Non Adaptive Partial Image Encryption

BRSNC - UG
Department of computer science
Suvasish Das . Samrat Mitra . Sayantan Das
Under supervision of Dr. Sukalyan Som

BARRACKPORE RASTRAGURU SURENDRANATH COLLEGE

- Department of Computer Science
- Presentation for **CMSACOR06P** on
- **Non adaptive Partial Image encryption**
- Supervised by **Dr. Sukalyan Som**

Suvasish Das

Roll: 6221103 02829

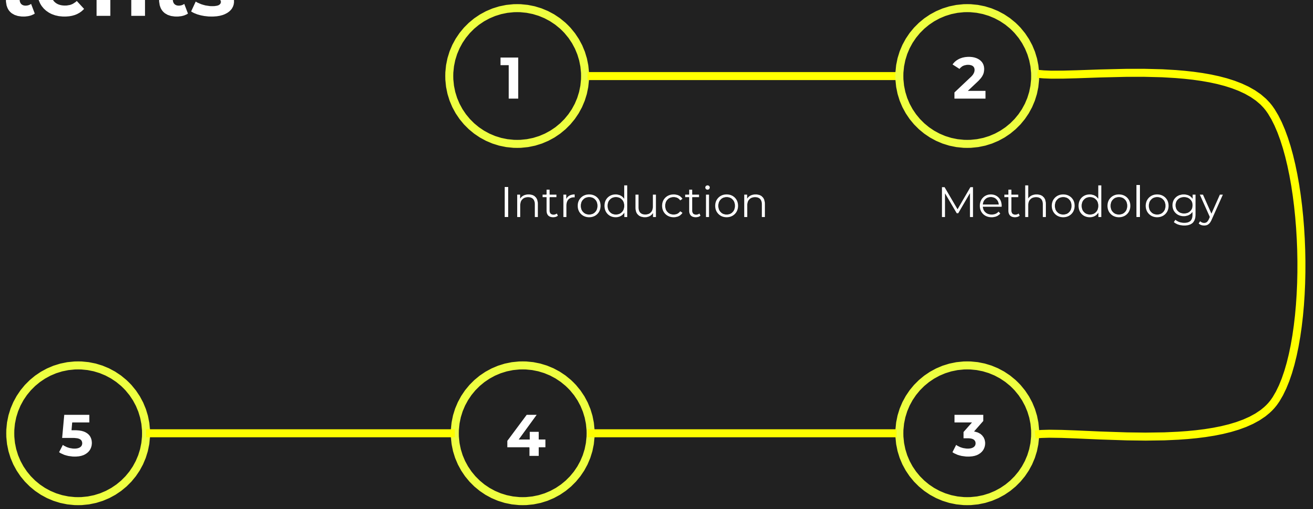
Samrat Mitra

Roll: 6221103 02812

Sayantan Das

Roll: 6221103 02810

Table of Contents



1 Introduction

2 Methodology

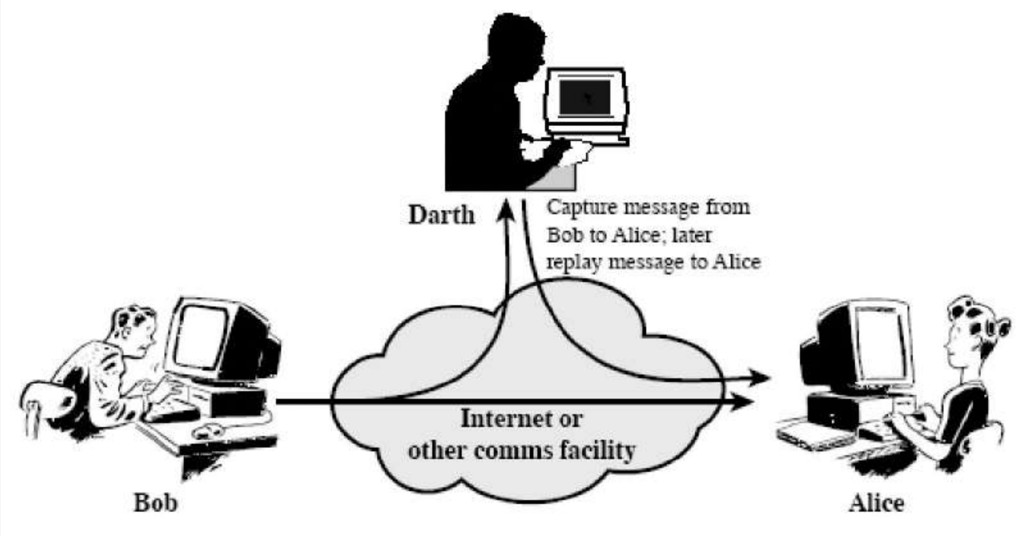
3 Visualization

4 Analysis

5 Conclusions

Introduction

Why Encryption is needed?


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

- Encryption can protect us from unauthorised access of our data
- Encryption increases the integrity of our data
- Encryption is cheap to implement
- Encryption increases the consumer’s trust

Objective

To develop,

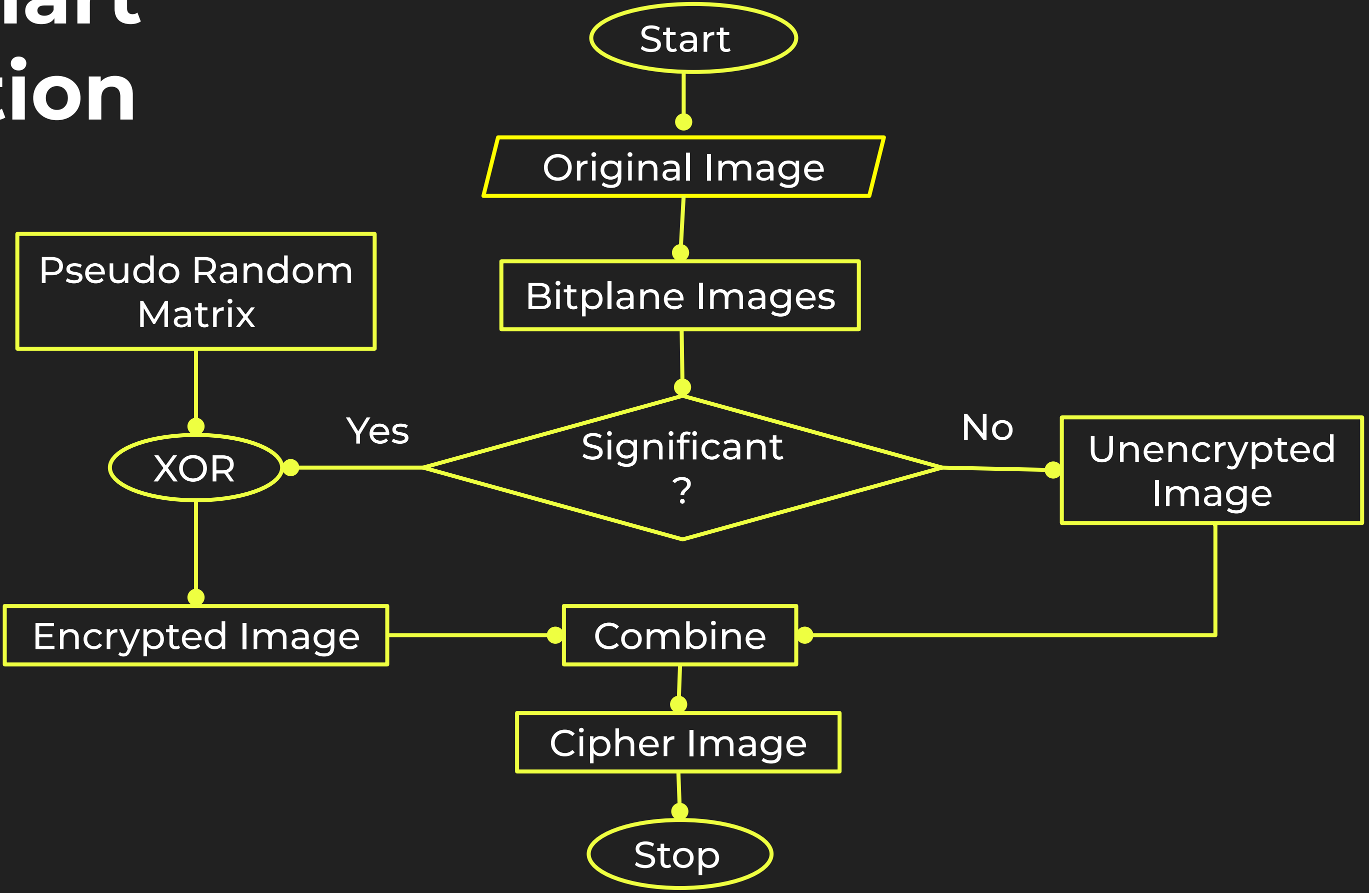
- A **non- adaptive partial image encryption** schemes based on chaos.

- Transmit through public network, and **restore the data**.

- Techniques to evaluate the **quality of encrypted image**.

Methodology

Flow Chart Illustration



How does this works ?

- An original image is first decomposed into its 8 binary bit planes among which the significant ones are non-adaptively determined.

- The significant bitplanes are encrypted with the key stream generated by a ‘***Pseudo Random Binary Bit Generator***’ and then combined with the unencrypted ones to form the cipher image.

- Performance of the technique is verified by tests based on image statistics Key sensitive and impermeability of cipher image.

- Noise generated by some asymptotic disturbance, reduced upto 95% using degradation models.

Pseudo Random Binary Number Generator

- The chaos based pseudo random binary number generator generate a single random bit by using previous random generated bit.

- By using the system parameter α and initial values of x_i and y_i we determine the next value of the sequence as –

$$x_{i+1} = f_1(\alpha, x_i)$$

$$y_{i+1} = f_2(a, y_i)$$

- The bit sequence g(x_{i+1} + y_{i+1}) is generated as follows –

$$g(x_{i+1}, y_{i+1}) = \begin{cases} 0 & \text{if} \quad x_{i+1} < y_{i+1} \\ 1 & \text{otherwise} \end{cases}$$

Method of Encryption

- Decompose the original image into bitplane images
- Determine the significant bitplane
- For each significant bitplane
    - Generate an pseudo random binary matrix using logistic map
    - Perform XOR operation with significant bitplane
- Combine the cipher bitplanes and unencrypted bitplanes to generate the cipher image.

Method of Decryption

- Get the key values
- Decompose the cipher image into bitplane images
- Determine the significant bitplanes from the key values
- For each significant bitplane
    - Generate an pseudo random binary matrix using logistic map
    - Perform XOR operation with significant bitplane
- Combine all the bitplanes to decrypt the cipher image.

Method of Noise Reduction

For an M X N image we need to perform median filter for each pixel of the image. The method of noise reduction can be described as –

For each pixel of the image:

- Get 8 neighbour of each pixels
- Determine the median value of the 3 X 3 matrix
- Replace the median value with the central pixel
- Combine all the bitplanes to decrypt the cipher image.

Visualization

Test Image

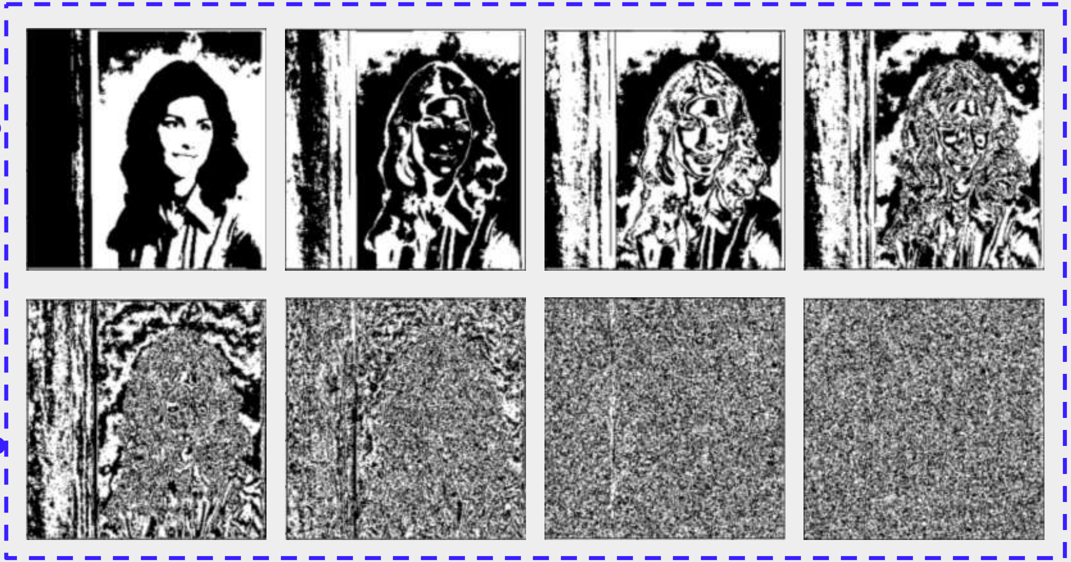
Consider the plain image to be original (x,y) of size M × N where x = 0,1,2, ..., M - 1, And y = 0,1,2, ..., N-1.

- Test Image Name: “Lena”
- Size: 512 x 512
- Type: Miscellaneous, Grayscale
- Format: Uint8

8 Bitplane Decomposition

Each pixel value P(x,y) in $I_{original}$ (x,y) is decomposed into its corresponding 8 bit binary equivalent and thus 8- planes BP(x,y) $\forall$ i = 1,2,...,8 are formed.

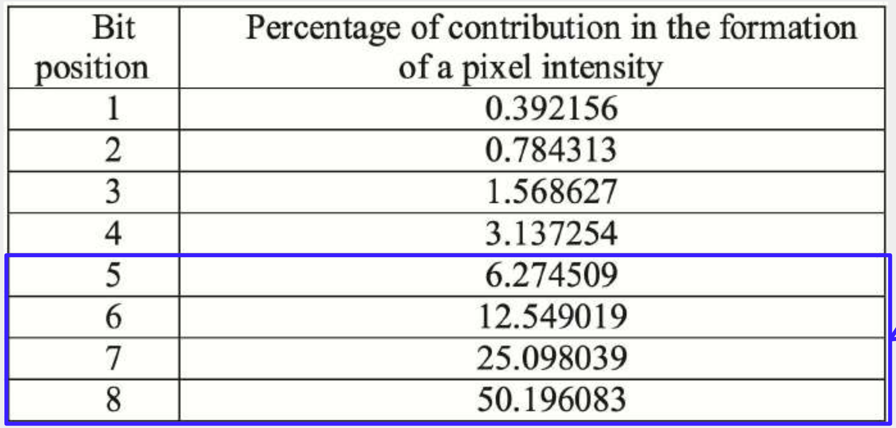
Original Image



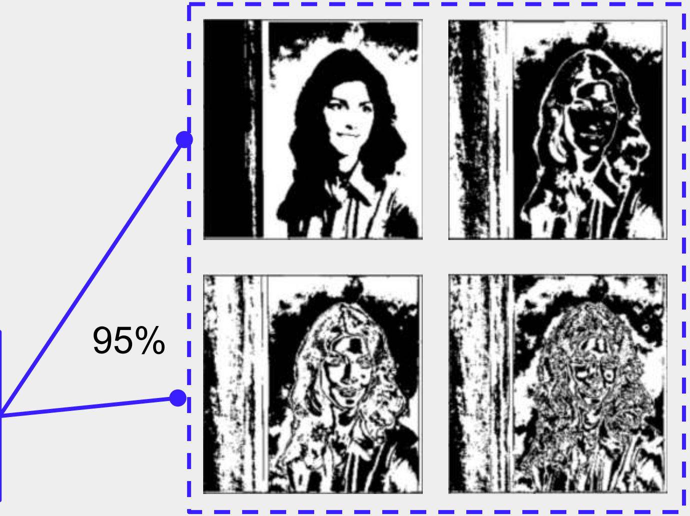
Bitplane Images

Significant Bitplanes Determination

Significant bit planes are determined by the level α critical region from the H_0: i^{th} bit-planes significant against the alternative hypothesis H_1: i^{th} bit-planes not significant where the test statistics is the percentage contribution of a bit plane in formation of a pixel.

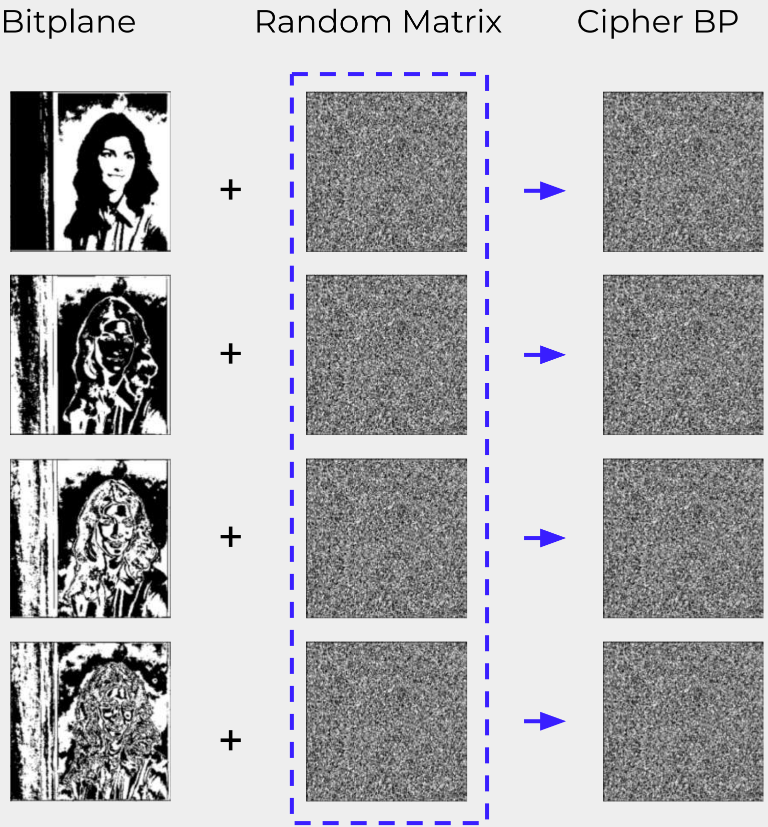


Bit position	Percentage of contribution in the formation of a pixel intensity
1	0.392156
2	0.784313
3	1.568627
4	3.137254
5	6.274509
6	12.549019
7	25.098039
8	50.196083



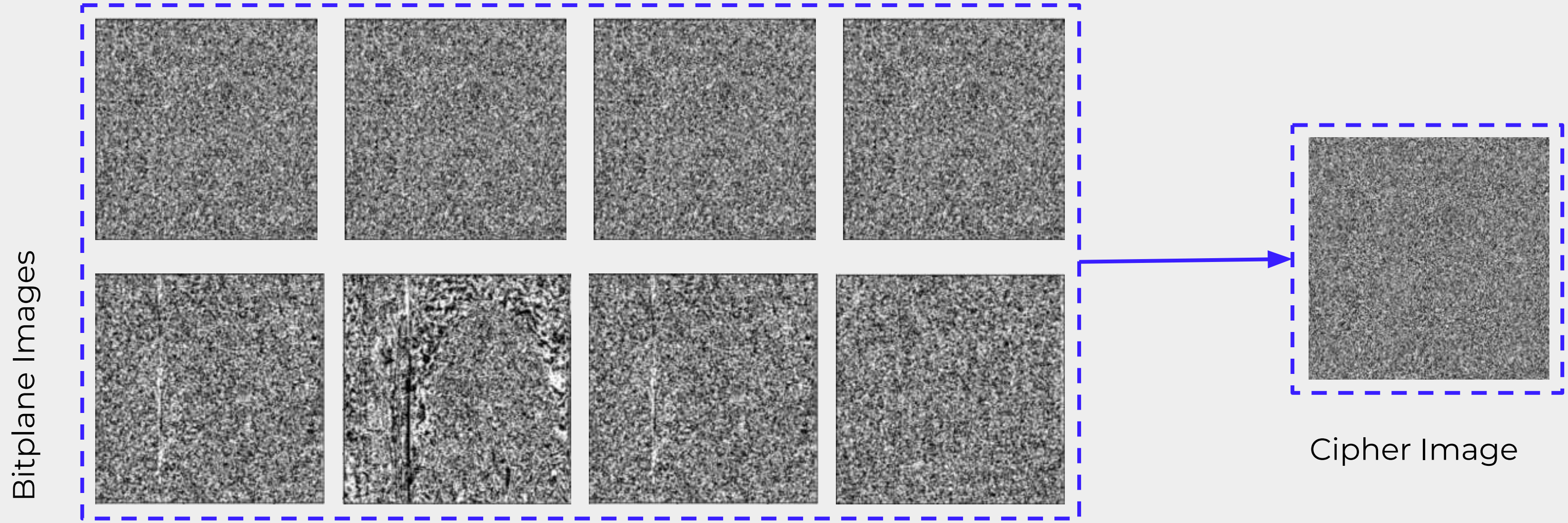
Cipher Bitplane Generation

The significant bit planes, determined by α% (0.05) level of significance, are ciphered as $CBP_j = BP_j \oplus K_j \ \forall \ j = 1,\ldots,4$.



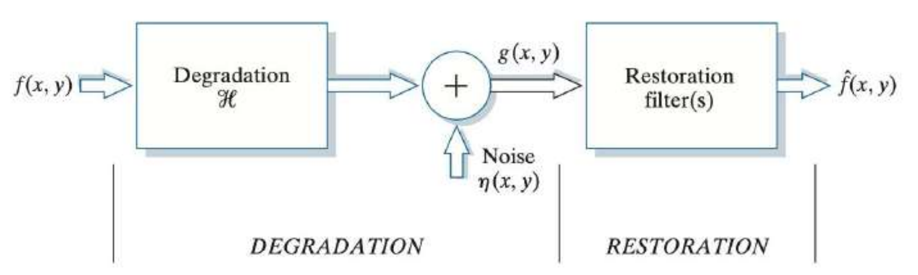
Cipher Image Composition

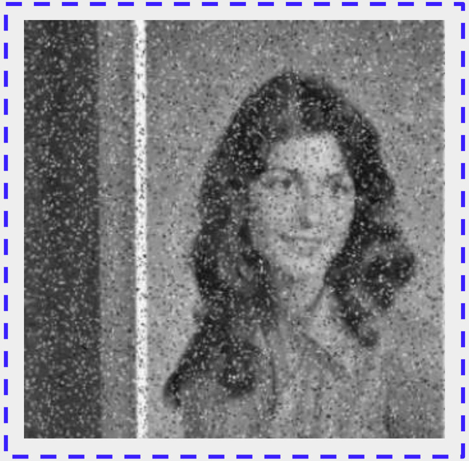
The cipher bit planes CBP_j and the encrypted bit plane BP_j are combined together to form cipher image as $C_i(x,y) = CBP_j + BP_k \forall i = 1,2...,8$, $j = 1,..4$ and $k = 5,...8$ where + is used for combining process.



Transmission Through Network

- when we transmit the data through some computer network, there is a high chance that the data gets distorted at some point due to some asymptotic disturbance.
- If the data gets distorted, then after decrypting the data, we get an image with noise added in it.

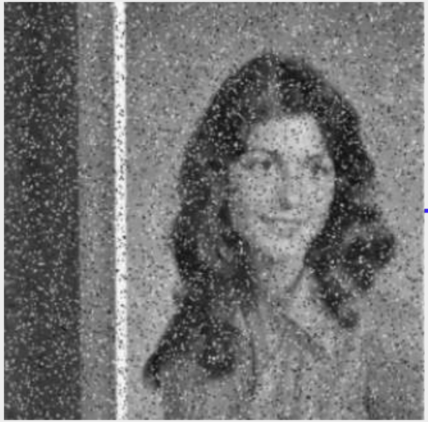




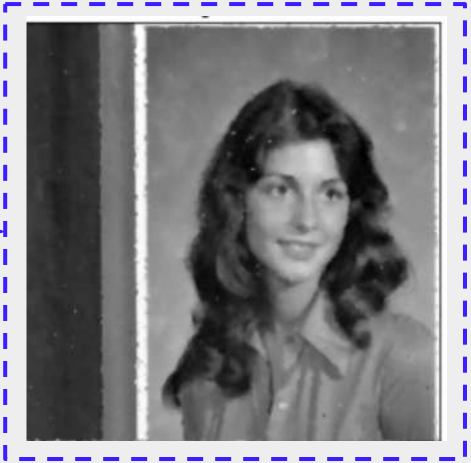
Decrypted Image with noise

Restoring Decrypted Image

To remove noise we use median filter which replaces the value of a pixel by the median of the intensity levels in a predefined neighborhood of that pixel as –
f'(x,y) = median { g(r,c) } where (r,c) ∈ Sx,y where, as before, Sx,y is a subimage (neighborhood) centered on point (x, y).



Decrypted Image with noise



Decrypted Image without noise

Analysis

Test Images

- Name: Lena
- Size: 512 x 512
- Type: Miscellaneous, Grayscale
- Format: Uint8

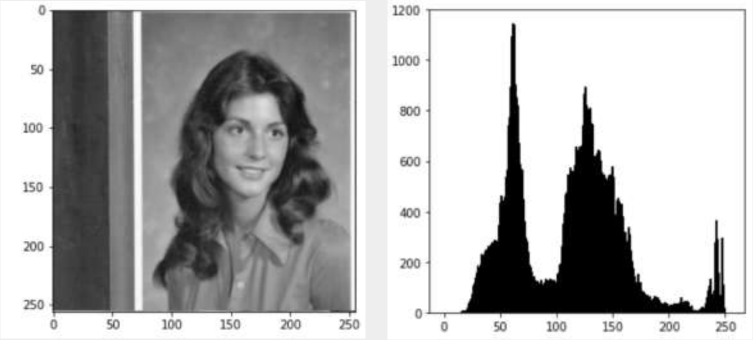
- Name: Baboon
- Size: 512 x 512
- Type: Miscellaneous, Grayscale
- Format: Uint8

- Name: Pappers
- Size: 512 x 512
- Type: Miscellaneous, Grayscale
- Format: Uint8

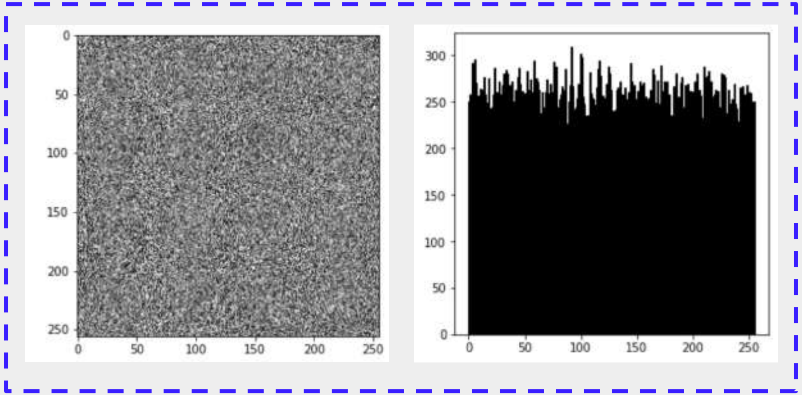
- Name: Map
- Size: 512 x 512
- Type: Aerials, Grayscale
- Format: Uint8

Histogram Analysis

- An image histogram demonstrates how pixels in an image are distributed by graphing the number of pixels at intensity level.
- In order to have a perfectly ciphered image the histogram of the image must exhibit uniformity of distribution of pixels against the intensity values.



Original

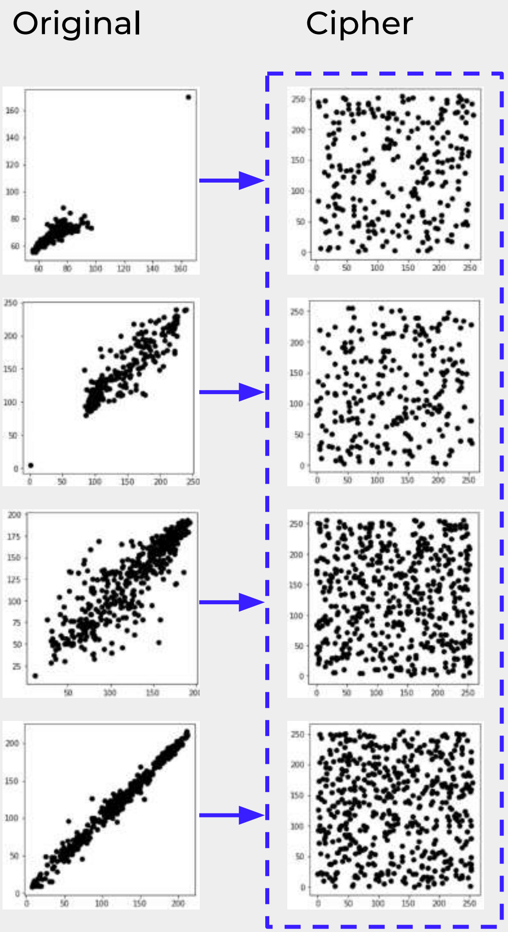


Cipher

Scatter Plot Analysis

- A scatter plot uses dots to represent values for two different numeric variables. The position of each dot on the horizontal and vertical axis indicates values for an individual data point.

- Scatter plot of original image residing in a particular region. But, in case of cipher image, the dots are distributed properly.



Measures of Central Tendency

- Measures of Central Tendency have been used as a measure of homogeneity.
- The measures in Cipher Images are uniform which shows that cipher images have uniform mean, median pixel intensities.

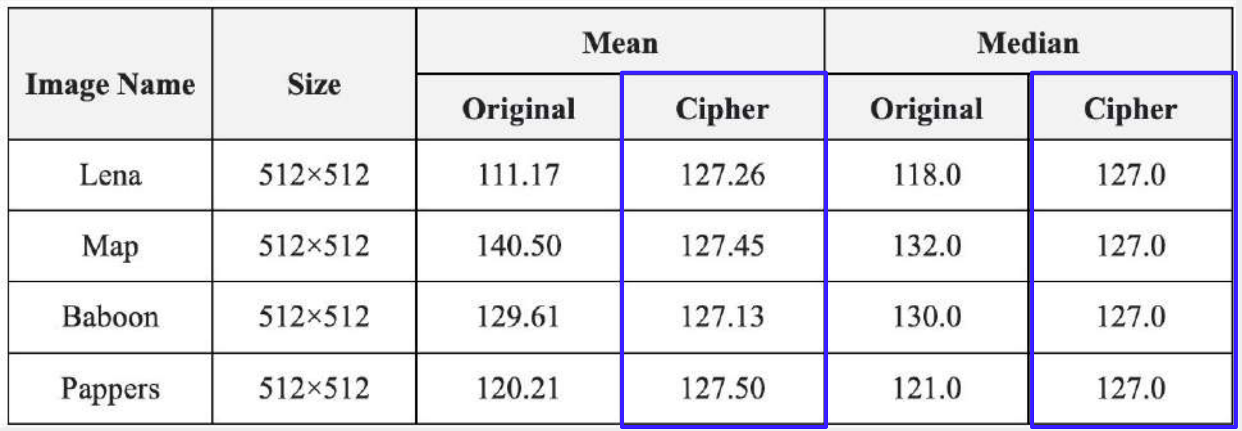


Image Name	Size	Mean		Median	
		Original	Cipher	Original	Cipher
Lena	512×512	111.17	127.26	118.0	127.0
Map	512×512	140.50	127.45	132.0	127.0
Baboon	512×512	129.61	127.13	130.0	127.0
Pappers	512×512	120.21	127.50	121.0	127.0

Measures of Dispersion

- It is a measure of spread of data about the mean.
- Standard deviation (SD) is the most commonly used measure of dispersion.

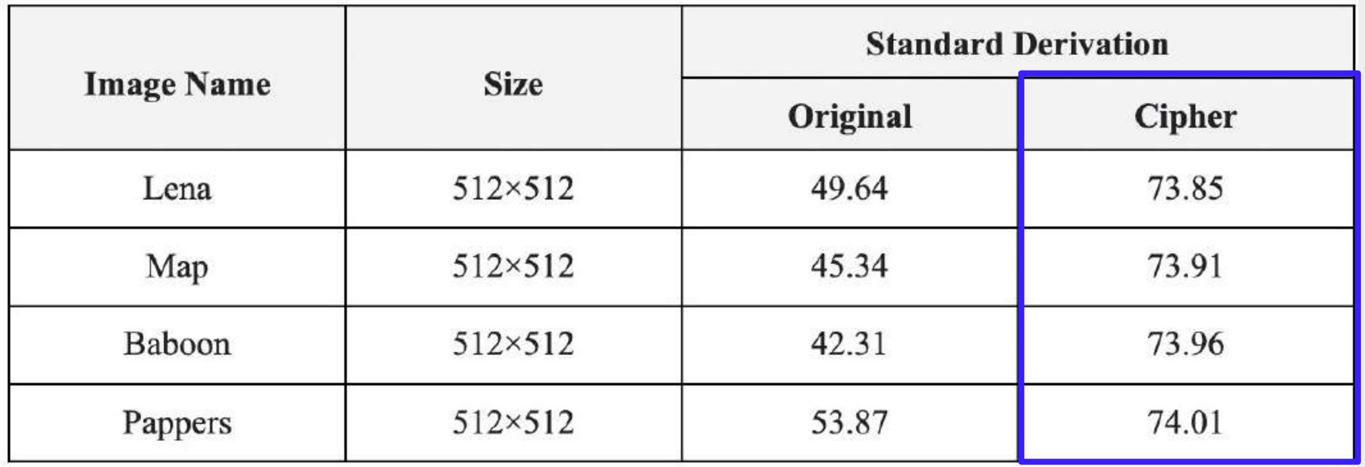


Image Name	Size	Standard Derivation	
		Original	Cipher
Lena	512×512	49.64	73.85
Map	512×512	45.34	73.91
Baboon	512×512	42.31	73.96
Pappers	512×512	53.87	74.01

Correlation Coefficient Analysis

In most of the plain images, there exists high correlation among adjacent pixels whereas poor correlation between the neighboring pixels of corresponding cipher image is observed. The formula used to get correlation coefficient is –

$$r_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} \text{where } cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})$$

$$\sigma_x = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2 \ and \ \sigma_y = \frac{1}{n}\sum_{i=1}^{n}(y_i - \bar{y})^2 \text{ with}\sigma_x \neq 0 \ and \ \sigma_y \neq 0$$

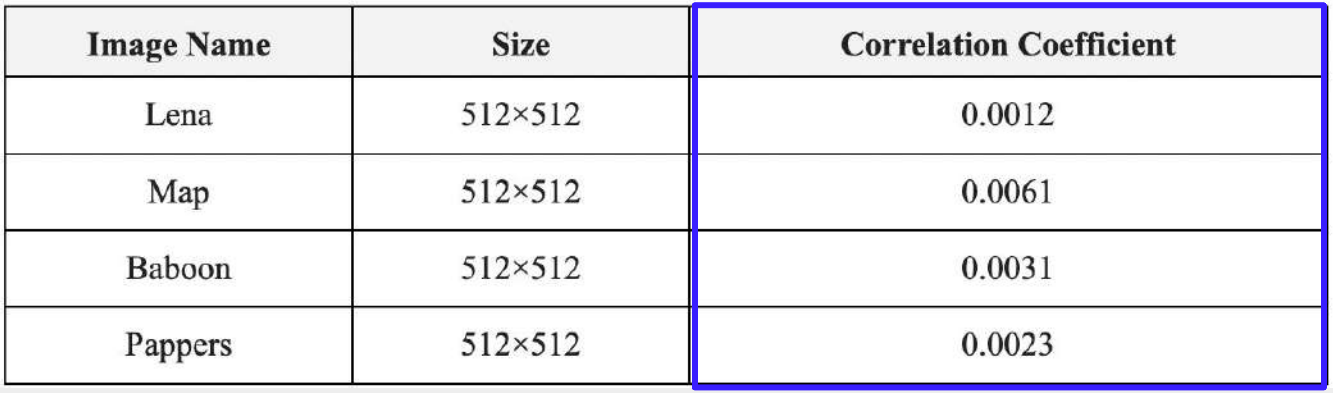


Image Name	Size	Correlation Coefficient
Lena	512×512	0.0012
Map	512×512	0.0061
Baboon	512×512	0.0031
Pappers	512×512	0.0023

Conclusions

Concluding Remarks

- Proposed scheme encrypts an image with efficiency which ensures the users privacy on their data.

- Pseudo random logistic map provide a superior security.

- A non-adaptive partial image encryption method is proposed, which saves 30% of computation by determining significant bit positions.

- A median filter degradation model used, which can reduce noise up to 95% to restore the original image.

Bibliography

1. Sukalyan Som, Sayani Sen, “**A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos**”, International Conference on Computational Intelligence: Modeling, Techniques and Applications, CIMTA-2013.
2. Narendra K Pareek, Vinod Patidar, Krishan K Sud, “**A Random Bit Generator Using Chaotic Maps**”, International Journal of Network Security, Vol.10, No.1, PP.32 (38, Jan. 2010).
3. **USC-SIPI Image Database**, USE-Viterbi school of engineering, University of South California, since 1981.
4. “**The Future of Encryption**”, by Richard Molds, published on Helpnetsecurity February 18, 2008.
5. Research Group VITS, Orebro University, Sweden, “**Information Security Fundamentals**”, 2003, Security Education and Critical Infrastructures, pp 95–107.
6. “**Cryptosystem**”, by Corinne Bernstein, June 2019, article published on Techtarget.

Thank You For Your Kind Attention