Image Encryption Techniques

Submitted by-

Name- Hrishikesh Magadum

Abstract

Images are one of the most important and popular forms of multimedia. Along with being stored on devices like phones, CDs, pen drives, etc., images are shared across multiple platforms and across the internet. With this kind of large-scale usage of images, it has become more difficult to keep images secure and safe from unauthorized users. With a more secure system, images can be shared and used more confidently. Most encryption algorithms were used to encrypt text messages. The conventional algorithms are not suitable for image encryption as images generally have large data capacity and require a large computational volume. An efficient algorithm for image encryption is needed to make it difficult for unauthorized users to view or use the images. In this proposed implementation we are going to implement image encryption using AES, Elliptical Curve Cryptography, and chaotic maps and compare their merits based on key sensitivity, adjacent pixel autocorrelation, and intensity histograms.

Introduction

Due to the regular transmission of digital photographs throughout the globe in recent years, it has become crucial to protect them against leaks. Many applications, including cable TV, personal online photo albums, medical imaging systems, military image databases, and secure video conferencing, need a reliable, quick, and powerful security system to store and transmit digital images. The need to meet the security requirements for digital photographs has prompted the development of effective encryption methods. Numerous encryption methods have been proposed in the literature during the past ten years based on various ideas. Chaos-based encryption methods stand out among them as being suitable for real-world applications because they offer a good balance of speed, high security, complexity, moderate computational overheads, and processing power, among other things. Digital images have some unique properties, such as data redundancy, a strong correlation between adjacent pixels, a lower sensitivity than text data, meaning that a small change in any pixel's attribute does not significantly impair the image's quality, and a large data storage capacity, among others. As a result, standard ciphers like IDEA, AES, DES, RSA, and others are not appropriate for real-time image encryption since they demand a lot of computational time and processing resources. The only ciphers that are preferred for real-time image encryption are those that are faster without sacrificing security. For real-time procedures, an encryption method that operates slowly, even if it has higher levels of security features, would be of little utility.

Literature Review

S.No	Name of Paper	Description	Results
[1]	A review of optical image encryption techniques Shi Liu, Changliang Guo , John T. Sheridan	The authors of this paper evaluate a number of optical image encryption methods that have been put out in the literature and were motivated by the design of the traditional optical Double Random Phase Encoding (DRPE) system. Examined and divided into all-optical techniques and picture scrambling techniques are a number of well-known optically inspired encryption	The range of validity of the hypothesis needs to be tested.

		algorithms. Each technique is numerically applied and contrasted with the optical DRPE scheme, which employs random phase diffusers (masks) after various modifications. This review enables a broad understanding of the numerical simulations of the associated optical encryption systems as well as a brief comparison and contrast of the additional degree of freedom (keys) supplied by various strategies that improve optical encryption security.	
[2]	A Survey On Different Image Encryption and Decryption Techniques. Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya	The various types of image encryption and decryption techniques are the major topic of this research. In order to obtain a decreased correlation between the pixels and an encrypted image, this study presents a survey of over 25 research papers addressing image encryption approaches that scramble the image's pixels. This study provides a survey of the various image encryption and encryption methods currently in use. It also emphasizes how well image encryption and decoding techniques work.	Each method is effective for real-time encryption. Each technique is distinct in its own manner and may be appropriate for a variety of applications. By using multiple chaotic schemes for picture encryption algorithms, newly proposed image encryption approaches increase security. Also examined was a brand-new colour image encryption technique.
[3]	Image encryption using a chaotic logistic map N.K. Pareek, Vinod Patidar, K.K. Sud.	To satisfy the need for secure picture transfer, the authors provide a novel method for image encryption based on chaotic logistic maps. Two chaotic logistic maps and an external secret key of 80 bits are used in the proposed image encryption system. After encrypting each block of sixteen pixels in the image, the secret key is changed to strengthen the cipher against any attacks. The suggested picture encryption strategy offers an effective and secure method for real-time image	The suggested encryption method encrypts an image's pixels using eight different types of operations, with the outcome of the logistic map determining which operation will be applied to a given pixel. After encrypting a block of sixteen pixels from the image, the secret key is changed to strengthen the cipher

		encryption and transmission, according to the findings of many experimental, statistical analyses, and key sensitivity tests.	against any attacks. To prove the security of the new picture encryption technique, the authors conducted a statistical analysis, key sensitivity study, and key space analysis.
[4]	Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm Qi Zhang Electronic Engineering College, Heilongjiang University Harbin, China ljittss@163.com Qunding* Electronic Engineering College, Heilongjiang University Harbin, China qunding@aliyun.com	In this paper, a digital image encryption method based on the AES algorithm and its MATLAB implementation were suggested. Then, digital image processing was carried out in order to obtain data that could be encrypted using the AES algorithm and combine both methods. The algorithm is then implemented in a MATLAB simulation, and the digital image can then be encrypted. The comparison between histogram analysis and key analysis revealed that the approach can more effectively capture the effects of encryption and decryption.	This method can produce a very good effect on image encryption based on the aforementioned experimental results and analysis, along with the histogram and key sensitivity analysis. Additionally, the decryption's core shares the same structure as encryption, making it simple to get the original image. The AES algorithm has established a solid foundation for subsequent image encryption in the transmission encryption on software and hardware because it is simple to implement in hardware and software.
[5]	A novel bit-level image encryption algorithm based on chaotic maps Lu Xu, Zhi Li, Jian Li, Wei Hua	In this study, a brand-new bit-level image encryption algorithm based on piecewise linear chaotic maps is presented. The plain image is first split into two equal-sized binary sequences. The two sequences are then mutually diffused using a new diffusion strategy that is introduced later. The control of a chaotic map, which can permute the bits in one bitplane into any other bitplane, is then used to switch the binary elements in the two sequences. With just	The suggested method, in contrast to many previous bit-level methods, can provide outstanding encryption performance with just one round. Additionally, the suggested approach is quicker than BPS and Teng's algorithm and can encrypt an image with a size of M * N. The proposed algorithm is proven

		one round, the suggested algorithm provides excellent encryption performance. The proposed algorithm is secure and dependable for image encryption, according to simulation results and performance analysis.	to be secure and dependable for image encryption by a large number of simulation results and performance analyses, including histogram analysis, correlation analysis, key space analysis, key sensitivity analysis, information entropy analysis, and differential analysis.
[6]	Image Encryption using Elliptic Curve Cryptography Laiphrakpam Dolendro Singh∗ and Khumanthem Manglem Singh	In order to achieve authenticity and integrity, Elliptic Curve cryptography is used in this paper to encrypt, decrypt, and digitally sign the cipher image.	In order to ensure the validity and integrity of the received image, the authors of the research have proposed an implementation technique for image encryption/decryption and the addition of a digital signature to the cipher image. They carried out our procedure by grouping the pixels and demonstrated the maximum number of groups that can be produced using the ECC settings. Instead of converting the grouped pixel values to Elliptic curve coordinates, they were paired.
[7]	A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher with Hill Cipher	This paper proposes a new image encryption method (ECCHC) that combines the Elliptic Curve Cryptosystem and the Hill Cipher to change the symmetric Hill Cipher algorithm into an asymmetric one, improve security and efficiency, and thwart hackers. Entropy, Peak Signal to Noise Ratio (PSNR), and Unified Average Changing Intensity (UACI) will be used to gauge the effectiveness of grayscale image encryption and to assess how well the	The new strategy works well and is robust to various assaults. The suggested method has a basic structure and faster computations, making it ideal for small devices and embedded systems and useful in wireless applications. The novel methodology was tested on grayscale photos in this study, and it will

		suggested encryption method performs when compared to the original image.	be updated for usage with RGB images and real-time multimedia applications in subsequent work.

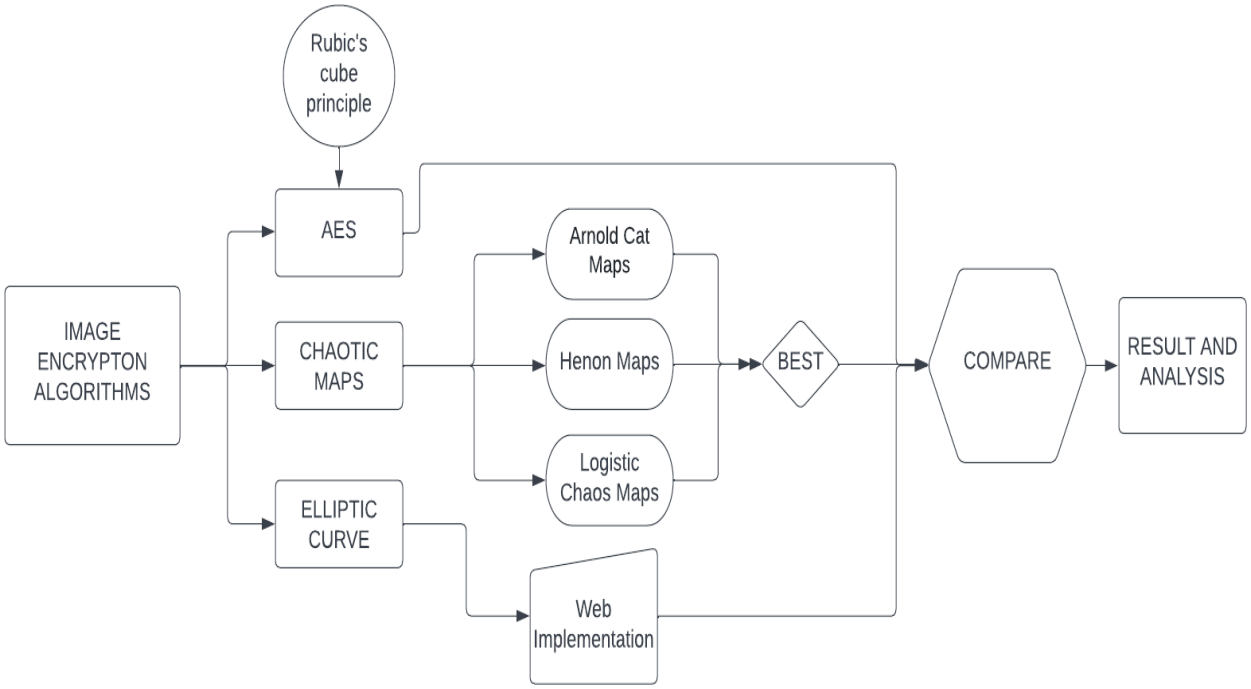
Methodology

Image encryption can be implemented with many algorithms but the efficient and more secure ones are usually preferred and recommended for widespread usage. Hence it becomes vital to design and implement algorithms that are improved versions of their predecessors. Advancements in technology and specifically in the processing time of computers have made it difficult to use any encryption algorithm for a long time due to its nature of being susceptible to being cracked by a supercomputer which in the end compromises the data to be encrypted. To provide a comparative study of some famous and efficient algorithms and test their effectiveness was one of the main objectives of this study. In this project, we have used 3 important encryption techniques which are AES, chaotic maps, and Elliptical Curve Cryptography. It has been observed that text encryption AES is the most secure algorithm to use. For images, we are dealing with pixels and hence it becomes our concern to generate randomness and unpredictability in the encryption techniques for it to be more difficult to crack. The chaotic maps we have implemented in this project are Arnold cat maps, Henon maps, and Logistic chaos maps. Elliptic Curve cryptography was implemented as a webpage to simulate a web application implementing an Encryption technique.

Software Used

1. *Jupyter Notebooks and Python*: AES and Chaotic Maps were implemented in Python as it was convenient to plot the graphs and make statistic comparisons among the algorithms.
2. *Python*: We performed Elliptical Curve Cryptography image encryption using tools like NumPy and PIL, and then utilized image processing methods to display the encrypted images on an image.
3. *Flask*: We performed Elliptical Curve Cryptography image encryption using tools like NumPy and PIL, and then utilized image processing methods to display the encrypted images on an image.
4. *Html, CSS, and Javascript*: To render front-end web pages, we employed both our prior experience and more recent knowledge of web development approaches. In particular, we applied the parallax effect to enhance the platform's visual appeal.

Architecture Diagram

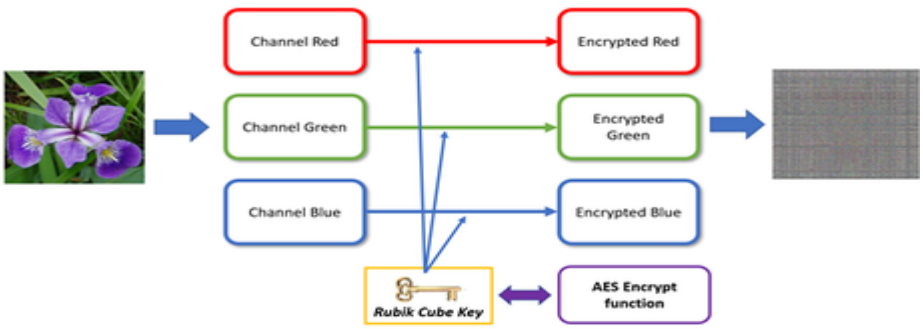


AES

The AES encryption method has three different key lengths: 128 bits, 196 bits, and 256 bits. The packet size is also all 128 bits, and the technique is quite flexible. As a result, both hardware and software utilize it extensively. The 128-bit key length is widely utilized in the three key lengths of the AES algorithm. 10 times of repetitive computation in the internal method when the key length is too short. Each round includes the following five parts in addition to the final round: AddRoundKey, ShiftRows, S-box, MixColumns, and SubBytes. We can first transform a digital image into a binary matrix before encrypting it using the AES algorithm. The coordinates at the spot where the image has been displayed on the screen are the matrix's row and column elements. The grey levels of pixels are what give the elements their value (Usually 256 grades, from 0 to 255). Due to the fact that the AES algorithm's state matrix is built on a 4*4 matrix whose elements each contain 8 bits. The matrix element's value ranges from 0 to 255. It usually matches the image's level of grey. So, following digitization, we can obtain a matrix for a digital image. To utilize the AES technique to handle this matrix in blocks, each 4*4 matrix in a block is encrypted using the AES encryption technique, starting at the upper left corner of the image before the block as a whole is created. The result is a matrix whose numbers are entirely different from those in the original numerical matrix. As a result, we altered the grayscale value of the original image to create the encrypting effect.

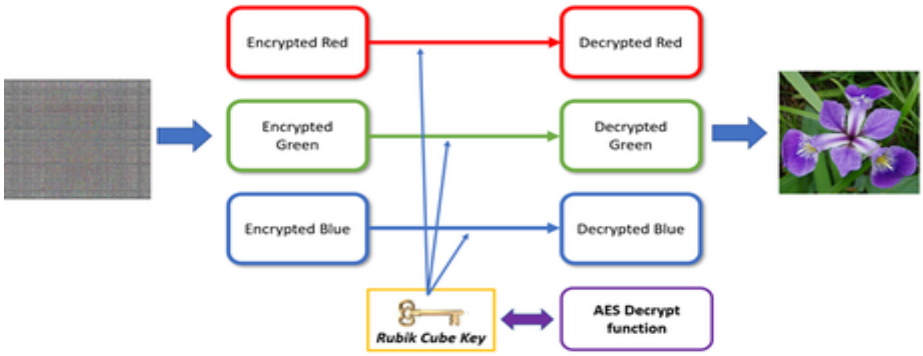
Encryption

- Before using the Rubik’s cube algorithm to encrypt the image, the three channels are divided. AES uses encryption to protect the secret keys. The Encrypted Image is then created by combining these encrypted channels.



Decryption

- The encrypted image was divided into three encrypted channels. The AES decrypt function then provides the original key. The decrypted key is used to decode the three channels.



CHAOTIC MAPS

A chaotic dynamical system is a deterministic system that can never be defined with infinite precision and displays behavior that appears random due to its sensitivity to its initial circumstances. Chaos is characterized by unpredictable activity, which is why it resembles noise. A chaos-based cryptographic algorithm is a logical choice for secure communication and cryptography due to the tight relationship between cryptography and chaos. Similar characteristics shared by chaotic maps and cryptographic algorithms include sensitivity to initial conditions and control parameter changes, pseudorandom behavior, and unstable periodic orbits with lengthy periods. The fundamental idea behind chaos-based picture encryption is based on some dynamic systems' capacity to generate random number sequences. These sequences are used to encrypt messages. Several chaos-based algorithms combine speed, high-security complexity, and minimal computational overheads. Additionally, several algorithms based on chaotic and other dynamical systems contain many crucial characteristics, including sensitive dependency on initial values, pseudorandom characteristics, ergodicity, and non-periodicity.

We are utilizing different chaos maps to encrypt images, evaluating the effectiveness of each one based on key sensitivity, adjacent pixel autocorrelation, and intensity histograms. Arnold cat maps, Henon maps, and logistic chaos maps were the chaos maps used.

1. **Arnold Cat Map**: Without erasing any of the image's information, Arnold's Cat chaotic mapping in two dimensions can be used to shift a pixel's position.
   Algorithm

```
ArnoldCatTransform(img, num):
rows, cols
ch <- img.shape
n <-rows
arnold_img < −np.zeroes([rows, cols, ch])
forxinrange(0, rows) :
    foryinrange(0, cols) :
        arnold_img[x][y] < −img[(x + y)
returnarnold_img

ArnoldCatEncryption(imageName, key) :
img < −cv2.imread(imageName)
foriinrange(0, key) :
    img < −ArnoldCatTransform(img, i)cv2.imwrite(imageName.split('.')[0]+
"_Arnoldcat Enc.png", img)
returnimg
```

2. **Henon map**: It is a dynamic, two-dimensional system. The Henon chaotic map produces two distinct chaotic sequences. The original/plain image's row and column permutations are then subjected to these sequences. To create a unimodal skew tent map that diffuses pixel values, XOR models are employed. In the final step of the method, each pixel is changed into a brand-new random pixel using Hussain's substitution box.

   Algorithm

   for i in range (m^2):
   $x_(i+1) = y_(i+1) + 1 - \alpha x_i^2$
   $y_(i+1) = \beta x_i$
   bit=0 if x_i<=0.4 else 1
   (Only the value of x is used. This is appended as rows of lists of 8-bit numbers, so that we can have a bitwise xor with the image).

   encryptedimage=bitwisexor(imagematrix,bitmatrix for R,G,B values in each pixel of imagematrix)
   decryptedimage=bitwisexor(imagematrix,bitmatrix for R,G,B values in each pixel of imagematrix)
   The bit matrix can be generated by knowing the inital values applied in the Henon map, making them the secret keys in this operation.

3. **Logistic map with key mixing**: The logistic map rather examines discrete time steps using a nonlinear difference equation. The logistic map translates the population's value at any time step to its value at the following time step, which is why it is so named.

ELLIPTICAL CURVE CRYPTOGRAPHY

With respect to the chosen key size, the difficulty of solving an elliptic curve discrete logarithmic problem increases exponentially. ECC is a great option for encryption and decryption processes compared to other cryptographic approaches that are linearly or sub-exponentially complex because of this attribute.

Algorithm

1. Grouping of pixels into a single integer
2. Getting the group of pixels from the big integer.
3. Image Encryption.
4. Digital signature on cipher image.
5. Image decryption
6. Signature verification

The implementation of the Elliptical Curve image Encryption, a constituent part of a webpage built using python and flask connecting frontend and backend. It's a fully functional application built to encrypt and decrypt images using an elliptical curve cryptography algorithm. The website was hosted on localhost and has features like saving images as well as a login page for users. The website was created in order to simulate a real-life web app that can help people store their images in encrypted format safely. The images can be decrypted anytime and anywhere with a click of a button. The encrypted image is embedded in another image making it even harder to crack it. To add more security one can encrypt the embedded image, adding a second layer of security that is impossible to crack.

The above-mentioned algorithms are compared based on intensity histogram, Adjacent Pixel Autocorrelation, and key sensitivity to obtain the merits of each image encryption technique and decide which technique can be used according to different scenarios.

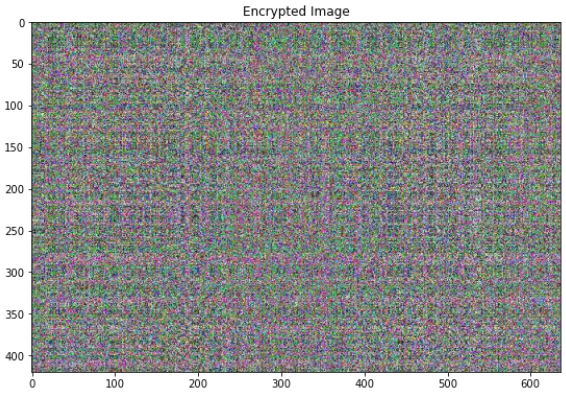
Intensity Histogram- One of the simplest ways to show the quality of image encryption is through cipher text image histogram analysis. An effective picture encryption technique usually transforms a plaintext image into a random, unintelligible form. Therefore, a good picture encryption technique creates a cipher image with an intensity histogram that is evenly distributed.

Adjacent Pixel Autocorrelation- It is desirable to have an encryption algorithm that reduces the high information redundancy that is present in photographs. Therefore, we use the correlation between neighbouring pixels in a direction as a measure of encryption performance (Horizontal, Vertical or Diagonal). The horizontal direction has been taken into account. The image's 1024 random pixels are chosen at random, and the correlation between each one and its rightmost neighbour is discovered and plotted. The correlation plot should look random with no obvious pattern for a decent algorithm.

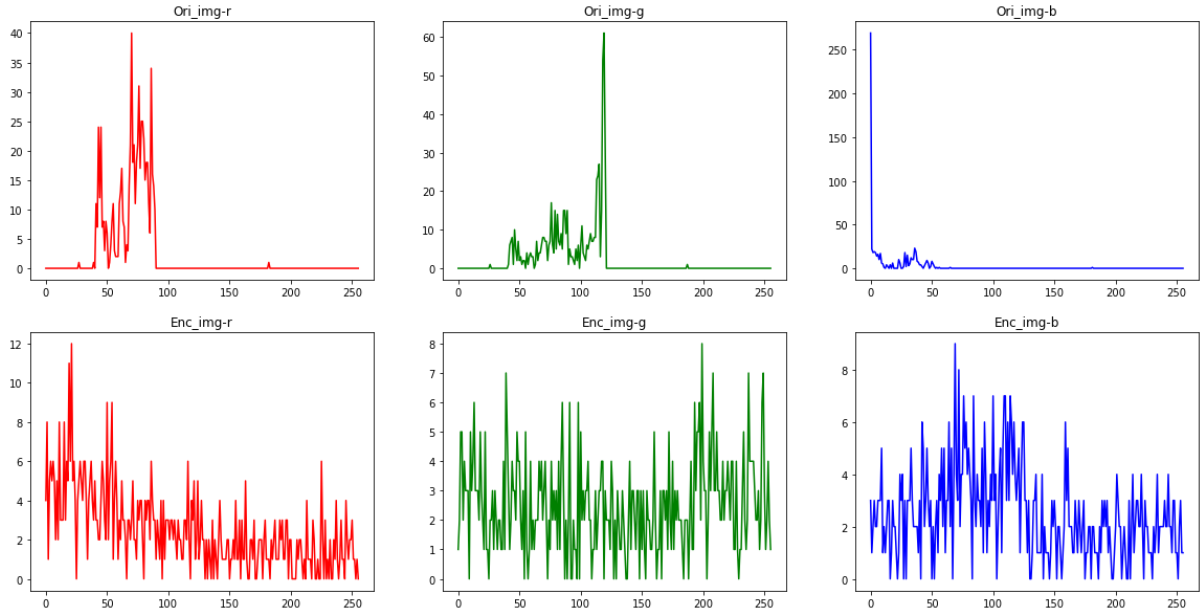
Key Sensitivity- To evaluate the key sensitivity, we encrypt the plain image with the three methods. An ideal image encryption technique should be sensitive with regard to the secret key, meaning a tiny change in the key should create a completely different encrypted image. We then attempt to decrypt them using a slightly modified key.

RESULTS AND ANALYSIS

A. AES Image Encryption



Histogram



1. NPCR (Number of Pixel Change Rate)

$$NPCR = \sum_{i=1}^{M}\sum_{j=i}^{N}\frac{D(i,j)}{M \times N} \times 100\%$$

NPCR for AES Image Encryption= 0.9959556254367575

2. The unified average changing intensity (UACI)

$$\text{Với } D(i,j) = \begin{cases} 1, & I_0(i,j) \neq I_{ENC}(i,j) \\ 0, & \text{còn lại} \end{cases}.$$

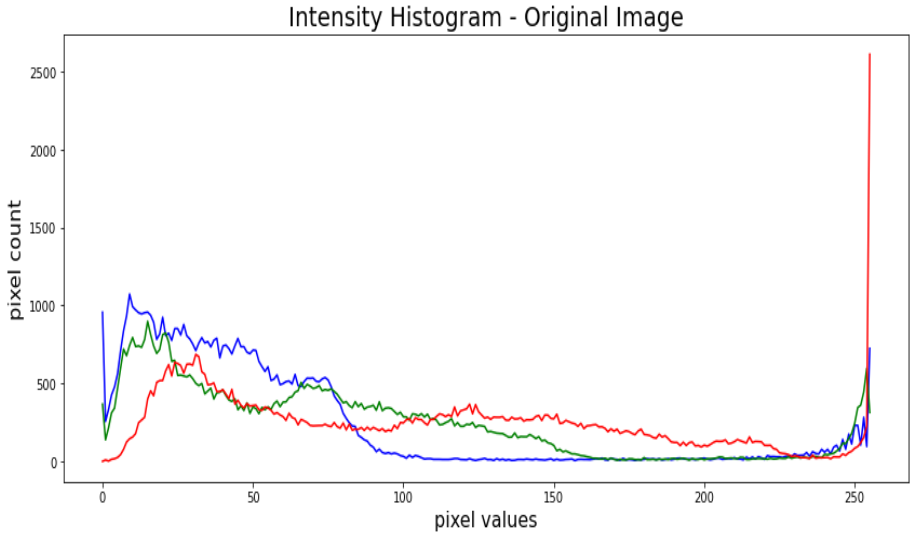
$$UACI = \sum_{i=1}^{M}\sum_{j=i}^{N}\frac{|I_0(i,j) - I_{ENC}(i,j)|}{(2^{\alpha} - 1) \times M \times N} \times 100\%$$

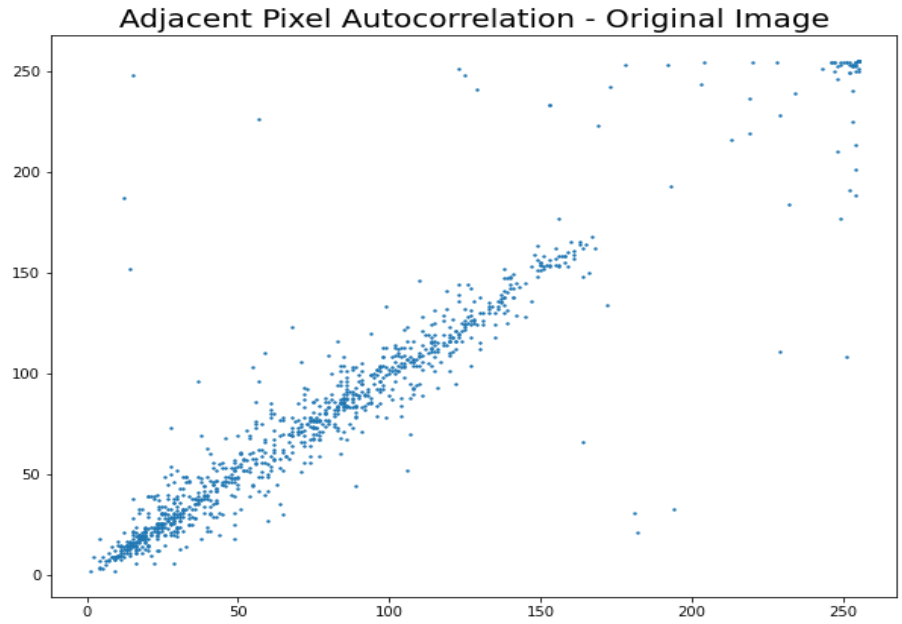
UACI for AES Image Encryption= 0.11910438529010486

B. Chaotic Encryption

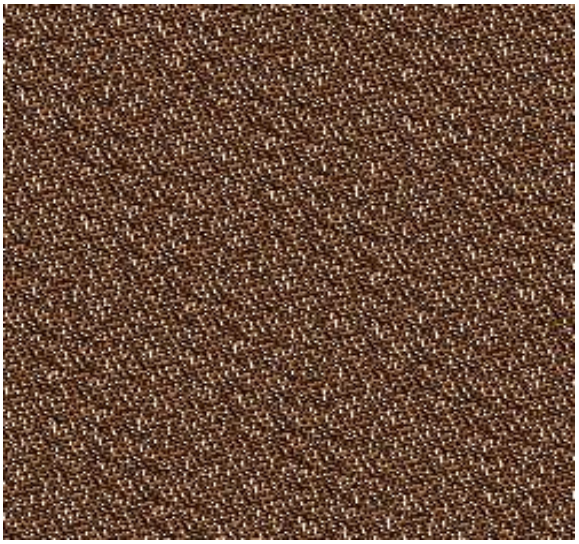
Original Image

Intensity Histogram of Original Image

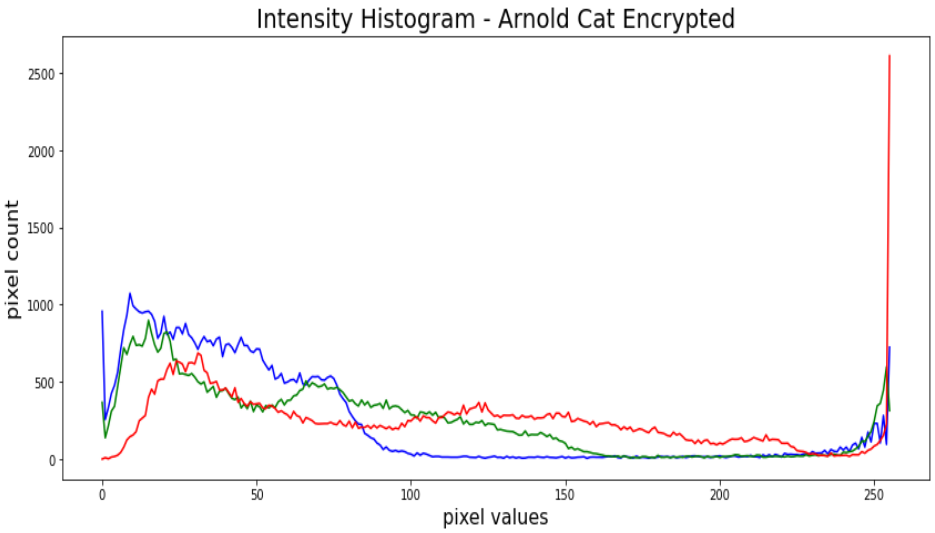


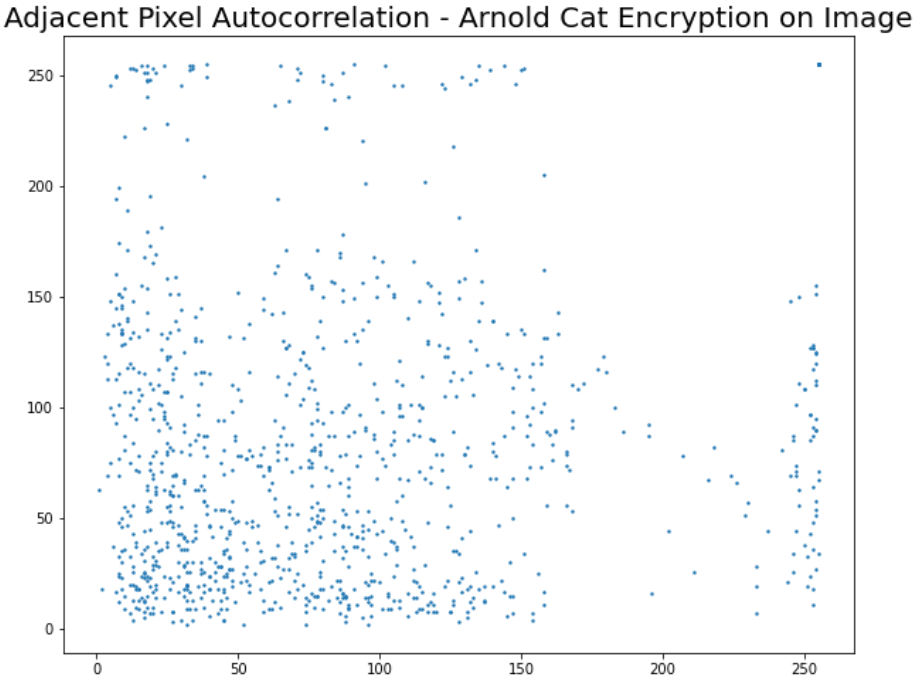


1. Arnold Cat Encryption

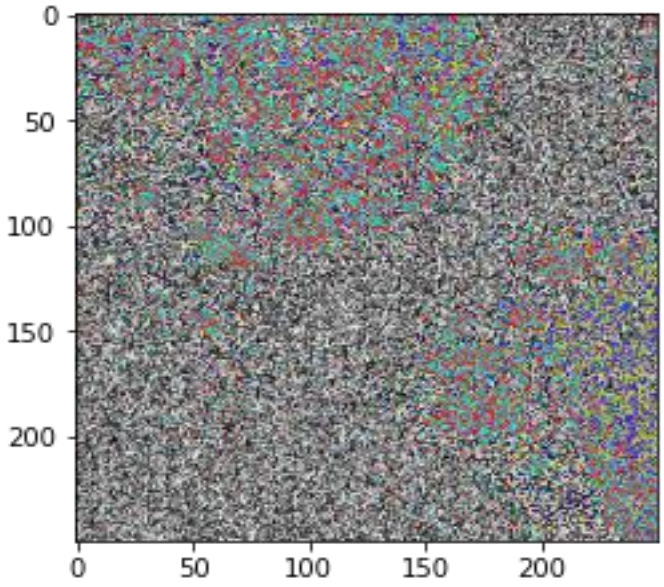


Encrypted Image

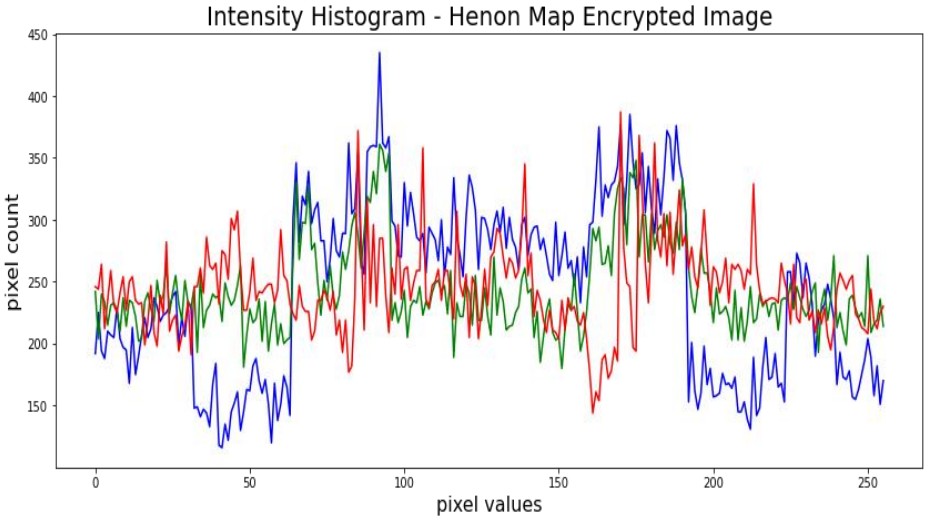


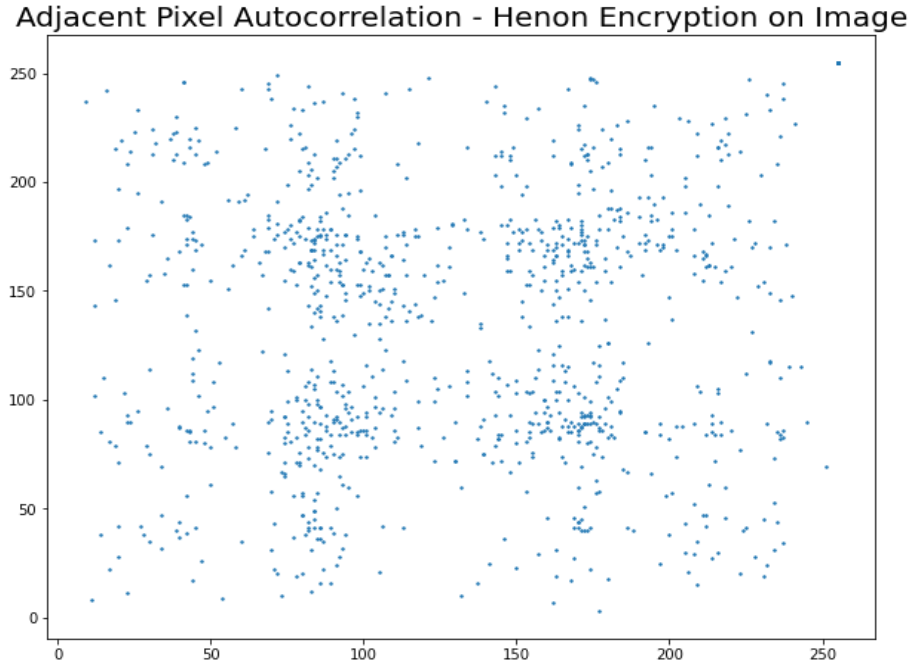


2. Henon Map Image Encryption

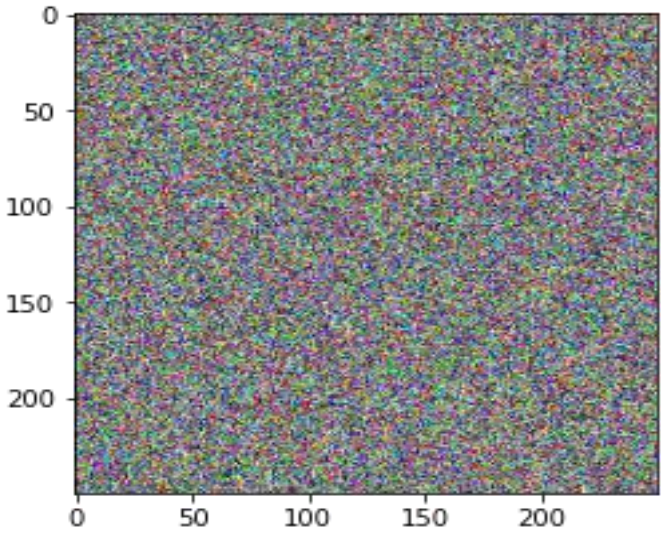


Encrypted Image

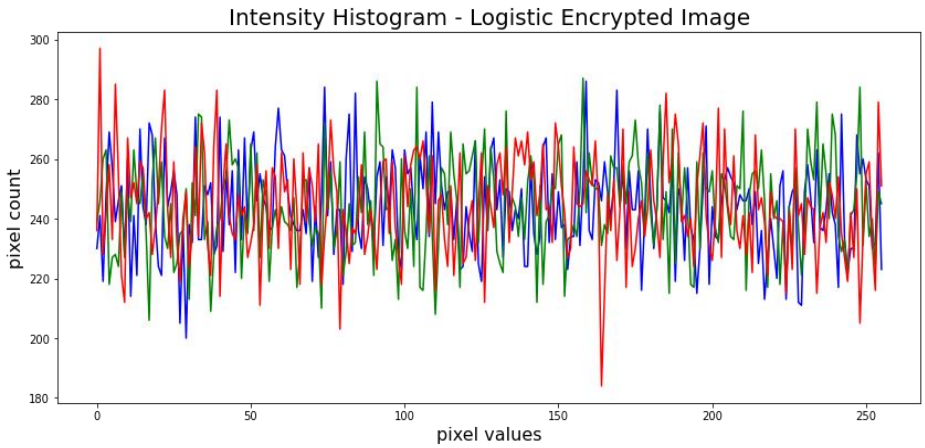


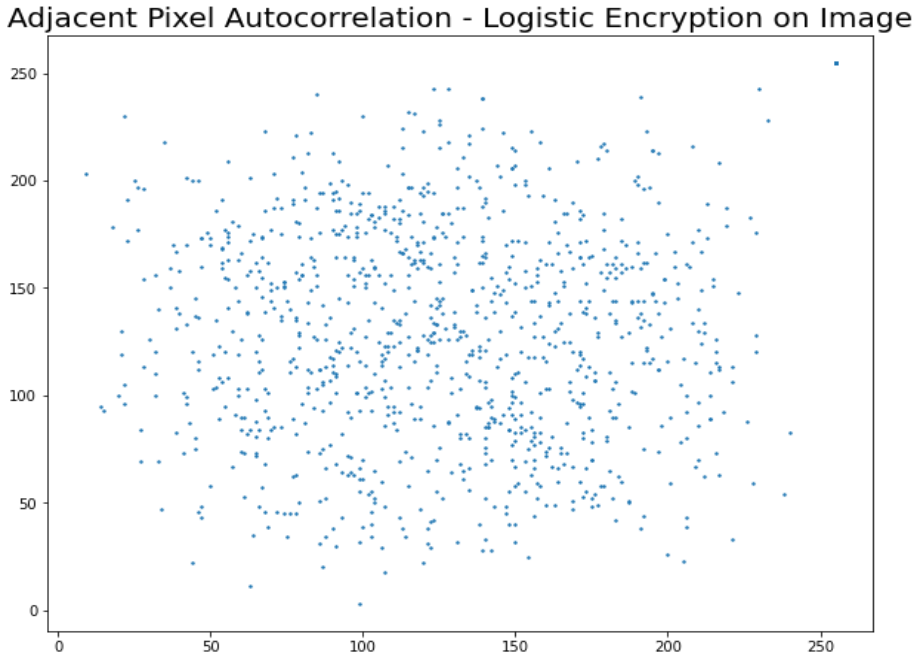


3. Logistic Chaos Maps with key mixing Image Encryption



Encrypted Image

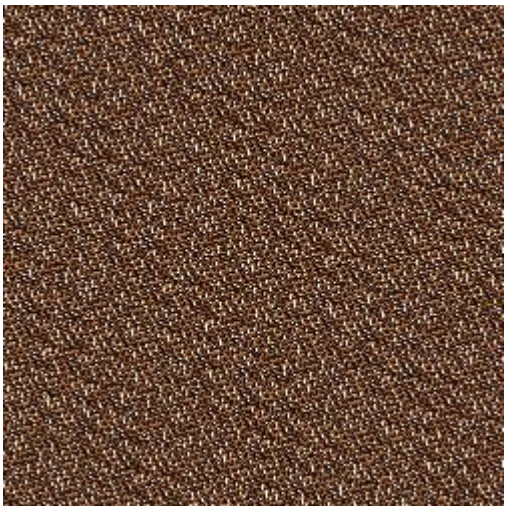




4. Key Sensitivity Comparison

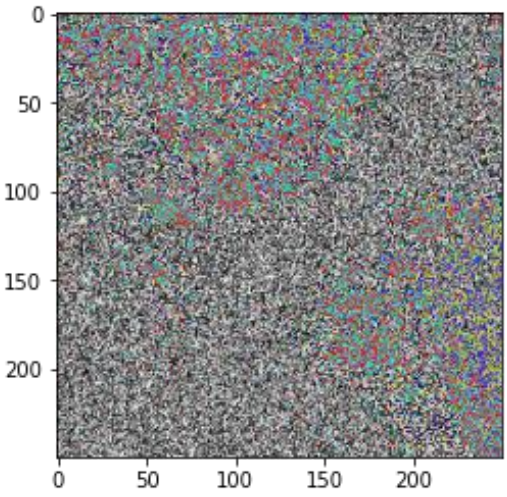
I. Arnold Cat Map

Encrypt with key = 20

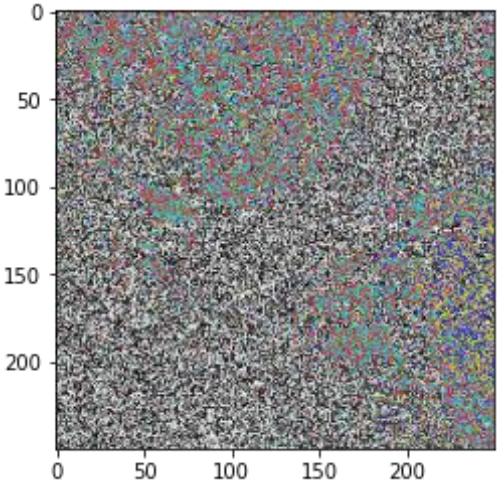


Encrypt with key = 19

II. Henon Cat Map

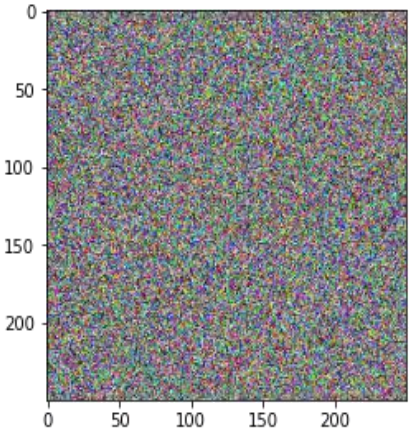


Encrypt with key (0.1, 0.1)

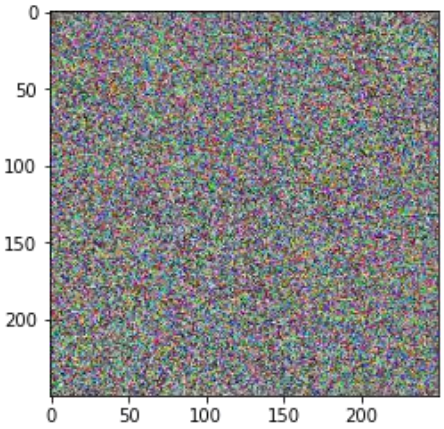


Encrypt with key (0.1, 0.101)

III. Logistic Map

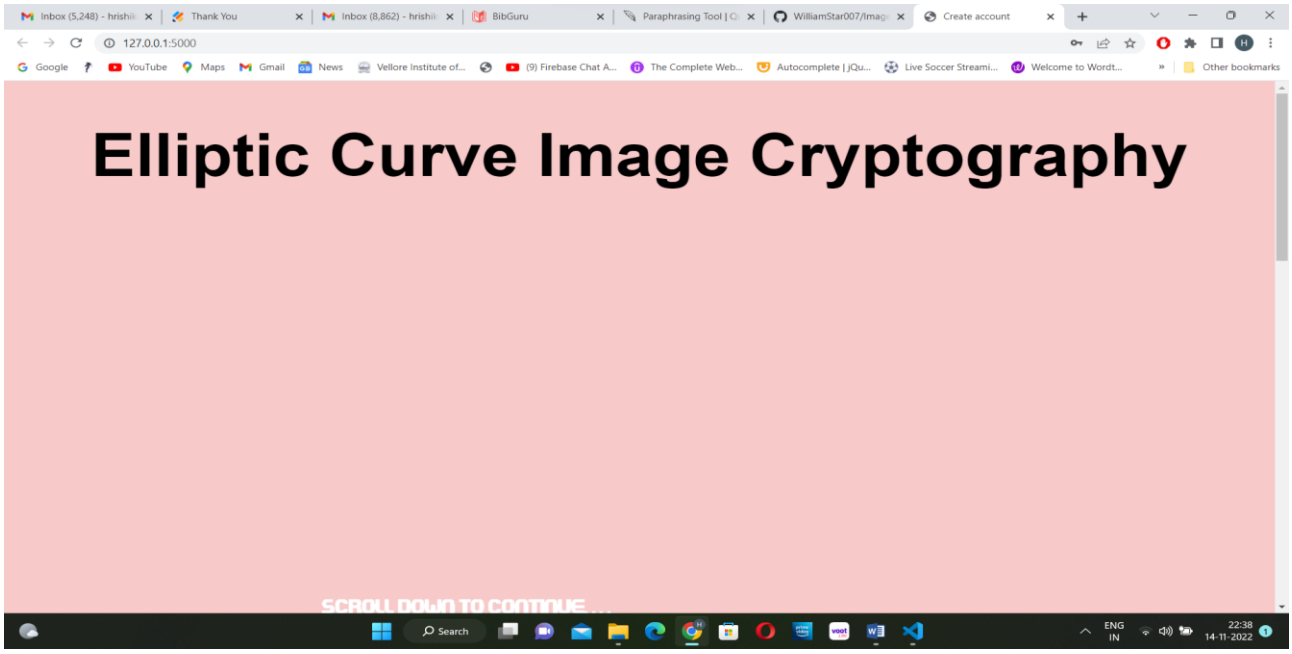


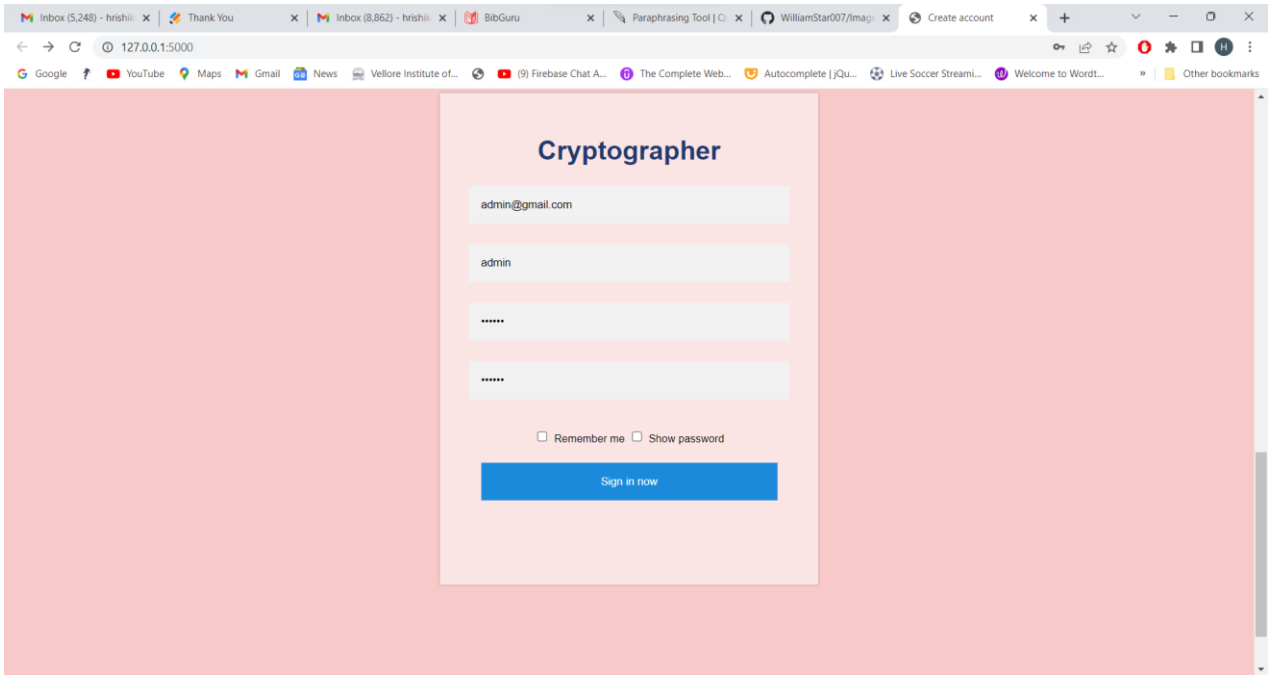
Decrypt with the key "supersecretke"

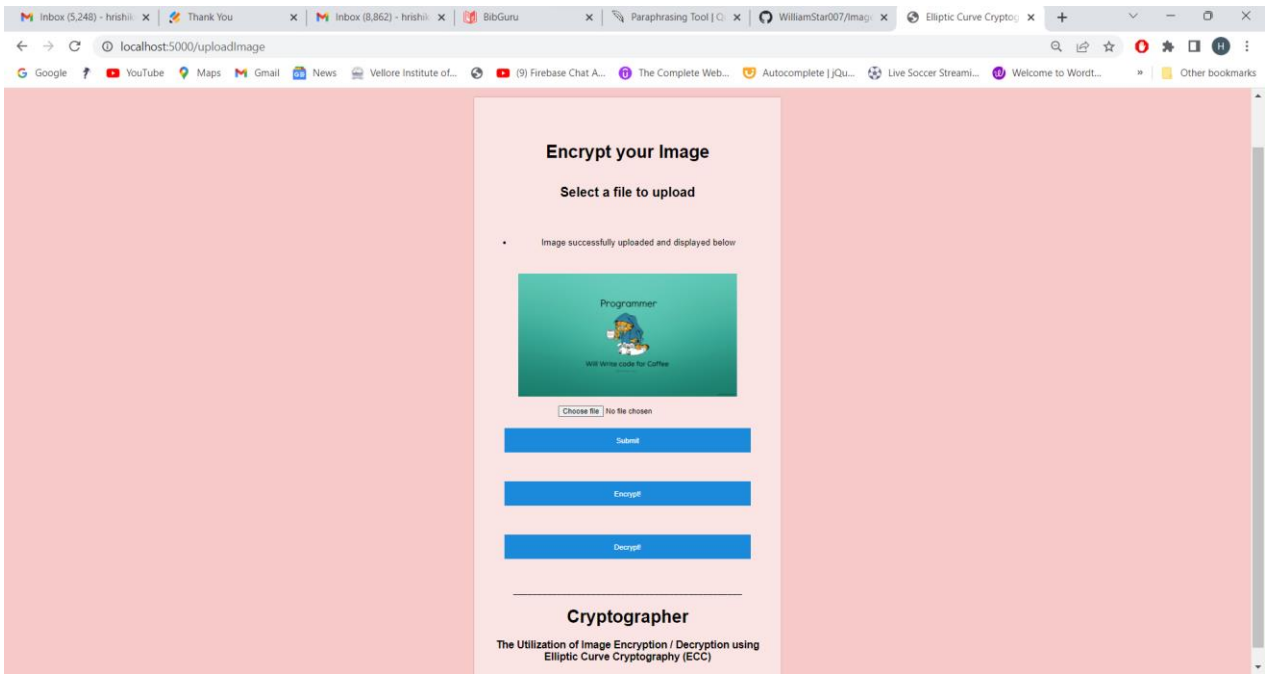


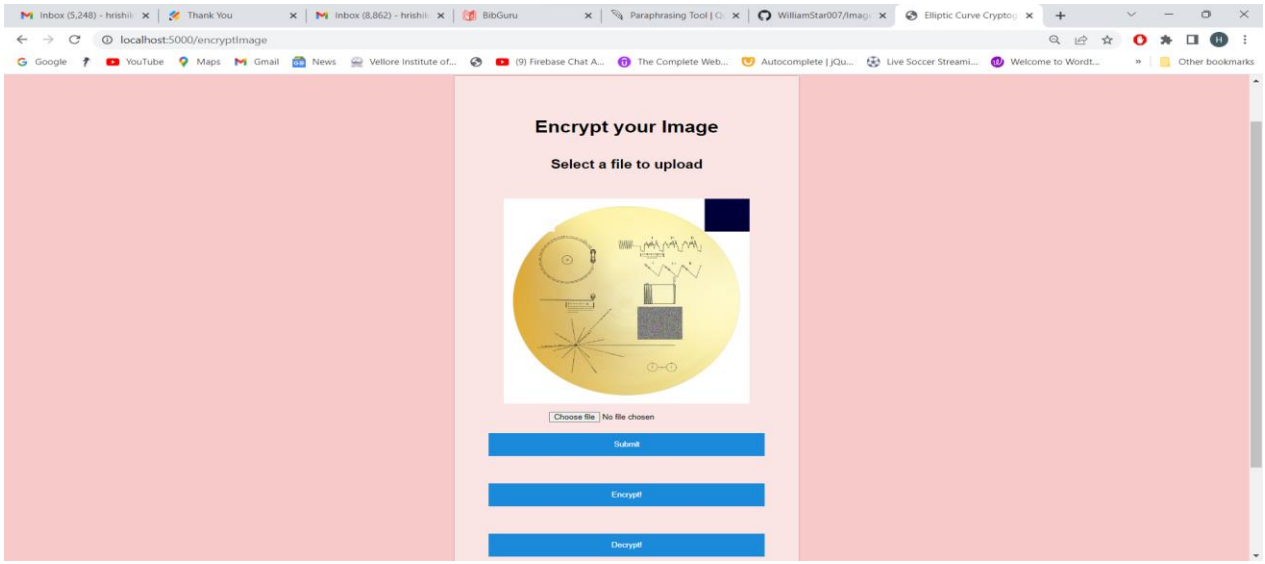
Decrypt with the key "supersecretkd"

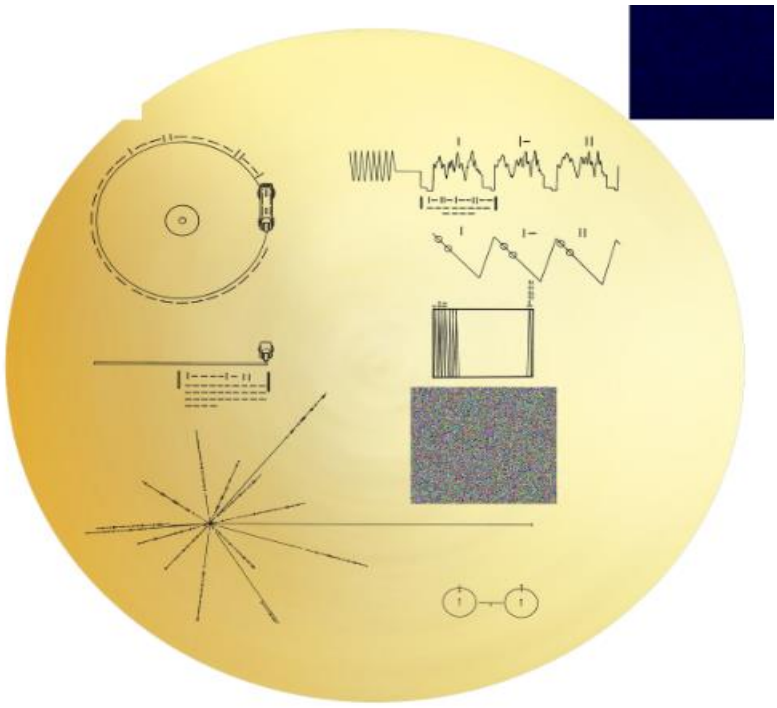
C. Elliptical Curve Image Encryption


Elliptic Curve Image Cryptography
SCROLL DOWN TO CONTINUE...


Cryptographer
admin@gmail.com
admin
Remember me
Show password
Sign in now


Encrypt your Image
Select a file to upload
Image successfully uploaded and displayed below
Choose file
No file chosen
Submit
Encrypt
Decrypt
Cryptographer
The Utilization of Image Encryption / Decryption using Elliptic Curve Cryptography (ECC)





Encrypted Image

CONCLUSION

The 3 Image Encryption Algorithms were implemented successfully. AES Image encryption (Rubik's cube method) performed better than simple AES encryption. To permute image pixels, this approach is based on the Rubik's cube theory. Using a key, the XOR operator is used to odd rows and columns of a picture to muddle the link between the original and encrypted images. Even rows and columns of the image are treated with the same key that has been flipped. The suggested algorithm's resistance to many forms of attacks, including statistical and differential attacks, has been tested experimentally with comprehensive numerical analysis (visual testing). Furthermore, performance evaluation experiments show how extremely secure the suggested picture encryption technique is. Additionally, it has quick encryption and decryption capabilities, making it appropriate for real-time Internet encryption and transmission applications.

When we compare Arnold Cat Maps, Henon Maps, and Logistic chaos maps, Arnold Cat Maps is not as effective as the other two. The intensity histogram Logistic Chaos Maps is more uniformly distributed

suggesting that it is a better technique than Arnold Cat Maps and Henon Maps. On comparing Adjacent Pixel Autocorrelation, Logistic Chaos Encryption has the most random plot without any visible pattern. It was followed by Henon Maps and Arnold Cat Maps. Key sensitivity of Logistic chaos Maps was observed to be the most sensitive when subjected to slight changes in the key.

It can be concluded from the observations that a combined system of AES and Logistic Chaos Maps will be one of the most secure Image encryption Algorithms. The individual attributes get added up and produce a brilliant algorithm to safely encrypt images.