IMPLEMENATION AND COMPARISON OF IMAGE CRYPTOGRAPHY TECHNIQUES

INDEX

INTRODUCTION

ENCRYPTION

Encryption is a process which uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data. With the help of key and the algorithm we can encrypt or decrypt the plaintext into cipher text and then cipher text back into plaintext.

METHODS OF ENCRYPTION

- **Symmetric Encryption Cryptography:** It uses the same secret key to encrypt the raw message at source, transmit the encrypted message to the recipient, and then decrypt the message at the destination. A simple example is representing alphabets with numbers – say, 'A' is '01', 'B' is '02', and so on. A message like "HELLO" will be encrypted as "0805121215," and this value will be transmitted over the network to the recipient(s). Once received, the recipient will decrypt it using the same reverse methodology – '08' is 'H', '05' is 'E', and so on, to get the original message value "HELLO." Even if unauthorized parties receive the encrypted message "0805121215," it will be of no value to them unless they know the encryption methodology. This method offers advantages of simple implementation with minimum operational overhead, but suffers from issues of security of shared key and problems of scalability.

- **Asymmetric Encryption Cryptography:** It uses two different keys – one public and one private – to encrypt and decrypt data. The public key can be disseminated openly, like the address of the fund receiver, while the private key is known only to the owner. In this method, a person can encrypt a message using the receiver's public key, but it can be decrypted only by the receiver's private key. This method helps achieve the two important functions of authentication and encryption for cryptocurrency transactions. The former is achieved as the public key verifies the paired private key for the genuine sender of the message, while the latter is accomplished as only the paired private key holder can successfully decrypt the encrypted message.

- **Hashing:** It is used to efficiently verify the integrity of data of transactions on a network or to verify the fidelity of data that has been copied or downloaded against the original. Typical hash functions take inputs of variable lengths to return outputs of a fixed length. Hashing works because it is very difficult to reconstitute the original data only given the hashed output. Hashing is also employed because it is computationally difficult, making block mining possible for cryptocurrencies. Additionally, Digital Signatures complement these various cryptography processes, by allowing genuine participants to prove their identities to the network.

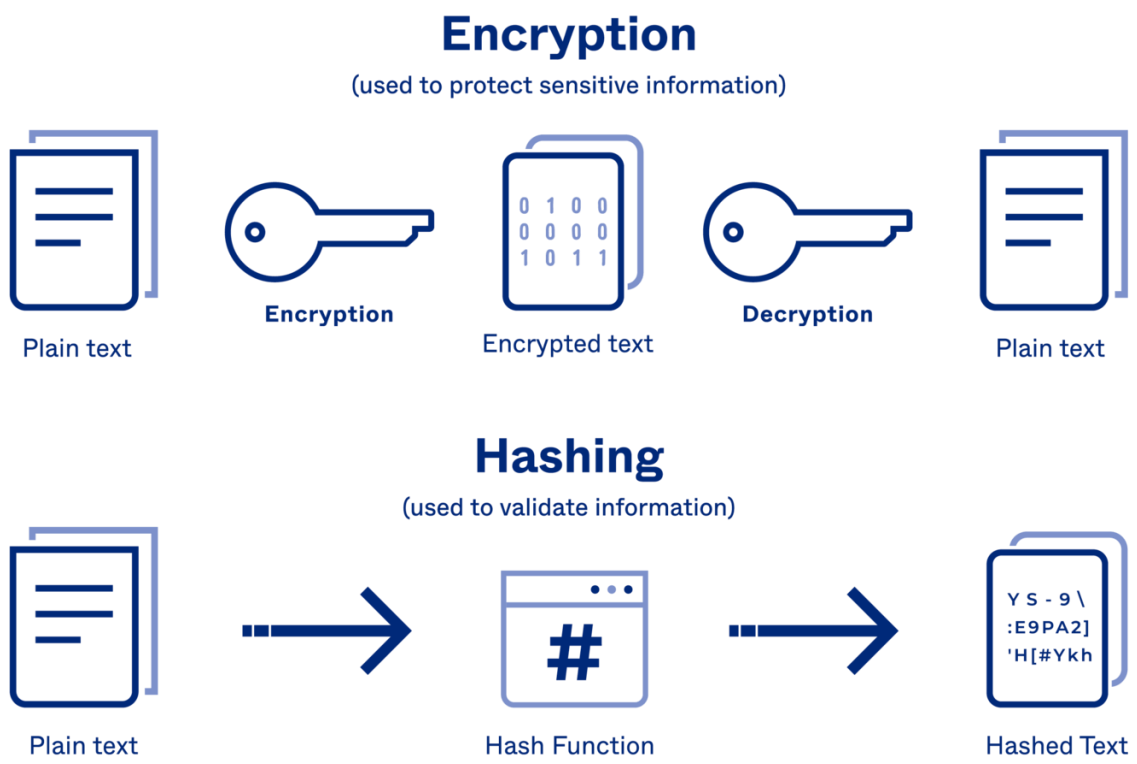

Figure 1: Encryption and Hashing

VISUAL CRYPTOGRAPHY

Visual Cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

IMAGE ENCRYPTION

Image Encryption can be defined as the process of encoding secret image with the help of some encryption algorithm in such a way that unauthorized users can't access it. Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different processes. Therefore, the security of image data from unauthorized access is important.

Image encryption plays an important role in the field of information hiding. Image encryption method prepares information that is unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet.

BACKGROUND

CHAOS MAPS

Chaotic systems are a simple sub-type of nonlinear dynamical systems. They may contain very few interacting parts and these may follow very simple rules, but these systems all have a very sensitive dependence on their initial conditions. Despite their deterministic simplicity, over time these systems can produce totally unpredictable and wildly divergent (chaotic) behavior. A few chaos-based algorithms provide a good combination of speed, high security complexity, low computational overheads. Moreover, certain chaos-based and other dynamical systems-based algorithms have many important properties such as:

- Pseudorandom properties
- Ergodicity and Non-periodicity
- Sensitive dependence on initial parameters

ARNOLD CAT MAP ENCRYPTION

Arnold's cat map is a chaotic map often used for pixel manipulation. It applies a transform on the image that essentially shuffles the pixels by stretching and folding the image. When an optimal number of iterations of the transformation are applied on the image, the resulting image becomes incomprehensible and hence encrypted. The Arnold cat mapping is non-Hamiltonian, nonanalytic, and mixing. However, it is area preserving since the determinant is 1.

The transform applied on the image is:

$$R([x, y]) = [(x + y)\ mod\ n, (x + 2y)\ mod\ n]$$

where, n is the dimensions of the image.

HÉNON MAP ENCRYPTION

The Hénon map, sometimes called Hénon-Pomeau attractor/map, is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. The Hénon map takes a point (x_n, y_n) in the plane and maps it to a new point:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases}$$

The map depends on two parameters, a and b. The classical Hénon map have values of a = 1.4 and b = 0.3. For the classical values the Hénon map is chaotic. For other values of a and b the map may be chaotic, intermittent, or converge to a periodic orbit. An overview of the type of behavior of the map at different parameter values may be obtained from its orbit diagram.

LOGISTIC MAP ENCRYPTION

The logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. The logistic map is a one-dimensional discrete-time map that, despite its formal simplicity, exhibits an unexpected degree of complexity. The logistic map uses a nonlinear difference equation to look at discrete time steps. It's called the logistic map because it maps the population value at any time step to its value at the next time step. Mathematically, the logistic map is written as:

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

where, x_n is a number between zero and one, that represents the ratio of existing population to the maximum possible population. The values of interest for the parameter r (sometimes also denoted μ) are those in the interval [−2, 4], so that x_n remains bounded on [−0.5, 1.5].

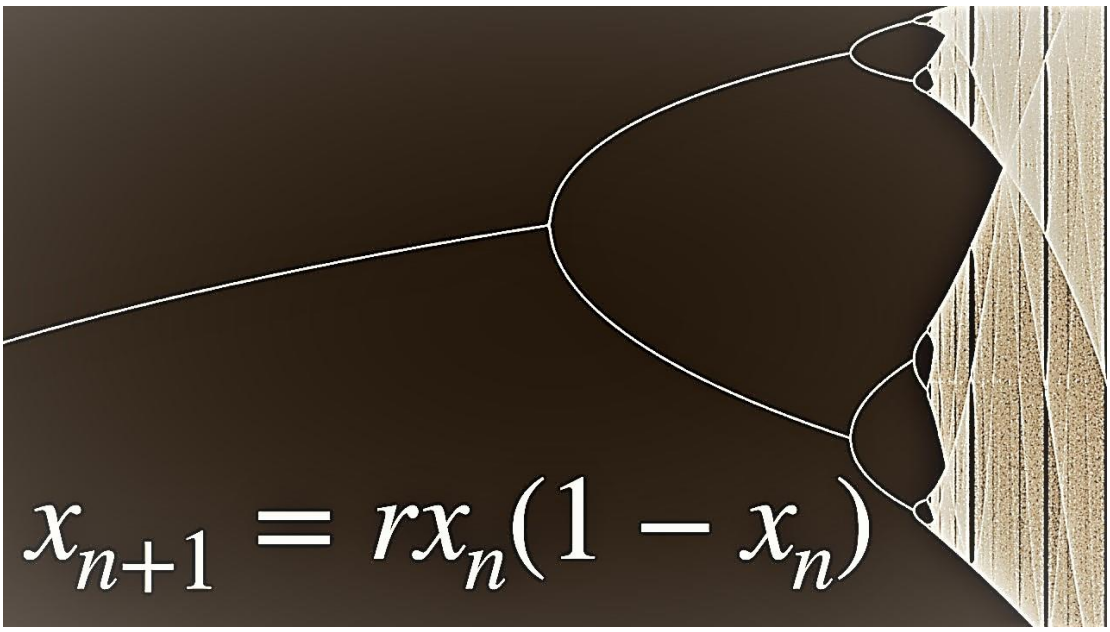

Figure 2: Bifurcation Diagram of Logistic Map

HILL CIPHER ENCRYPTION

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. In simple words, it is a cryptography algorithm used to encrypt and decrypt data for the purpose of data security. The algorithm uses matrix calculations given in Linear Algebra. In hill cipher algorithm every letter (A-Z) is represented by a number modulus 26.

To encrypt and decrypt the text using hill cipher, following operations are performed:

$$E(K, P) = (K * P)\ mod\ 26$$
$$P(K, E) = (K^{-1} * E)\ mod\ 26$$

where, K is the key matrix, P is plain text and E is generated cipher text.

ADVANCED ENCRYPTION STANDARD

The Advanced Encryption Standard (AES) algorithm also known as the Rijndael algorithm is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits. The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

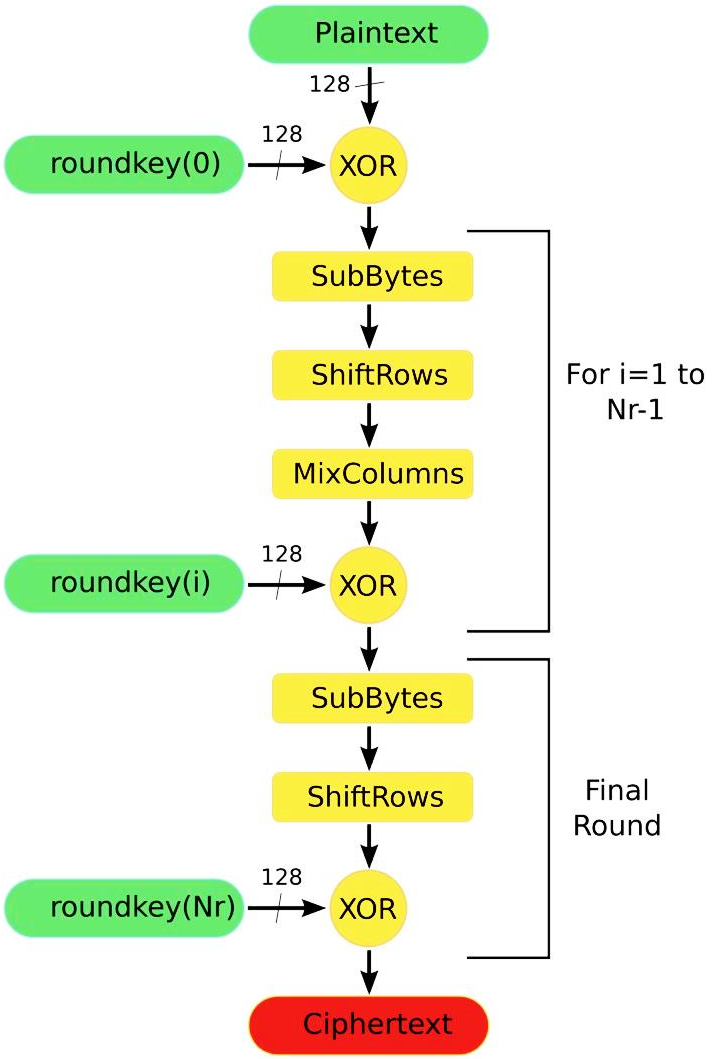

Figure 3: Encryption Process of AES Algorithm

ENCRYPTION PROCESS

- Substitution of the bytes
- Shifting the rows
- Mixing the columns
- Adding the round key

DNA BASED IMAGE ENCRYPTION

DNA encryption is the process of hiding or perplexing information by a computational method in order to improve privacy. The existing image encryption algorithms based on DNA coding involve four basic processes:

- Scrambling the pixel position of the image by using a chaotic sequence.
- Encoding the scrambled image matrix to the DNA sequence.
- Disturbing the DNA sequence matrix by using a chaotic sequence combined with addition, subtraction, XOR, or complement operation, or a combination of these operations.
- Obtaining the encrypted image by DNA decoding and recombination.

Fixed DNA coding rules are simple to implement, have high computational efficiency, and one can even disturb a pixel value by selecting decoding rules that are different from the encoding rules.

RUBIK'S CUBE IMAGE ENCRYPTION

It is one of the latest methods for performing image encryption. It involves generating two random keys of length equal to number of rows and columns in the original image respectively. The original image is scrambled using the principle of Rubik's cube, which only changes the position of the pixels. Using two random secret keys, the bitwise XOR is applied into the odd rows and columns. Then, the bitwise XOR is also applied to even rows and columns using the flipped secret keys. These steps can be repeated while the number of iterations is not reached. Decryption algorithm simply involves inverting the encryption process.

HISTOGRAM ANALYSIS

An **Image Histogram** is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. Image histograms are present on many modern digital cameras. Photographers can use them as an aid to show the distribution of tones captured, and whether image detail has been lost to blown-out highlights or blacked-out shadows. This is less useful when using a raw image format, as the dynamic range of the displayed image may only be an approximation to that in the raw file.

The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the total number of pixels in that particular tone. The left side of the horizontal axis represents the dark areas, the middle represents mid-tone values and the right-hand side represents light areas. The vertical axis represents the size of the area (total number of pixels) that is captured in each one of these zones. Thus, the histogram for a very dark image will have most of its data points on the left side and center of the graph. Conversely, the histogram for a very bright image will have most of its data points on the right side and center of the graph.

The cipher text image histogram analysis is one of the most straight-forward methods of illustrating the image encryption quality. A good image encryption method tends to encrypt a plaintext image to a random incomprehensible form. Thus, a good image encryption technique generates a cipher image that has a uniformly distributed intensity histogram.

ADJACENT PIXEL AUTO-CORRELATION

Images exhibit high information redundancy. Thus, it is desirable to have an encryption algorithm that breaks this redundancy. As a metric of encryption performance, we find the correlation between adjacent pixels in a direction (Horizontal, Vertical or Diagonal). Some random pixels are picked up from the image and its correlation between its rightmost neighbor is found and plotted. For a good algorithm, the correlation plot should appear random with no discernable pattern.

APPROACH

The main objective of this project involves application and comparison of various Image Cryptography algorithms. Different image cryptography algorithms use different encryption and decryption techniques resulting in varying strength of encrypted output, quality of decrypted image and total time taken. In order to study image cryptography algorithms, following approach is taken:

- **Input Image:** The image that needs to be encrypted is taken as input. The input image is resized into a 300 x 300-pixel image.
- **Image Cryptography Algorithms:** After resizing the image, cryptography algorithms are applied to encrypt the image from the sender's end. Encrypted image is passed through decryption process of cryptographic algorithm to get decrypted image at receiver's end. Following cryptographic algorithms are applied:
    - Chaos Map based Image Cryptography:
        - Arnold Cat Map Encryption
        - Hénon Map Encryption
        - Logistic Map Encryption
    - Hill Cipher Encryption
    - Advanced Encryption Standard (AES)
    - Rubik's Cube Image Encryption
    - DNA Based Image Encryption
- **Histogram Analysis:** Encrypted Image Histogram is used to analyse the strength and quality of encrypted image. Basically, the more uniform the histogram is, higher the strength of encrypted output is. Intensity Distribution Score is calculated as the mean of standard deviations of three color channels.
- **Adjacent Pixel Auto-Correlation:** It is used to analyse the performance of encryption algorithm. The correlation between some random points of encrypted image are plotted in order to visualize any observable pattern among them. A pattern in Adjacent Pixel Auto-Correlation plot generally refers to low strength and quality of encryption algorithm.
- **Key Sensitivity:** An ideal image encryption procedure should be sensitive to the secret key. It means that a little change in a secret key should produce completely different image.
- **Algorithm Running Time:** The time taken to encrypt and decrypt an image is a major deciding factor among cryptographic algorithms for use in real life applications.
- **Decrypted Image Quality:** The decrypted image is compared to the input image.

Comparative Study of Image Cryptographic Algorithms is performed using the above-mentioned properties and the results are presented in a tabular form.

IMPLEMENTATION AND RESULTS

INPUT IMAGE

Figure 4.1 represents the image to be encrypted using different cryptographic algorithms. The input image is resized to 300 x 300-pixel image.

Figure 4.1: Input Image

Figure 4.2 represents the Intensity Histogram of Input Image. Large number of lower pixel values is observed in blue color channel. In contrast, large number of higher pixel values is obtained in red color channel. Green pixel values follow a more uniform distribution compared to blue and red color channels. Thus, the image contains darker blue tones alongside brighter red tones with uniformly distributed green tones.

Figure 4.2: Intensity Histogram of Input Image

IMAGE CRYPTOGRAPHY ALGORITHMS

1. Arnold Cat Map Encryption

Figure 5.1 represents encrypted image and Figure 5.2 represents decrypted image.

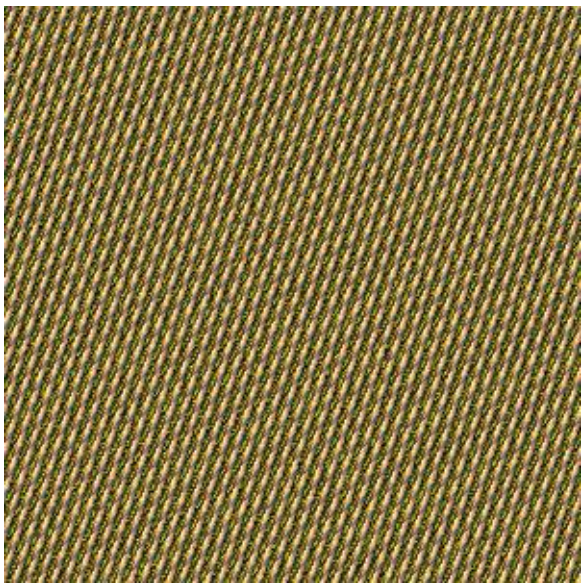

Figure 5.1: Encrypted Image

Figure 5.2: Decrypted Image

Encrypted Image obtained using Arnold Cat Map Encryption Algorithm retains all pixel values of input image in a shuffled manner such that it becomes inconceivable.

Figure 5.3 represents the Intensity Histogram of Encrypted Image obtained from Arnold Cat Map Encryption Algorithm. It comes out to be exactly same as that of Input Image. This verifies that Encrypted Image contains the same pixel values as that in Input Image but in a shuffled manner. The strength of encryption obtained is low since the Intensity Distribution Score is quite high (249.2488).

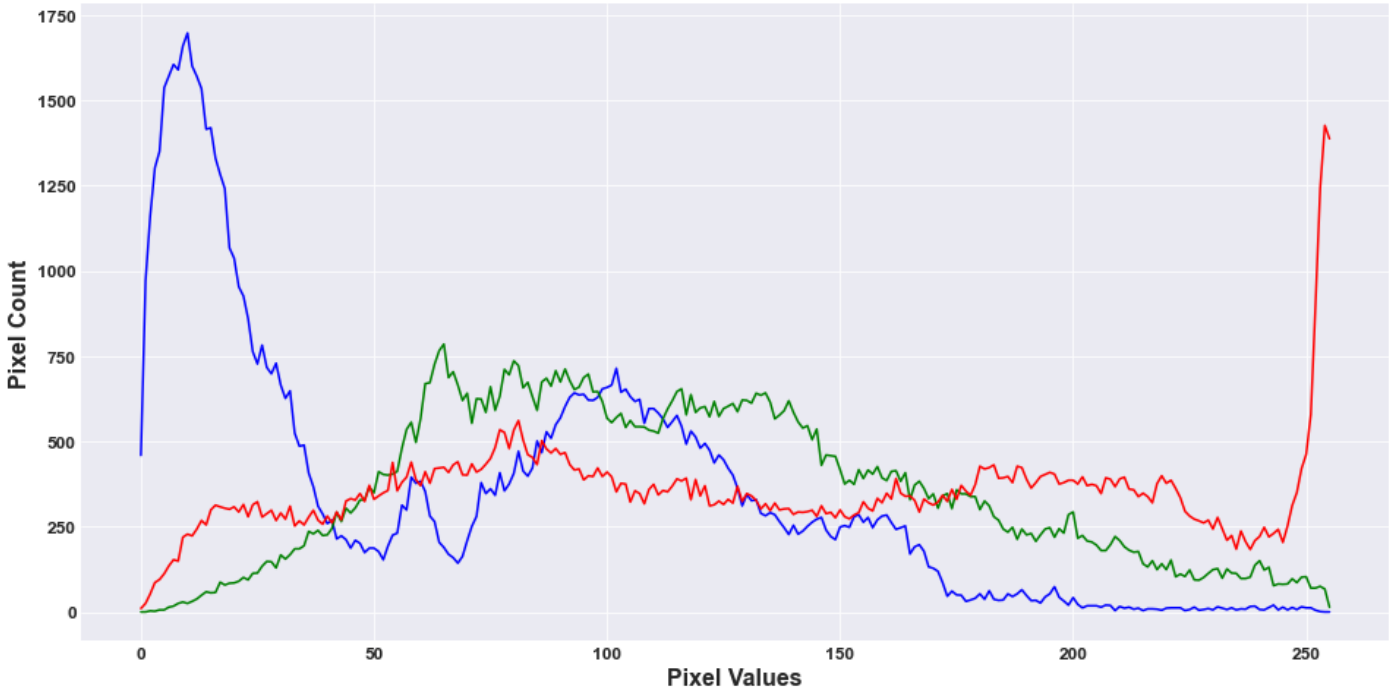

Figure 5.3: Intensity Histogram of Encrypted Image

Figure 5.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is relatively uncorrelated and has a correlation coefficient of 0.2568.

Figure 5.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two different keys 20 and 21 respectively. The two encrypted images are very different from each other, with 99.42% pixel values being different. Thus, it has high key sensitivity.

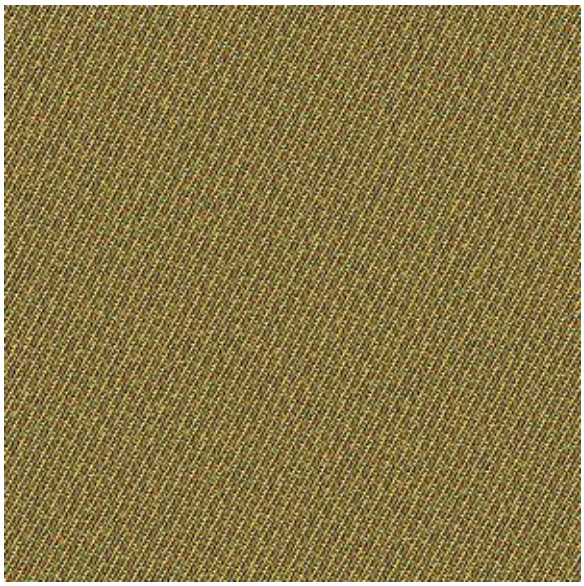

Figure 5.5.1: Encrypted Image with Key = 20

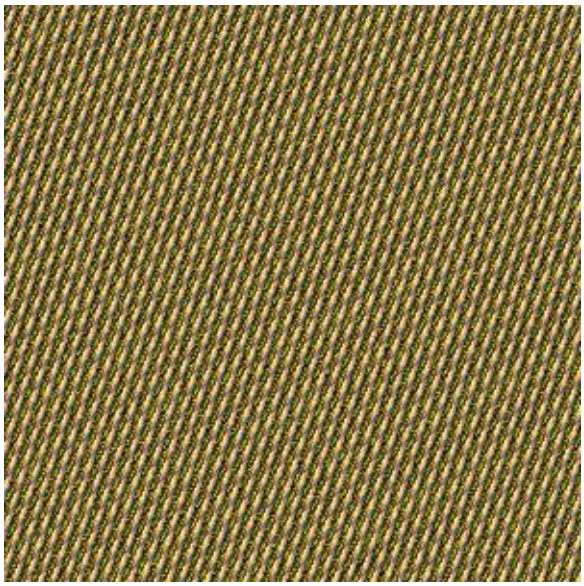

Figure 5.5.2: Encrypted Image with Key = 21

2. Hénon Map Encryption

Figure 6.1 represents encrypted image and Figure 6.2 represents decrypted image.

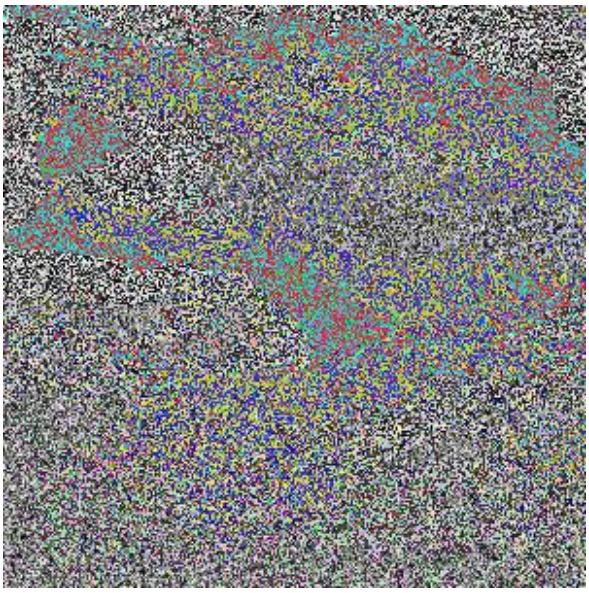

Figure 6.1: Encrypted Image

Figure 6.2: Decrypted Image

Figure 6.3 represents the Intensity Histogram of Encrypted Image obtained from Hénon Map Encryption Algorithm. It is more uniformly distributed over the range of pixel values as compared to that of Input Image. Red color channel is more uniformly distributed as compared to Green and Blue color channel.

The Encrypted Image contains entirely different pixel values as that in Input Image. As a result, its encryption strength is higher than that obtained from Arnold Cat Map Encryption. Still the strength of encryption obtained is average since the Intensity Distribution Score is little high (60.7352).

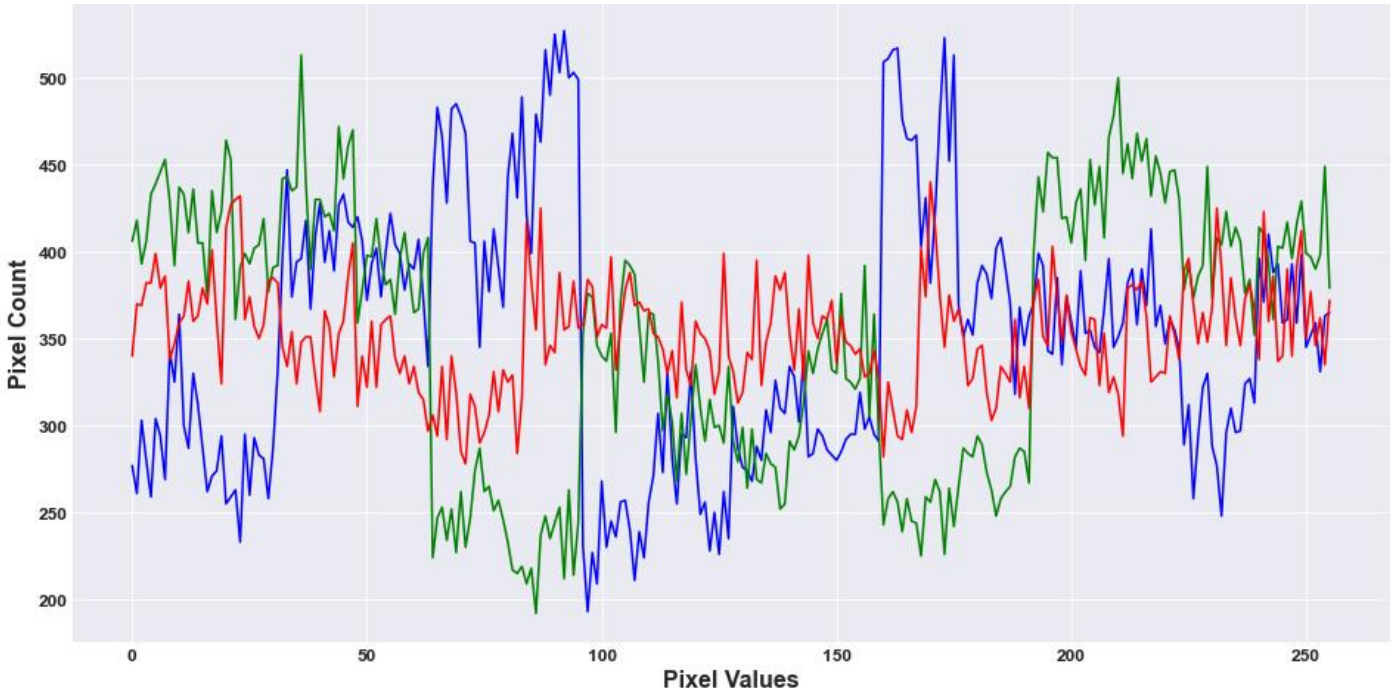

Figure 6.3: Intensity Histogram of Encrypted Image

Figure 6.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is almost uncorrelated and has a correlation coefficient of 0.0034.

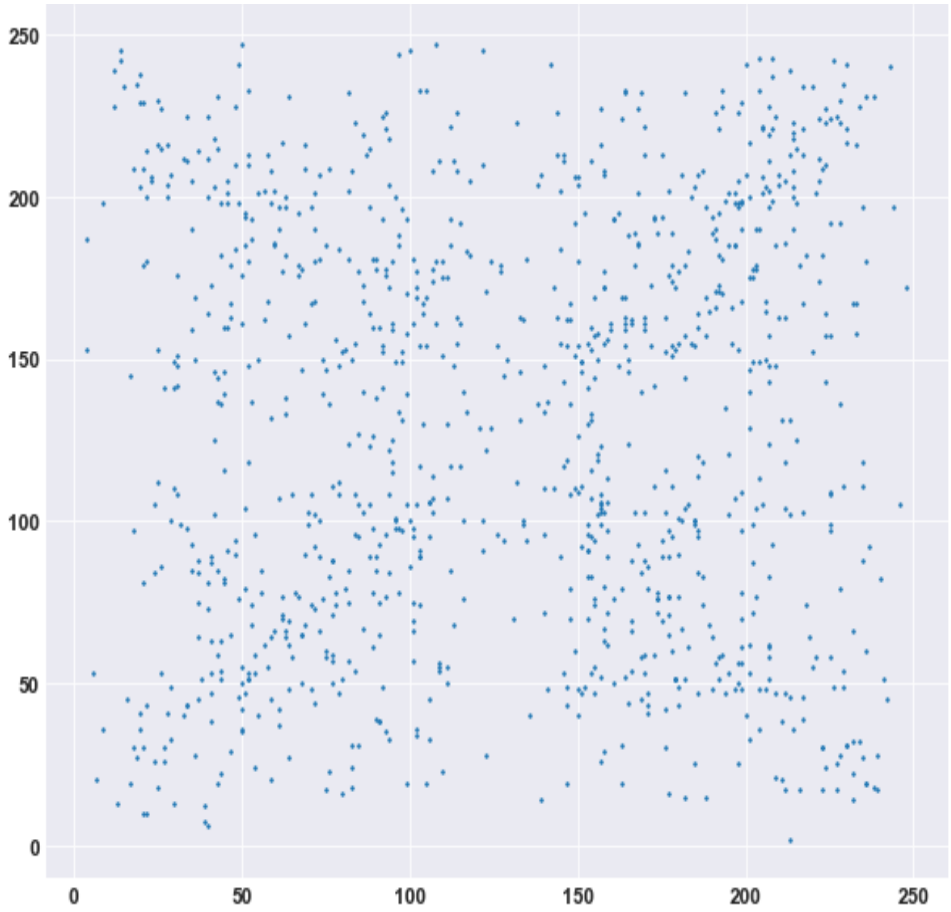

Figure 6.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two different keys (0.1, 0.1) and (0.101, 0.101) respectively. The two encrypted images are very different from each other, with 97.01% pixel values being different. Thus, it has relatively lower key sensitivity.

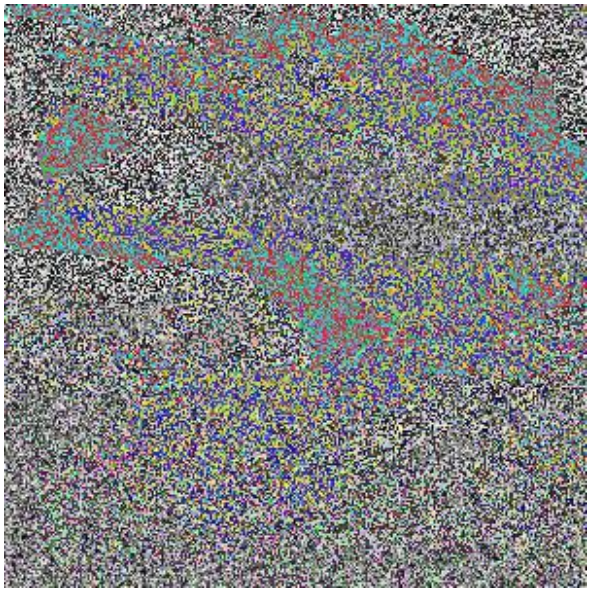

Figure 6.5.1: Encrypted Image with Key = (0.1, 0.1)

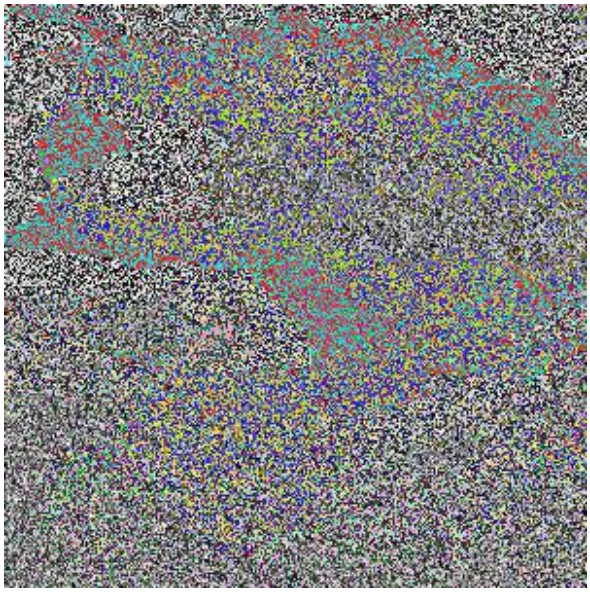

Figure 6.5.2: Encrypted Image with Key = (0.101, 0.101)

3. Logistic Map Encryption

Figure 7.1 represents encrypted image and Figure 7.2 represents decrypted image.

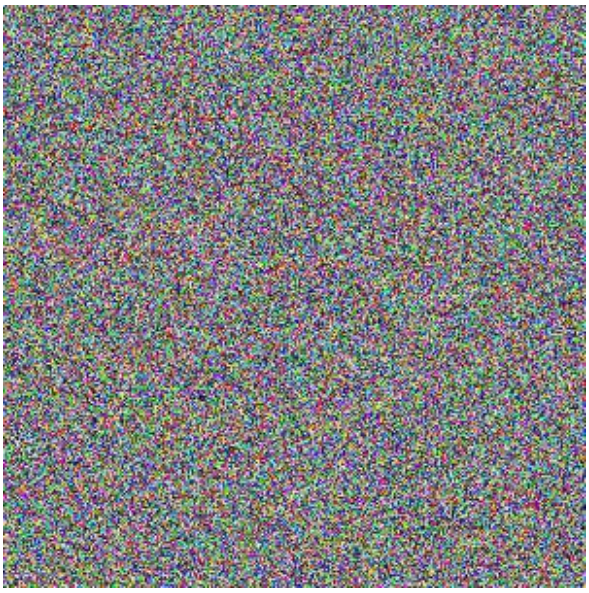

Figure 7.1: Encrypted Image

Figure 7.2: Decrypted Image

Figure 7.3 represents the Intensity Histogram of Encrypted Image obtained from Logistic Map Encryption Algorithm. It is more uniformly distributed over the range of pixel values as compared to that of Input Image. Large number of spikes of high pixel count is observed in all three channels of the Encrypted Image.

The Encrypted Image contains entirely different pixel values as that in Input Image. Its intensity distribution is more uniform than above-mentioned Chaos Map Based Encryption Algorithms. The strength of encryption obtained is high since the Intensity Distribution Score is relatively low (19.1990).

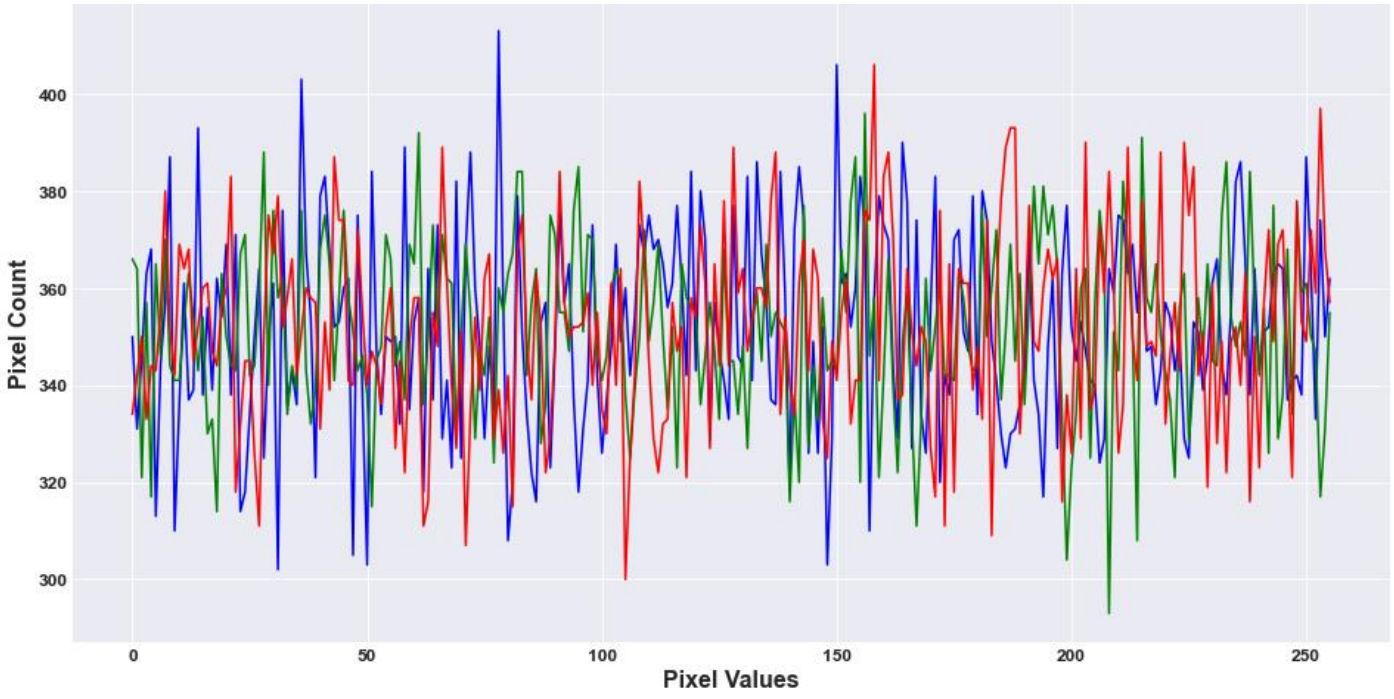

Figure 7.3: Intensity Histogram of Encrypted Image

Figure 7.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is highly uncorrelated and has a correlation coefficient of 0.0103.

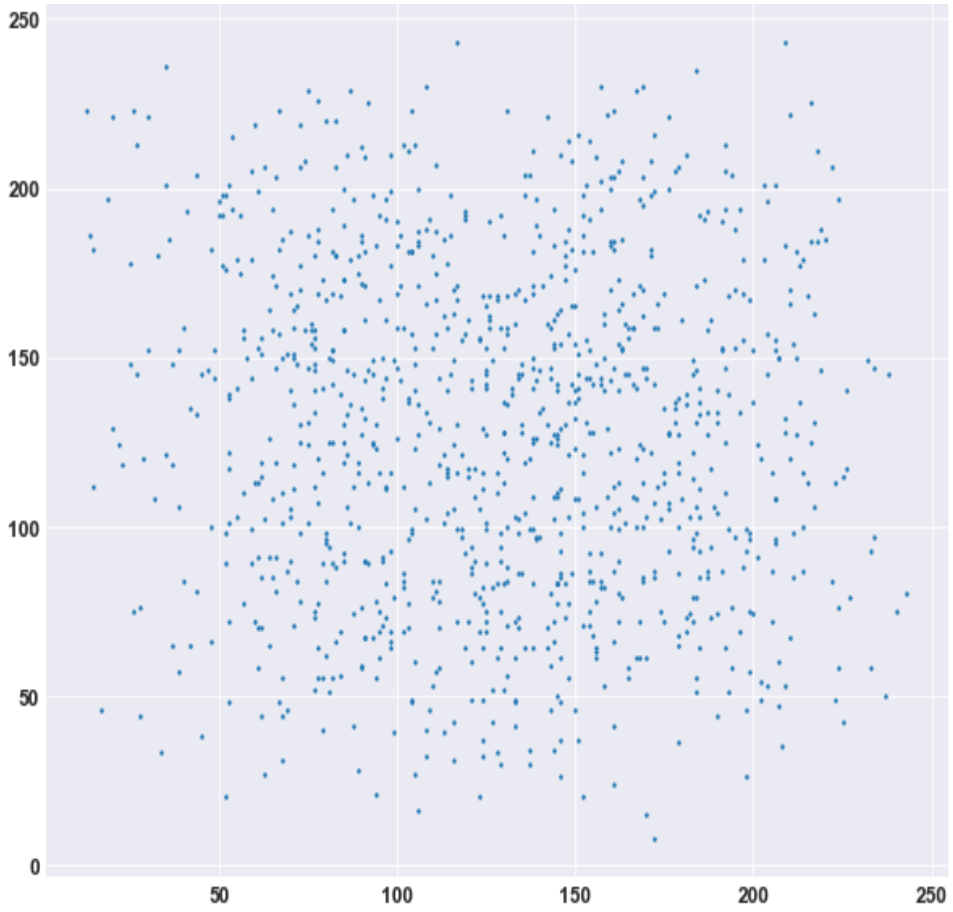

Figure 7.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two different keys "supersecretkeye" and "supersecretkeyd" respectively. The two encrypted images are very different from each other, with 99.59% pixel values being different. Thus, it has high key sensitivity.

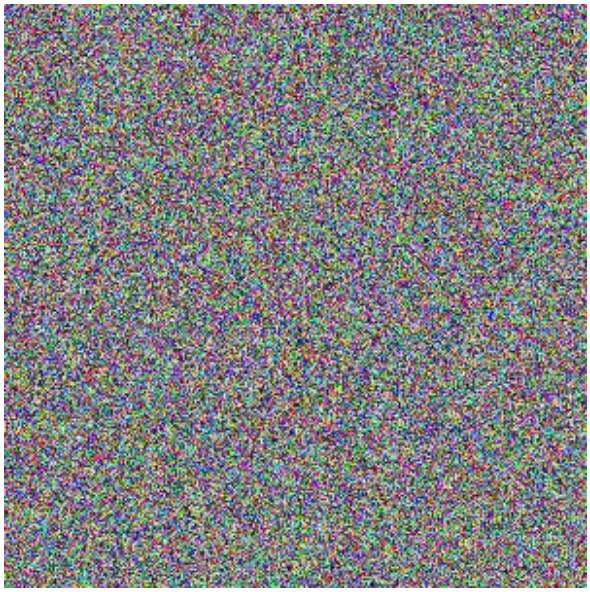

Figure 7.5.1: Encrypted Image with Key = supersecretkeye

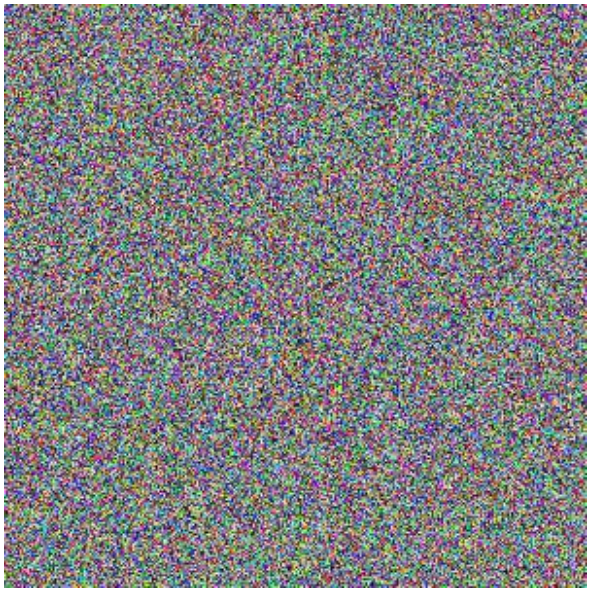

Figure 7.5.2: Encrypted Image with Key = supersecretkeyd

4. Hill Cipher Encryption

Figure 8.1 represents encrypted image and Figure 8.2 represents decrypted image.

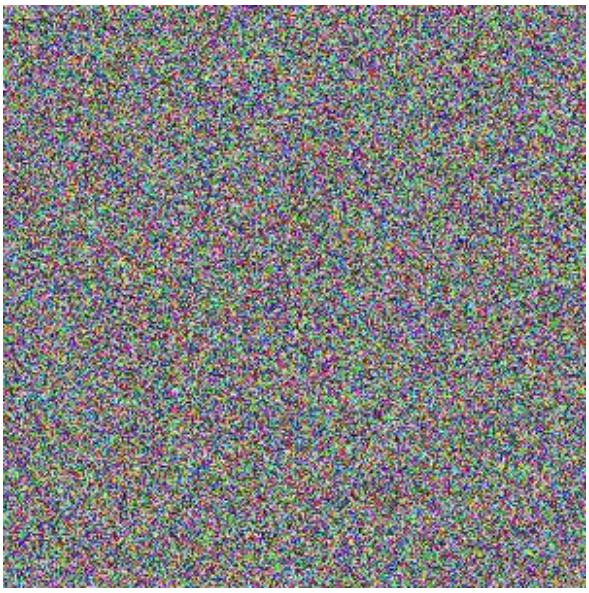

Figure 8.1: Encrypted Image

Figure 8.2: Decrypted Image

Figure 8.3 represents the Intensity Histogram of Encrypted Image obtained from Hill Cipher Encryption Algorithm. It is more uniformly distributed over the range of pixel values as compared to that of Input Image. Large number of spikes of high pixel count is observed in all three channels of the Encrypted Image. High amount of overlapping is observed among the three color channels.

The Encrypted Image contains entirely different pixel values as that in Input Image. The Pixel Count varies from 290 to 415 pixels. The strength of encryption obtained is high since the Intensity Distribution Score is relatively low (18.6418).

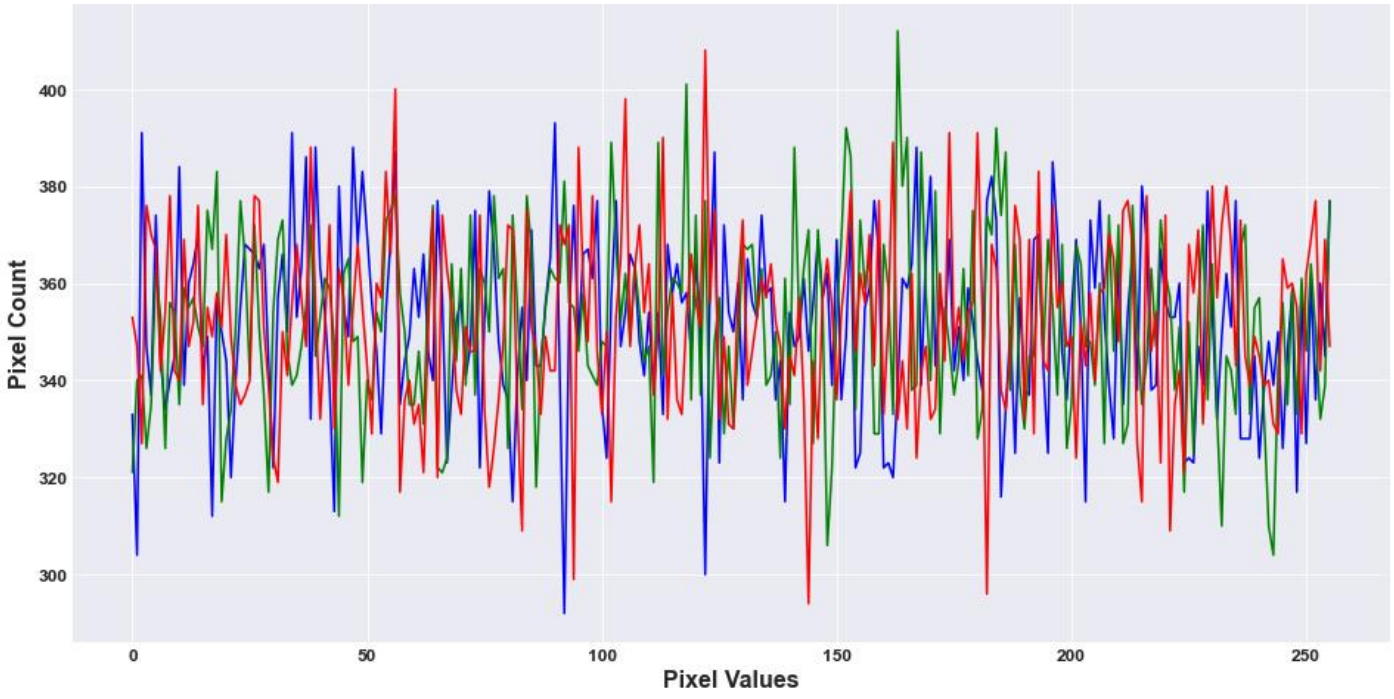

Figure 8.3: Intensity Histogram of Encrypted Image

Figure 8.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is relatively uncorrelated and has a correlation coefficient of 0.0402.

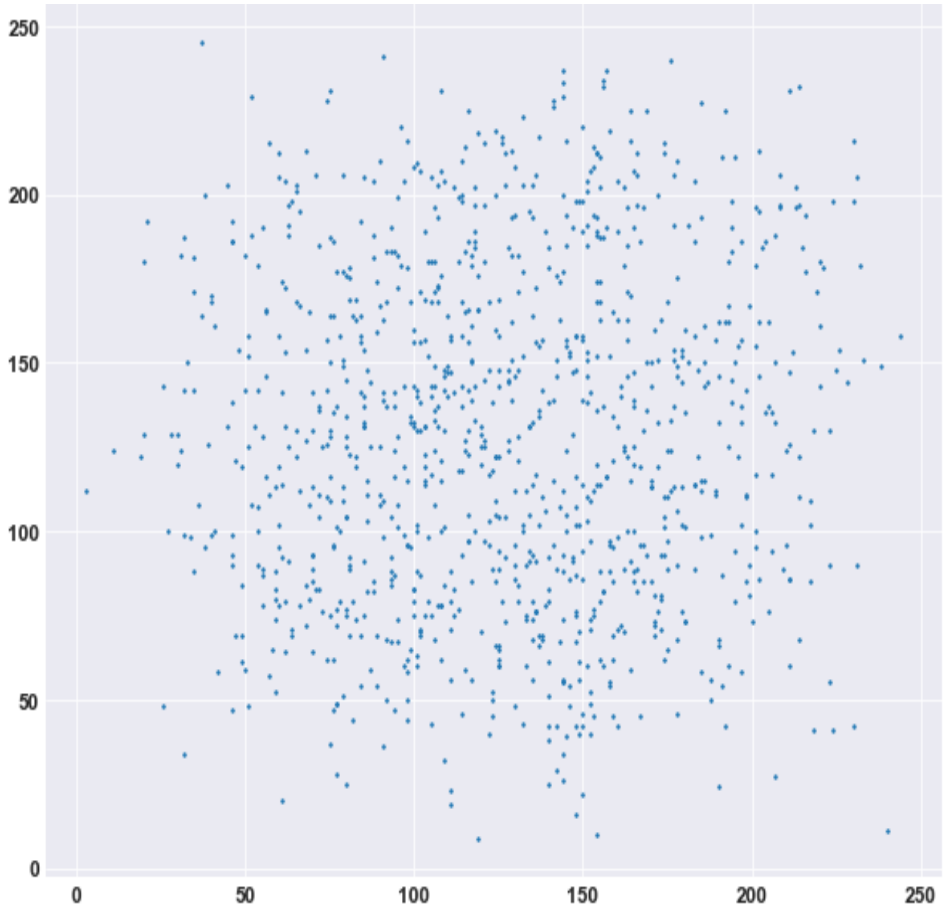

Figure 8.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two random keys respectively. The two encrypted images are very different from each other, with 99.61% pixel values being different. Thus, it has high key sensitivity.

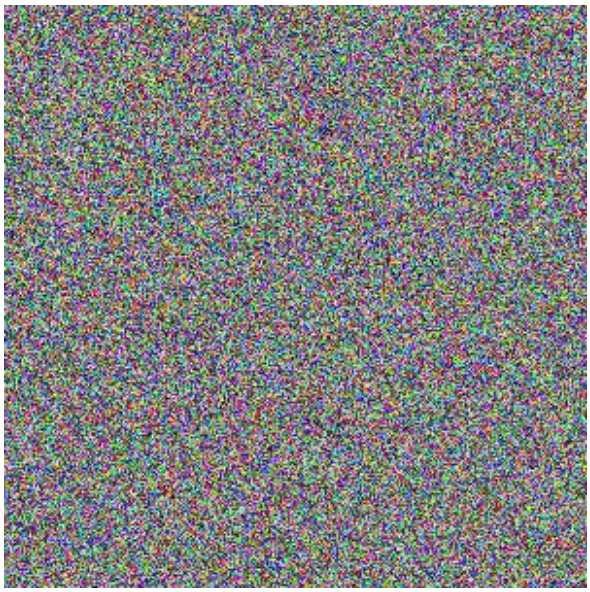

Figure 8.5.1: Encrypted Image with a random key

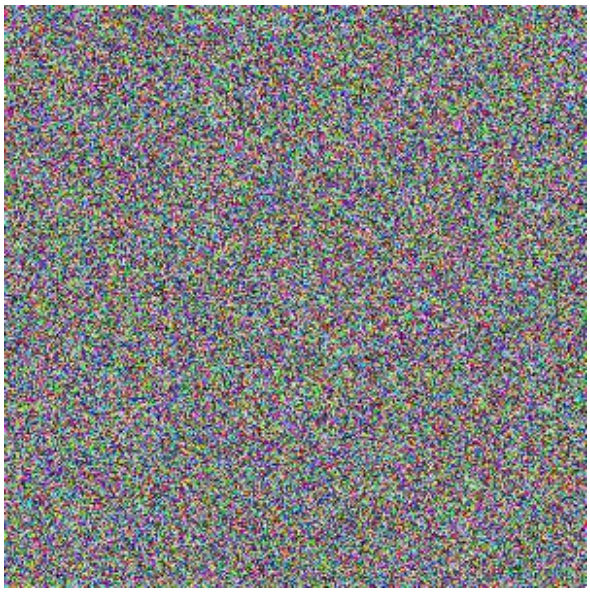

Figure 8.5.2: Encrypted Image with a random key

5. Advanced Encryption Standard (AES)

Figure 9.1 represents encrypted image and Figure 9.2 represents decrypted image.

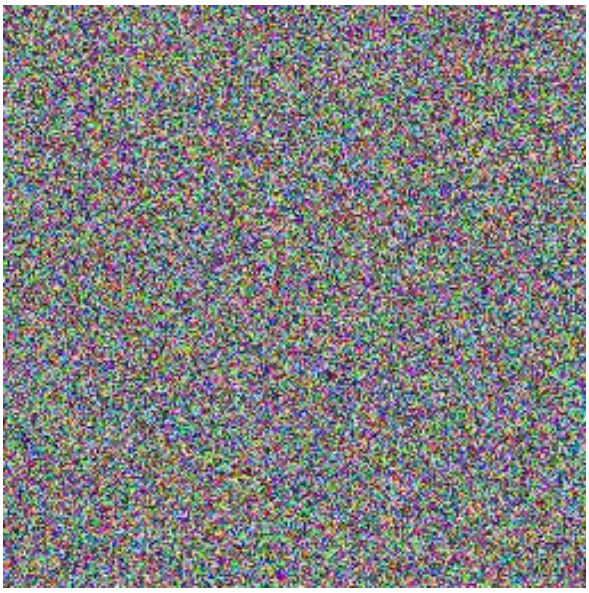

Figure 9.1: Encrypted Image

Figure 9.2: Decrypted Image

Figure 9.3 represents the Intensity Histogram of Encrypted Image obtained from AES Algorithm. It is more uniformly distributed over the range of pixel values as compared to that of Input Image. Large number of spikes of high pixel count is observed in Red and Blue color channels of the Encrypted Image.

The Encrypted Image contains entirely different pixel values as that in Input Image. The Pixel Count varies from 205 to 315 pixels. Average Pixel Count comes out to be 255 pixels as compared to 350 pixels obtained using Hill Cipher. The strength of encryption obtained is high since the Intensity Distribution Score is relatively low (16.0745).

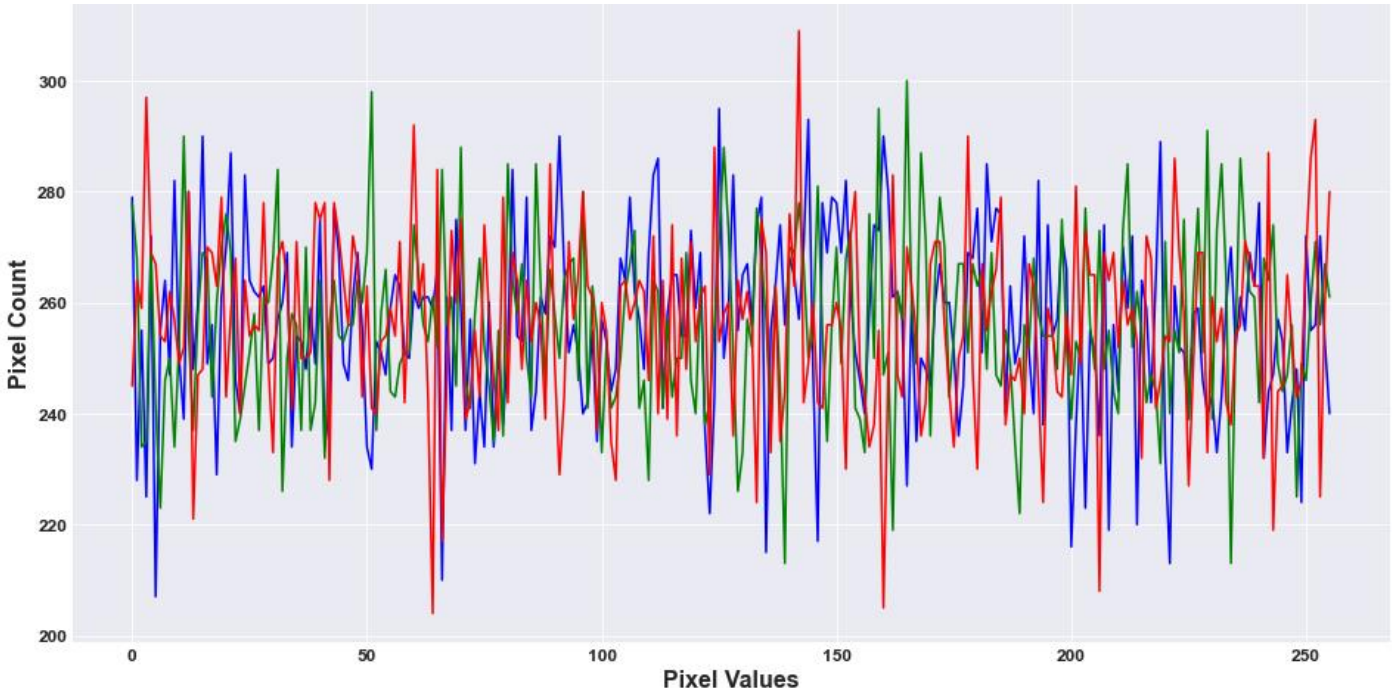

Figure 9.3: Intensity Histogram of Encrypted Image

Figure 9.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is almost uncorrelated and has a correlation coefficient of 0.0054.

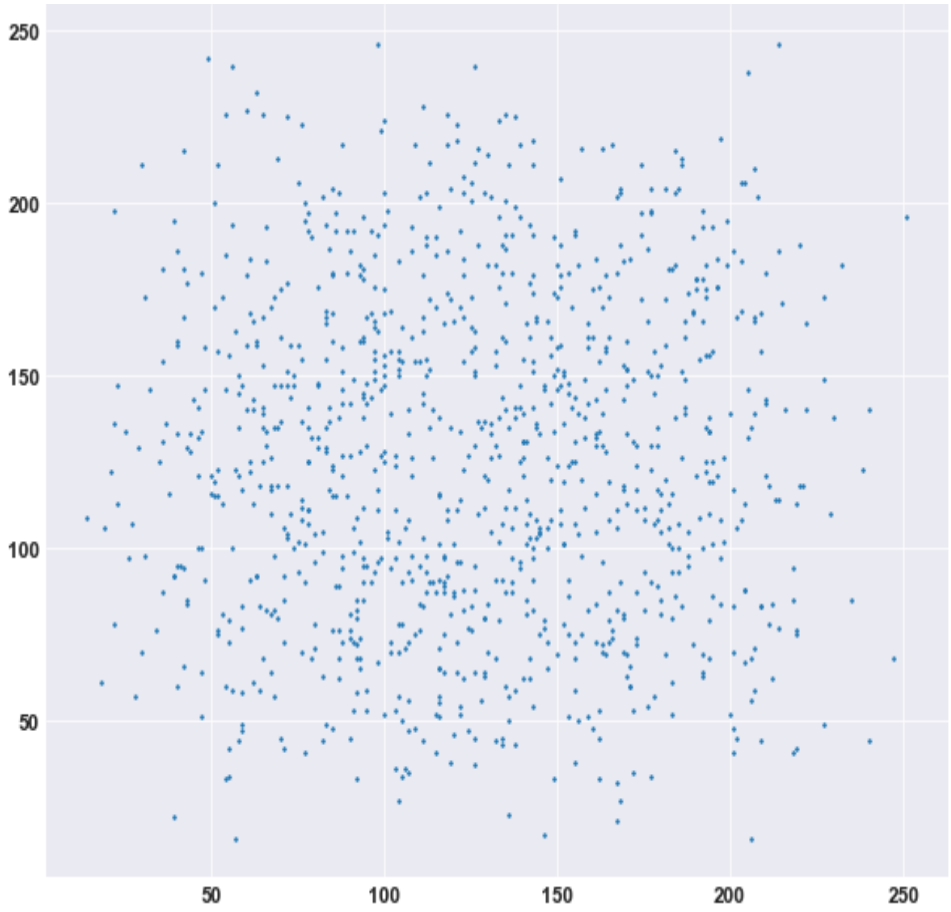

Figure 9.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two random keys respectively. The two encrypted images are very different from each other, with 99.57% pixel values being different. Thus, it has high key sensitivity.

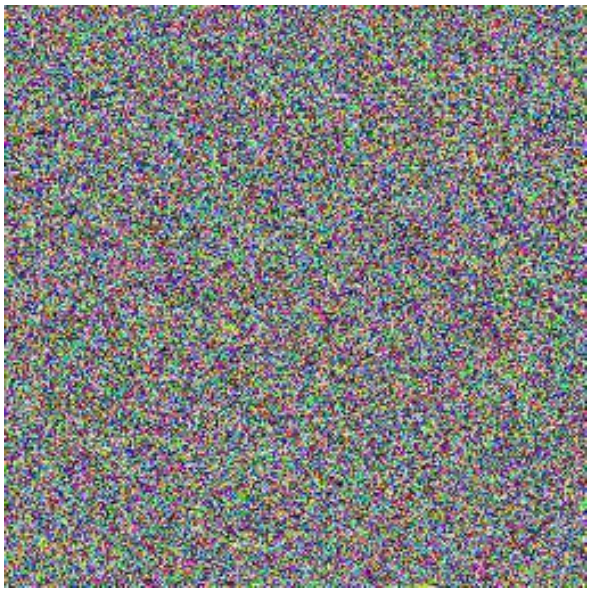

Figure 9.5.1: Encrypted Image with a random key

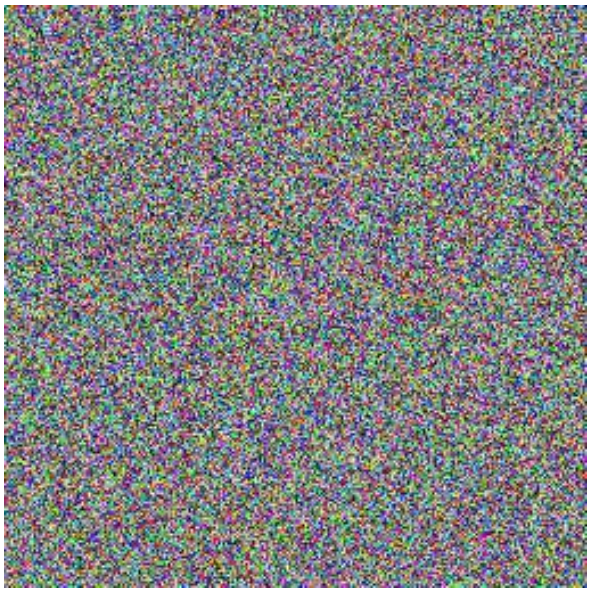

Figure 9.5.2: Encrypted Image with a random key

6. Rubik's Cube Image Encryption

Figure 10.1 represents encrypted image and Figure 10.2 represents decrypted image.

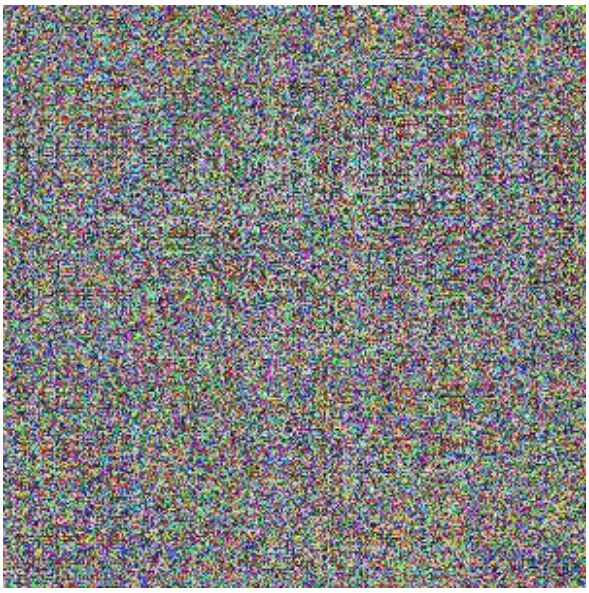

Figure 10.1: Encrypted Image

Figure 10.2: Decrypted Image

Figure 10.3 represents the Intensity Histogram of Encrypted Image obtained from Rubik's Cube Image Encryption Algorithm. It is more uniformly distributed over the range of pixel values as compared to that of Input Image. Large number of spikes of high pixel count is observed in all color channels of the Encrypted Image.

The Encrypted Image contains entirely different pixel values as that in Input Image. The Pixel Count varies from 295 to 415 pixels. Average Pixel Count comes out to be 345 pixels. The strength of encryption obtained is high since the Intensity Distribution Score is relatively low (19.2337).

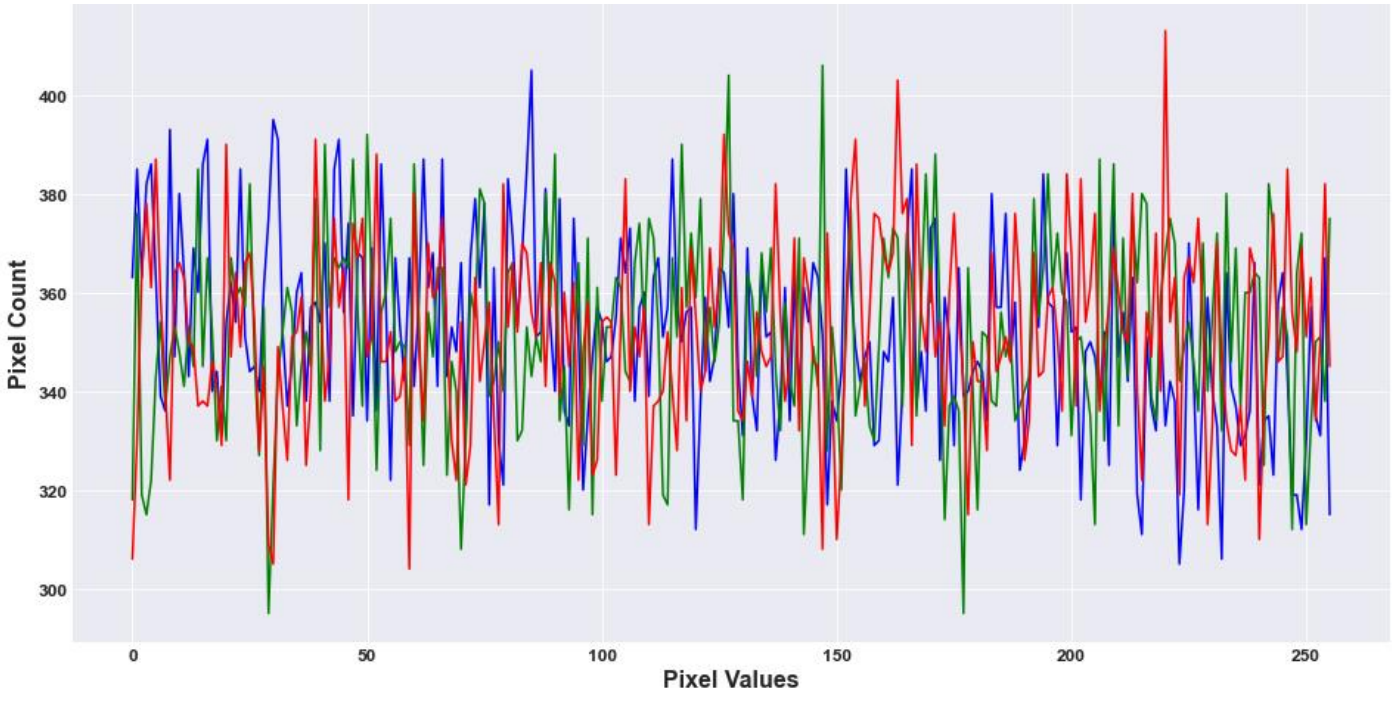

Figure 10.3: Intensity Histogram of Encrypted Image

Figure 10.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is almost uncorrelated and has a correlation coefficient of 0.0042.

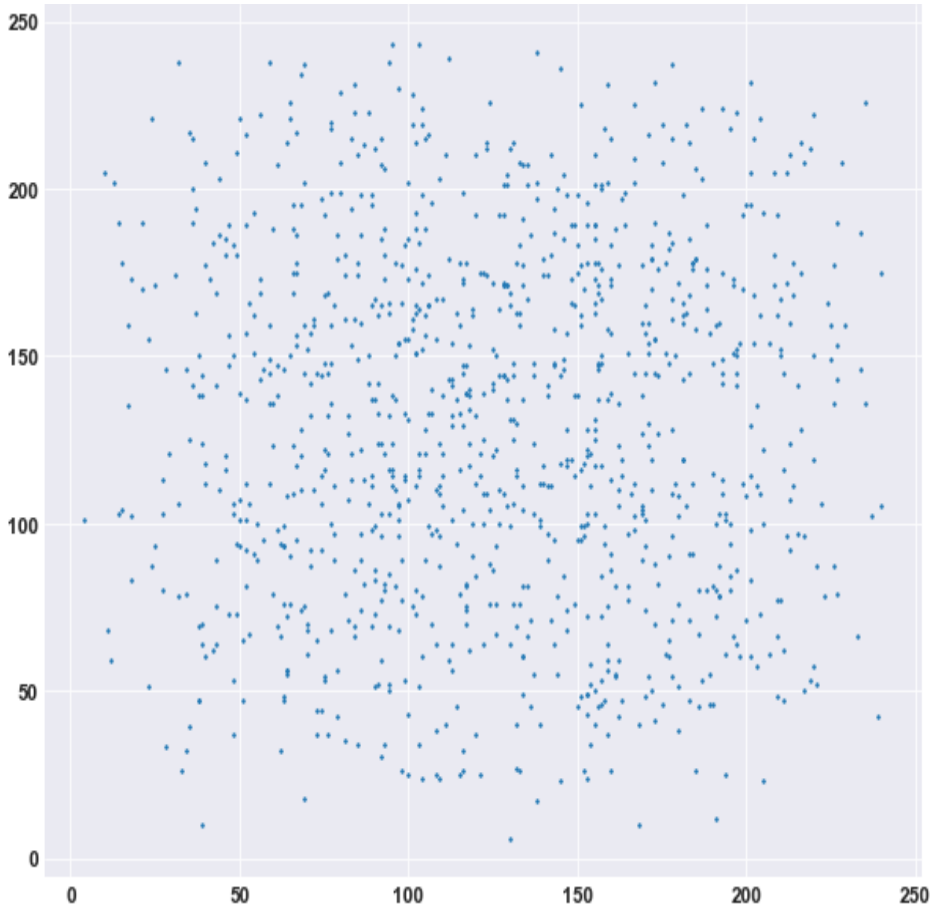

Figure 10.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two random keys respectively. The two encrypted images are very different from each other, with 99.60% pixel values being different. Thus, it has high key sensitivity.

Figure 10.5.1: Encrypted Image with a random key

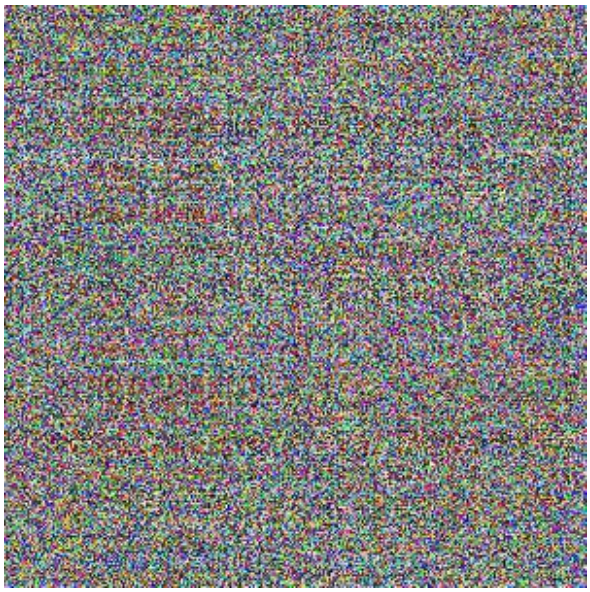

Figure 10.5.2: Encrypted Image with a random key

7. DNA Based Image Encryption

Figure 11.1 represents encrypted image and Figure 11.2 represents decrypted image.

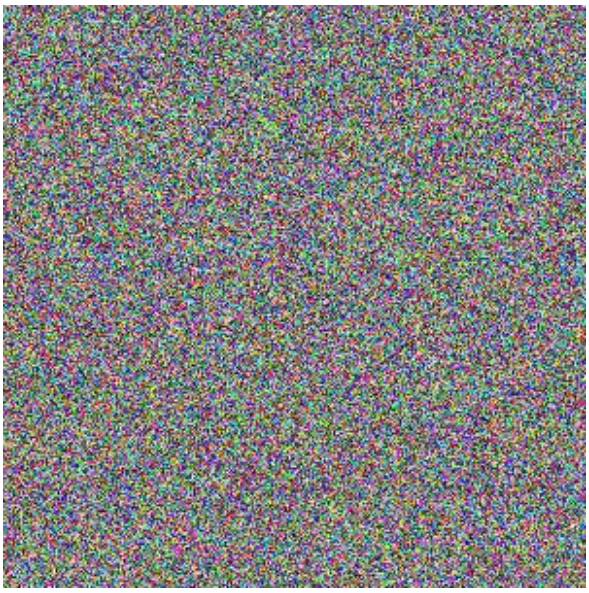

Figure 11.1: Encrypted Image

Figure 11.2: Decrypted Image

Figure 11.3 represents the Intensity Histogram of Encrypted Image obtained from DNA Based Image Encryption Algorithm. It is more uniformly distributed over the range of pixel values as compared to that of Input Image. Large number of spikes of high pixel count is observed in Green color channel of the Encrypted Image. Red and Blue color channels highly overlap each other.

The Encrypted Image contains entirely different pixel values as that in Input Image. Average Pixel Count comes out to be 350 pixels. The strength of encryption obtained is above average since the Intensity Distribution Score is relatively low (27.7349).

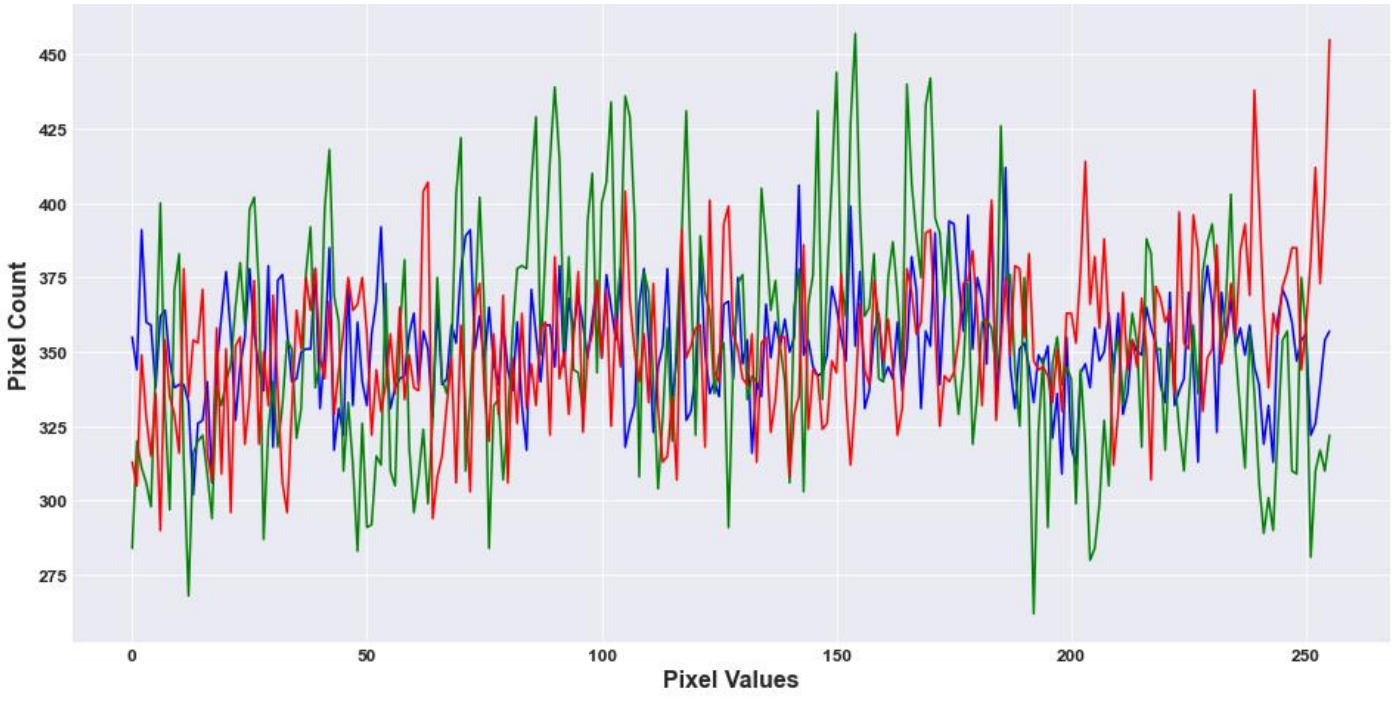

Figure 11.3: Intensity Histogram of Encrypted Image

Figure 11.4 represents the Adjacent Pixel Auto-Correlation Map of Encrypted Image. The image is highly uncorrelated and has a correlation coefficient of 0.0421.

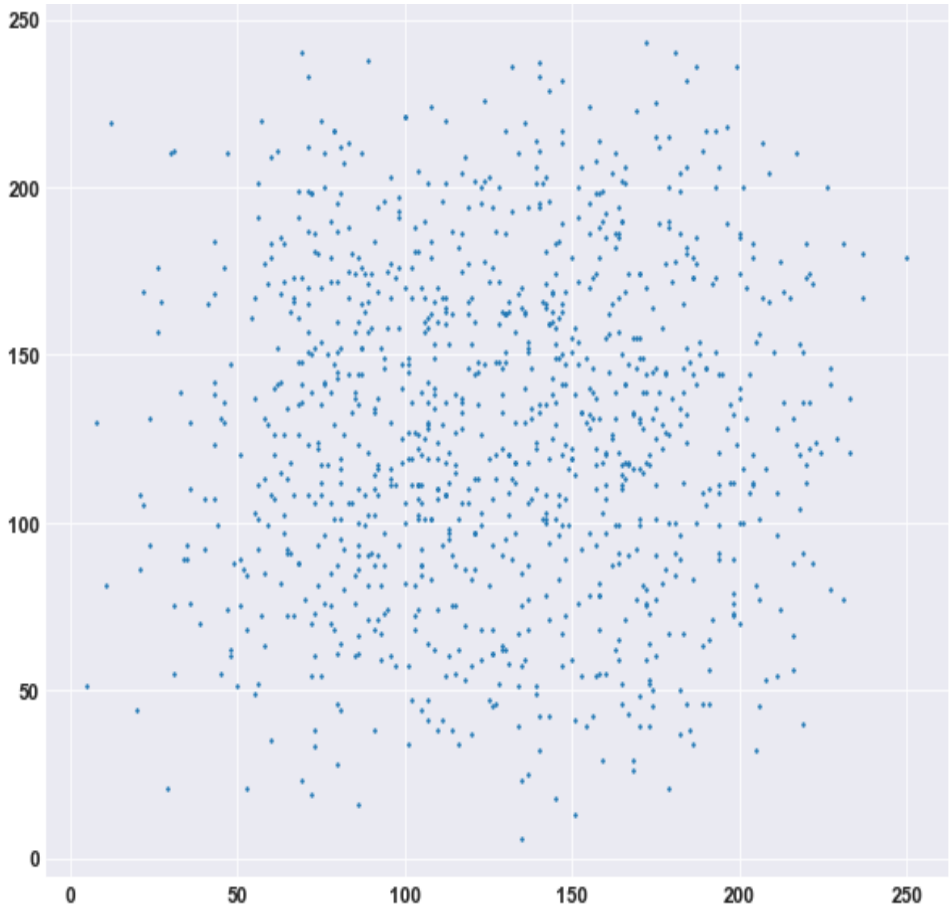

Figure 11.4: Adjacent Pixel Auto-Correlation Map of Encrypted Image

Figures below show encryption of Input Image with two random keys respectively. The two encrypted images are very different from each other, with 99.54% pixel values being different. Thus, it has high key sensitivity.

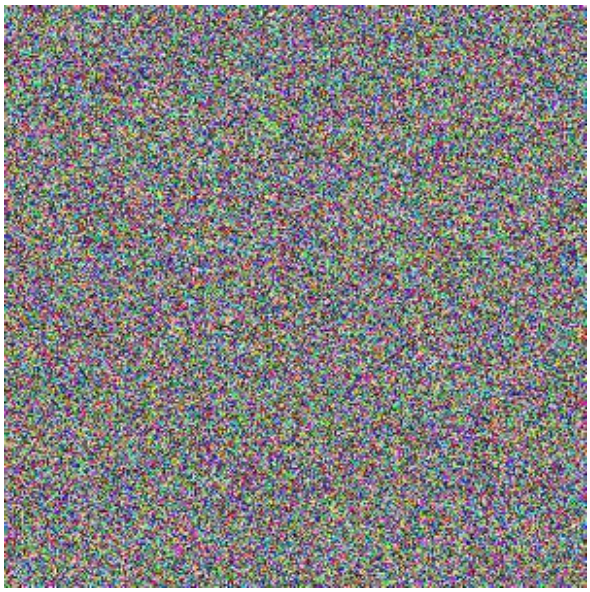

Figure 11.5.1: Encrypted Image with a random key

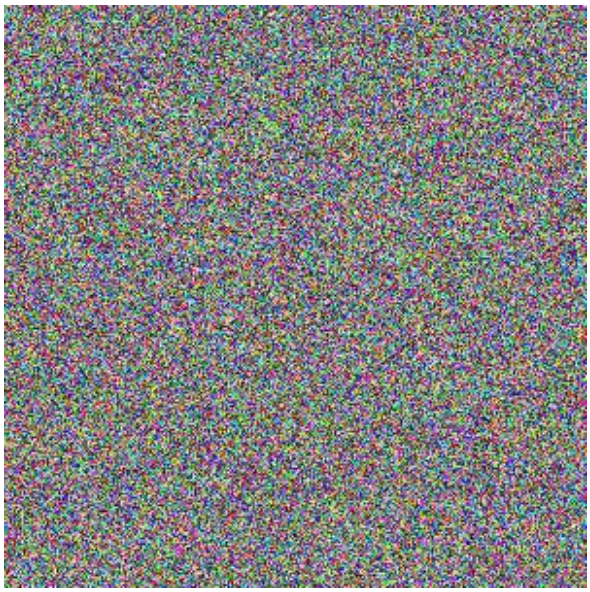

Figure 11.5.2: Encrypted Image with a random key

COMPARATIVE RESULTS

The comparative results of all Image Encryption Algorithms are provided in the below table. The comparative study is done on the basis of characteristics mentioned in approach section. Each algorithm has been allotted scores out of 5 based on the performance in each of the characteristics. Thus, total score of each algorithm is calculated out of 25 as the sum of its scores in different characteristics.

Algorithm	Intensity Distribution (Histogram Analysis)	Adjacent Pixel Auto-Correlation	Key Sensitivity	Run Time	Decrypted Image Quality	Total Score
Arnold Cat Map	1/5	1/5	4/5	1/5	4/5	**11/25**
Henon Map	2/5	5/5	2/5	4/5	3/5	**16/25**
Logistic Map	4/5	4/5	4/5	4/5	5/5	**21/25**
Hill Cipher	4/5	3/5	4/5	5/5	3/5	**19/25**
AES	5/5	5/5	4/5	3/5	2/5	**19/25**
Rubik's Cube	4/5	5/5	4/5	3/5	4/5	**20/25**
DNA Based	3/5	3/5	4/5	2/5	3/5	**15/25**

Observations:

- Based on the comparison table, it is observed that Logistic Map Image Cryptography Algorithm achieves the maximum score i.e., 21 out of 25. It performs well in all the characteristics used for comparison. It also gives highest quality of decrypted image.
- Rubik's Cube Image Encryption, Hill Cipher Encryption and AES algorithms achieve a similar score. Hill Cipher and AES algorithms fails to retain the quality in the decrypted image whereas Rubik's Cube Algorithm takes more time to complete the encryption and decryption process.
- Henon Map Encryption and DNA Based Image Encryption algorithms perform relatively poor in the comparative study. Henon Map Encryption Algorithm has poor Intensity Distribution and Key Sensitivity whereas DNA Based Image Encryption Algorithm is computationally expensive. Arnold Cat Map performs the worst out of all algorithms and thus, achieves a low score of 11 out of 25.

CONCLUSION

Visual Cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image. Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different processes. Therefore, the security of image data from unauthorized access is important. Image encryption plays an important role in the field of information hiding. Image encryption method prepares information that is unreadable.

In this project, following Image Cryptography Algorithms have been studied and compared:

- Chaos Map based Image Cryptography:
  - Arnold Cat Map Encryption
  - Hénon Map Encryption
  - Logistic Map Encryption
- Hill Cipher Encryption
- Advanced Encryption Standard (AES)
- Rubik's Cube Image Encryption
- DNA Based Image Encryption

The comparison among algorithms is carried out based on their performance in following characteristics:

- Intensity Distribution (Histogram Analysis) of encrypted image
- Adjacent Pixel Auto-Correlation of encrypted image
- Key Sensitivity
- Algorithm Run Time
- Decrypted Image Quality

Based on the comparative study, it is observed that Logistic Map Image Cryptography Algorithm achieves the maximum score i.e., 21 out of 25. It performs well in all the characteristics used for comparison. It is followed by Rubik's Cube, Hill Cipher and AES algorithms. Henon Map, DNA Based Image Encryption, Arnold Cat Map Encryption algorithms perform relatively poor.

REFERENCES

- https://en.wikipedia.org/wiki/List_of_chaotic_maps
- http://fibonacci.math.uri.edu/~kulenm/diffeqaturi/victor442/index.html
- https://geoffboeing.com/2015/03/chaos-theory-logistic-map/
- https://scialert.net/fulltext/?doi=jai.2014.123.135
- https://www.jigsawacademy.com/blogs/cyber-security/hill-cipher/
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- https://www.hindawi.com/journals/jece/2012/173931/
- https://www.sciencedirect.com/science/article/pii/S0895717710002761