



PES University, Bangalore

(Established under Karnataka Act No. 16 of 2013)

MAY 2020: IN SEMESTER ASSESSMENT (ISA) B.TECH. IV SEMESTER

UE18MA251- LINEAR ALGEBRA

MINI PROJECT REPORT

ON

ENCRYPTION AND DECRYPTION OF TEXTUAL AND RGB DATA USING NOVEL MATRIX OPERATIONS

Submitted by

- | | | |
|----|----------------|---------------|
| 1. | Rahil N Modi | PES1201802826 |
| 2. | Sooryanath.I.T | PES1201802827 |
| 3. | Himanshu Jain | PES1201802828 |

Branch & Section : Computer Science Engineering (CSE) & J section

PROJECT EVALUATION

(For Official Use Only)

Sl.No.	Parameter	Max Marks	Marks Awarded
1	Background & Framing of the problem	4	
2	Approach and Solution	4	
3	References	4	
4	Clarity of the concepts & Creativity	4	
5	Choice of examples and understanding of the topic	4	
6	Presentation of the work	5	
	Total	25	

Name of the Course Instructor :

Signature of the Course Instructor :

Encryption and Decryption of Textual and RGB Data using Novel Matrix Operations

Abstract—In every communication channel or medium, there has always been an inevitable necessity of secure transmission from the sender to the authentic receiver without the interference of a third party. This paper mainly discusses the novel Linear Algebraic methods to securely handle the types of data represented as images and text. The cryptography technique discussed for the RGB image is an application of Linear Transformation on Vector Space whereas, for the textual data, a Gauss-Jordan inversion technique is discussed. The process of encryption consists of an algorithm and a key. The key is the value independent of the plain text or image. The process of converting cipher text/image to its original is called Decryption. The algorithm will produce a legitimate output depending on the specific key being used at the time. Since the key is shared and remains the same in the due course of cryptography, the process is symmetric. Towards the end we draw comparison between the cryptography techniques with respect to few dominating factors.

Index Terms — Linear transformation, Symmetric key, Cryptography, Gauss Jordan inversion, Cipher object.

I. INTRODUCTION

One of the most interesting topics among researchers is cryptography which is an art of secret writing [4]. Privacy is a key term when it comes to confidential data of any organization. Passwords, bank details, medical reports, etc. are some data that require security [5]. To maintain this privacy many secure methods are implemented and the important one among them is cryptography. Encryption and decryption are the two main phases of cryptography [2]. Encryption mainly deals with obscuring information and decryption is the inverse of it. Both of them together help in the secure transmission of data.

Cryptography mainly deals with text and images which uphold the basis of any information. From the point of view of the text, the encryption deals with the transformation of plain text into cipher-text with the help of secure key(/keys) [5]. Cipher-text is considered to be the value of encryption. While decryption, on the other hand, helps in retrieving original information using a restricted set of unique operations. Depending on the secure key, encryption algorithms vary in variety. Further, the key size is directly related to the strength of encryption. More brawny keys would increase the efficiency of cryptography.

Protection of copyright and integrity of digital images has led to many relevant techniques like image hashing, watermarking, etc. [6]. The cryptography of these digital images is a challenging task due to their three-dimensional nature (red,

green, blue) very similar to 3D vector spaces.

Further, the precision and accuracy of original and decrypt images are of huge concern in particular studies like forensics, astronomy, etc. Few important standards like time, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are defined to check efficiency [6].

Cipher generating keys and its inverses in encryption and decryption form a very important application of matrices in our area of research. Concepts of Linear Algebra serve as a cornerstone to make cryptosystems simple and strong. Linear transformation of matrices (vector spaces for images) majorly helps in encoding into different suitable formats. LU decomposition and Gauss Jordan Inversion help in fetching the original information from the available encoded forms. Modulo method of generating a matrix key adds on to the list giving a tinge of flavor to existing methods. The RGB images are considered to be 3D vector spaces with red, green, blue matrices being the basis of its sub spaces. Projecting 3D images (3D vectors) to 2D images (2D vectors) using projection matrices also can be seen in image reformations [6]. Hence, a number of concepts involving matrix transforms have been dealt with in cryptography out of which few are shown in detail here.

The remaining part of the paper is categorized as follows: we have the research and review of previously existing solutions in section II, the methods and algorithms being formulated in section III, their detailed implementation with examples in section IV, informative results of implemented examples and comparison of different algorithms in section V and finally concluding with the further improvements possible in this field discussed in section VI.

II. RELATEDWORK

Matrix, as a fundamental mathematical object, is widely used in many scientific and engineering computing fields. The algorithms with fundamental matrix operations, such as Matrix Multiplication Computation (MMC), Matrix Inversion Computation (MIC), and Matrix Determinant Computation (MDC), have become an important component of modern scientific computing. We address textual and RGB image cryptography. Three security goals, namely, confidentiality, integrity, and availability are aimed to be achieved. [2] Under the modulation of a prime number, the key will be a lower triangular matrix in the encryption process, while in the decryption process the key will be the upper triangular matrix. Plain text is converted to cipher text (encrypted data). After transmitting it to the receiver, it is decrypted back to plain text.

Secrecy is maintained by a secret key, private key, and Finite state machine. It is very challenging to break the cipher text without the chosen finite state machine and proper key.

[3] Yet another and a powerful method that uses the fundamental concept of Fourier Transformation is proposed. This method is used for textual cryptography. It uses a Moore finite machine. Fourier transform will encrypt the data and inverse Fourier transform will decrypt it. The inverse Fourier transform considers a complex frequency domain function and gives a function defined in the time domain. Secrecy is kept at three levels, the secret key, the chosen Moore machine, and the Fourier Transformations. The achieved cipher text becomes relatively difficult to break even if the algorithm is known. [5] Matrix representation of linear transformation can be used to encrypt and decrypt data. Each character of the message is converted to a number and then transformed into another number. This transformation is different for each character of the message depending upon the position of a character in the sequence. Square matrix of the order of linear transformation relative to basis is generated for encryption and its inverse will be used for decryption. The security of the message increases as the basis set and linear transformation is not unique for a vector space.

[6] Color images are widely used by different users, and several applications need certain and consistent 'security in data communication and security in storing', so the need for image encryption-decryption must have a priority with the highest level. True-color image is a 3D matrix, the first dimension represents the red color, and the second one represents the green color, while the third one represents the blue color. These matrices will be used to encrypt and decrypt images. Image encryption techniques try to convert an image to another image that is hard to understand; to keep the image confidential between users. Many methods of encryption-decryption are based on matrix multiplication, if we multiply the original image matrix by a secret key then we can get the encrypted image, and if multiply the encrypted image by the key inverse we can get the decrypted original matrix. The efficient output can be expected if many iterations are performed on the image to get the key. The used method of encryption must destroy the original image in order to make it impossible to be understood by a third party or by unauthorized person.

III. METHODOLOGY

1) TEXT :

A) Mathematical definitions:

➤ Linear Transformations:

Any transformation $T(x)$ is said to be linear transformation if it satisfies the rule of linearity, that is

$$A(cx + dy) = c(Ax) + d(Ay)$$

It is represented using $T : V1 \rightarrow V2$ where $V1$ and $V2$

are vector spaces and $T(x)$ follows both additive and multiplicative properties. [7]

➤ Inverse of a matrix:

The inverse of matrix A is B if and only if $AB = I$ and $BA = I$ where I is an Identity matrix of order n . It is denoted by A^{-1} . Gauss – Jordan Inversion is a standard method to find inverse of matrix. [8]

➤ Congruence Modulo Method:

Let m be a positive integer, we say that a is congruent to $b \pmod{m}$ if m divides $(a - b)$, where a and b are integers i.e., $a - b = km$ where $k \in \mathbb{Z}$. It can be written as $a \equiv b \pmod{m}$ called congruence relation and the number m is called modulus of congruence.

Inverse of integer a to modulo m is $a^{(-1)}$ such that, $[a \cdot a^{(-1)}] \equiv 1 \pmod{m}$. [4]

B) Algorithms:

Encryption Algorithm:

1. Initially a hash table of all the characters included in encryption is randomly numbered which is unique for this problem.
2. The confidential word which is to be encrypted is taken and divided into multiple parts of fixed length say ' n ' characters.
3. Once the fixed length of each part is known then an invertible key matrix $M = [m_{ij}]_{n \times n}$ can be generated based on sender's and receiver's approval.
4. Then in each part all ' n ' characters are converted to non-negative integers using the above hash table and stored into vectors of order $n \times 1$.
5. Further these vectors are linearly transformed to another set of vectors using key matrix (M) and congruence modulo method where the modulus of congruence m is total number of characters in hash table.

$$T_1 : V_1 \rightarrow V_2 \\ \text{where } T_1 = M * (\text{mod } m)$$

6. Finally the integers in transformed vectors are converted to characters using hash table which gives the cipher (encrypted) text.

Decryption Algorithm:

1. The cipher text is transmitted on to the receiver's end while the hash table and key matrix (M) are known as was approved by him earlier.
2. Again the cipher text is divided into multiple parts of fixed length ' n ' and converted to vectors of order $n \times 1$ using

ing the hash table.

3. Now the inverse of key matrix i.e., M^{-1} is found using Gauss-Jordan or any efficient method.

4. All these vectors are linearly transformed to original set of vectors using M^{-1} matrix and congruence modulo method where m is same as considered in encryption algorithm.

$$T_2 : V_2 \rightarrow V_1$$

$$\text{where } T_2 = M^{-1} * (\text{mod } m)$$

5. Converting original set of vectors back to characters using hash table completes the decryption process and the original message is decoded successfully.

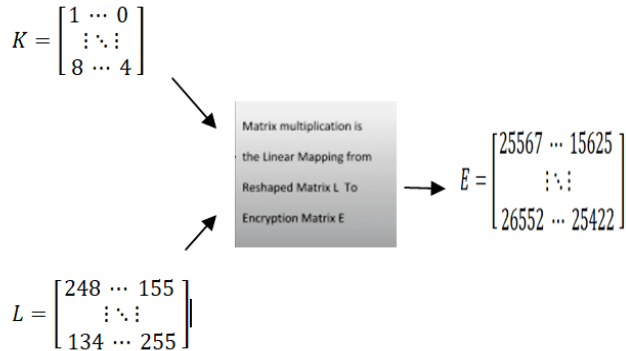
2) IMAGES:

The cryptographic algorithm is developed by using linear transformation on vector space. Here, the vector space is a reshaped into two-dimensional RGB image represented as L with dimension $(m \times n)$. A linear transformation is a linear map defined as shown below, where K is the key matrix used in the cryptosystem with dimension $(m \times m)$, K is considered as a function that maps. Every column vector in L which belongs to space R^m to another form which also belongs to the same R^m space. The linear transformation of K onto columns of L results in a new vector space E called the Encrypted matrix with dimension $(m \times n)$.

$$K : R^m \rightarrow R^m \quad (\text{A linear transformation or mapping})$$

$$K * L \rightarrow E$$

The domain of the transformation K is the columns of matrix L , whereas the columns of E constitute the range. K is always a randomly generated matrix, hence ensures security as there is no hidden pattern or periodicity in the generation of Key. The key is to be shared among the receiver and user. The encrypted matrix is then sent to the receiver of interest. The below block diagram shows the process of encryption clearly.



Encryption Algorithm:

1) Choose an image to be encrypted and store it in the form

of 3D RGB pixel data (height x width x 3)

2) Reshape the chosen image into 2D matrix of order $(m \times n)$, to make a total ordering on linear transformation and call it L .

3) Generate and load a random key matrix K of order $(m \times m)$.

4) Multiply the reshaped matrix L with the Cipher Key K , resulting in the 2D encrypted matrix E .

5) Finally, reshape the E matrix again into a 3D matrix to visualize the encrypted pixel RGB data and save the image.

Decryption Algorithm:

1) Get the encrypted 3D image E .

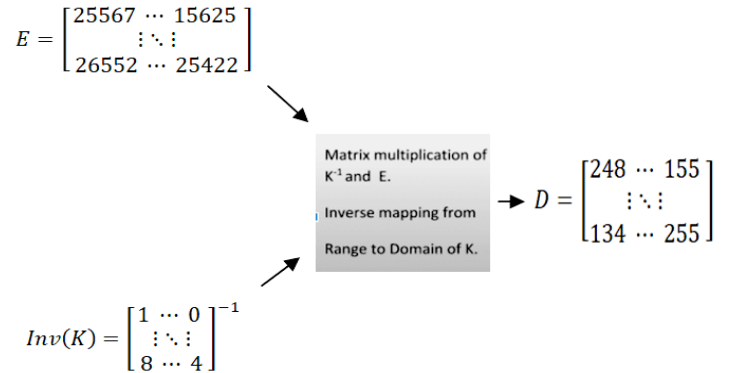
2) Reshape the 3D RGB matrix to 2D vector space.

3) Load the key K .

4) Adjust the key to suit the 2D matrix.

5) Get the decrypted 2D matrix D by applying matrix multiplication of the inverse of the Cipher Key K and 2D matrix E . This is regarded as inverse mapping.

6) Reshape the decrypted matrix D to retrieve the original input image in the pixel RGB data format.



The above procedures when followed lead to desirable results. It is to be noted that encryption and decryption time taken will drastically differ for images with different pixel representations.

We then compare the MSE(mean squared error) between the encrypted and original image and PSNR(Peak signal to noise ratio) between the decrypted and Original Image using given equations. Where I and K represent the Images to be compared, m and n represent the dimensions of the image. R represents 255, the MAX value achieved in 8 bit color scheme.

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2$$

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

We expect MSE to be of high value, which strengthens the encryption process and makes the input image and the encrypted image highly differentiable. The PSNR value is expected to be as high as possible, it's a reality check between decrypted image and the input image.

Traditional image encryption algorithms such as private key encryption standards (DES and AES), public key standards, and matrix multiplication methods may not be the most desirable candidates for image encryption, especially for fast and real-time communication applications.

Color image encryption by XORing the image with the private secret key is implemented and analyzed. A huge 3D matrix is generated which is used as a private key. This private key is adjusted to the dimensions of the 3D image matrix size. The encrypted 3D matrix is obtained by performing XOR of input image matrix and key matrix. To decrypt the image, secret key has to be kept safe and secure. On applying XOR to encrypted image matrix and key matrix, the original image is obtained.

IV. IMPLEMENTATION

1) TEXT :

A) Example for textual cryptography:

The hash table consists of 26 uppercase alphabets with an underscore (_) as an indicator of space. Hence we will have matrix modulo $m = 27$. The mapping of characters is as follows:

A	B	C	D	E	F	G	H	I
26	25	24	23	22	21	20	19	18
J	K	L	M	N	O	P	Q	R
17	16	15	14	13	12	11	10	9
S	T	U	V	W	X	Y	Z	_
8	7	6	5	4	3	2	1	0

Consider the text "**CONFIDENT**" which is to be encrypted. We divide the word into multiple parts of fixed length 3 and encode them into vectors of order 3×1 .

$$CON = \begin{bmatrix} 24 \\ 12 \\ 13 \end{bmatrix}_{3 \times 1} \quad FID = \begin{bmatrix} 21 \\ 18 \\ 23 \end{bmatrix}_{3 \times 1} \quad ENT = \begin{bmatrix} 22 \\ 13 \\ 7 \end{bmatrix}_{3 \times 1}$$

$$\text{Let the key matrix, } M = \begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}_{3 \times 3}$$

It is chosen after the approval of both sender and receiver. By Gauss-Jordan Method inverse of key matrix is

$$M^{-1} = \begin{bmatrix} -24 & 20 & -5 \\ 18 & -15 & 4 \\ 5 & -4 & 1 \end{bmatrix}_{3 \times 3} * (mod 27)$$

$$M^{-1} = \begin{bmatrix} 3 & 20 & 22 \\ 18 & 12 & 4 \\ 5 & 23 & 1 \end{bmatrix}_{3 \times 3}$$

Now the vectors are linearly transformed to another set of vectors called cipher vectors.

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}_{3 \times 3} * \begin{bmatrix} 24 \\ 12 \\ 13 \end{bmatrix}_{3 \times 1} = \begin{bmatrix} 89 \\ 138 \\ 120 \end{bmatrix}_{3 \times 1} * (mod 27) = \begin{bmatrix} 8 \\ 3 \\ 12 \end{bmatrix}_{3 \times 1}$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}_{3 \times 3} * \begin{bmatrix} 21 \\ 18 \\ 23 \end{bmatrix}_{3 \times 1} = \begin{bmatrix} 136 \\ 198 \\ 135 \end{bmatrix}_{3 \times 1} * (mod 27) = \begin{bmatrix} 1 \\ 9 \\ 0 \end{bmatrix}_{3 \times 1}$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}_{3 \times 3} * \begin{bmatrix} 22 \\ 13 \\ 7 \end{bmatrix}_{3 \times 1} = \begin{bmatrix} 57 \\ 99 \\ 135 \end{bmatrix}_{3 \times 1} * (mod 27) = \begin{bmatrix} 3 \\ 18 \\ 10 \end{bmatrix}_{3 \times 1}$$

By using hash table,

$$\begin{bmatrix} 8 \\ 3 \\ 12 \end{bmatrix}_{3 \times 1} = SXO \begin{bmatrix} 1 \\ 9 \\ 0 \end{bmatrix}_{3 \times 1} = ZR_ \begin{bmatrix} 3 \\ 18 \\ 10 \end{bmatrix}_{3 \times 1} = XIQ$$

Therefore, the cipher text (encoded message) is "**SXOZR_XIQ**".

Cipher text is normally transmitted while the hash table and key matrix is known to the receiver as he had approved for it. On receiver end the text can be decrypted by transforming it back to original matrices.

Therefore by using hash table,

$$SXO = \begin{bmatrix} 8 \\ 3 \\ 12 \end{bmatrix}_{3 \times 1} \quad ZR_ = \begin{bmatrix} 1 \\ 9 \\ 0 \end{bmatrix}_{3 \times 1} \quad XIQ = \begin{bmatrix} 3 \\ 18 \\ 10 \end{bmatrix}_{3 \times 1}$$

Transforming the matrices using M^{-1} gives the original message.

$$\begin{bmatrix} 3 & 20 & 22 \\ 18 & 12 & 4 \\ 5 & 23 & 1 \end{bmatrix}_{3 \times 3} * \begin{bmatrix} 8 \\ 3 \\ 12 \end{bmatrix}_{3 \times 1} = \begin{bmatrix} 348 \\ 228 \\ 121 \end{bmatrix}_{3 \times 1} * (mod 27) = \begin{bmatrix} 24 \\ 12 \\ 13 \end{bmatrix}_{3 \times 1}$$

$$\begin{bmatrix} 3 & 20 & 22 \\ 18 & 12 & 4 \\ 5 & 23 & 1 \end{bmatrix}_{3 \times 3} * \begin{bmatrix} 1 \\ 9 \\ 0 \end{bmatrix}_{3 \times 1} = \begin{bmatrix} 183 \\ 126 \\ 212 \end{bmatrix}_{3 \times 1} * (mod\ 27)$$

$$= \begin{bmatrix} 21 \\ 18 \\ 23 \end{bmatrix}_{3 \times 1}$$

$$\begin{bmatrix} 3 & 20 & 22 \\ 18 & 12 & 4 \\ 5 & 23 & 1 \end{bmatrix}_{3 \times 3} * \begin{bmatrix} 3 \\ 18 \\ 10 \end{bmatrix}_{3 \times 1} = \begin{bmatrix} 589 \\ 310 \\ 439 \end{bmatrix}_{3 \times 1} * (mod\ 27)$$

$$= \begin{bmatrix} 22 \\ 13 \\ 7 \end{bmatrix}_{3 \times 1}$$

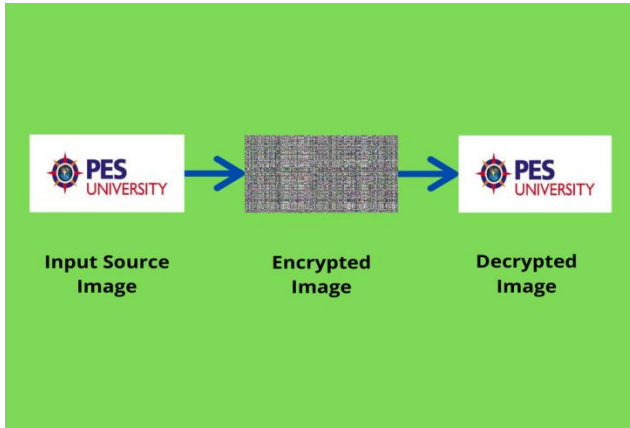
Finally using hash table,

$$\begin{bmatrix} 24 \\ 12 \\ 13 \end{bmatrix}_{3 \times 1} = CON \begin{bmatrix} 21 \\ 18 \\ 23 \end{bmatrix}_{3 \times 1} = FID \begin{bmatrix} 22 \\ 13 \\ 7 \end{bmatrix}_{3 \times 1} = ENT$$

Therefore, finally the decoded message is "**CONFIDENT**". Thus the confidential word remains same without any changes when transmitted from sender to receiver.

2) IMAGES:

An Image to be sent to the receiver is loaded into the 3D array of dimensions (height *width *pixels). As matrix operations cannot be applied onto a 3D array component, we reshape the input RGB data in to a $(m \times n)$ matrix for further matrix transforms. The reshaped matrix is stored as L. Generate a Random Cipher key matrix K of dimension $(m \times m)$ containing integers, adopt the functionalities of Random library to generate K, share the K matrix with the receiver.



The input source image is reshaped into 2D matrix:

$$L = \begin{bmatrix} 244 & \dots & 248 \\ \vdots & \ddots & \vdots \\ 247 & \dots & 248 \end{bmatrix}$$

Cipher Key Matrix Generated Randomly:

$$K = \begin{bmatrix} 1 & \dots & 2 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{bmatrix}$$

The RGB data is now distributed among the cells of K. As a result of matrix multiplication, we obtain a 2D encrypted matrix E, which is further reshaped into RGB format to obtain the Real Encrypted 3D image.

It has the same pixel dimensions as that of Source image, but the RGB value at every pixel is encrypted into a new value. Store this in a matrix E.

Now reshape the color Matrix E into a 2D matrix. With the help of the shared key, we generate its inverse K^{-1} . We multiply K^{-1} with Encryption matrix to obtain the decryption matrix, which retrieved the source image that was transmitted via encryption. The decrypted image is shown below.

To measure the efficiency and the strength of encryption, we find the values of MSE and PSNR between the original, encrypted and decrypted images.




V. RESULTS

There is no such quantitative measure to check textual cryptography as the decoded message is same as original message. But the algorithm being used can be checked for its efficiency. Asymptotic analysis of algorithms is the best way by which different algorithms can be compared in terms of time and space complexities. In hashing table, characters are mapped to integers in $O(1)$ time complexity and as the message is divided into multiple parts the linear transformation of those vectors can be independently carried out in $O(n)$ time complexity. Here, original message is taken in the form of multiple column vectors so that more of parallel code is generated which in-turn reduces time by Amdahl's law. The only part which takes maximum time i.e., $O(n^3)$ time complexity is calculating the inverse of key matrix using Gauss-Jordan Method. This can be improvised by using Le Gall matrix multiplication algorithm which can be used to find inverse of matrix in $O(n^{2.37286})$ time complexity. Further, the key matrix takes n^2 of space and n column vectors with order $n \times 1$ takes another n^2 of space in encryption, same is seen in decryption. Asymptotically, $O(n^3)$ is the time complexity and $O(n^2)$ is the space complexity for this algorithm. There is a hope for improvement if the inversion algorithm is modified.

Experimental tests have been carried out with detailed numerical analysis which demonstrates the robustness of the proposed algorithm against several types of attacks such as statistical and differential attacks (visual testing). Moreover, performance assessment tests demonstrate that the proposed image encryption algorithm is highly secure. It is also capable of fast encryption/decryption which is suitable for real-time Internet encryption and transmission applications.

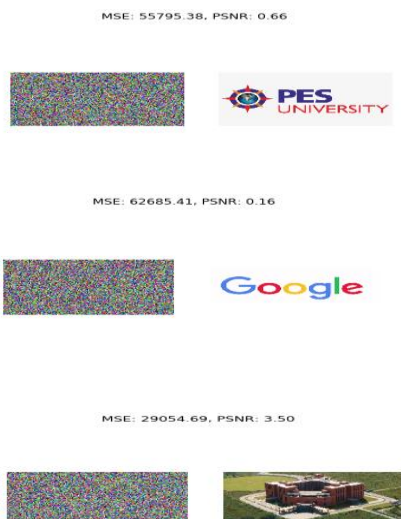
Color image encryption by applying XORing operation between the image blocks with a private secret key is a time-efficient method as reflected in the experimental results. But when we look at the security of the secret key, it is the same in both cases. Matrix multiplication operations are costly but due to advancements in computational power, we can achieve good results based on multiple iterations of the algorithm and secure key generation scheme. The efficiency and performance of the method are analyzed using python.

These are the results from images and the time taken for encryption and decryption.

Image	Matrix Multiplication Method Execution Time	XOR Method Execution Time
	0.6695	0.2484
	1.2341	0.1002
	1.1366	0.106

From this table, we can see that the proposed method gave the best efficiency parameters by decreasing both the encryption-decryption times.

Peak signal to noise ratio (PSNR) and mean square error (MSE) are used to comparing the squared error between the original image and the reconstructed image. There is an inverse relationship between PSNR and MSE. The higher PSNR values indicate that the encrypted image is similar to the original image. For a good encryption scheme, the PSNR should be as low as possible. Hence, the Mean Square Error needs to be high for encrypted images.



VI. CONCLUSION

The above used algorithm for text cryptography secures the transmitted message by using linear transformation and column vectors. As there can be different possible combination of column vectors the secrecy is maintained. The key matrix, hash table and column vectors together make up the whole process of cryptography. Further, this process can be improved by using Le Gall matrix multiplication algorithm to efficiently find the inverse of key matrix. As the key matrix size increases the strength of secrecy too increases, hence in future we can generate very big symmetric and asymmetric key matrices to encrypt messages.

It can be seen from the results that the proposed methods are highly efficient and can be used in real-world applications. The performance parameters in terms of MSE and PSNR values have been evaluated for all the images. A low signal to noise ratio indicates high loss to the original image quality, which is a characteristic of all the test images in this research work. The perceptibility and image quality after decryption for colored images was found to be excellent and no trails of image modification are evidently visible. The MSE and PSNR have been evaluated which give a mathematical analysis of the research work.

Future work in this direction could be exploiting other ways to improve the utilization of public images for secure communication. The encryption and decryption technique proposed can be used as a robust data hiding technique, if the number of bits to decrypt the message is further reduced. Future work also includes implementing the proposed stream encryption algorithms in hardware to test its speed.

REFERENCES

1. Zhang, S., Tian, C., Zhang, H., Yu, J., & Li, F. (2019). Practical and secure outsourcing algorithms of matrix operations based on a novel matrix encryption method. *IEEE Access*, 7, 53823-53838.
2. Mittal, A., & Gupta, R. K. ENCRYPTION AND DECRYPTION SCHEME INVOLVING FINITE STATE MACHINE AND LU DECOMPOSITION.
3. Mittal, A., & Gupta, R. K. An Encryption Method Involving Fourier Transform And Moore Machine
4. Vinothkumar, L., & Balaji, V. (2019). Encryption and Decryption Technique Using Matrix Theory. *Journal of Computational Mathematics*, 3(2), 1-7.
5. Gupta, R. K. (2019). Encryption Technique using Matrix Representation of Linear Transformation. *Journal of the Gujarat Research Society*, 21(8), 1186-1190.
6. Rasras, Rashad & Abuzalata, Mohammed & Alqadi, Ziad & Al-Azzeh, Jamil & Jaber, Qazem. (2019). Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation. 8. 14-26.
7. Linear Algebra and its applications, David C Lay, Addison-Wesley Publication Company, 3rd Edition, 2002.
8. Linear Algebra and its applications, Gilbert Strang, illustrated, Thomson, Brooks/Cole, 2006.