International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 08 | Aug 2020 www.irjet.net p-ISSN: 2395-0072

Cryptography and Image Processing by Matrices

Mr. Sawant Laxman S.[1], Mr. Patil Shankar A.[2]

[1,2]*Department of Mathematics DKTE Textile and Engg. Institute Ichalkaranji, Maharashtra, India*

Abstract: Modern cryptography exists at the intersection of the disciplines of Mathematics, Computer Science, Electrical Engineering and Communication Science. Applications of Cryptography includes Electronic Commerce, chip based payment cards, digital currencies, computer passwords and military communications. The cryptography literature often uses the name "Alice"(A) for the sender, "Bob"(B) for the intended recipient, and "Eve"(eavesdropper) for the adversary. Modern cryptography is heavily based on Mathematical Theory and Computer Science practice. One discipline that is sometimes used in Cryptography is Linear Algebra. One method of encryption by using Linear Algebra, specifically Matrix operations. Also in Image processing there is widely uses matrices and matrix operations

Keywords: *Image compression, linear algebra, matrix, linear transformation, jpeg technique, Cryptography, Congruence, Decrypt, Encrypt, Invertible matrices, Matrix Multiplication.*

I. INTRODUCTION

Cryptology is defined as the science of making communication incomprehensible to all people except those who have right to read and understand it Also defines cryptography as the study of mathematical techniques related to aspect of information security such as confidentiality, data integrity, entry authentication and data origin authentication Cryptography, the art of encryption and decryption , plays a major part in cellular communications, such as e-commerce, computer password, pay- TV, sending emails, ATM card, security, transmitting funds, and digital signatures. Nowadays, cryptography is considered as a branch of computer science as well as mathematics. At present time cryptography is usually classified into two major categories, symmetric and asymmetric. In symmetric cryptography, the sender and receiver both use the same key for encryption and decryption while in asymmetric cryptography, two different key are used. Both of these cryptosystems have their own advantage and disadvantages.

In 1989, Joint Photographic Experts Group, known as JPEG, discuss and standard image compression method to minimize data usage in image storing because most computers that day weren't capable of handling image files, which are quite large. Hence, they form a universal standard to ease data handling since different these data needed to be interchangeable. In 1991, the chairman of JPEG, Gregory Wallace, published a paper outlining their compression standard. This compression standard was then adopted in 1994, and became so widespread that it is even used today. The reason for its success is simple. This compression standard by JPEG, allows large data to be compressed down to a much smaller size, while maintaining its quality. In Image Processing well known JPEG based on DCT is lossy compression techniques with relatively high compression ratio which is done by exploiting human eye perception. JPEG is a commonly used compression standard and has been widely used in the Internet and other applications. JPEG compression is the most popular scheme for image compression nowadays.

II. Application of matrices in cryptogyphy

At present time cryptography is usually classified into two major categories, symmetric and asymmetric. In symmetric cryptography, the sender and receiver both use the same key for encryption and decryption while in asymmetric cryptography, two different key are used. Both of these cryptosystems have their own advantage and disadvantages.

Cryptography system was invented in 1929 by an American mathematician, Lester S. Hill. The idea of Hill Cipher, assigning a numerical value to each letter of the words, in English Language we have 26 alphabets, therefore Hill work on modulo 26, for more information see. The study of cryptology consist of two parts: cryptography, concerns with the secrecy system and its design and cryptanalysis concerns with the breaking of the secrecy system above. Most of us associate cryptography with the military war and secret agents. Indeed these areas have seen extensive use of cryptography but not limited.

A cryptogram is a message written according to a secret code. Below, I will illustrate one method of using matrix multiplication to **encode** and **decode** a message.Being by assigning a number to each latter in the alphabet (0 assigned to a blank space) as follows,

0	1	2	3	4	5	6	7	8	9
-	A	B	C	D	E	F	G	H	I

10	11	12	13	14	15	16	17	18	19
J	K	L	M	N	O	P	Q	R	S

20	21	22	23	24	25	26
T	U	V	W	X	Y	Z

The the message is converted into numbers and partitioned into uncoded row matrices, each have n entries.

For example, let's write the uncoded row matrices of size 1×3 for the message MEET ME MONDAY. The matrices can be 1×n. I choose n=3 for convenience. See how it is done below.

[13 5 5] [20 0 13] [5 0 13] [15 14 4] [1 25 0]

M E E T - M E - M O N D A Y -

Notice the blank space at the end is to fill out the last uncoded row matrix.

To encode the message, choose an n×n invertible matrix A and multiply the uncoded row matrices by A to obtain coded row matrices. Let's use the invertible matrix $A=\begin{bmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{bmatrix}$ to encode the message" MEET ME MONDAY".

Uncoded Encoded Coded row

Row Matrix Matrix A Matrix

$$[13\ 5\ 5]\begin{bmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{bmatrix} = [\ 13\ -26\ 21\ ]$$

$$[\ 20\ 0\ 13\ ]\begin{bmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{bmatrix} = [\ 33\ -53\ -12\ ]$$

$$[\ 5\ 0\ 13\ ]\begin{bmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{bmatrix} = [\ 18\ -23\ -42\ ]$$

$$[\ 15\ 14\ 4\ ]\begin{bmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{bmatrix} = [\ 5\ -20\ 56\ ]$$

$$[\ 1\ 25\ 0\ ]\begin{bmatrix}1 & -2 & 2\\ -1 & 1 & 3\\ 1 & -1 & -4\end{bmatrix} = [\ -24\ 23\ 77]$$

The sequence of coded row matrices is [13 -26 21] [33 -53 -12] [18 -23 -42] [5 -20 56] [-24 23 77].

Finally, removing the brackets produce the cryptogram below,

13 -26 21 33 -53 -12 18 -23 -42 5 -20 56 -24 23 77

For those that do not know matrix A, decoding the cryptogram is difficult. But for an authorized receiver who knows the matrix A, decoding is simple. The receiver need only multiply the coded row matrices by A^{-1} (known as the decoding matrix) to retrieve the uncoded row matrices.

That is if (uncoded row matrix)*(encoded matrix A) = (coded row matrix),

then

(Coded row matrix)*(decoding matrix A^{-1}) = (decoded row matrix)

Now here the decoding matrix $A^{-1}=\begin{bmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{bmatrix}$

Therefore performing above operation on each coded row matrix, we get

$$[\ 13\ -26\ 21\ ]\begin{bmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{bmatrix} = [\ 13\ 5\ 5\ ]$$

$$[\ 33\ -53\ -12\ ]\begin{bmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{bmatrix} = [\ 20\ 0\ 13\ ]$$

$$[\ 18\ -23\ -42\ ]\begin{bmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{bmatrix} = [\ 5\ 0\ 13\ ]$$

$$[\ 5\ -20\ 56\ ]\begin{bmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{bmatrix} = [\ 15\ 14\ 4\ ]$$

$$[\ -24\ 23\ 77]\begin{bmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{bmatrix} = [\ 1\ 25\ 0\ ]$$

The sequence of decoded row matrices is [13 5 5] [20 0 13] [5 0 13] [15 14 4] [1 25 0].

Finally, removing the brackets produce the decoded sequence is

13 5 5 20 0 13 5 0 13 15 14 4 1 25 0

M E E T - M E - M O N D A Y -

This is the complete procedure to uncode and decode the any type of information which is very confidential by using matrices and inverse if matrices, Also to increase the complexity of decoding we use rotation of matrices as well as transpose of matrices.

III. APPLICATIONS OF MATRICES IN IMAGE PROCESSING

- **Image compression**

Image compression is the process of minimizing down the size of an image with minimum damage to the quality of the image. The minimized image allows for easier access, storage, and transport. Image compression technique may be lossy or lossless. Lossless image compression compresses an image without introducing errors, thus retaining the image information. Lossless compression is generally used in compressing text files and program files because a single error may prove fatal in a program, On the other hand, lossy image compression compacts an image while losing information during the compression. Though it may seem true, lossless compression is not always suitable for every image compression. Lossy compression results in better compression due to its nature of "losing" useless information. This compression method is generally used in JPEG compression because the discarded information are mostly imperceptible to human eyes, thus retaining the quality visually.

- **Matrix as an Image**

An image can be represented by using matrices. For example, a Felix the cat image as follows.

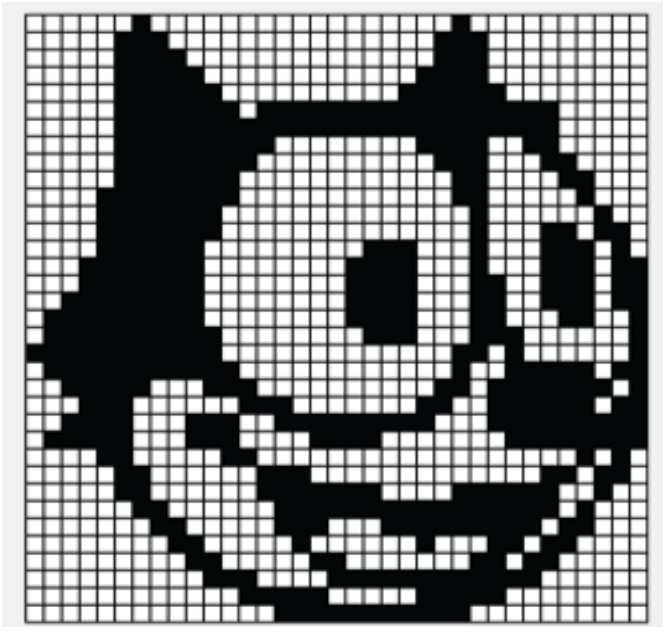

Fig. 3.1(a): Felix image of Cat

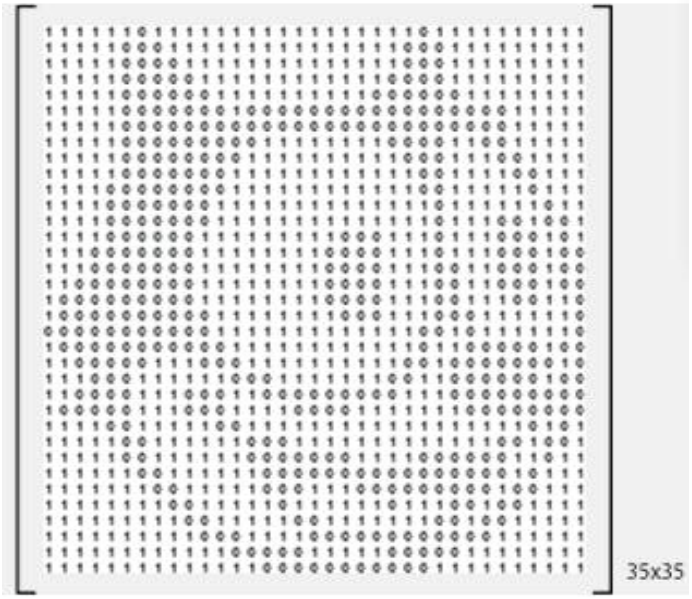

Fig. 3.1(b): Matrix corresponding to Felix the Cat

Figure 3.1(a-b) shows an example of an image represented by a matrix. Each element in the matrix corresponds to each pixel in the image, a 0 indicating black and 1 indicating white. This type of image, that only uses two colors are called boolean images or binary images. A grayscale image, may also be represented with a matrix, with each element corresponding with the image shows the intensity of the pixel. The data in each pixel usually uses an integer to represent the intensity, with 0 as black and 255 as white, allowing one to use 256 different shades of gray. On the other hand, colored images, also known as true color, can be represented with three or more matrices, depending on its coloring system. A few coloring system are known to computers today, with RGB and CMYK the most generally used.

An RGB image are represented with three matrices. Each matrix represent one shades of color, with red, green, and blue respectively. Similar to a grayscale image matrix, each RGB image matrix element are represented with an integer number from 0 to 255. To construct the image, the three matrix will then overlap each other to represent a color.

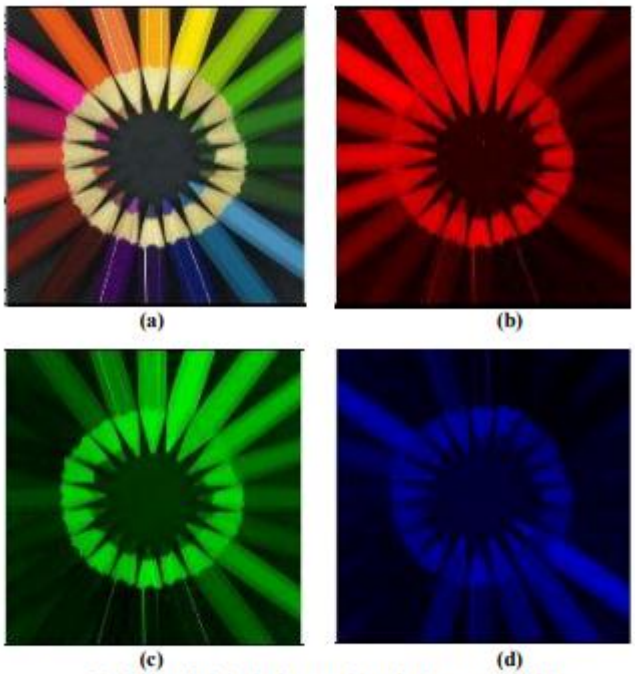

Fig 3.2 (a) Original picture, (b) red, (c) green, (d) blue components

Therefore, in RGB system, a single pixel can be represented with 2563 = 16777216 colors.

- **Image Processing**

After an image are represented with matrices, it is possible to operate the image into several transformation. For example, consider the following figure

Fig 3.3 (a) Original image, (b) transposed image, (c) reflected image

In figure 2.3, a binary image of Felix the cat (a) can be transposed into (b). While the image (c) is the reflected image of (a). Let C be the matrix of image (c) and A be the matrix of image (a), thus Cij = Ai,35-j+1, allowing the image to be reflected by the vertical axis.

IV. CONCLUSION

Matrices are well known tool for storage of huge data. In this paper, many of the important encryption techniques have been presented in order to make familiar with the various encryption schemes used in encrypting the data using different matrices. Every scheme has advantages and disadvantages based on their techniques which are mainly based on finding the inverse of key matrix. Image compression is one of the first acknowledge image compression method. This method is ideal for storing images that does not heavily rely on its precision and unimportant information, and not recommended for use in medical sector and/or technical drawings. This type of compression is considered lossy compression, thus suitable for photographs.

V. REFERENCES

[1] Khan F. H., Shams R., "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix", International Journal of Innovative Science and Modern Engineering (IJISME), Volume-3 Issue-3, 2015.

[2] Gomes, J.; Velho, L. Image Processing for Computer Graphics and Vision. Springer-Verlag, 2008.

[3] Gonzalez, R. C.; Woods, R. E. Digital Image Processing. Third Edition. Prentice Hall, 2007

[4] Impact of Quantization Matrix on the Performance of JPEG, Mr.S. V. Viraktamath, and Dr. Girish V. Attimarad International Journal of Future Generation Communication and Networking Vol. 4, No. 3, September, 2011

[5] Rick A. Vander Kam, Ping Wah Wong, "Customized JPEG Compression for Grayscale Printing", 1068-031U94 $3.00 0 1994 IEEE.

[6] A, Nectoux. Matrices and Digital Images. Retrieved on 14 December 2015. From Klein Project Blog: http://blog.kleinproject.org/?p=588.

[7] Application of Matrix in Image Compression by Vitra Chandra, Makalah IF2123 Aljabar Geometri – Informatika ITB –Semester I Tahun 2015/2016

[8] Application of Non-Singular Matrices in Encryption and Decryption text of Cryptography by Babita Bist Ramola, IJRASET, Volume 4 Issue IV, April 2016 IC Value: 13.98 ISSN: 2321-9653

[9] Raja P. V K., Chakravarthy A. S. N., "a cryptosystem based on Hilbert matrix using cipher block chaining mode", International Journal of Mathematics Trends and Technology, Issue 2011

[10] S, Franco. T, Prince. I, Salva. C, Windolf. Mathematics behind Image Compression. Journal of Student Research. 2014.

[11] S, Venna. J, Krishna. Image Compression and Linear Algebra. 15 Nov. 2013.

[12] Using Matrix Method for the Application of Graph Theory to Electrical Circuits by Poorva V. Adhyapak, IOSR Journal of Mathematics (IOSR-JM) e-ISSN: 2278-5728, p-ISSN:2319-765X. Volume 15,Issue 5