

Rupal Shah
210002065

DIGITAL SIGNAL PROCESSING

EE 304

INTRODUCTION

Image Encryption and Decryption based on scrambling and the reality-preserving fractional discrete cosine transform

ENCRYPTION

Image encryption is the process of hiding images from unauthorized access using a secret key

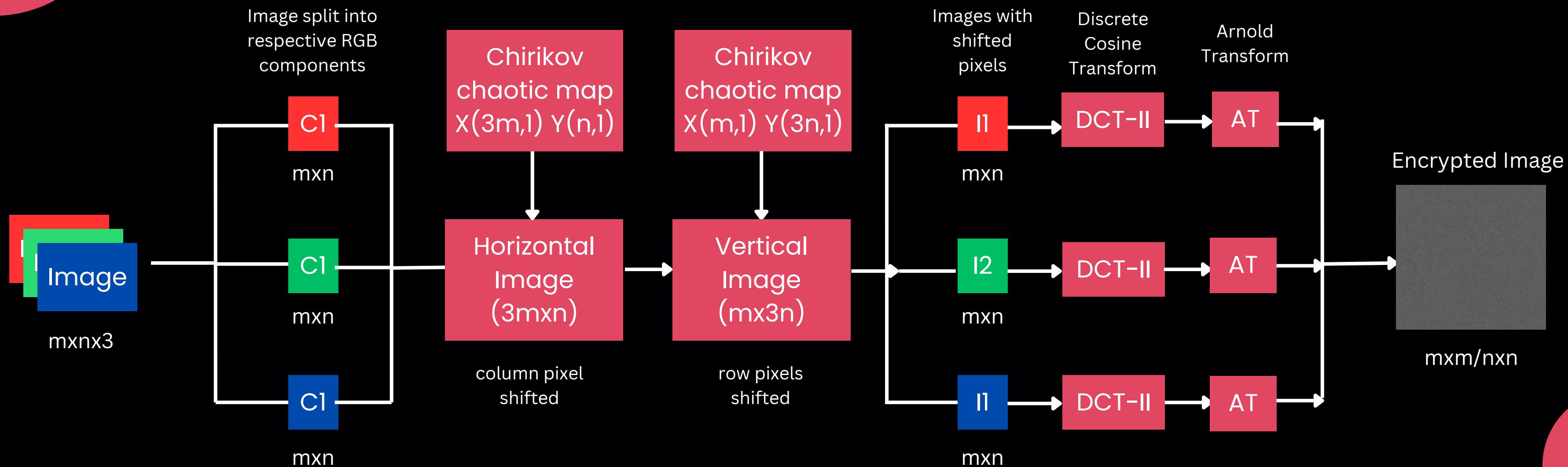
DECRYPTION

Decryption means the conversion of encrypted data into its original form is nothing but Decryption.



Fig 1: Google Image

ENCRYPTION ALGORITHM



Parameters are used in generating the chaos maps and are generated using a hashing algorithm

FORMULATION

Chirikov Standard Map

Invertible area preserving chaotic map for two canonical dynamical variables from a square with side 2

$$x_{i+1} = (x_i + y_i) \bmod 2\pi$$

$$y_{i+1} = (x_i + \delta \sin(x_i + y_i)) \bmod 2\pi$$

$$X = \text{floor}(x \times 10^{14}) \bmod N, \quad Y = \text{floor}(y \times 10^{14}) \bmod 3M$$

Fig 2: Research Paper

Discrete Cosine Transform-II

The above transforms help to increase the complexity of the encryption and makes it more secure and susceptible to change even on change of parameters in the order of 1e-14.

$$C_\alpha = 2\operatorname{Re} \left[\sum_{n=1}^{N/2} U_n e^{j\omega_n \alpha} \right] = \sum_{n=1}^{N/2} (A_n \cos \omega_n \alpha + B_n \sin \omega_n \alpha)$$

Arnold Transform

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N$$

Fig 2: Research Paper



Input Image



Chirikov Chaotic map



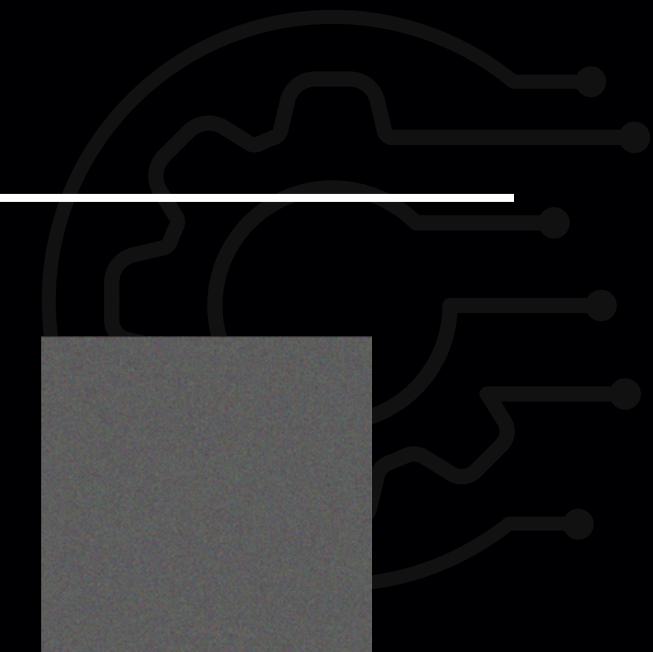
Vertical shift image



Horizontal shift image



DCT-II Encryption



Encryption

Encryption



Decrypted Image



Decrypted Image with wrong key

Decryption

RESULTS

RESULTS AND CODE

Lossless encryption of images provided a key.

Some novelties implemented are:

- Hashing Algorithm to create the encryption key and the parameters.
- Extended the algorithm for $m \times n$ images instead of square images.

REFERENCES

- 1) [Research Paper1](#) - base paper followed
- 2) [Research Paper2](#) – for arnold transform
- 3) [Research Paper3](#) – for hashing algorithm

[Link for the code](#)

THANK YOU