AI in Encryption

Presentation 2

Vaishnavi D
Aarushi Garg
Ishita Singh
Sunayana

LITERATURE SURVEY

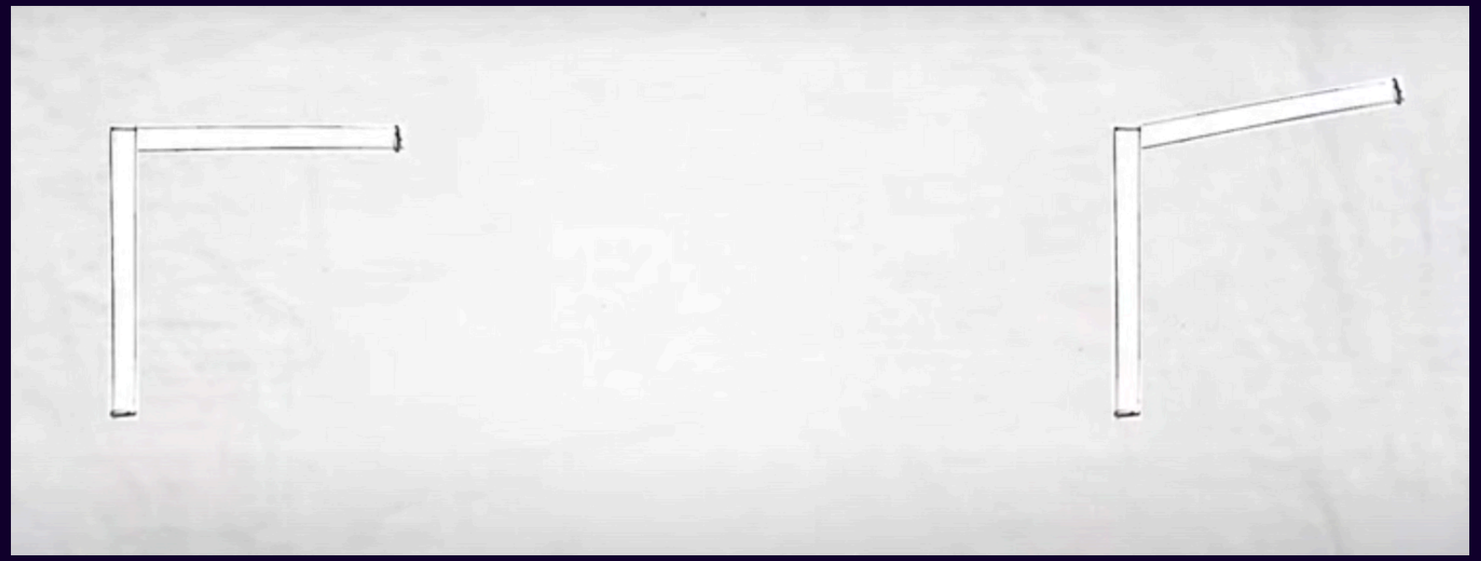
RESEARCH PAPER 1:

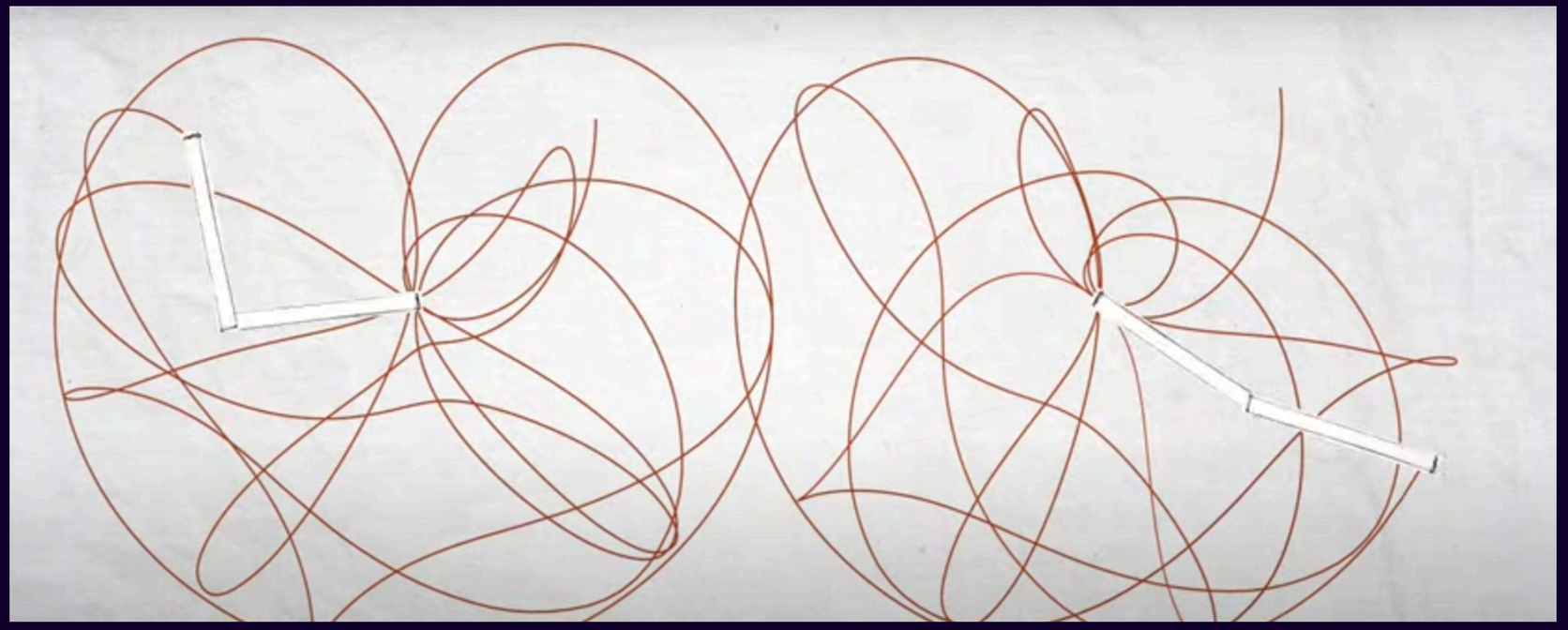
Chaos-based image encryption algorithm (2005)

src: https://www.researchgate.net/publication/259665875_Chaos-based_image_encryption_algorithm

Chaos theory, in mechanics and mathematics, the study of apparently random or unpredictable behaviour in systems governed by deterministic laws. A more accurate term, deterministic chaos, suggests a paradox because it connects two notions that are familiar and commonly regarded as incompatible.

src: https://www.britannica.com/science/chaos-theory





Keypoints

1. Arnold Cat map:

In order to disturb the high correlation among pixels, we adopt Arnold cat map to shuffle the pixel positions of the plain-image. Without loss of generality, we assume the dimension of the original grayscale image I is N × N. The coordinates of the pixels are S = {(x, y) | x,y = 0, 1, 2,...,N − 1}. Arnold cat map is described as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \pmod N$$

$$= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \qquad (1)$$

where p and q are positive integers, $\det(A) = 1$. The map is area-preserving since the determinant of its linear transformation matrix equals (1). The (x', y') is the new position of the original pixel position (x, y) when Arnold cat map is performed once. Iterated actions of A on a pixel $r_0 \in S$ form a dynamical system

$$r_{n+1} = A^n r_0 \pmod N \quad \text{or} \quad r_{n+1} = A r_n \pmod N,$$

Demonstration

https://demonstrations.wolfram.com/ArnoldsCatMap/

2. Encryption by Chen's chaotic system

Chen's chaotic system is first presented by Prof. G. Chen in 1999, which is described as following

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz, \end{cases}$$

where a, b and c are parameters. If one chooses a = 35, b = 3, c $\in$ [20, 28.4]

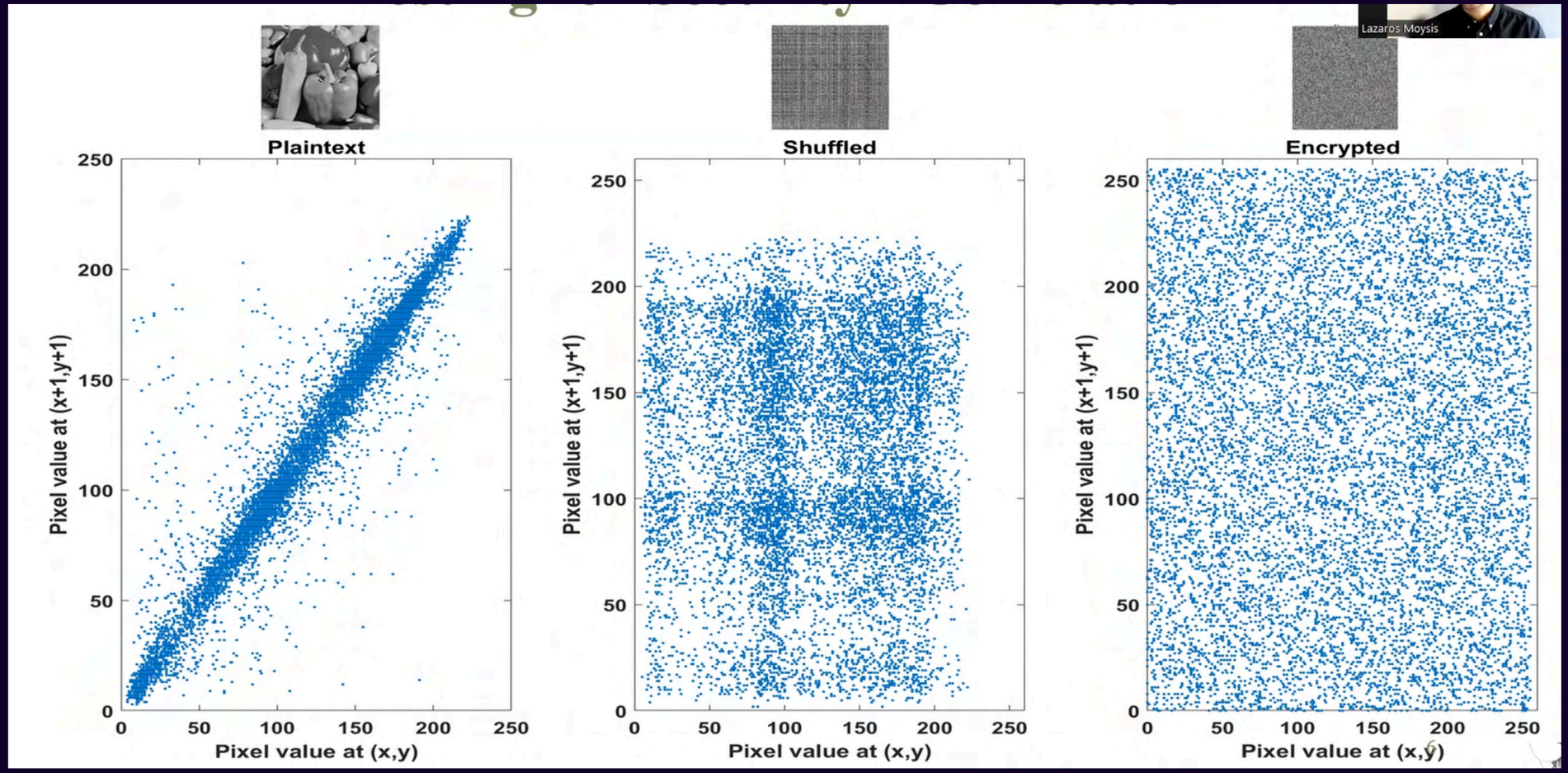
The encryption process consists of three steps of operations.

(1) The pixels of the shuffled image are arranged by the order from left to right and then top to bottom and we can get a set $S = \{S_1, S_2, \ldots, S_{N\times N}\}$, in which each element is the decimal grey value of the pixel. Convert decimal pixel values to binary numbers and we can get a new set $B = \{B_1, B_2, \ldots, B_{N\times N}\}$.

(2) Iterate the Chen's chaotic for N_0 times.

(3) The Chen's chaotic system is iterated continuously. For each iteration, we can get three values x_i, y_i and z_i. These decimal values are preprocessed first as follows

$$B_{x_i} = \mathrm{de2bi}\big(\mathrm{mod}\big(\big(\mathrm{Abs}(x_i) - \mathrm{Floor}\big(\mathrm{Abs}(x_i)\big)\big) \times 10^{14}, 256\big)\big),$$



src: https://www.youtube.com/watch?v=HutBEwJxfts&list=PL9y6bivP9mhEXxZGThfzyIJEZp5-BakCi&index=4

EXPERIMENTAL RESULTS

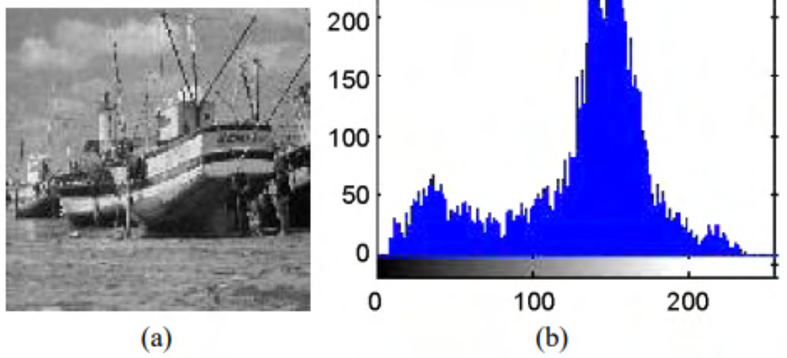


Fig. 2. Plain-image and its histogram: (a) plain-image; (b) histogram of the plain-image.

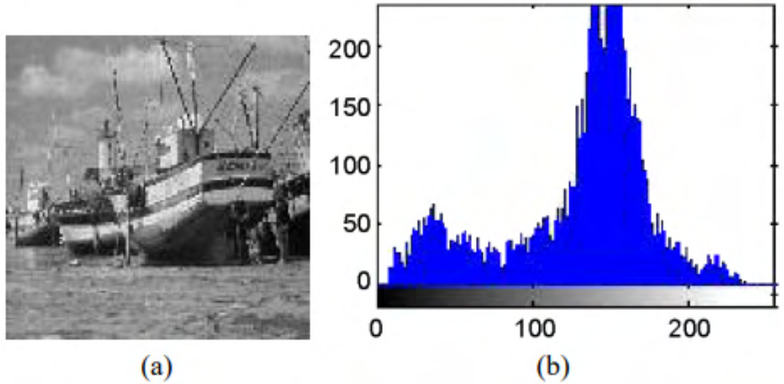


Fig. 5. Decrypted image and its histogram: (a) decrypted image; (b) histogram of the decrypted image.

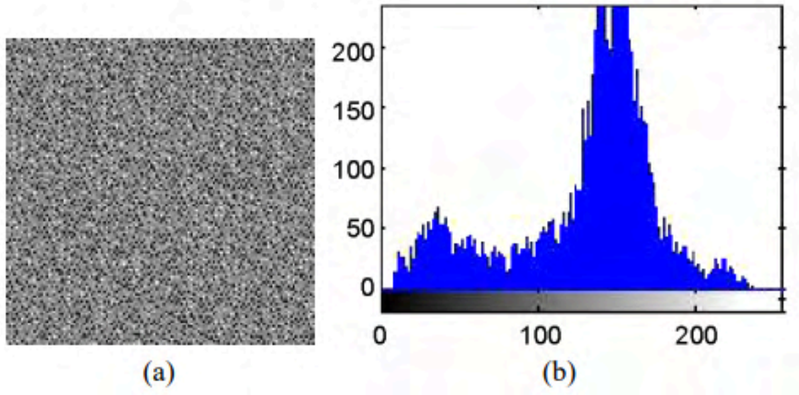


Fig. 3. Encryption by using Arnold cat map: (a) shuffled image; (b) histogram of the shuffled image.

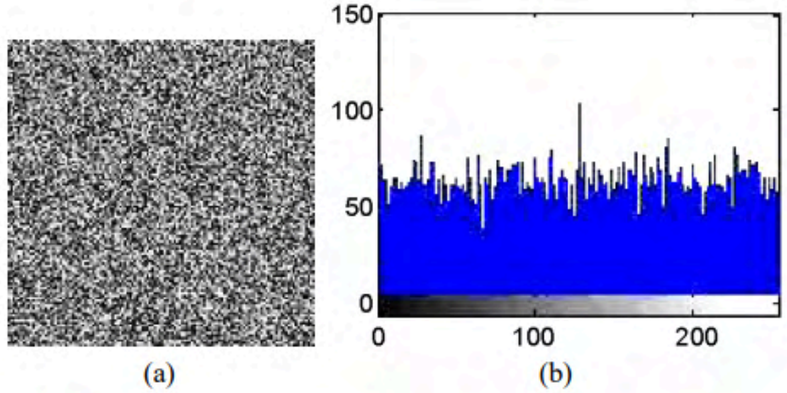


Fig. 4. Encryption by Chen's chaotic system: (a) cipher-image; (b) histogram of the cipher-image.

RESEARCH PAPER 2:

A novel image encryption algorithm based on chaos and Line map (2015)

src:https://www.sciencedirect.com/science/article/abs/pii/S0925231215006785

KEY POINTS

- The symmetrical image encryption algorithm proposed in this paper get rid of the limitation of the width be equal to the height of the image using a new designed Line map.
- The algorithm is suitable for encryption of both gray-scale image and color image.
- In addition, the algorithm can be implemented parallelly to improve speed performance.
- Security analysis shows great robustness against related attacks such as chosen plaintext attack due to large key space, uniform pixels distribution and high input sensitivity.
- More rounds of encryption are strongly recommended when there are much higher requirements for security

Fig. 4. Experimental results. (a) Plain-image of Lena; (b) cipher-image of Lena; (c) success of decryption of Lena; (d) failure of decryption of Lena; (e) plain-image of Couple; (f) cipher-image of Couple; (g) success of decryption of Couple; (h) failure of decryption of Couple; (i) plain-image of Couple; (j) cipher-image of Couple; (k) success of decryption of Couple; (l) failure of decryption of Couple. (For interpretation of the references to color in this figure, the reader is referred to the web version of this paper.)

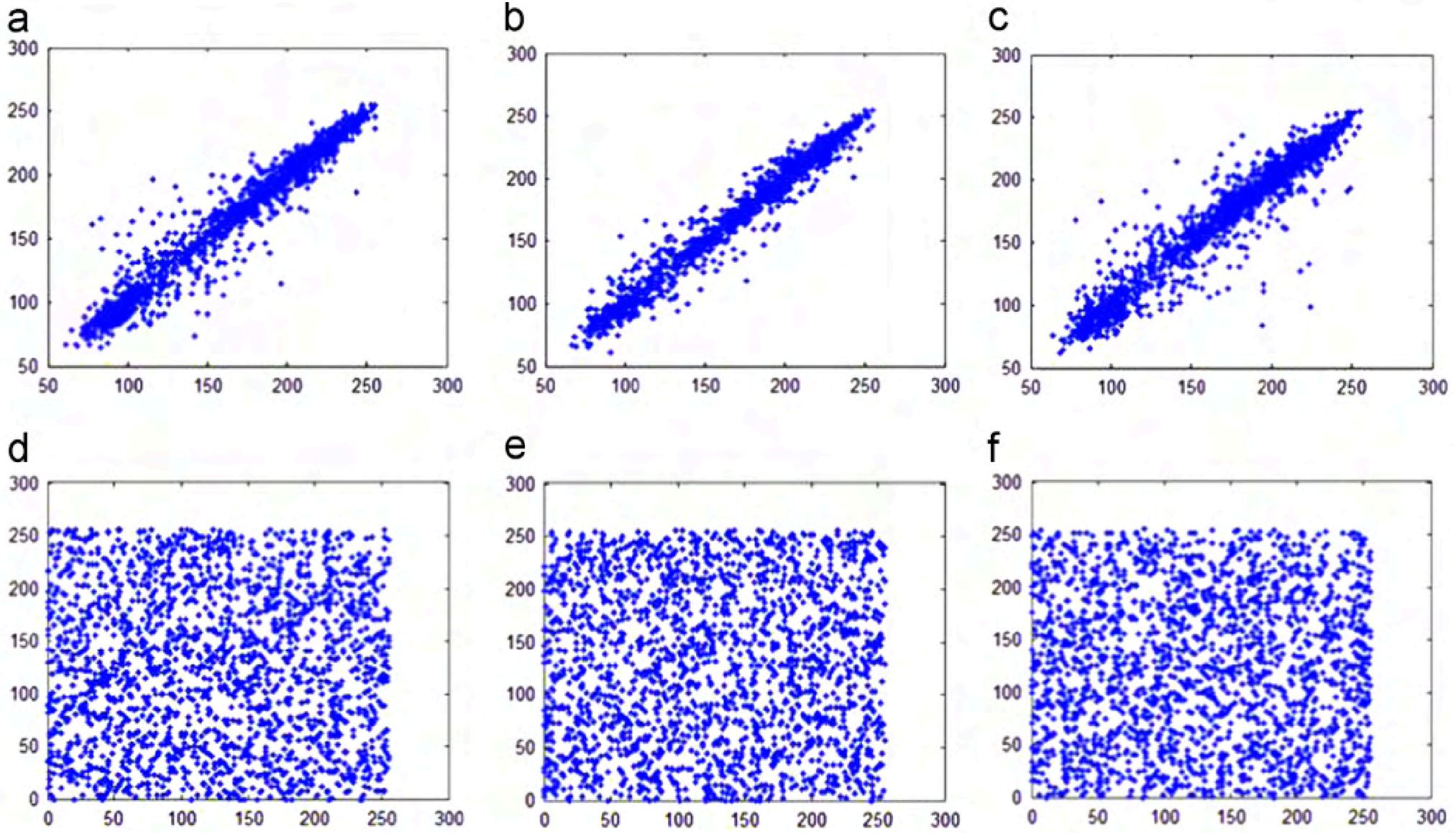
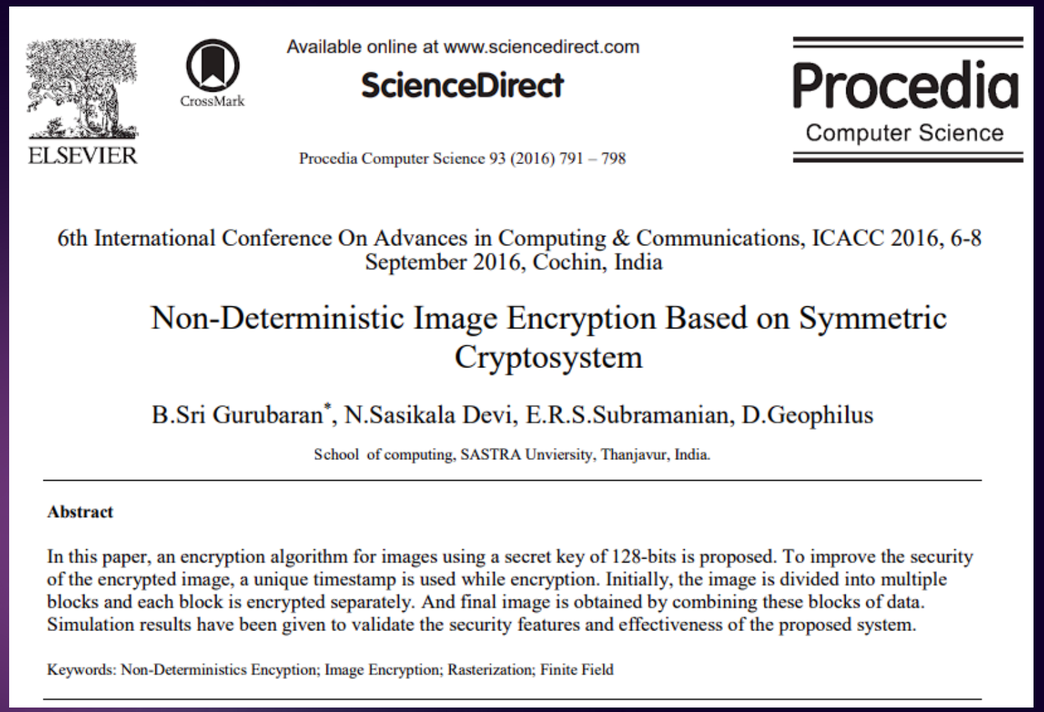


Fig. 6. Correlation analysis of image Lena in R channel. (a) plain-image in horizontal; (b) plain-image in vertical; (c) plain-image in diagonal; (d) cipher-image in horizontal; (e) cipher-image in vertical; (f) cipher-image in diagonal.

RESEARCH PAPER 3:

Non-Deterministic Image Encryption Based on Symmetric Cryptosystem (2016)

B.Sri Gurubaran , N.Sasikala Devi, E.R.S.Subramanian, D.Geophilus



ELSEVIER

CrossMark

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 93 (2016) 791 – 798

Procedia Computer Science

6th International Conference On Advances in Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

Non-Deterministic Image Encryption Based on Symmetric Cryptosystem

B.Sri Gurubaran*, N.Sasikala Devi, E.R.S.Subramanian, D.Geophilus

School of computing, SASTRA Unviersity, Thanjavur, India.

Abstract

In this paper, an encryption algorithm for images using a secret key of 128-bits is proposed. To improve the security of the encrypted image, a unique timestamp is used while encryption. Initially, the image is divided into multiple blocks and each block is encrypted separately. And final image is obtained by combining these blocks of data. Simulation results have been given to validate the security features and effectiveness of the proposed system.

Keywords: Non-Determinstics Encyption; Image Encryption; Rasterization; Finite Field

src:

https://www.sciencedirect.com/science/article/abs/pii/S0925231215006785

Key Points

- Proposes a 128-bit symmetric encryption algorithm for images.
- Utilizes a unique timestamp for enhanced security.
- Images are divided into blocks for individual encryption.
- Achieves semantic security, ensuring different ciphertexts for the same plaintext and key.
- Experimental results validate the algorithm's effectiveness in providing high security and robustness.

Framework

The framework proposed implements non-deterministic encryption to a symmetric cryptosystem, where instead of using traditional text based encryption algorithm an alternate way for image encryption is suggested. From Fig.1.

It is clear that the image file is broken down into blocks of data and processed individually following a Cipher Block Chaining (CBC) encryption method, and to impart non-determinism a unique timestamp is mixed with the first data block and since CBC encryption method is used this brings about a vast change in the consequent blocks (an Avalanche effect is observed).

Table 2. Correlation coefficient of the encrypted images from different instances of time

Image	Correlation Coefficient of Red Component	Correlation Coefficient of Green Component	Correlation Coefficient of Blue Component
Fig.8(a)	0.0014	0.0026	-0.001
Fig.8(b)	-0.0001	-0.0013	0.0031
Fig.8(c)	-0.0005	0.0027	0.0005
Fig.8(d)	0.001	-0.0011	0.0041

From Table 2 it is evident that, even though the histograms may not show the variation between them, clearly their correlation coefficients vary appreciably to say that the generated images are different from one another.

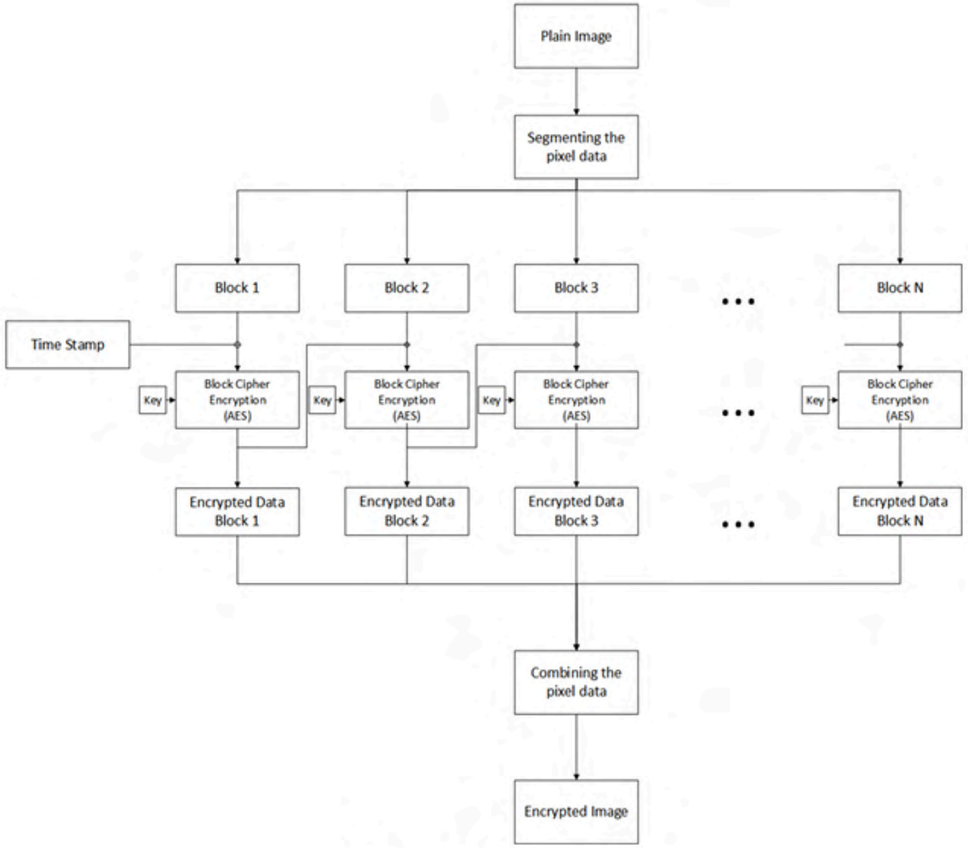
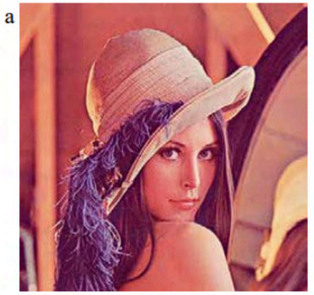


Fig.1. Non-Deterministic encryption scheme

4.1. Histogram Analysis

First experiment is the histogram analysis of the original, encrypted and the decrypted images. In this analysis the image histograms of the respective images are considered to show that the original and encrypted images vary vastly and the original and decrypted images are one and the same.

a



b

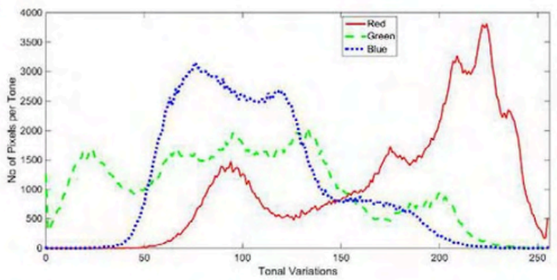
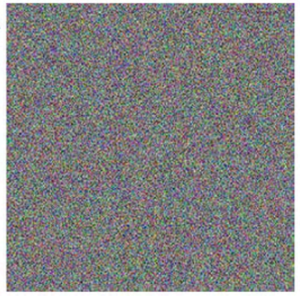


Fig. 2. (a) Original Image (Lena); (b) Image histogram of (a)

Fig.2(b) Plots Tonal Variations Vs Number of Pixels per Tone for red, green and blue components of the image.

a



b

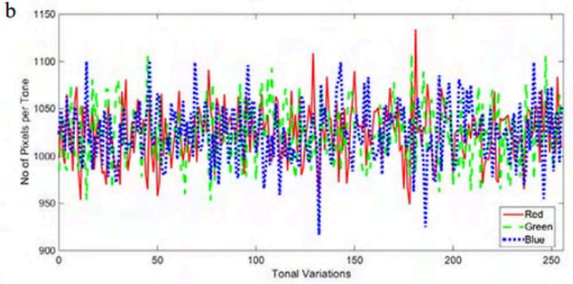
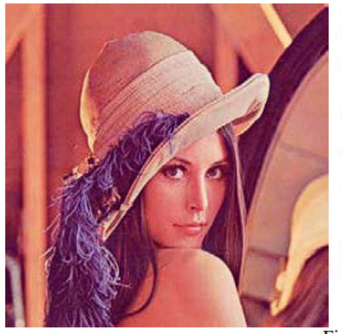


Fig. 3. (a) Encrypted Image; (b) Image histogram of (a)

a



b

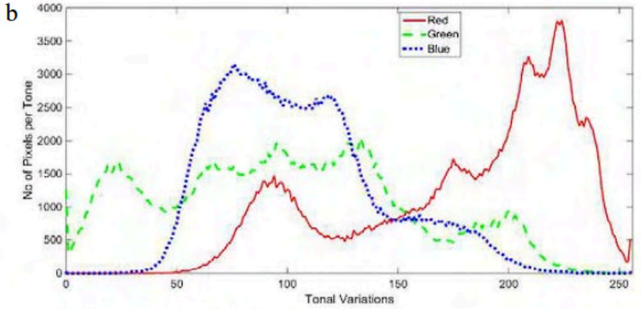


Fig. 4. (a) Decrypted Image; (b) Image histogram of (a)

It is evident from the histogram and image that it is same as the original image.

4.2. Comparison between compressed and uncompressed image

In this experiment the same image and same cipher key are considered, but with different image formats say BMP and JPG. Then the correlation coefficient and mean square error (MSE) for the set of images are found. This is to prove that the file format plays a role in the encryption process of the image.

a

b

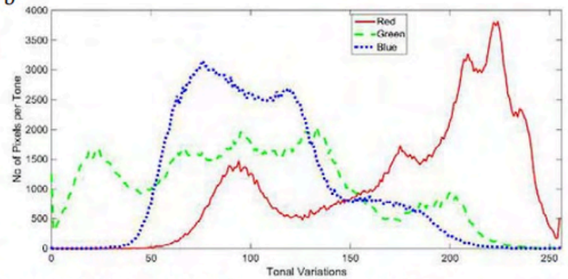
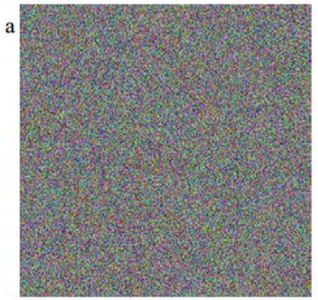


Fig. 5. (a) Original Image (BMP, JPG); (b) Image histogram of (a)

Fig.5(a) and 5(b) shows the original image and its corresponding histograms for both BMP and JPG file formats they turn out to be the same.

a



b

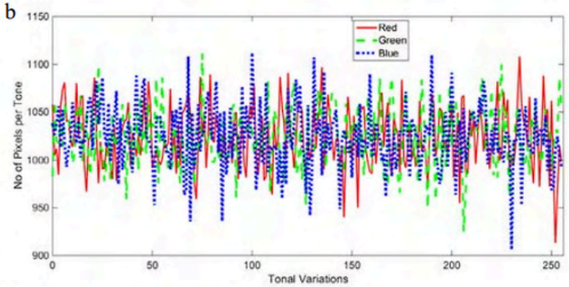
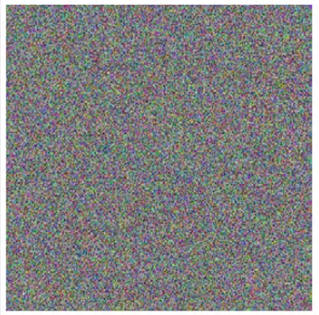


Fig. 6. (a) Encrypted Image (BMP); (b) Image histogram of (a)



b

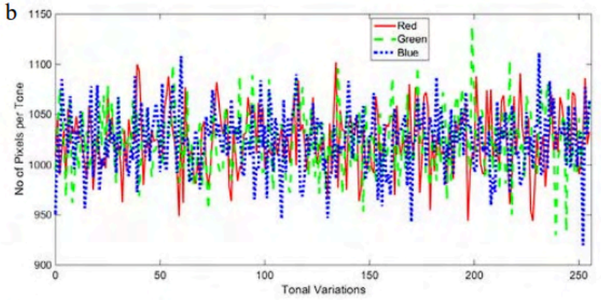


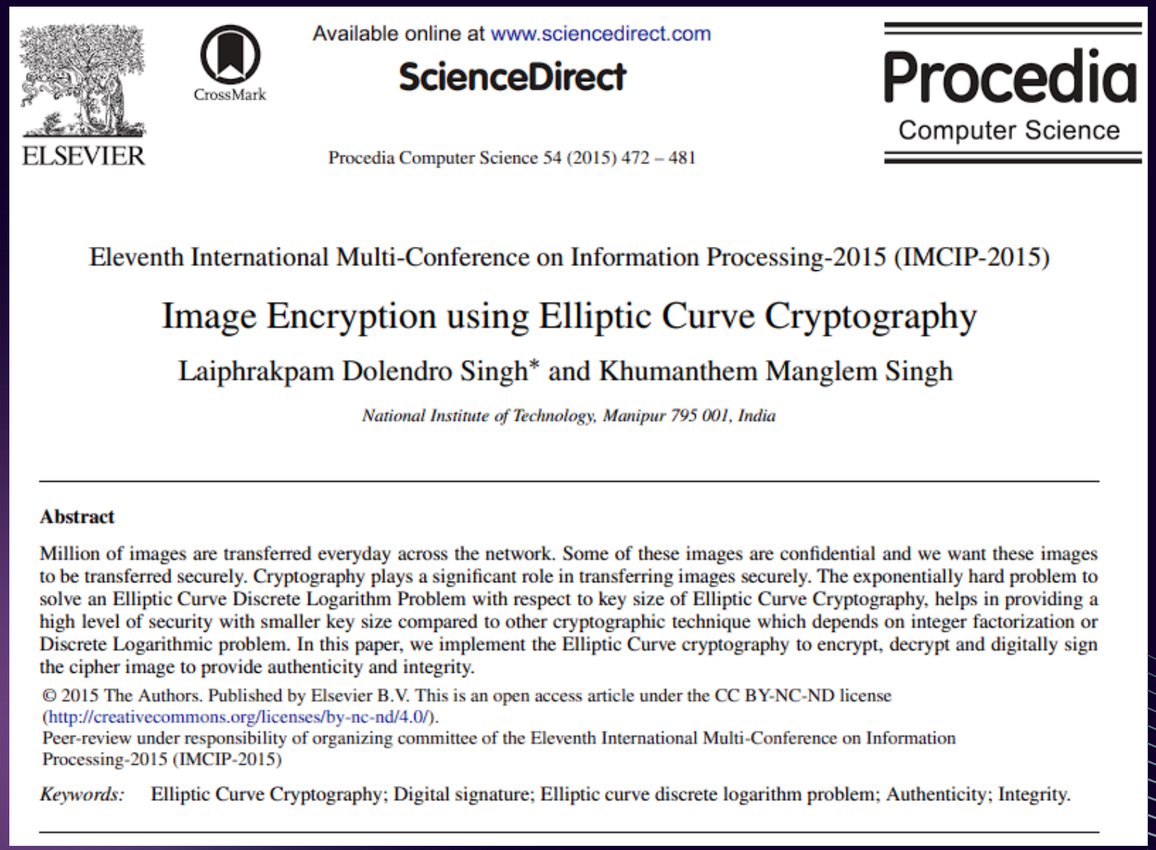
Fig. 7. (a) Encrypted Image (JPG); (b) Image histogram of (a)

Though the difference may not be evident in the images, the variation between the encrypted images can clearly be seen in the histograms.

RESEARCH PAPER 4:

Image Encryption using Elliptic Curve Cryptography (2015)

Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh



Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 54 (2015) 472 – 481

Procedia Computer Science

Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

Image Encryption using Elliptic Curve Cryptography

Laiphrakpam Dolendro Singh* and Khumanthem Manglem Singh

National Institute of Technology, Manipur 795 001, India

Abstract

Million of images are transferred everyday across the network. Some of these images are confidential and we want these images to be transferred securely. Cryptography plays a significant role in transferring images securely. The exponentially hard problem to solve an Elliptic Curve Discrete Logarithm Problem with respect to key size of Elliptic Curve Cryptography, helps in providing a high level of security with smaller key size compared to other cryptographic technique which depends on integer factorization or Discrete Logarithmic problem. In this paper, we implement the Elliptic Curve cryptography to encrypt, decrypt and digitally sign the cipher image to provide authenticity and integrity.

Keywords: Elliptic Curve Cryptography; Digital signature; Elliptic curve discrete logarithm problem; Authenticity; Integrity.

src: https://www.sciencedirect.com/science/article/abs/pii/S0925231215006785

Key Points

- ECC offers high security with smaller key sizes.
- The proposed algorithm groups pixels into single integers to reduce computation.
- Includes digital signatures for authenticity and integrity.
- Security analysis shows low correlation in cipher images and high entropy values.

Encryption Process Overview

- **Pixel Value Modification**: Each pixel of the image is randomly altered by adding 1 or 2 to generate a low correlated cipher image.
- **Pixel Grouping:** The modified pixel values are grouped and converted into a single large integer for each group.
- **Key Generation**: A random integer 'k' is selected, and the public key 'Pb' of the receiver is computed.
- **Cipher Text Creation**: Point addition is performed using the public key and the grouped pixel values to create the cipher text.
- **Value Conversion**: The cipher text is converted to a range of 0 to 255 for pixel representation.
- **Padding:** The resulting values are padded with zeros to maintain consistent formatting.

Fig. 6. (a) Cipher image of house; (b) Decrypted image with correct key nB; (c) Decrypted with key as $nB - 1$.

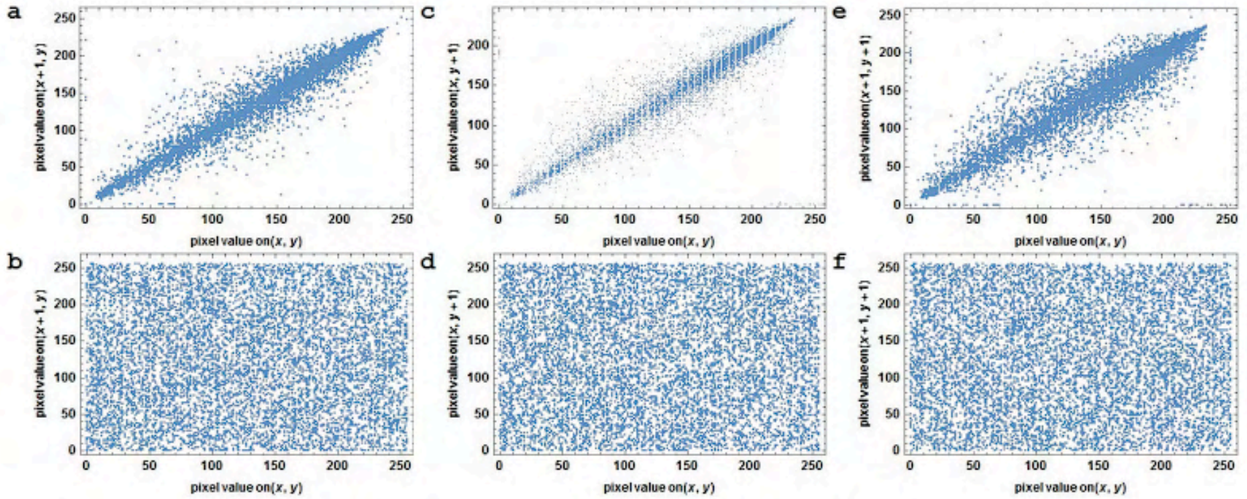


Fig. 7. Correlation of adjacent pixel (a) Along horizontal direction for plane image; (b) Along horizontal direction for cipher image; (c) Along vertical direction for plane image; (d) Along vertical direction for cipher image; (e) Along diagonal direction for plane image; (f) Along diagonal direction for cipher image.

Fig. 2. (a) Plain image of mandrill; (b) Plain image of peppers; (c) Plain image of lena.

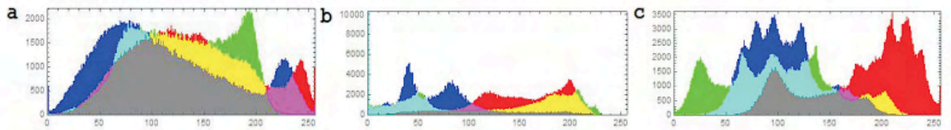


Fig. 3. (a) Histogram of mandrill; (b) Histogram of peppers; (c) Histogram of lena.

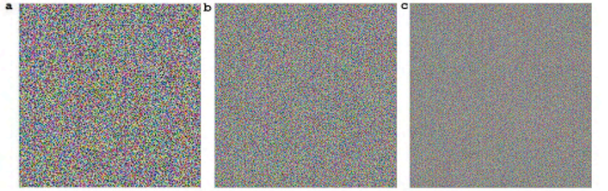


Fig. 4. (a)Cipher image of mandrill; (b) Cipher image of peppers; (c) Cipher image of lena.

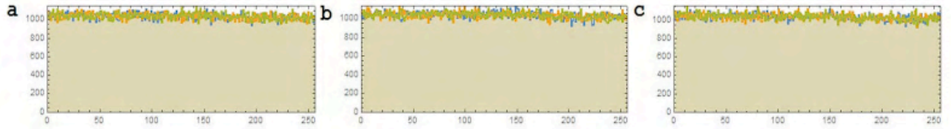


Fig. 5. (a) Histogram of cipher mandrill; (b) Histogram of cipher peppers; (c) Histogram of cipher lena.

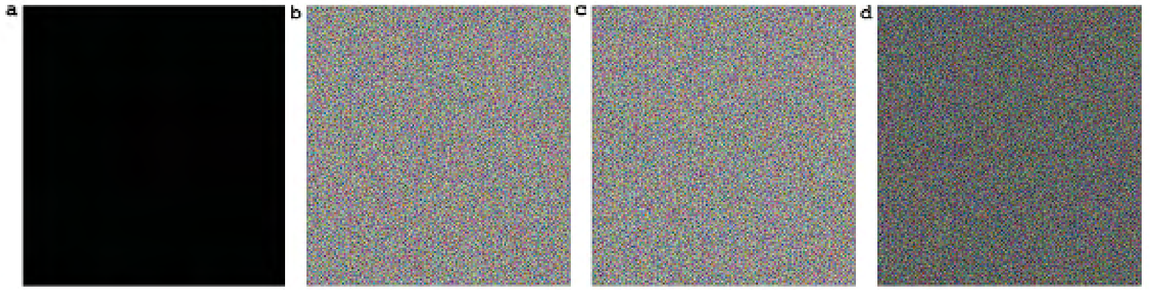


Fig. 8. (a) Totally black plane image; (b) Cipher image generated on first execution with key nB; (c) Cipher image generated on second run with key nB; (d) Image difference between the two cipher images.

RESOURCES

https://www.sciencedirect.com/science/article/pii/S1877050915013782

https://dl.acm.org/doi/10.1145/3600211.3604681

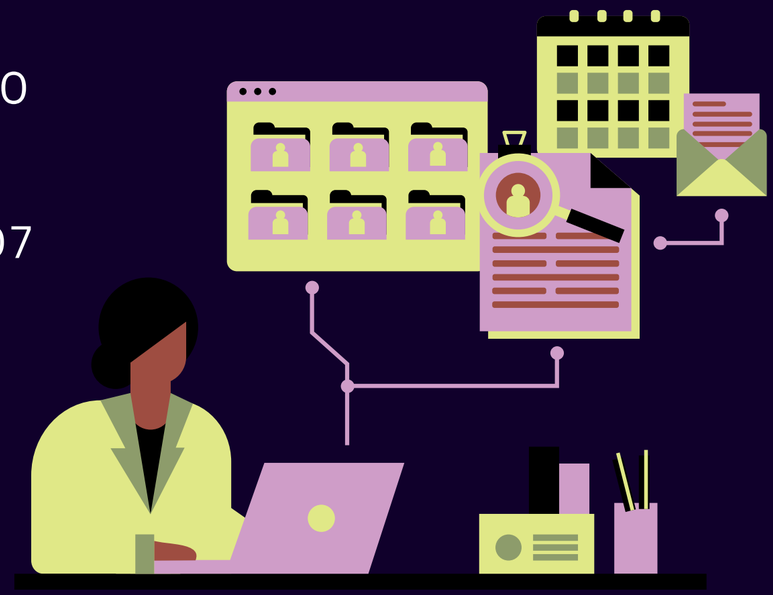
https://www.sciencedirect.com/science/article/abs/pii/S1568494609002658

https://www.sciencedirect.com/science/article/pii/S1877050916315423

https://people.cs.uchicago.edu/~ravenben/publications/pdf/organic-ccs24.pdf

https://www.sciencedirect.com/science/article/abs/pii/S0960077905006661

https://www.sciencedirect.com/science/article/pii/S2589004220307070




Thank
You