IMAGE ENCRYPTION AND DECYPTION

PRESENTED BY
K.SWETHA
THE KAVERY ENGINEERING COLLEGE
BE COMPUTER SCIENCE AND ENGINEERING

WHAT IS ENCRYPTION ?

- Encryption is a process which uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form.
- Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data.
- With the help of key and the algorithm we can encrypt or Decrypt the plaintext into cipher text and then cipher text back into plaintext.

WHY ENCRYPTION AND WHY IMAGE ENCRYPTION ?

- Nowadays, information security is becoming more important in data storage and transmission.
- Images are widely used in different-different processes. Therefore, the security of image data from unauthorized uses is important.
- Image encryption plays a important role in the field of information hiding.
- Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet

REQUIREMENTS OF IMAGE ENCRYPTION

- Ability to get the pixels of the original image.
- Create a strong encryption image such that it cannot be hacked easily.
- Faster encryption time such that encrypted image is transferred faster to the person.
- Perfection in the original image we obtain after decrypting it.

PROJECT DESIGN

- The ALGORITHM which is used to design IMAGE ENCRYPTION is GAUSSIAN ELIMINATION WITH PARTIAL PIVOTING AND ROW EXCHANGE.
- Each image is actually a matrix consisting of RGB and alpha values.
- The first step of the project involves extracting the matrix from the image
  - The average of RGB values is then taken (which converts the color to grayscale image) so as to get one image matrix.
  - Gaussian Elimination (and row exchanges is necessary) is then applied on the image matrix to get an upper-triangular matrix (U) which is the encrypted image matrix and the decryption key (L) is generated. The encrypted image matrix is converted back into the image, image is executed and encryption process is completes. The program waits for decryption signal.
  - As soon as the user approves decryption ,the encrypted image matrix(U) and the decryption key(L) are multiplied so as to get back the original image matrix(A).The original image matrix(A) is converted back into image(which is in grayscale),image is executed and decryption process completes.

GAUSSIAN ELIMINATION EXAMPLE

- The goal of Forward Elimination is to transform the coefficient matrix into an Upper Triangular Matrix

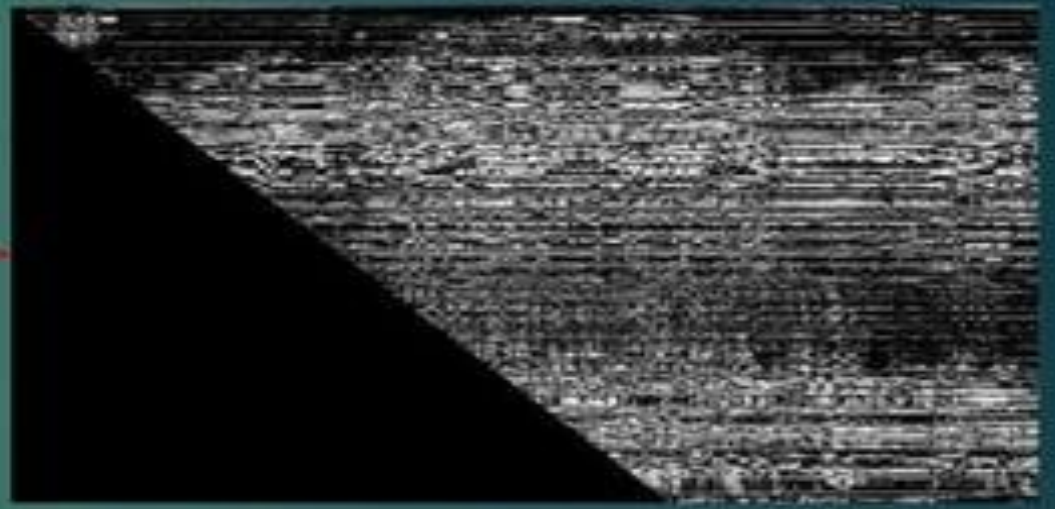
$$\begin{bmatrix} 25 & 5 & 1 \\ 64 & 8 & 1 \\ 144 & 12 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 25 & 5 & 1 \\ 0 & -4.8 & -1.56 \\ 0 & 0 & 0.7 \end{bmatrix}$$

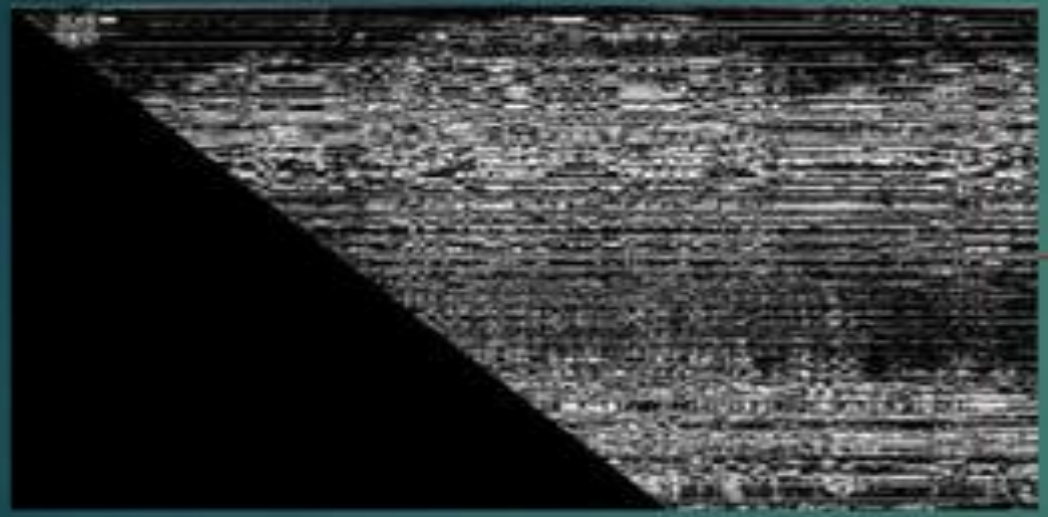
TEST CASES CONSIDERED

RESULTS AND SNAPSHOTS

CASE 1 :
BREADTH >HEIGHT

AFTER ENCRYPTION

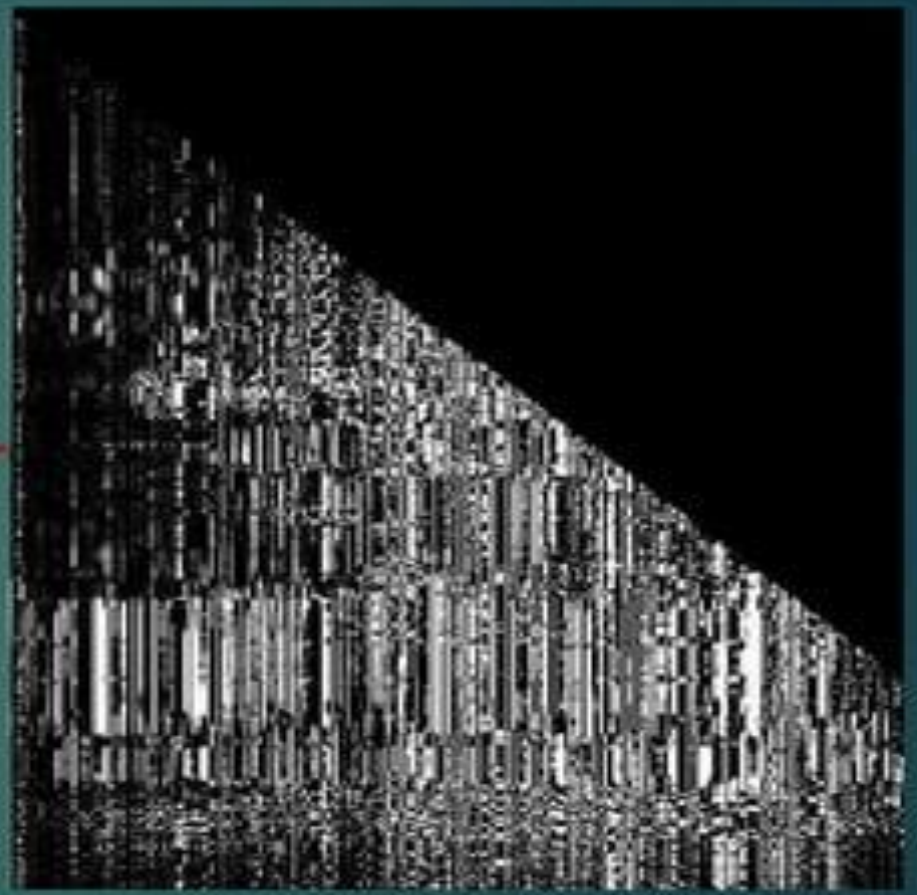




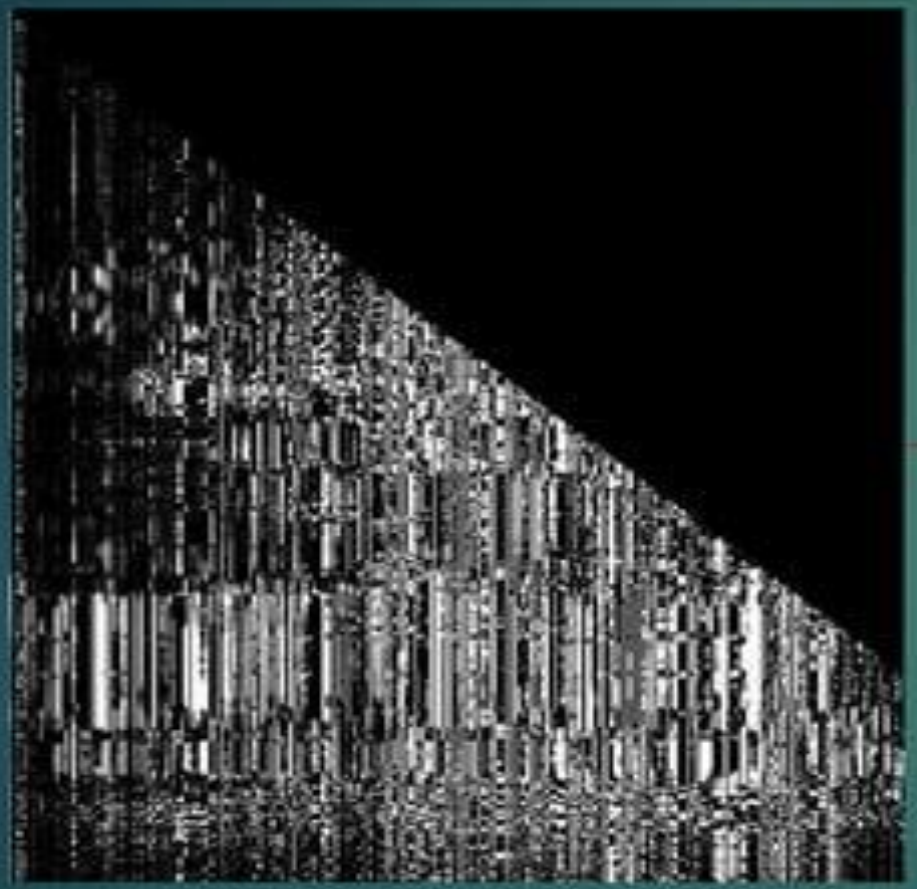
AFTER DECRYPTION

CASE 2 :
BREADTH <HEIGHT

AFTER
ENCRYPTION



CASE 2 :
BREADTH <HEIGHT



AFTER
DECRYPTION

FUTURE SCOPE OF IMPROVEMENT

We are very excited by the vast future possibilities that our project has to offer. Possible improvements include getting back the decrypted image in color. We are also looking forward to encrypt videos by extracting each frame and encrypting the images simultaneously. We know that all the videos have sound. So we are planning to encrypt frames and sound simultaneously. Finally aft achieving all of the above, we are planning to create an app which will do all of the above. With two people having the app, one will become the sender and other t receiver at a time, based on the requirements of either o the two. This is future of our project we are looking at a looking forward to implementing all of the above successfully.

ADVANTAGES AND DISADVANTAGES OF THIS ALGORITHM

ADVANTAGES :

- Simplicity: It's simpler, cheaper.
- Ratio: Encryption takes ¼ th time the decryption process takes.
- Robust: The encrypted image is hard to hack to obtain the original image.
- Pixels obtained after Gaussian elimination is fully distorted, so the key is needed to obtain original image because it's hard to crack that encrypted form.
- We have reduced time taken by encryption by smartly by updating row exchanges using another matrix. So basically it's a Space for time tradeoff.

DISADVANTAGES

- Efficiency of our algorithm is 2/3 * O(n^3).
- Decryption takes 4 times larger the time taken by Encryption.

CONCLUSION

Thus, the project entitled "Image Encryption and Decryption' was successfully completed. A complex project involving the conversion of image into matrix form, using a mathematical concept to encrypt and decrypt it, was instrumental in giving us a thorough understanding of how the concepts of ADA and Linear Algebra together can actually be implemented in the real world. By the end of the project, we have gained valuable skills including a grounding of how to interact with the operating system, file handling in java, optimizing algorithms, calculating the efficiencies, and learning how to form and manipulate images.

Thank you

T