

# Image Encryption using Feistel Transformation and Hill Encryption



**Mentor:**  
**Er. Manoj Wairya**

## **Group details:**

Harsh Nayak [20164076]  
Akarsh Dubey [20164055]  
Cherukuri Lakshmi Lahari [20164001]  
Gugulothu Rajashekar [20164143]

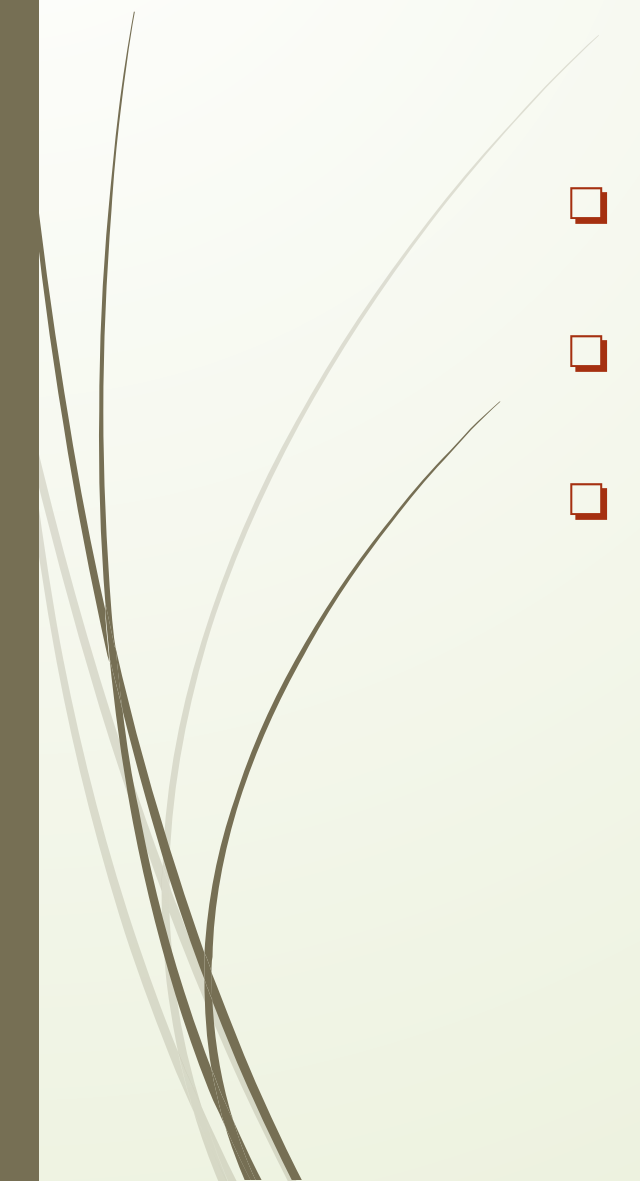


# Contents

- 
- ❑ Motivation
  - ❑ Problem Statement
  - ❑ Scope
  - ❑ Feistel Network
  - ❑ Dynamic DNA Encoding
  - ❑ Chaotic Sequence
  - ❑ Hill Cipher Encryption
  - ❑ Ciphertext Feedback
  - ❑ Image Encryption Algorithm
  - ❑ Sample Encryption
  - ❑ Classic Attack Analysis
  - ❑ Future Scope
  - ❑ References




# Motivation

- ❑ Cyber security is a major issue which is affecting social stability, national security, and personal property.
  - ❑ To implement an image encryption method that provides multifold security in data security transmission.
  - ❑ The massive data storage capacity of the DNA and its high parallel computing power provides security guarantees for the current DNA encryption methods.
- 

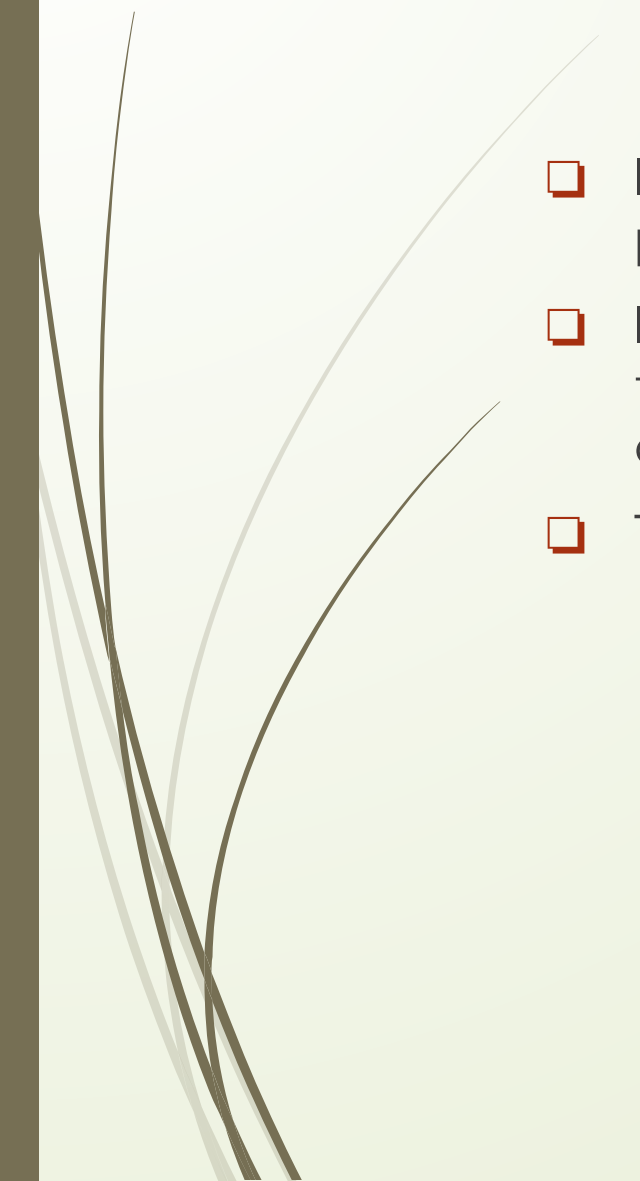


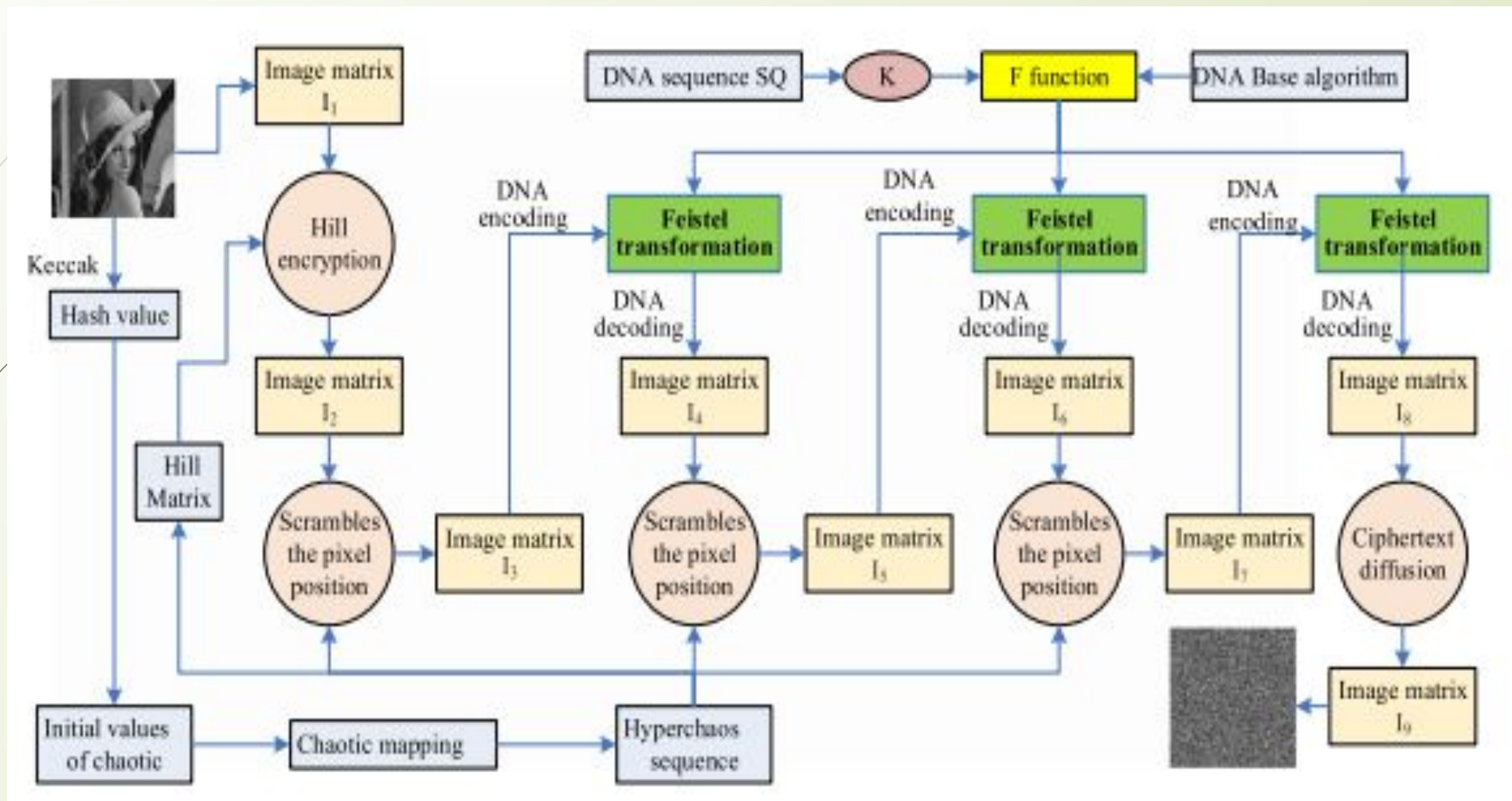
# Problem Statement

- 
- ❑ To implement a new and robust image encryption method using Feistel Transformation and Hill Encryption, which is able to permute, scramble, diffuse and confuse the image data into an encrypted image.

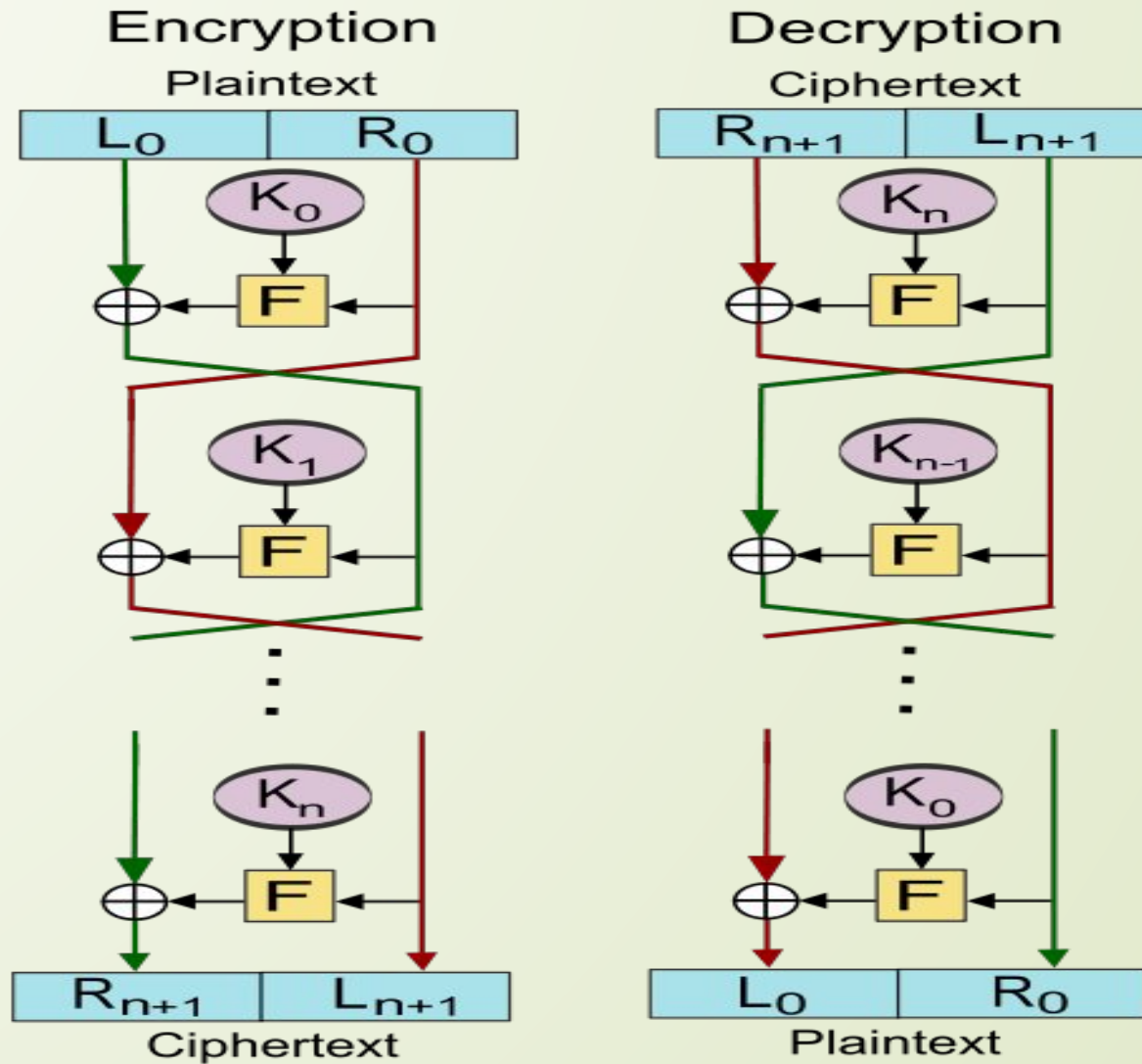


# Scope

- ❑ It can be used in fields such as military, air-force, navy or at any other place where data security has utmost priority.
  - ❑ It can be embedded in applications that will facilitate the users to transfer the data to each other over the internet without any threat of data loss.
  - ❑ The LOC of the project is 500.
- 



# Feistel Network



# Feistel Network

- ❑ The symmetric structure used in block ciphers is called Feistel cipher.
- ❑ The plaintext block (P) is divided into the left and right parts in the Feistel cryptography scheme ( $P = (L_0, R_0)$ ); for every round  $i$  of the encryption process, here  $i = 1, 2, \dots, n$ , a new left half part and right half part is generated according to the following rules:

$$L_i = R_{i-1}$$

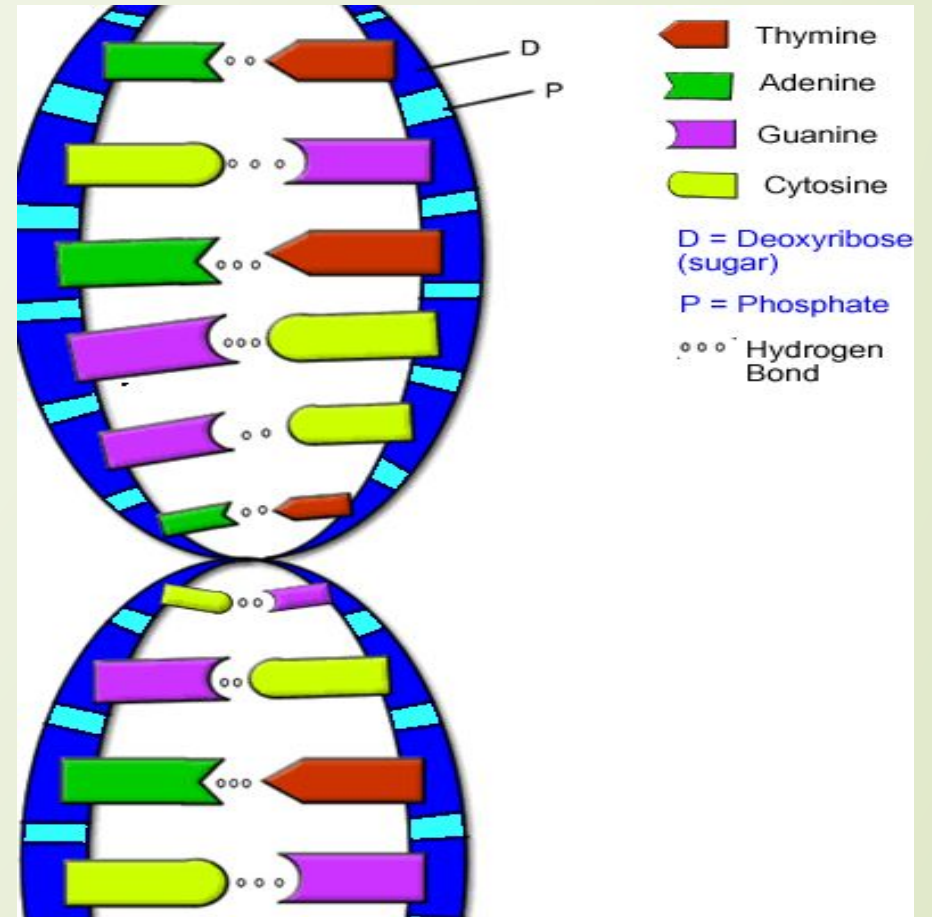
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

$\oplus$  denotes bit XOR operation,  $F$  is the round function, and  $K_i$  is the sub-key of the  $i$ th round. The output of the  $F$  function is the XOR of  $R_{i-1}$  and  $K_{(i)}$ .



# DNA Encoding

- The DNA molecule is composed of four DNA nucleotides, including adenine (A), guanine (G), cytosine (C), and thymine (T).



# Dynamic DNA Encoding

- ❑ Dynamic DNA encoding is used to overcome the weakness in DNA encoding.
- ❑ The encryption of pixel matrix is done using one of the 8 rules depending the pixel position.

Rule	1	2	3	4	5	6	7	8
00	A	A	C	G	C	G	T	T
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C
11	T	T	G	C	G	C	A	A

# Dynamic DNA Encoding

- ❑ The DNA encoding rule  $R(i,j)$  for the pixel  $P(i,j)$  is calculated as follows :

$$R(i,j) = \text{Mod}((i - 1) * n + j, 8) + 1.$$

Where  $i \in \{1, 2, 3, \dots, m\}$ ,  $j \in \{1, 2, 3, \dots, n\}$

- ❑ As each pixel value can be represented using 8-bit binary, thus, each pixel is encoded as 4 bases of DNA.

# Chaotic sequence

SHA-3 encrypted hash key value  $K$  is used together with some initial standard values to generate a chaotic sequence and the non-repeated generated values are used when the system reaches in a hyper-chaotic state. This sequence helps in obtaining a set of randomly generated values.

Initial values of  $x'_0, y'_0, z'_0, w'_0$  is 0.000000005,

and  $j = 6(i - 1), i = 1, 2, 3, 4$

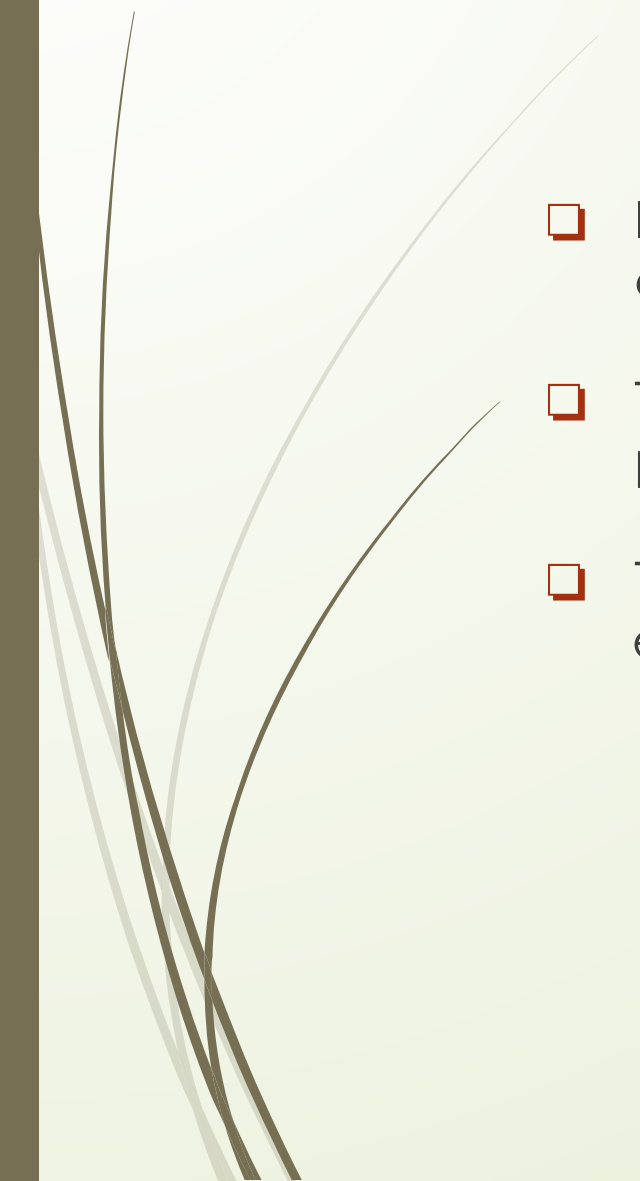
$$h_i = \frac{(k_{j+1} \oplus k_{j+2} \oplus k_{j+3}) + k_{j+4} + k_{j+5} + k_{j+6}}{256}$$

$$\begin{cases} x_0 = x'_0 + \text{abs}(\text{round}(h_1) - h_1) \\ y_0 = y'_0 + \text{abs}(\text{round}(h_2) - h_2) \\ z_0 = z'_0 + \text{abs}(\text{round}(h_3) - h_3) \\ w_0 = w'_0 + \text{abs}(\text{round}(h_4) - h_4) \end{cases}$$

$$\begin{cases} B_1 = (A_1 - [A_1]) \\ B_2 = (A_2 - [A_2]) \\ B_3 = (A_3 - [A_3]) \\ B_4 = [\text{mod}(10000 * (A_4 - [A_4]), 256)] \end{cases}$$



# Hill Cipher Encryption

- ❑ In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra.
  - ❑ The  $4 \times 4$  reversible matrix  $M$  is constructed, then the Hill encryption is performed on each set of images.
  - ❑ The image which is to be encrypted is divided into blocks with 4 pixels in each block, and the each block of pixel is converted into  $4 \times 1$  matrix,  $I$ .
- 

# Construction of Hill Encryption Matrix

$$E = (M * I) \bmod 256 = \begin{bmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{bmatrix} * \begin{bmatrix} I_{11} \\ \vdots \\ I_{41} \end{bmatrix} \bmod 256 = \begin{bmatrix} E_{11} \\ \vdots \\ E_{41} \end{bmatrix}$$

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix}$$

$$M_{11} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$$

1. The  $B_4$  sequence generated is used to fill sub-matrix  $M_{11}$ .
2. Sub-matrix  $M_{12} = I - M_{11}$
3. Sub-matrix  $M_{22} = -M_{11}$
4. Sub-matrix  $M_{21} = I + M_{11}$

# Ciphertext Feedback

- ❑ Ciphertext feedback operation is used to disrupt the relationship between the plaintext and ciphertext image.
- ❑ The image matrix is converted into a one-dimensional sequence:

$$S = \{s_1, s_2, s_3, \dots, s_{mn}\}$$

- ❑ The new one-dimensional sequence formed is:

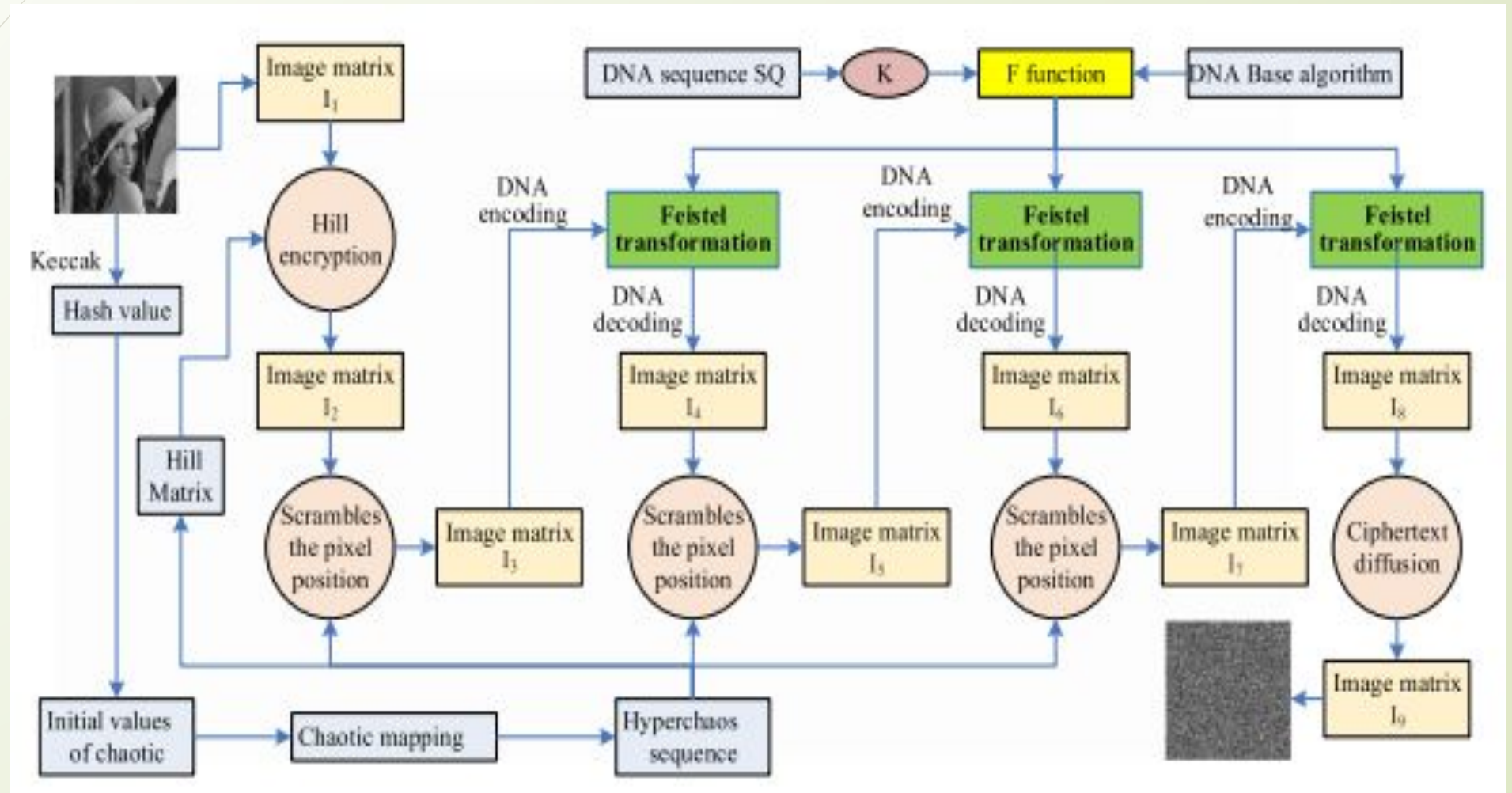
$$SE = \{se_1, se_2, se_3, \dots, se_{mn}\}$$

$$se(i + 1) = s(i) \oplus se(i - 1)$$

Where initial elements  $se(0) = 127$ ; and  $i = 1, 2, 3, \dots, m*n$



# Image Encryption Algorithm







# Image Encryption Algorithm

- ❑ Convert the image  $P$  in a 2D matrix  $P_1$  with size  $m \times n$ .
- ❑ Hash value  $K$  using SHA-3 function with  $P_1$  as input and chaotic sequences are generated.
- ❑  $B_4$  sequence from chaotic Chen system is used to fill initial matrix and construct the Hill encryption matrix.
- ❑ Every 4 pixels is used as a matrix and its XOR is taken with Hill encryption matrix to generate a new matrix and this new matrix replaces the old matrix.

# Image Encryption Algorithm

- ❑ A DNA sequence is used as the key  $K$  in the in the  $F$  function of the Feistel transformation.
- ❑ From the initial chaotic sequence generated,  $B_1$  sequence is used to scramble the pixel positions of the image matrix  $P_2$  and obtain a new scramble matrix  $P_3$  using following rule:
$$i = i' + \text{mod}(\text{floor}(B_1(i)) * 1015, M-i)$$
$$j = j' + \text{mod}(\text{floor}(B_1(j)) * 1015, N-j)$$
- ❑ The image matrix  $P_3$  is divided into blocks of 8 pixels. Each pixel is encoded into a DNA encoding according to its position in the matrix and then passed through Feistel transformation followed by DNA decoding to get image matrix  $P_4$ .
- ❑ The second round of transformation and scrambling is done using  $B_2$  to obtain image matrix  $P_5$  on which DNA encoding, decoding and Feistel transformation is performed to restore  $P_6$ .



# Image Encryption Algorithm

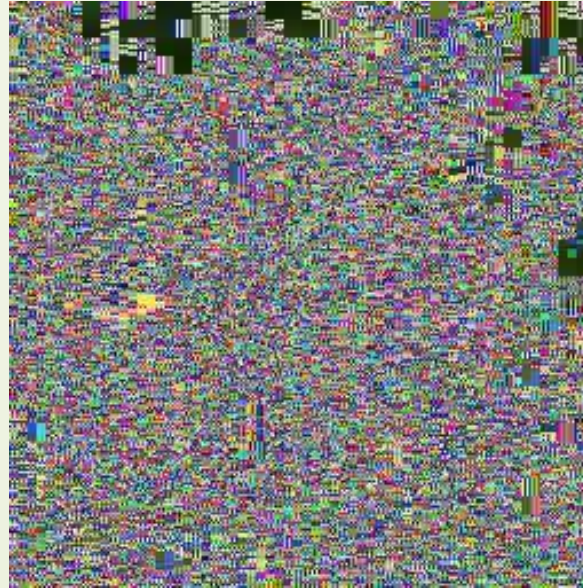


- ❑ Similarly transformation and scrambling is performed again using  $B_3$  sequence to obtain image matrix  $P_7$  which is used to restore image matrix  $P_8$ .
- ❑ The image matrix is  $P_8$  is subjected to ciphertext diffusion.
- ❑ The new image matrix  $P_9$  is generated which is simply the XOR operation with the values of the previous pixels.

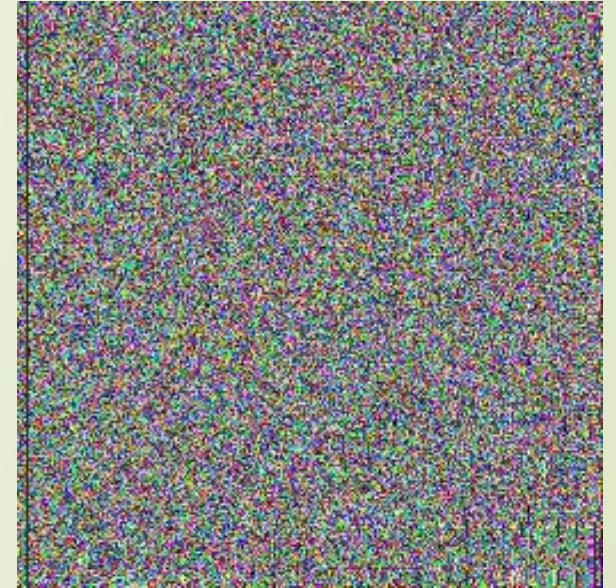
# Sample Encryption



Original image



Hill Encrypted image



Encrypted image






# Classic Attack Analysis



- ❑ There are 4 types of typical attacks, including a ciphertext-only attack, a known plaintext attack, a chosen plaintext attack and a chosen ciphertext attack. If a cryptosystem resists the chosen ciphertext attack, it can resist the remaining three attacks.
- ❑ In this algorithm is very sensitive to initial parameters and initial values, if one of them changes the sequences  $B_1, B_2, B_3, B_4$  are always different.
- ❑ In Feistel permutation and the ciphertext diffusion phase, the encrypted value is neither related to plaintext nor related to ciphertext of previous pixel.
- ❑ Thus this method resist the chosen plaintext attack or chosen ciphertext attack.



# Shortcomings

- ❑ This image encryption algorithm is limited for encryption of image of size 256 X 256.
- 




# Future Scope



- ❑ **Decryption** : The next step in the project is to implement the decryption method to decrypt the encrypted image and obtain the original image ensuring that the encryption and decryption of image is robust.
- ❑ **A user friendly web-app** : To develop a user-friendly web-app which can be used for the secure live streaming of any confidential or any high profile cases in which outsiders interference is not acceptable in any case.



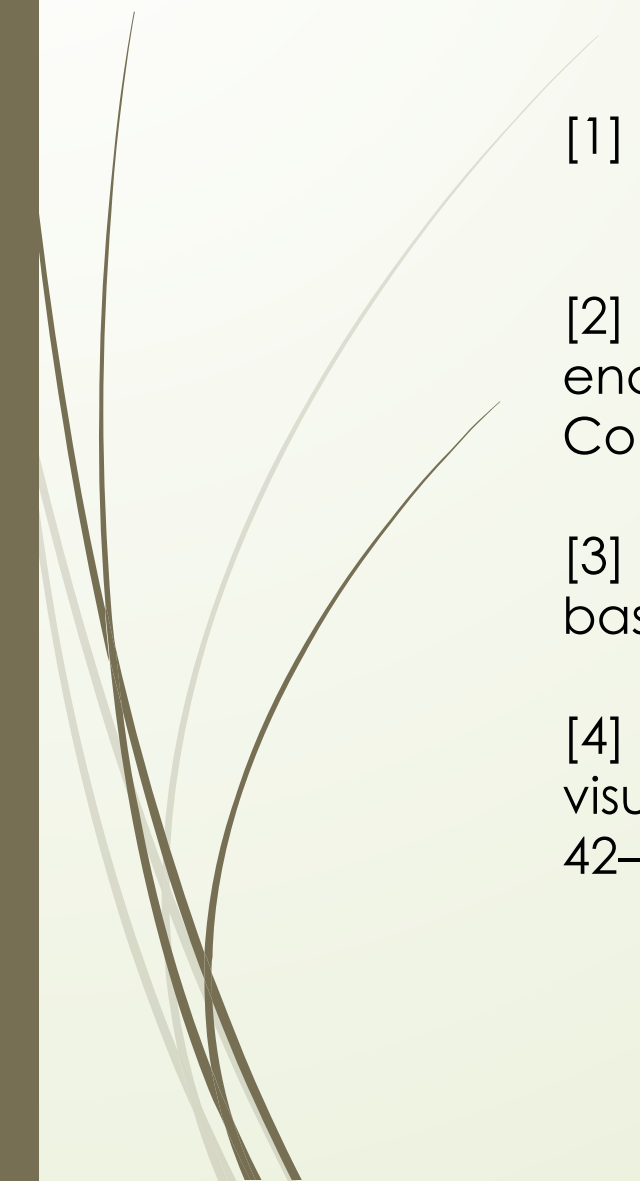
# What we learnt from this project!

- ❑ Concepts of Feistel Network and DNA encoding.
  - ❑ The implementation of image encryption in order to develop it for other specified domains like military, etc.
- 



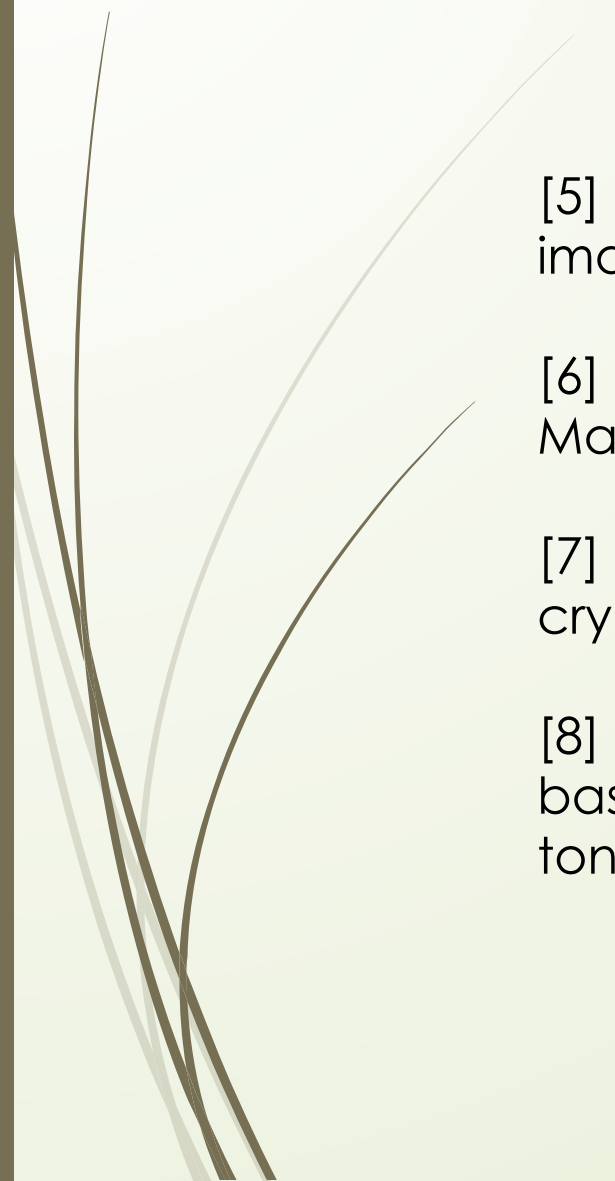


# References

- 
- [1] D. Heider, A. B. Dna-based watermarks using the dna-crypt algorithm 1–10.
  - [2] K. Pujari, G. Bhattacharjee, S. B. A hybridized model for image enr encryption through genetic algorithm and dna sequence. Procedia Computer Science 125 (2018), 165–171.
  - [3] M. R. Biswas, K. M. R. Alam, A. A. Y. M. A dna cryptographic technique based on dynamic dna encoding and asymmetric cryptosystem.
  - [4] M. T. I. Siyam, K. M. R. A., and Jami, T. A. An exploitation of visual cryptography to ensure enhanced security in several applications. 42–46.



# References

- 
- [5] Ozkaynak, F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics* 92, 2 (2018), 305–313.
  - [6] Vinyals, O. Sequence to sequence learning with neural networks. Master's thesis, Google, December 2014.
  - [7] X. Wang, S. Wang, Y. Z. C. L. A one-time pad color image cryptosystem based on sha-3 and multiple chaotic systems. 1–8.
  - [8] Xuncaizhang, Zheng Zhou, Y. N. An image encryption method based on the feistel network and dynamic dna encoding. *IEEE Photonics* 10 (2018).



***Thank You***