Presentation Title

Presentation Subtitle

Security Analysis of Encrypted Image

- Key Space Analysis
- Histogram Analysis
- Correlation Analysis
- Intensity Tampering Analysis

Key Space Analysis

Key spaces imply the total number of different keys which can be used for the purpose of encryption and decryption.

The algorithm proposed in the paper uses a 32 character, i.e., $32 \times 8 = 256$ bits key, so that the key space is 2^{256} , which is large enough to avoid brute-force attack according to the present computational speed.

Key Space Analysis (continued)

On the other hand the encryption and decryption algorithm is highly sensitive to the secret key.

Key Space Analysis

The change of a single bit in the secret key should produce a completely different encrypted/decrypted image. Two encrypted images using two different keys [zxcvbnmlkjhgfdsa1234567890!@#$%**x**] and [zxcvbnmlkjhgfdsa1234567890!@#$%**y**] (these two key have only one bit different) are more than 99% different in terms of pixel values.

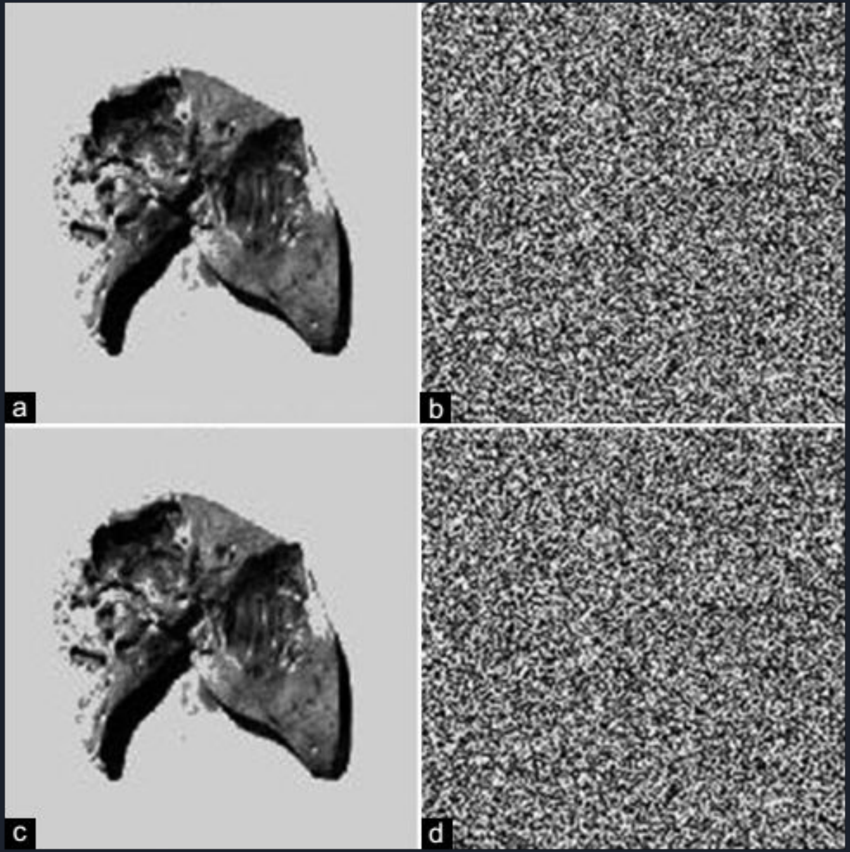


Figure
(a) Plane image
(b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%x
(c) Decrypted image using same key of encryption
(d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%y

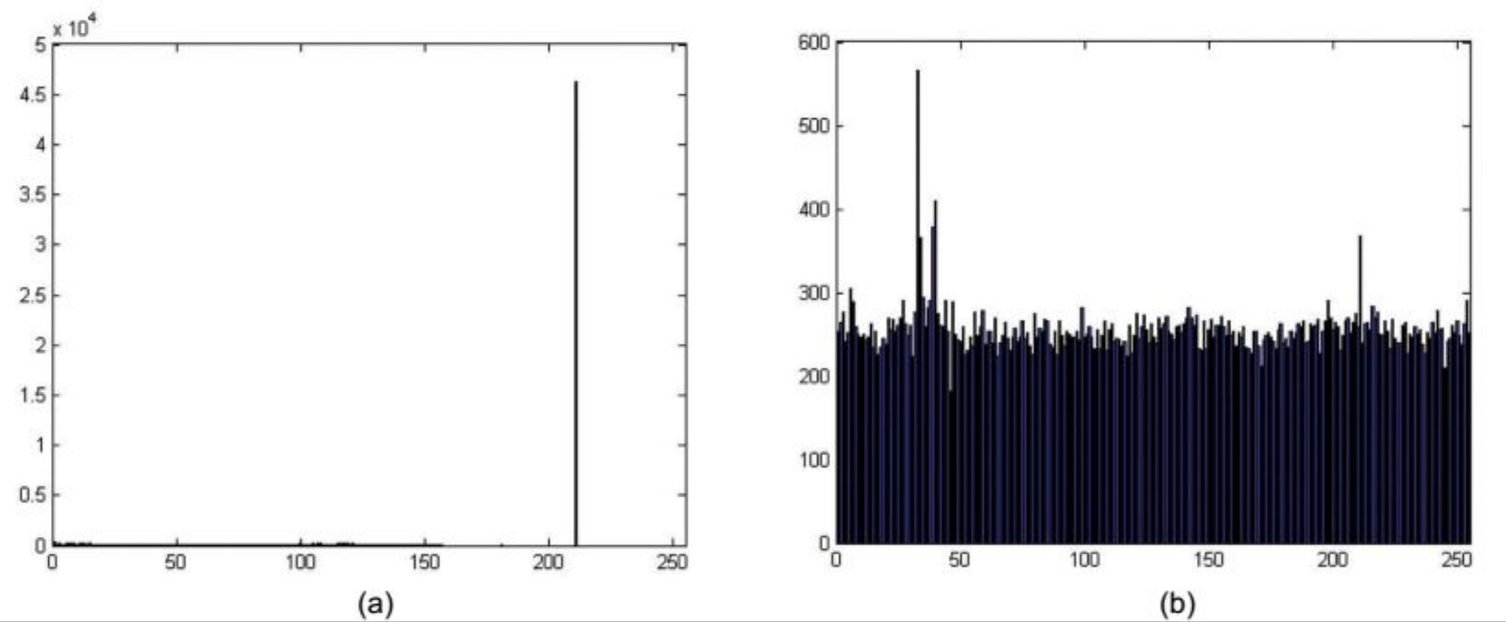
Ref : Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay & Debashis Nandi (2012) An Image Encryption Process based on Chaotic Logistic Map, IETE Technical Review, 29:5, 395-404

Histogram Analysis

Image histogram describes how the image pixels are distributed by plotting the number of pixels (along the y-axis) at each intensity level (along the x-axis)

A good image encryption system should provide uniform image histogram for all encrypted images irrespective the nature of the original plane image.

Histogram Analysis



Histogram of the (a) Plane image and (b) Encrypted image of liver.

Ref : Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay & Debashis Nandi (2012) An Image Encryption Process based on Chaotic Logistic Map, IETE Technical Review, 29:5, 395-404

Correlation Coefficient Analysis

Higher the correlation coefficient indicates high similarities between adjacent pixels and correlation coefficient decreases for adjacent pixels having different intensity.

In case of plane image each pixel is usually highly correlated with its adjacent pixels but for good encrypted image these correlations will be very small.

Correlation Coefficient Analysis (cont)

Higher the correlation coefficient indicates high similarities between adjacent pixels and correlation coefficient decreases for adjacent pixels having different intensity.

The correlation coefficient can be calculated by using the following formula

$$\rho = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Correlation Coefficient Analysis (cont)

To calculate the value of the following discrete formulas can be used

$$E(x) = \frac{1}{I}\sum_{i=1}^{I} x_i$$

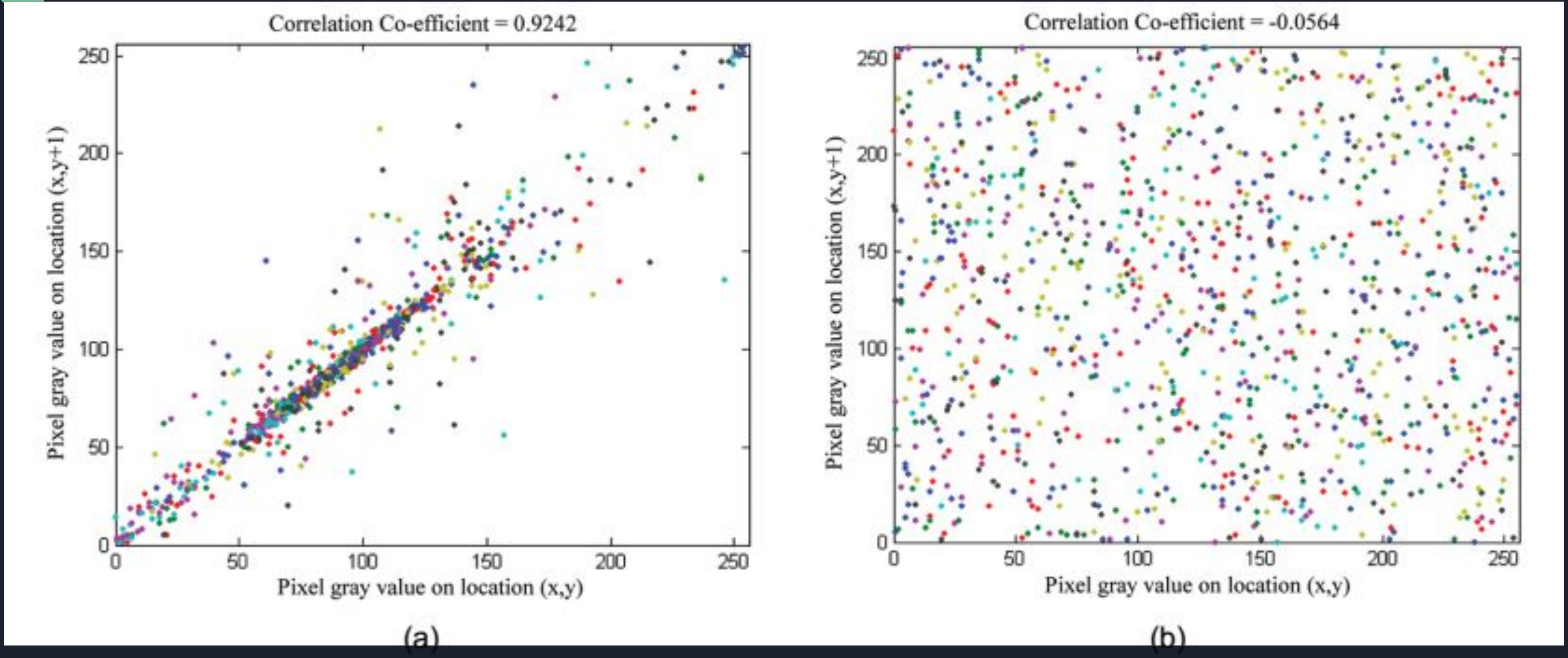
$$D(x) = \frac{1}{I}\sum_{i=1}^{I} \left(x_i - E(x)\right)^2$$

$$\operatorname{cov}(x,y) = \frac{1}{I}\sum_{i=1}^{I} \left(x_i - E(x)\right)\left(y_i - E(y)\right)$$

Where I is the number of pixel pairs selected

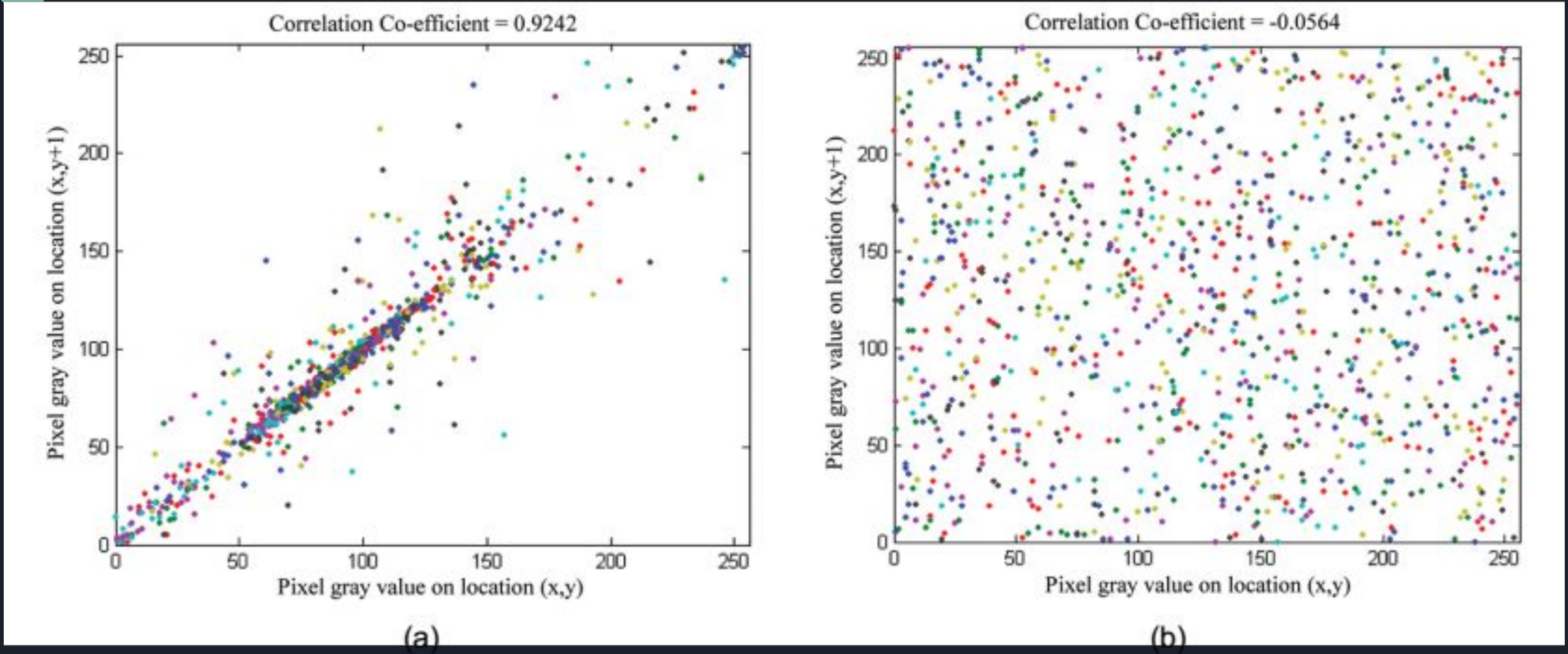
To calculate correlation coefficient first randomly selects 1000 or more pairs of two adjacent pixels from both the images (i) plane image and (ii) ciphered image.

Correlation Coefficient Analysis (cont)



The correlation analysis of two horizontally adjacent pixels of Lena (a) Plane image; (b) Encrypted image.

Correlation Coefficient Analysis (cont)



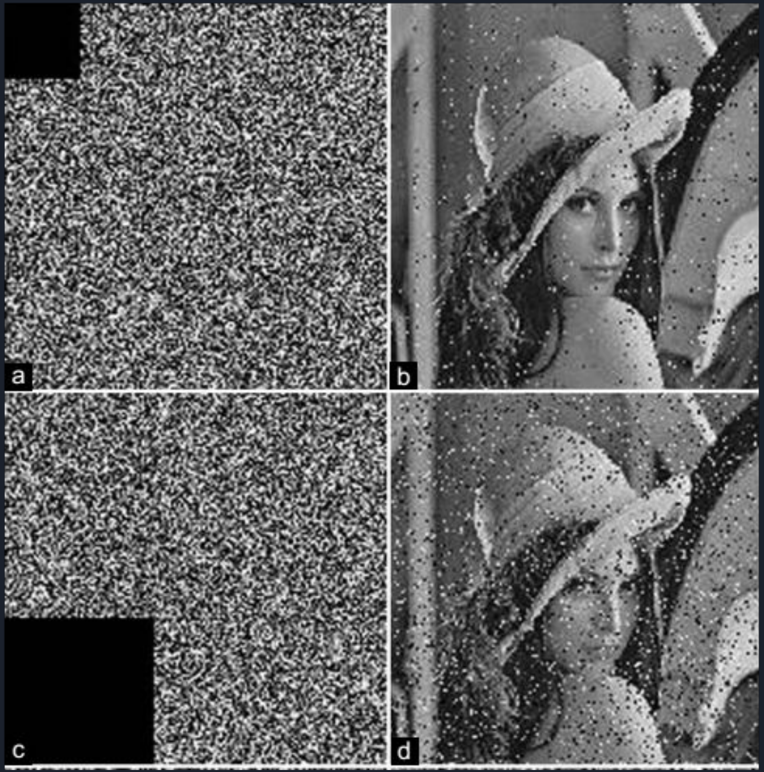
Ref : Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay & Debashis Nandi (2012) An Image Encryption Process based on Chaotic Logistic Map, IETE Technical Review, 29:5, 395-404

Intensity Tampering Analysis

The proposed image encryption/decryption algorithm can resist illegal tampering of the intensity of the encrypted image to a certain extent.

If an attacker modified the encrypted image intensity then the receiver will receive encrypted image with some distortion. So, this algorithm can resist illegal tampering to some extent.

Intensity Tampering Analysis (cont)



Illegal tampering of encrypted image and corresponding decrypted image

Ref : Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay &
Debashis Nandi (2012) An Image Encryption Process based on Chaotic Logistic Map, IETE Technical Review, 29:5, 395-404

Final point

A one-line description of it

Chaotic Map used

$f(x) = rx(1\text{-}x)$

$x_{n+1} = f(x_n)$

This is the logistic map.

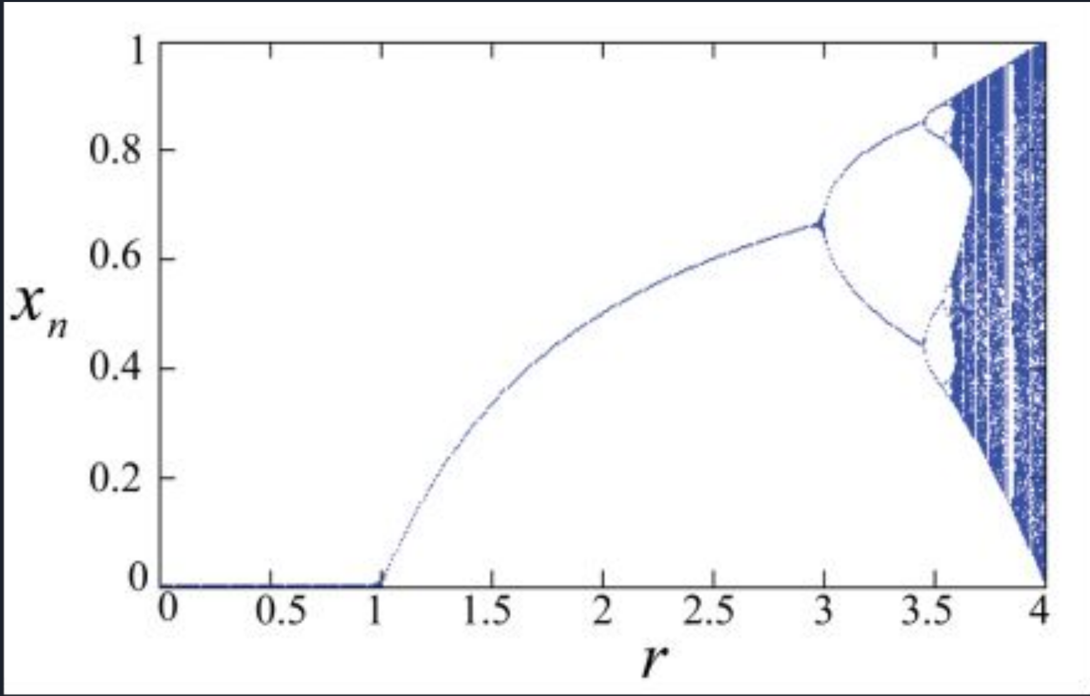


Figure 2: Bifurcation diagram of the logistic map.

Ref : Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay & Debashis Nandi (2012) An Image Encryption Process based on Chaotic Logistic Map, IETE Technical Review, 29:5, 395-404

Encryption algorithm

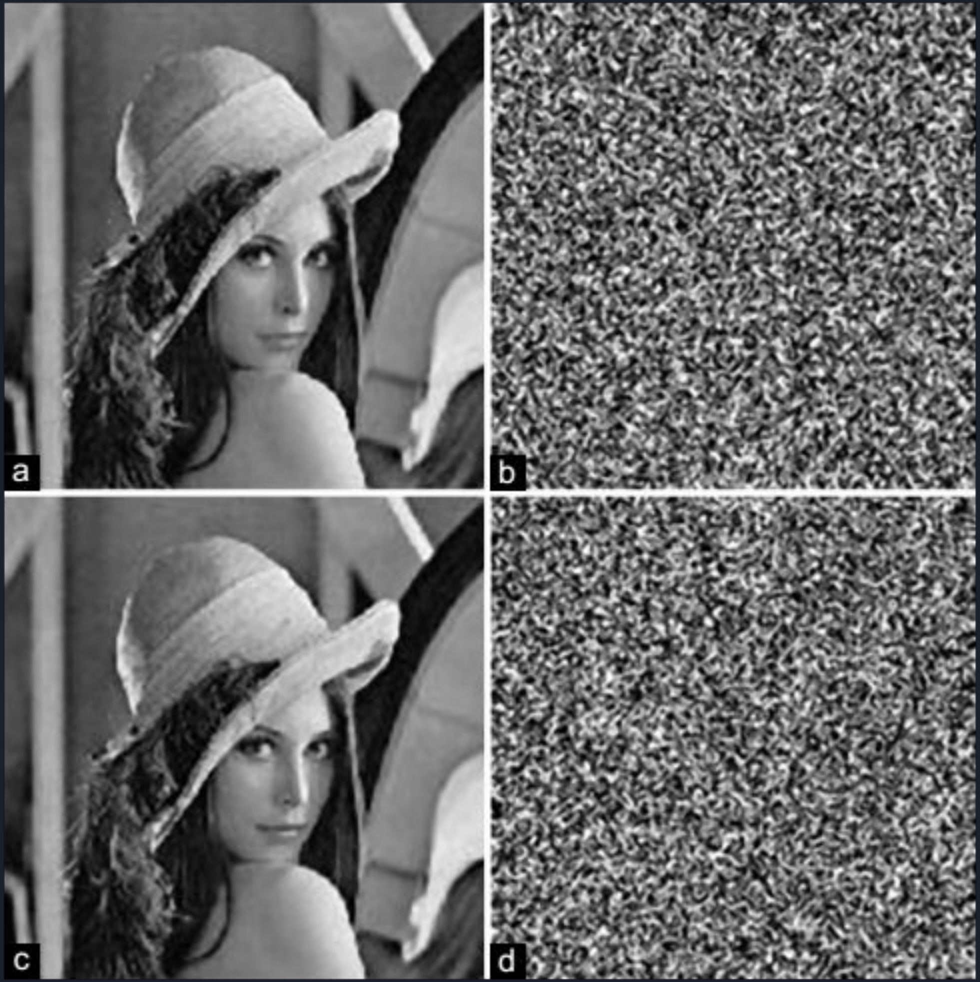
Step 0 - Choose an encryption key from a large key space.

Step 1 - Transform the image of size M×N pixels into
an array of P_i = { P_1, P_2….} , where i = 1 2 , , , 3 , and n = M×N.

Encryption algorithm

Step 2 - Generate n number of chaotic sequence $x_i = \{x_1,x_2,..x_n\}$, n in the range 0 to 1 using the logistic map mention in Eq. (1) with initial condition x_0 and taking the parameter r = 3.99. Next convert xi into unsigned integer in the range of 0 to 255 using mod operation.

Step 3 - Generate the sequence $C_i = P_i \oplus x_i$ for confusing the pixel value. The sign $\oplus$ indicates bitwise XOR operation.



Application of the encryption/decryption algorithm to the image Lena: (a) Plane image; (b) Encrypted image using key zxcvbnmlkjhgfdsa1234567890!@#$%x; (c) Decrypted image using same key of encryption; (d) Decrypted image using wrong key zxcvbnmlkjhgfdsa1234567890!@#$%y.

This is the most important takeaway that everyone has to remember.

Simplified Algorithm

Step 1 - Choose x_0 between 0 and 1 as the encryption key with 8 decimal places. This ensures the key space of 9^8.

Step 2 - Use x_0 to generate a logistic map sequence upto M X N terms, where M and N are width and height of the image in pixels.

Simplified Algorithm

Step 3 - $(256 * x_i) \bmod 256$ to get an array of unsigned integers from 0 to 255.

Step 4 - Confusing pixel values

$C_i = P_i \oplus x_i$ bitwise XOR operation

Since C_i is an unsigned integer from 0 to 255, it acts as a greyscale value for the encrypted image

Decryption Algorithm

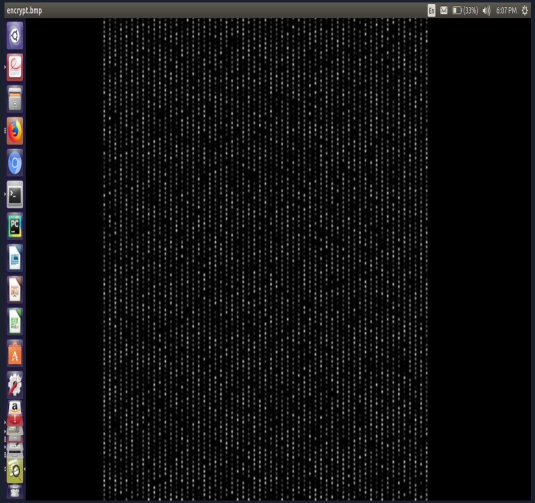
Step 1 - Using the property that

$$(a \oplus b) \oplus b = a,$$

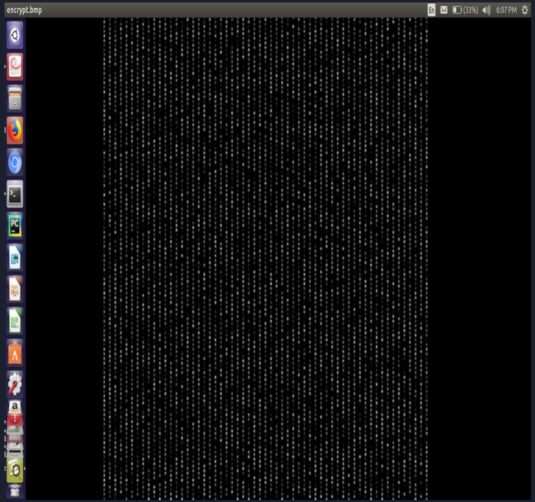
We get $P_i = C_i \oplus X_i$

- Thus we can get the pixel value of the original image from the encrypted pixel value and logistic sequence


puppy.jpeg
Edit View Go Help
6:07 PM


encrypt.bmp
6:07 PM


puppy.jpeg
Edit View Go Help
6:07 PM


encrypt.bmp
6:07 PM