ELL Project Report:

Image encryption and decryption

Vinayak Rastogi • 2016CS10345
Manav Rao • 2016CS10523

What is Encryption?

- Encryption : Process which uses an algorithm (a finite set of instructions) to convert original message (plain-text) into its encrypted form (cipher-text)
- Cryptographic algorithms normally require a key (a set of characters) to encrypt or decrypt data
- With the help of the key and the algorithm we can encrypt the plaintext into ciphertext, and then ciphertext back into plaintext

Why image encryption?

- Information security is rapidly becoming more important in data storage and transmission, and as images are being used for a number of tasks with various potential privacy and security issues, security of image data from unauthorised usage is highly important
- Image encryption methods render image information unreadable, making the original message (or other type of transmitted information) inaccessible to hackers and eavesdroppers (incl. server admins etc.) over public networks like the Internet.

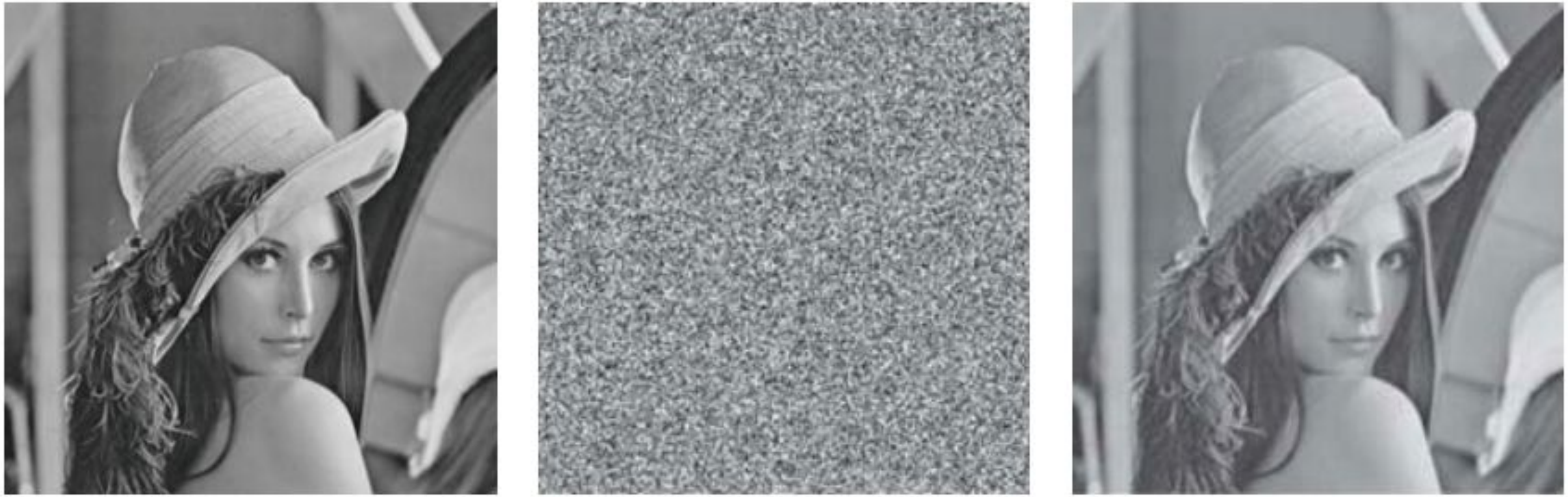
Image Encryption Algorithm: Based on Rubik’s Cube Principle

Reference: “A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle” Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai

THE ENCRYPTION ALGORITHM

1. We generate Kr and Kc randomly.
   (the keys corresponding to row and column dimensions)
2. For each row i
   We compute sum of all elements and find mod 2
   a. If answer is 0 the row is circularly right shifted by Kr[i] steps
   b. If answer is 1 the row is circularly left shifted by Kr[i] steps
3. For each column j; we repeat same using Kc
4. The odd columns of the scrambled images are XORed with Kc
5. The even columns of the scrambled images are XORed with reversed Kc
6. The odd rows of the scrambled images are XORed with Kr
7. The even rows of the scrambled images are XORed with reversed Kr

8. Steps 2 to 7 can be repeated for further complexity, making the algorithm more secure
   Kr, Kc, Number of iterations form the key set



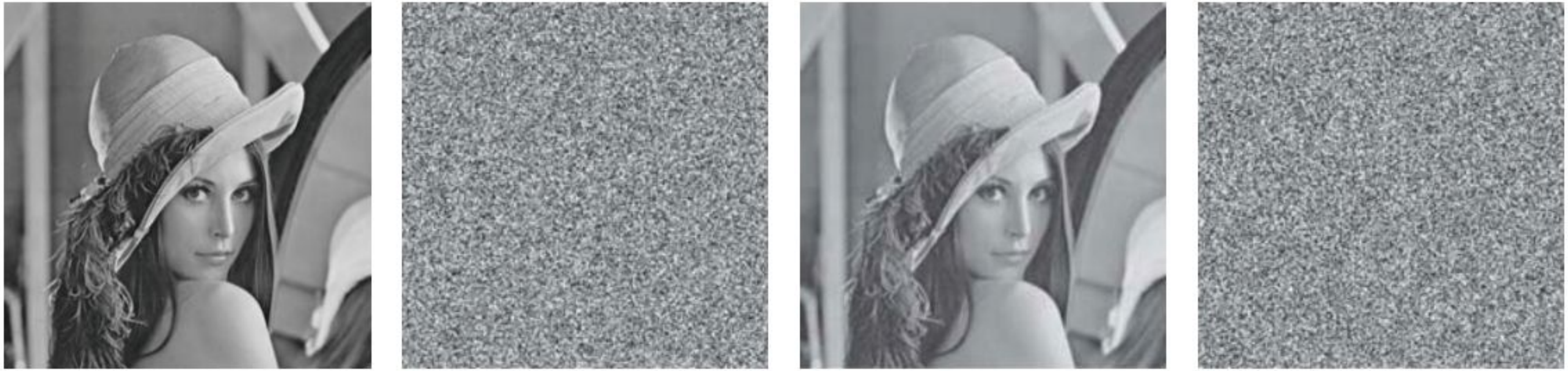
(a) Original image: Lena

(b) Encrypted image (a) with key K_1

(c) Decrypted image (b) using correct key K_1

Reference: “A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle” Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai

Testing of the Algorithm



(a) Original image: Lena

(b) Encrypted image (a) with key K_1

(c) Decrypted image (b) using correct key K_1

(d) Decrypted image (b) using wrong key K_2

Reference: “A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle” Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai

Testing of the Algorithm

Number of pixels change rate (NPCR), indicate the percentage of different pixels between two images.
Unified average changing intensity (UACI), which measures the average intensity of differences in pixels between two images.

To approach the performances of an ideal image encryption algorithm, NPCR values must be as large as possible and UACI values must be around 33%.

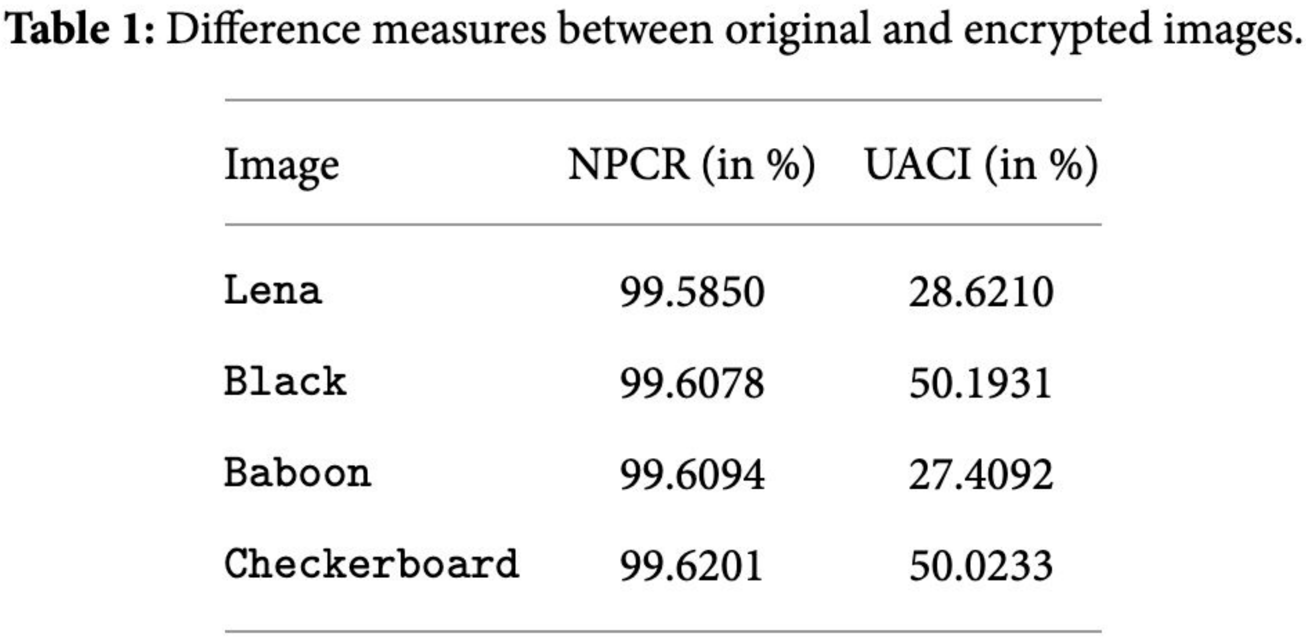
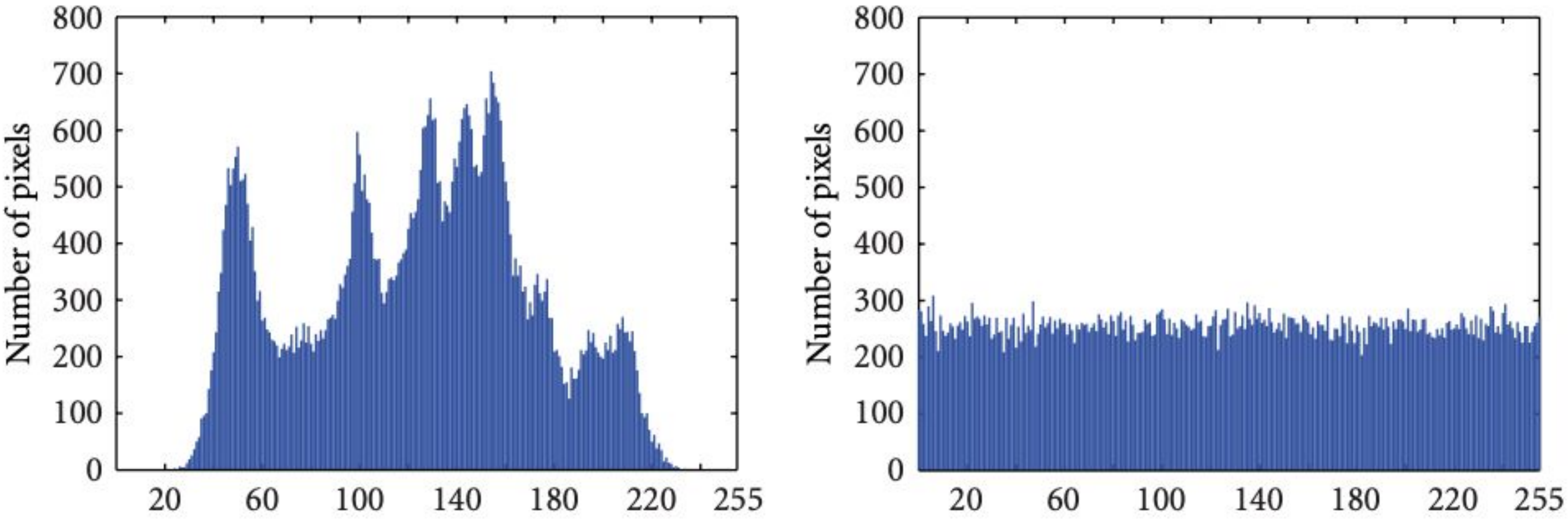


Table 1: Difference measures between original and encrypted images.

Image	NPCR (in %)	UACI (in %)
Lena	99.5850	28.6210
Black	99.6078	50.1931
Baboon	99.6094	27.4092
Checkerboard	99.6201	50.0233

Reference: “A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle” Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai

Testing of the Algorithm



(a) Original image: Lena

(b) Encrypted image: Lena

Reference: “A Secure Image Encryption Algorithm Based on Rubik’s Cube Principle” Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai

Additional Features

Audio Files Encryption into Image

In this we try and encrypt an audio file in the pixels of an image. We scale the values to a range of 255 and strategically place them in the grid.

Text Files Encryption into Image

Here we try to encrypt a text message upto the length of 255 characters into an image

Demo

Thank You

Reference: http://downloads.hindawi.com/journals/jece/2012/173931.pdf