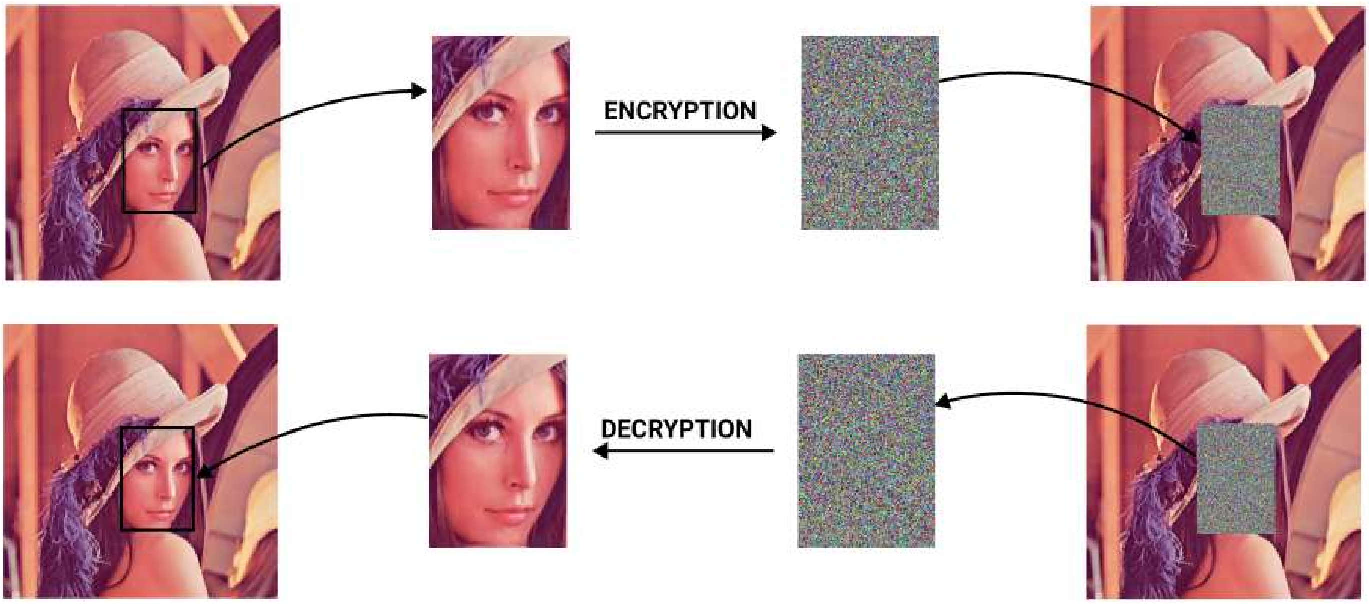

Original Image
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
Encrypted matrix
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$
Key matrix

Scrambling: In this step we perform row and column rotation on the pixels obtained from the previous step. The main aim of this step is to increase the entropy of the pixels. The pixels cannot remain close to their original position. In our algorithm we perform row rotation of pixels followed by column rotation of the pixels. This set of operations is performed 2 times to get the optimum scrambling. The rotation is based on the modulus of the key value obtained from the hash array. Thus the scrambling is unique to each key and provides added security.We alternate the direction of rotation based on the row and column number to further increase the randomness. This is a simple yet very powerful step that makes the algorithm more secure. It changes the location of the pixels making it harder to decrypt with the wrong key. Thus by effectively scrambling the pixels all across the image, we can recover most of the original image even if a part of it is lost.


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ROTATION
$a_{0,1}$ $a_{0,2}$ $a_{0,3}$ $a_{0,0}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$

RSA: RSA algorithm is an asymmetric encryption technique and its strength is based on the tremendous difficulty of factorising two large Pseudo Random Prime numbers generated during encryption.Therefore greater the key length,the longer it takes to crack the prime numbers thereby increasing the security. RSA is good for plain text,but not very effective for images as the picture may retain its visual feature after encryption. In the RSA algorithm pixels with the same value obtain the same encrypted value, and since we are using an image, the similarity of the pixels can be clearly identified. In our algorithm we perform RSA in the last step when the image has no recognizable feature because of the 2 precursor steps. Thus we overcome this drawback of RSA while adding an extra layer of security to our proposed algorithm. After encryption we provide the user with the public as well as the private key used for the encryption.The advantage of RSA is that even if the user guesses a number close to the original key, the obtained decrypted image is not recognisable. The original key alone can decrypt the original image,no other key can give the decrypted image and cracking of the original key is very time consuming and next to impossible when the key length is very large.

Thus our proposed system will have a **Multistep Key Authentication** during image decryption. The user will have to enter the **Original Key (User Generated)** as well as the **RSA Key (System Generated)** provided at time of decryption. Thus even if one of the keys is compromised, the original image will not be retrievable. By incorporating traditional XOR operation with the RSA algorithm we have come up with an effective hybrid algorithm that is very secure.



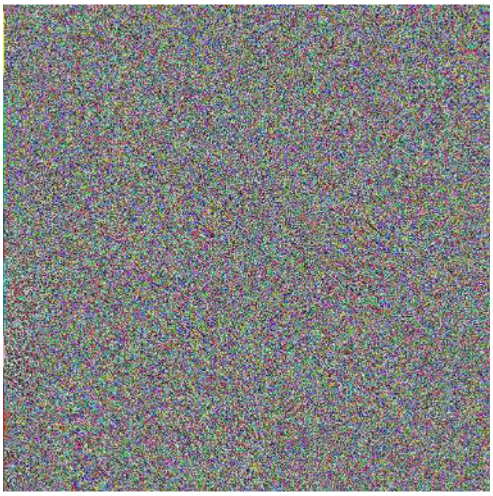
RESULTS:

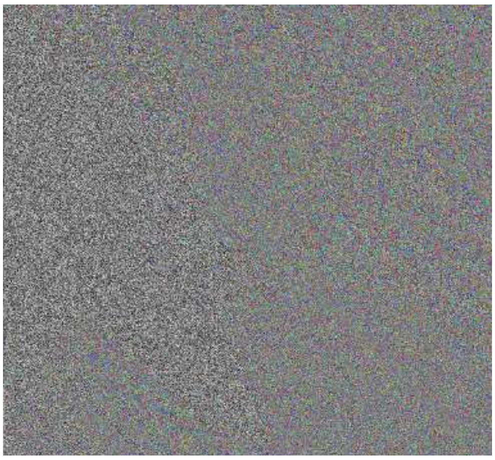
CBC:

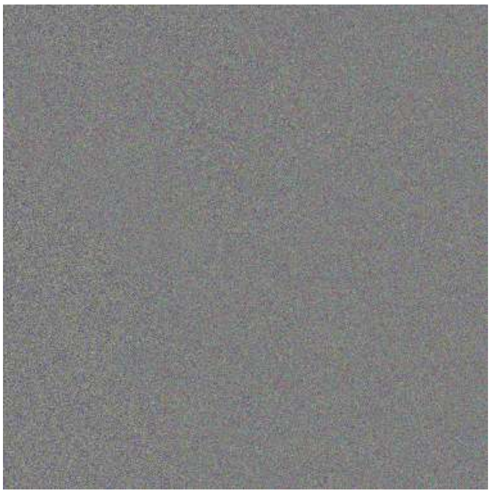
Encryption is performed by XORing the pixel value with the key from the Hash array and the previous encrypted pixel.

Original Image

Encrypted Image





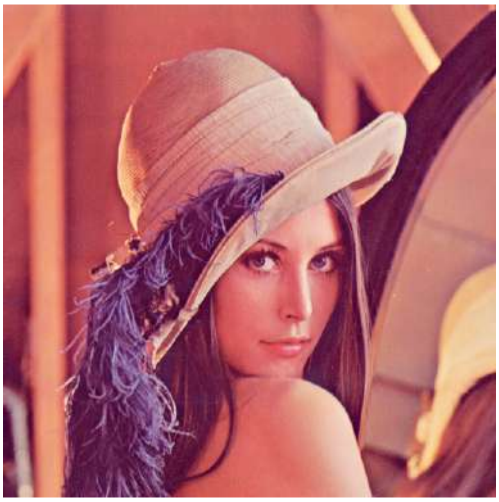


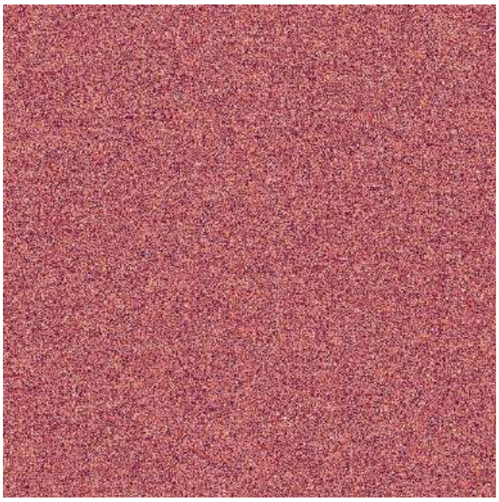
Scrambling:

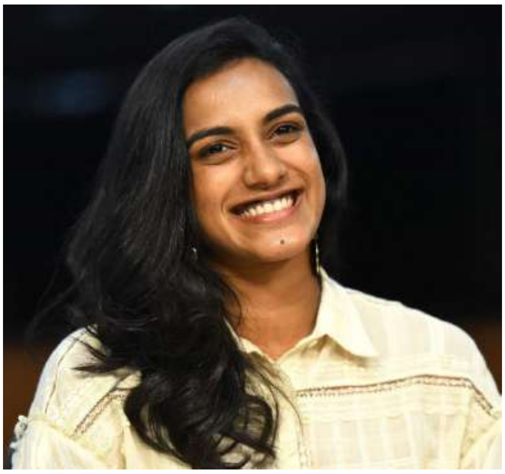
We have performed row rotation and column rotation based on key values from Hash array

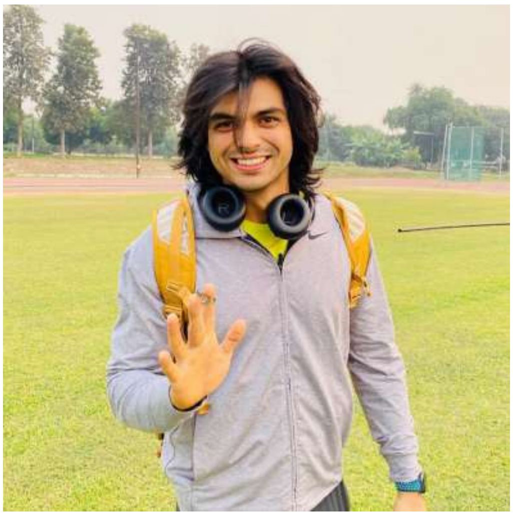
Original Image

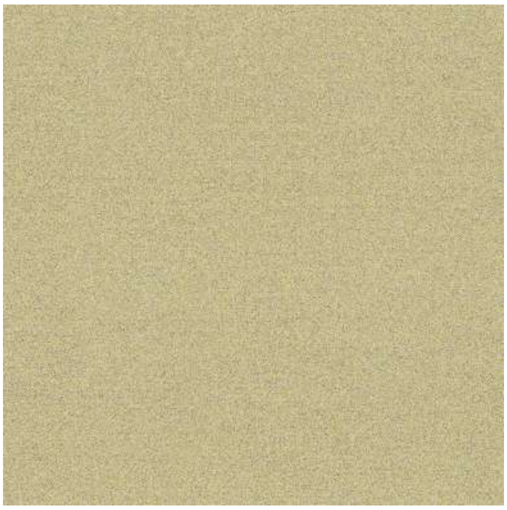
Encrypted Image









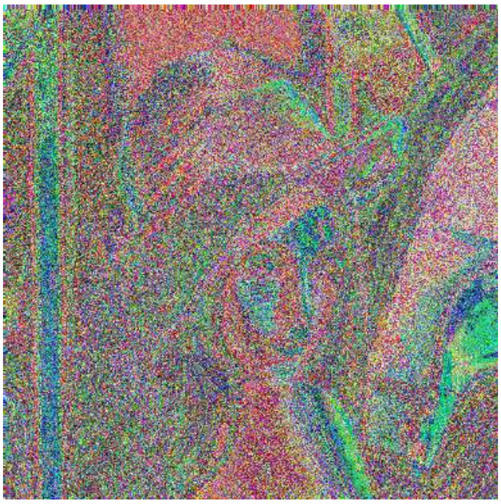


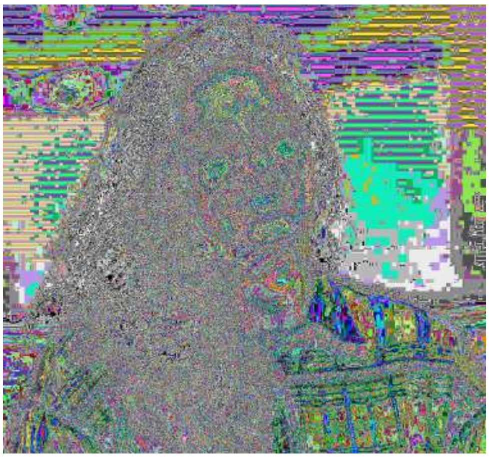
RSA:

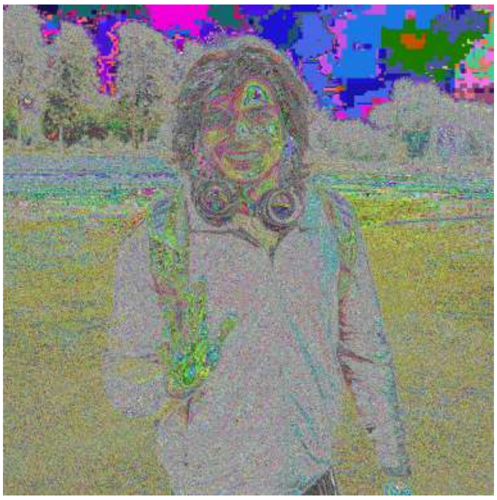
Although RSA is a very strong encryption algorithm,each value is mapped to another based on a formula. Hence in an image,pixels with similar values have similar encrypted values.

Original Image

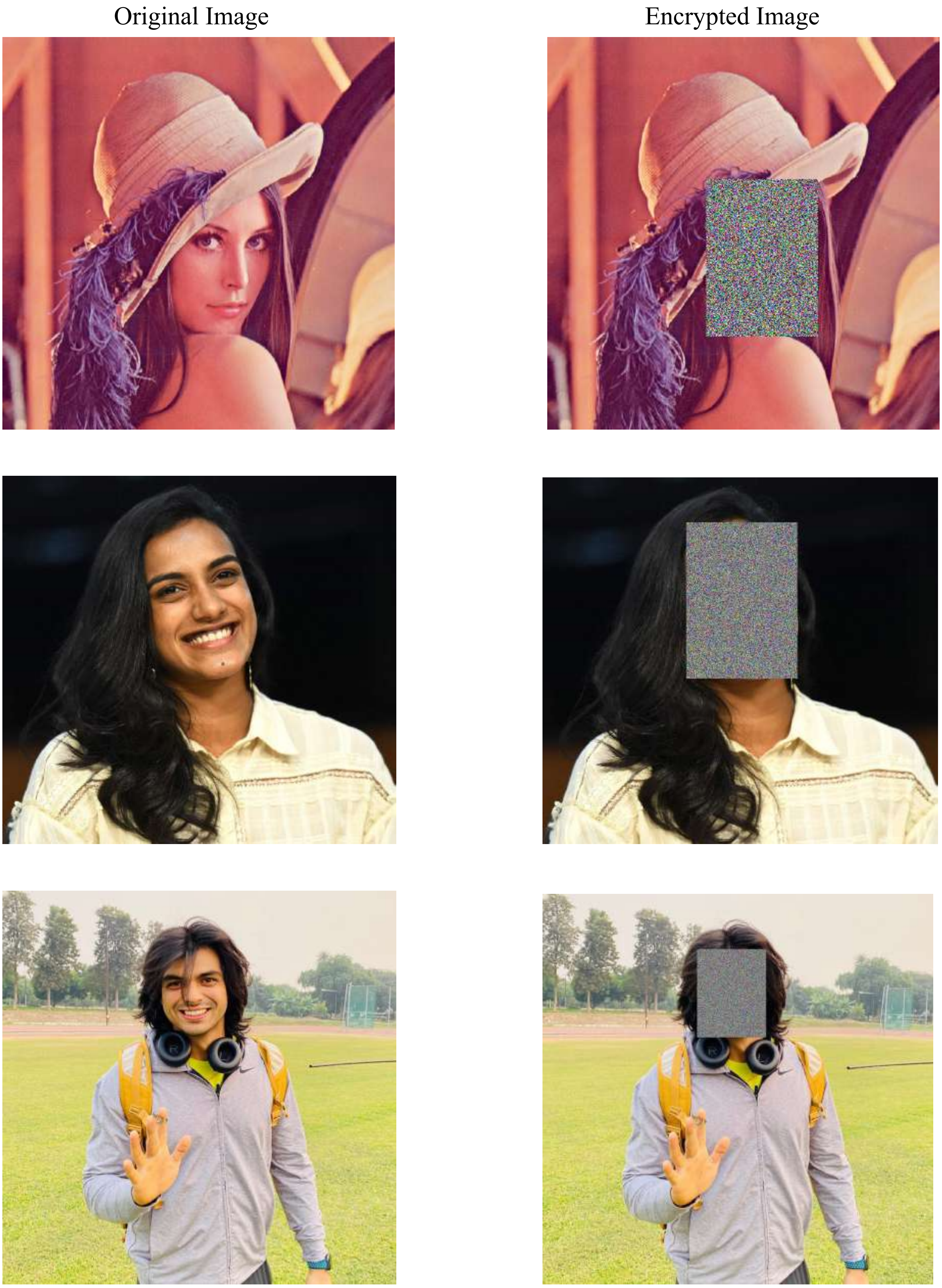
Encrypted Image







Proposed Method:



Original Image

Encrypted Image

Various Image Formats:

Original Image

Encrypted Images

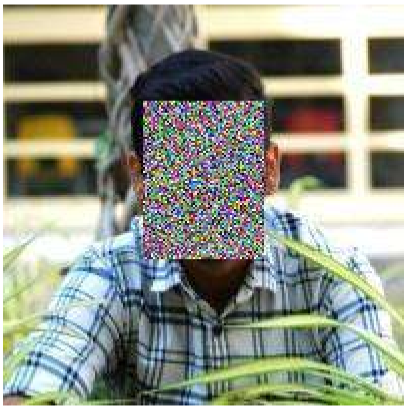


Image Type: jpeg
Key: Pratyush
Public key: 774492365267
Private key: 178728597493

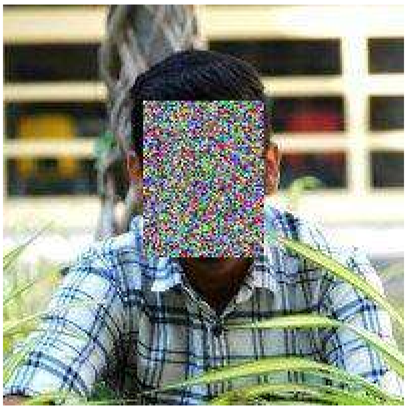


Image Type: jpg
Key: Pratyush
Public key: 457927076303
Private key: 176125275877

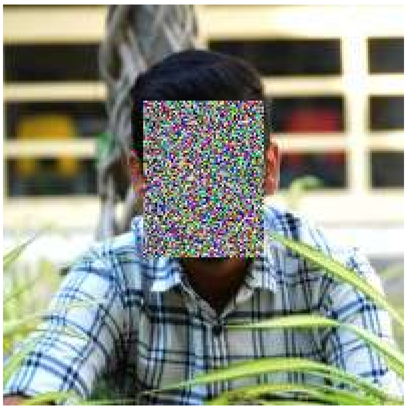


Image Type: png
Key: Pratyush
Private key: 564225798751
Public Key: 153879353483

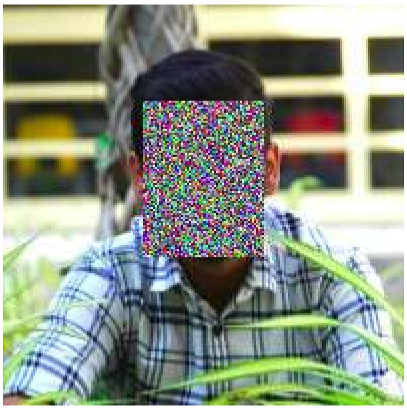


Image Type: tiff
Key: Pratyush
Public key: 753068264203
Private key: 115856388997

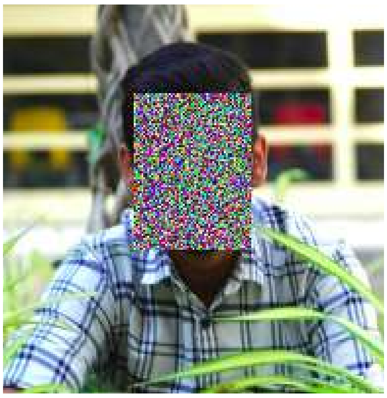


Image Type: bmp
Key: Pratyush
Public key: 463186608557
Private key: 378969711971

A)Key generation:

Algorithm:

```
key = pbkdf2_hmac("sha256", password, salt, 50, 2048)
for key in key:
  key_array.append(ord(key) % mod)
for i in range(len(key_array) - 5):
  # adding the alternate numbers

sum=key_array[i]+key_array[i+1]+key_array[i+2]+key_array[i+3]+key_array[i+4]+key_array[i+5]
  final_key_array.append(sum % mod)
```

Steps:

1. Use key extension algorithm PBKDF2 to generate a key of desired length from the given user key
2. The ASCII value of each character of the derived key is then inserted into an array.
3. Finally, we add five consecutive elements of the key array to give the final array of keys (this is done to increase the randomness)

B)CBC:

Algorithm:

```
for q in range(column):
  for r in range(row):
      reds = pix[q, r][0] ^ pix[(q - 1) % size[0], (r - 1) % size[1]][0]
      greens = pix[q, r][1] ^ pix[(q - 1) % size[0], (r - 1) % size[1]][1]
      blues = pix[q, r][2] ^ pix[(q - 1) % size[0], (r - 1) % size[1]][2]
      pix[q, r] = (reds, greens, blues)
      reds = pix[q, r][0] ^ (key_array[q * r % len(key_array)] ** 2 % 256)
      greens = pix[q, r][1] ^ (key_array[q * r % len(key_array)] ** 2 % 256)
      blues = pix[q, r][2] ^ (key_array[q * r % len(key_array)] ** 2 % 256)
      pix[q, r] = (reds, greens, blues)
```

Steps:

1. XOR the current pixels with the previous encrypted pixel value. This previous pixel can be any encrypted pixel value. In our algorithm, we have XORed with the encrypted pixel[row-1][col-1].
2. The formula we have used to select the key from the key array is : (key_array[q * r % len(key_array)]).

3. After selecting the key from the key array we raise it to the power of 2 and then find mod 256. We have done this in order to increase the entropy of keys, making it more secure.
4. XOR the result of step1 with the key value found in step3.

C)Scrambling:

Algorithm:

```
for i in range(2):
  for q in range(row):
      var = final_key_array[q] % 2
      if var:
          rotateRowLeft((final_key_array[q  % len(final_key_array)] ** 2) % column)
      else:
          rotateRowRight((final_key_array[q % len(final_key_array)] ** 2) % column)

   for q in range(column):
      var = final_key_array[q] % 2
      if var:
          rotateColUp((final_key_array[q  % len(final_key_array)] ** 2) % row)
      else:
          rotateColDown((final_key_array[q % len(final_key_array)] ** 2) % row)
```

Steps:

1. In this step we first perform row rotation followed by column rotation.
2. We perform row rotation based on the final key array value. If the key is even then we do rotateRowLeft(), else we do rotateRowRight().
3. The number of rotations are calculated by the formula : final_key_array[q % len(final_key_array)] ** 2) % column. Based on this formula, the number of rotations are decided.
4. We perform column rotation based on the final key array value. If the key is even then we do rotateColumnUp(), else we do rotateColumnDown().
5. The number of rotations are calculated by the formula : final_key_array[q % len(final_key_array)] ** 2) % row. Based on this formula, the number of rotations are decided.
6. Repeat step 2 one more time. Finally, the image undergoes two sets of row and column rotations to give a perfectly scrambled image.

D)RSA:

Algorithm:

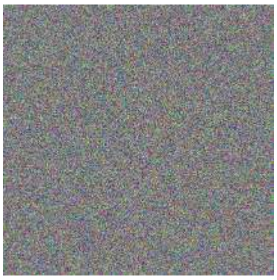
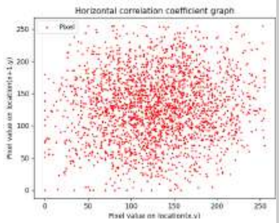
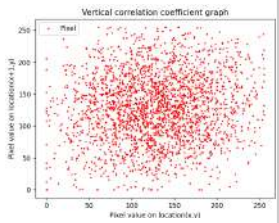
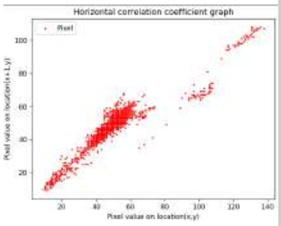
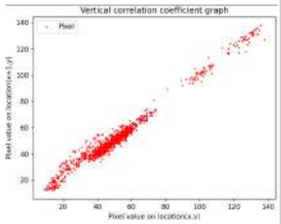
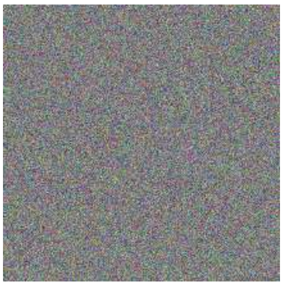
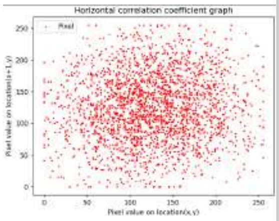
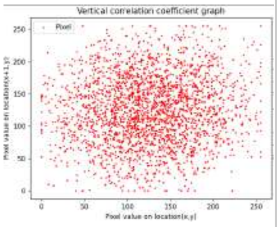
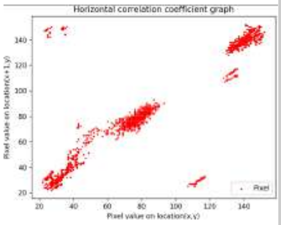
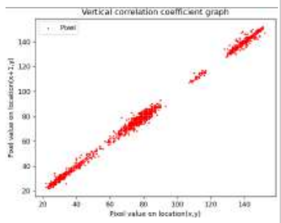
```
P = generatePrimeNumber(length)
Q = generatePrimeNumber(length)
N = P * Q
eulerTotient = (P - 1) * (Q - 1)
E = generatePrimeNumber(4)
while GCD(E, eulerTotient) != 1:
  E = generatePrimeNumber(4)
D = gcdExtended(E, eulerTotient)

for i in range(row):
  for j in range(col):
     r, g, b = pix[i, j]
     C1 = pow(r, E, N)
     C2 = pow(g, E, N)
     C3 = pow(b, E, N)
     file.append((C1, C2, C3))
     pix[i, j] = (C1 % 256, C2 % 256, C3 % 256)
```

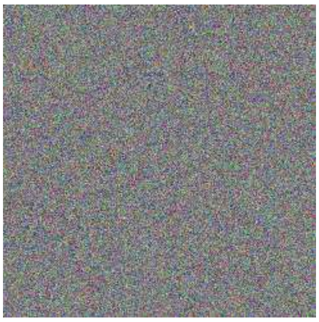
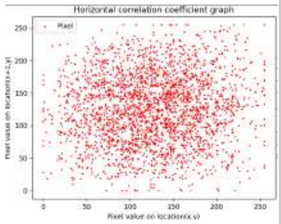
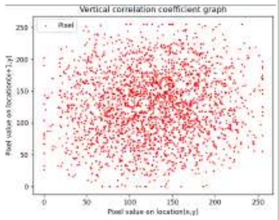
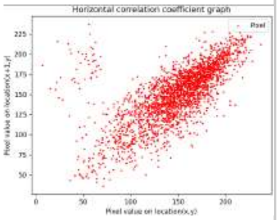
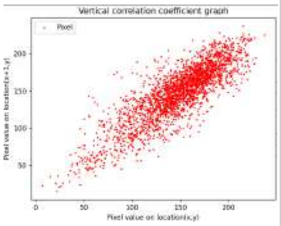
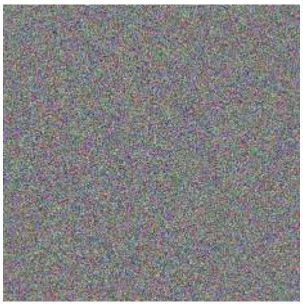
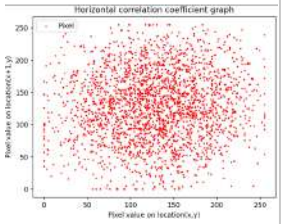
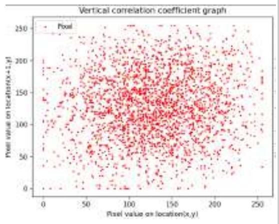
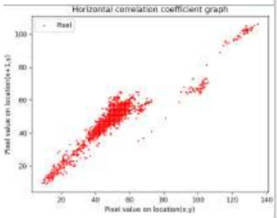
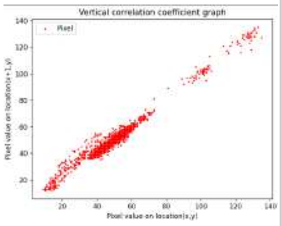
Steps:

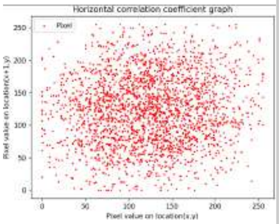
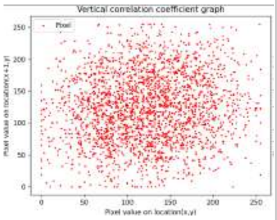
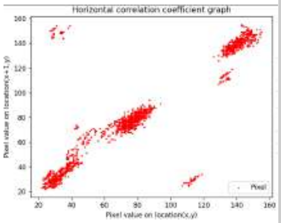
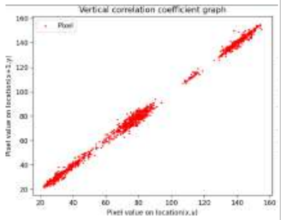
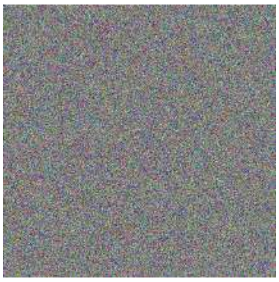
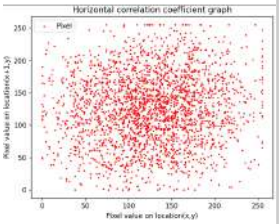
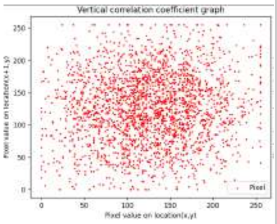
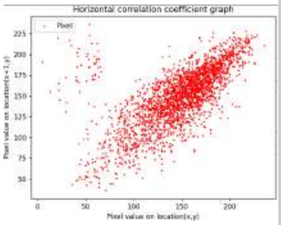
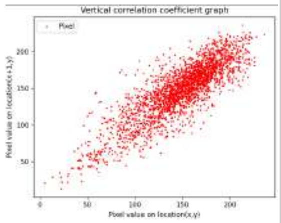
1. First we generate Pseudo Random Prime Numbers P and Q.
2. From P, Q we obtain the public key N and private key D.
3. We perform RSA encryption on the RGB value of each pixel with the obtained E and N values using the formula pow(r, E, N).
4. We store the encrypted values in a file,for later use to decrypt the original pixels
5. After this step we perform a mod 256 on each of the encrypted values to display it as a pixel.

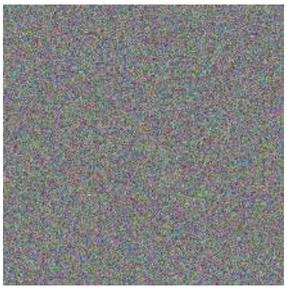
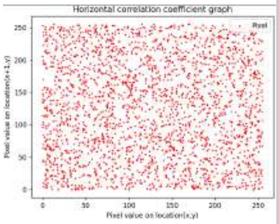
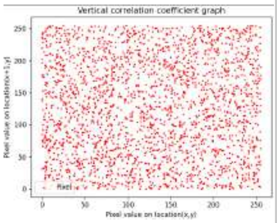
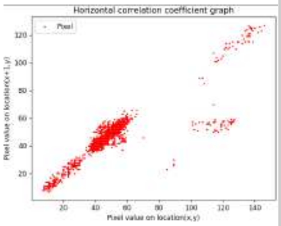
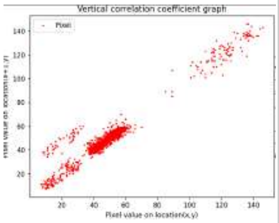
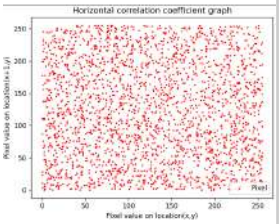
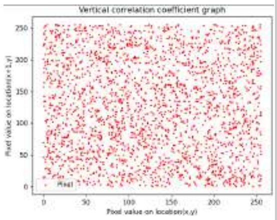
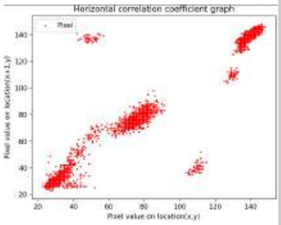
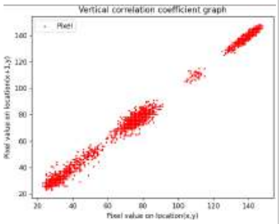
We perform these 4 steps consecutively in a sequential manner to obtain our proposed algorithm.

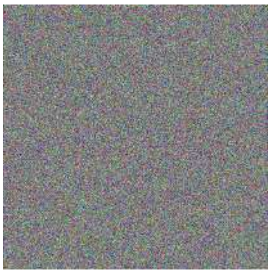
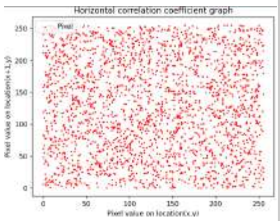
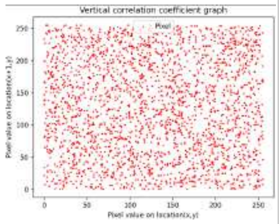
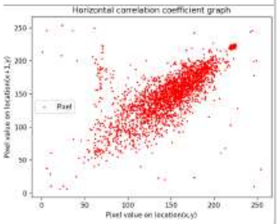
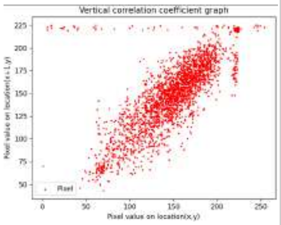
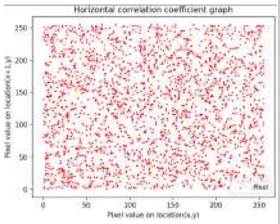
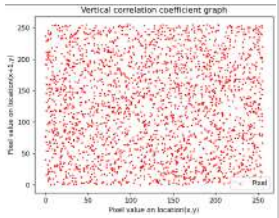
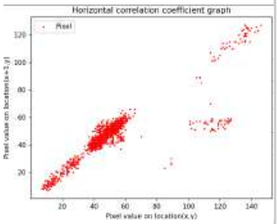
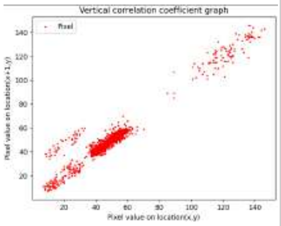
METRICS:

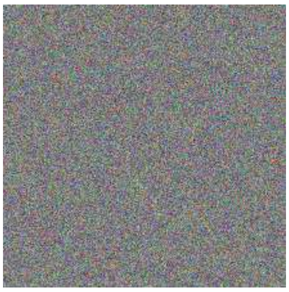
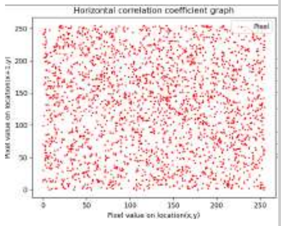
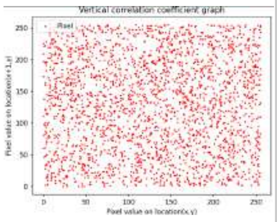
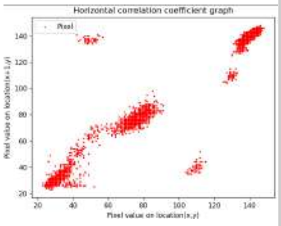
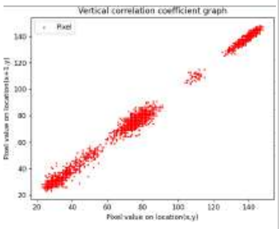
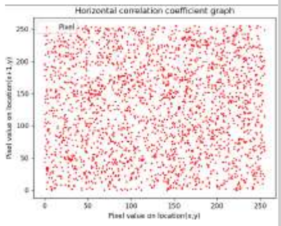
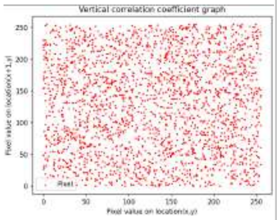
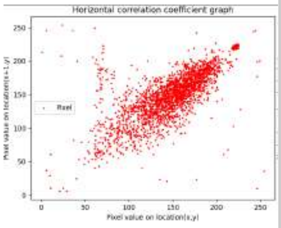
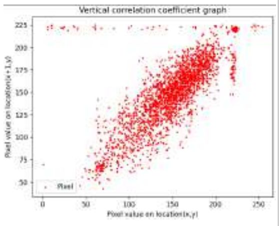
Format	Bit size	Metric	Encrypted		Decrypted	
Jpeg	8	Image A				
		Corelation Graph				
		Time	2.9026 seconds		2.5052 seconds	
		Corelation Coefficient	0.08992335924232525		0.965909895822119	
		RMSE	956850275.0780665			
		NPCR	99.49315388997395			
		UACI	26.26128851200239			
		Image B				
		Corelation Graph				
		Time	2.9861 seconds		2.5750 seconds	
		Corelation Coefficient	0.08982494854060075		0.9848734078796183	
		RMSE	1481559819.0543556			
		NPCR	99.63353474934895			
		UACI	30.889508116491438			

Format	Bit size	Metric	Encrypted		Decrypted	
Jpeg	8	Image C				
		Corelation Graph				
		Time	2.8474 seconds		2.5186 seconds	
		Corelation Coefficient	0.08857759633378513		0.9560701991129199	
		RMSE	1192097422.0737507			
		NPCR	99.52901204427083			
		UACI	25.13979145126626			
	16	Image A				
		Corelation Graph				
		Time	2.8363 seconds		2.4979 seconds	
		Corelation Coefficient	0.08917125299309249		0.9659012235961123	
		RMSE	955136570.3026186			
		NPCR	99.48832194010417			
		UACI	26.19385214414426			

Format	Bit size	Metric	Encrypted		Decrypted	
		Image B				
		Corelation Graph				
		Time	2.8767 seconds		2.5375 seconds	
		Corelation Coefficient	0.08913326052264177		0.9848243430181783	
		RMSE	1478775629.15602			
		NPCR	99.64154561360677			
		UACI	30.947509466444878			
		Image C				
		Corelation Graph				
		Time	2.8606 seconds		2.5260 seconds	
		Corelation Coefficient	0.0916989133783651		0.956024106890203	
		RMSE	1193666943.9931157			
		NPCR	99.54210917154948			
Jpeg	16	UACI	25.06103814818641			

Format	Bit size	Metric	Encrypted		Decrypted	
PNG	8	Image A				
		Corelation Graph				
		Time	2.8827 seconds		2.6343 seconds	
		Corelation Coefficient	0.006084985549095393		0.006084985549095393	
		RMSE	1413960072.1018384			
		NPCR	99.59526062011719			
		UACI	31.078579472572525			
		Image B				
		Correlation Graph				
		Time	2.8899 seconds		2.6126 seconds	
		Correlation Coefficient	0.005730358957372695 5		0.9836518515219717	
		RMSE	1944383855.5867245			
		NPCR	99.61649576822917			
		UACI	34.26315158022024			

Format	Bit size	Metric	Encrypted	Decrypted
PNG	8	Image C		
		Correlation Graph	 	 
		Time	2.8704 seconds	2.5502 seconds
		Correlation Coefficient	0.007095939177669683	0.9543662602436974
		RMSE	1654682563.413798	
		NPCR	99.60721333821614	
		UACI	30.201320274216638	
	16	Image A		
		Correlation Graph	 	 
		Time	2.9015 seconds	2.6470 seconds
		Correlation Coefficient	0.005718051805353635	0.9629626929353957
		RMSE	1413964146.4352596	
		NPCR	99.61166381835938	
		UACI	31.13331514247460	

Format	Bit size	Metric	Encrypted		Decrypted	
PNG	16	Image B				
		Correlation Graph				
		Time	3.2359 seconds		2.6482 seconds	
		Correlation Coefficient	0.004115199255828882		0.9836518515219717	
		RMSE	1941331753.633475			
		NPCR	99.61382548014323			
		UACI	34.24464057474541			
		Image C				
		Corelation Graph				
		Time	3.1400 seconds		2.5692 seconds	
		Corelation Coefficient	0.001999174968796856		0.9543662602436974	
		RMSE	1656185149.104787			
		NPCR	99.5989481608073			
		UACI	30.148859959036294			

ANALYSIS:

- RSA is a very secure encryption algorithm that is used for secure data transmission.When used for images,it is observed that pixels with the same r,g,b value have the same encrypted value. This makes the encrypted image visually recognisable, and thus is not used for image encryption. Our proposed method overcomes this drawback by introducing a precursor step. Before inputting the image to the RSA algorithm we first perform diffusion and scrambling using the user defined key. This process distorts the image, therefore making it visually unidentifiable. Thus when RSA is performed after this step the encrypted image is fully secure and not recognisable.

- Our proposed method is a two step encryption process. The first layer encrypts the image based on the user provided key. We perform PBKDF2 on the user provided key to obtain a unique and secure key that can be used for encryption. This hash value is used to encrypt the image using Diffusion and Scrambling. The second layer generates two Pseudo Random Prime numbers that are used by RSA to obtain the private and public key. Thus by using a combination of user provided key, as well as computer generated key we make our algorithm extremely secure .

- CBC and scrambling are symmetric algorithms that use the same user provided key to encrypt and decrypt the image. RSA on the other hand is an asymmetric algorithm that uses different keys for encryption and decryption.Together the two algorithms synergize to provide a very secure encryption technique.

- In our project we also reduced the computations performed by the RSA algorithm. Pixel values range between 0 to 255. Thus there will be 255 encrypted values. RSA is performed on all values between 0 to 255 and is stored in hashmap. During the encryption of each pixel, we compare the pixel value with the mapped RSA values to determine its encrypted value. This significantly reduces the computation time thereby making it more efficient.

- In our proposed method we encrypt only the sensitive parts of the image. This allows us to reduce unwanted computation,and the time and resources saved can be used to enhance the security of the sensitive part. This also has the added advantage of identifying the surroundings of the image without decrypting the sensitive part.

CONCLUSION

Thus from our proposed algorithm it can be noticed that our algorithm reduces the computation required by encrypting only the sensitive regions of the image. We have also proposed a robust and secure encryption mechanism that improves the existing RSA algorithm.CBC(symmetric encryption technique) synergises perfectly with RSA (an asymmetric algorithm) to provide a two-layer security mechanism that further enhances the robustness of the encryption algorithm. This two layer system makes use of the user provided key as well as the system generated public and private key to enhance the security of the existing algorithm. Our proposed method has been used to detect only faces present in images, in future it can also be used to detect other sensitive information like signatures as well.

References

[1] Janwg, W., & Lee, S. Y. (2020). Partial image encryption using format-preserving encryption in image processing systems for the Internet of things environment. International Journal of Distributed Sensor Networks, 16(3), 1550147720914779.

[2] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics, 92(4), 1745-1759.

[3] Zhang, X., Wang, L., Niu, Y., Cui, G., & Geng, S. (2019). Image Encryption Algorithm Based on the H-Fractal and Dynamic Self-Invertible Matrix. Computational intelligence and neuroscience, 2019.

[4] Jiao, K., Ye, G., Dong, Y., Huang, X., & He, J. (2020). Image encryption scheme based on a generalized arnold map and RSA algorithm. Security and Communication Networks, 2020.

[5] Patel, S., & Muthu, R. K. (2020). Image encryption decryption using chaotic logistic mapping and dna encoding. arXiv preprint arXiv:2003.06616.

[6] Jassem, A. H., Hashim, A. T., & Ali, S. A. (2019, December). Enhanced Blowfish algorithm for image encryption based on chaotic map. In 2019 First International Conference of Computer and Applied Sciences (CAS) (pp. 232-237). IEEE.

[7] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75(10), 6663-6682.

[8] Sheela, S. J., Suresh, K. V., & Tandur, D. (2018). Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimedia Tools and Applications, 77(19), 25223-25251.

[9] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[10] Xu, C., Sun, J., & Wang, C. (2020). An image encryption algorithm based on random walk and hyperchaotic systems. International Journal of Bifurcation and Chaos, 30(04), 2050060.

[11] Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. Information Sciences, 480, 403-419.

[12] Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Alqahtani, H. F., Alqahtani, N. N., & Ali, A. A. (2020, March). Image Encryption Based on AES and RSA Algorithms. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

[13] Naik, R., Lathi, A., Pariani, S., Satpute, N., & Singh, A. (2021). Comparison of Different Encryption Algorithm and Proposing an Encryption Algorithm. Available at SSRN 3867982.

[14] Ray, A., Potnis, A., Dwivedy, P., Soofi, S., & Bhade, U. (2017, October). Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption. In 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE) (pp. 274-278). IEEE.

[15] Srivatsava, J. G. M., & Sheeja, M. R. (2020). Implementation of Triple DES ALGORITHM in Data Hiding and Image Encryption Techniques.

[16] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[17] Hazra, T. K., Mahato, A., Mandal, A., & Chakraborty, A. K. (2017, August). A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques. In 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON) (pp. 137-141). IEEE.

[18] Han, C. (2019). An image encryption algorithm based on modified logistic chaotic map. Optik, 181, 779-785.

[19] Rodríguez César, H., Gayoso Martínez, V., Hernández Encinas, L., & Martín Muñoz, A. (2019). Format-Preserving Encryption: Image Encryption Under FF1 Scheme.

[20] Ray, A., Potnis, A., Dwivedy, P., & Soofi, S. An Advance Approach of Image Encryption using AES, Genetic Algorithm and RSA Algorithm.