DESIGN OF AES BASED AUTHENTICATED ENCRYPTIONS FOR IMAGES

PROJECT REPORT

Submitted by

DEVI PRIYAA M R **(18BEC016)**

DIVYA T **(18BEC106)**

VIDHYA SRI S **(18BEC107)**

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

Dr. MAHALINGAM COLLEGE OF ENGINEERING AND TECHNOLOGY

An Autonomous Institution

Affiliated to ANNA UNIVERSITY

CHENNAI – 600 025

MAY 2022

Dr. MAHALINGAM COLLEGE OF ENGINEERING AND TECHNOLOGY, POLLACHI -642 003

(An Autonomous Institution Affiliated to Anna University, Chennai - 600 025)

BONAFIDE CERTIFICATE

Certified that this project report titled **"Design of AES Based Authenticated Encryptions for Images"** is the bonafide work of

DEVI PRIYAA M R	**(18BEC016)**
DIVYA T	**(18BEC106)**
VIDHYA SRI S	**(18BEC107)**

who carried out the project work under my supervision

_____ _____

Dr R. SUDHAKAR M.E., Ph.D.,
PROFESSOR AND HEAD
Department of ECE
Dr. Mahalingam college of
Engineering and technology
Pollachi – 642003

Dr S. BHARATHI M.E., Ph.D.,
SUPERVISOR
Assistant Professor (SG)
Department of ECE
Dr. Mahalingam college of
Engineering and technology
Pollachi – 642003

Submitted for the autonomous End Semester Innovative and Creative Project Viva- Voce Examination held on _____

INTERNAL EXAMINER-I INTERNAL EXAMINER - II

ABSTRACT

In communication security, information is very important. Data confidentiality is a priority so that maintaining the information security needs an application that can encrypt the data. Retrieving the relevant images from the database by using feature vector is the challenging and important task. It is also need to retrieve the images from variety of the domain that is the application of CBIR that domains are medicine, crime prevention, Biometrics, architecture, Fashion and publishing. This paper present the method developed to search and retrieve the similar image using bit plane image. Bit plane images are formed by using threshold and using bit plane slicing. Mean, standard deviation and third moment of row and column pixel distribution of bit plane image is used as a feature vector. One of the methods used to design a data security application is cryptography, in which there are many methods can be used to encrypt a data. However, the best method is Advanced Encryption Standard method (AES). There are many types of AES that can be used but the most effective is AES-128. So, the aim of this study is to design image cryptographic application using the AES-128 method. Process of design applications with this method is through several stages, such as process of encryption, decryption, key generation, and testing of the methods used. The attacks test is given by cropping, blurring, and enhancing the ciphertext image. In previous studies, there was never been an attack on the results of ciphertext, so this study will be accompanied by testing of attacks on ciphertext to determine the resistance of the method used. From the result of encryption and decryption, it is known that this AES128 method was successfully applied to the image. While on the attack test, it was found that this method is resistant to cropping attacks, but not resistant to blurring and enhancement attacks.

ACKNOWLEDGMENT

We wish to express our sincere thanks to all who have contributed to do this project through their support, encouragement, and guidance.

We extend our gratitude to our management for having provided us with all facilities to build my project successfully. We express our sincere thanks to our honourable Secretary, **Dr. C. Ramaswamy, M.E., Ph.D., F.I.V.**, for providing the required amenities. We take this opportunity to express our deepest gratitude to our principal **Dr. A. Rathinavelu, M.Tech., Ph.D.**, who provide suitable environment to carry out the project.

We express our extreme gratefulness to **Dr. R. Sudhakar, M.E., Ph.D.**, professor and Head of the department of Electronics and Communication Engineering, for his constant support and encouragement.

We wish to express our deep sense of gratitude and thankfulness to our project guide **Dr S. Bharathi M.E., Ph.D.,** for her valuable suggestion and guidance offered during the course of the project.

We take this opportunity to express our sincere thanks to our project coordinator **Dr.K. Mohaideen Abdul Kadhar, M.Tech., Ph.D.,** for his valuable help and encouragement in developing and completing this project. Finally, we committed to place our heartfelt thanks to all those who had contributed directly and indirectly towards the success of the completion of this project.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

Nowadays usage of digital image is widely found and due to usage of the network, the security of image is highly threatened. So, the image encryption becomes the most effective way to secured transmit security of images. Image data security is the essential portion in communication and multimedia world. During storing and sharing, third party access of data is one of the challenging task. Providing security of data is the clever work. Many protection algorithms are used in recent years. Protection may be given by a data which will be converting the original into some unknown form, signals, sketch etc., which will be not understand by anyone. Cryptography is the best technique of image data security. In Greek, crypto refers hidden and graph refers script. Cryptography has two processes namely encryption and decryption. Encryption achieves the conversion by possessing a key of original data into unreadable form called encoding. Restoring of encrypted data into original is decoding or decryption. Key, code, or password is the vital role in cryptography. This paper presents the performance of encryption and decryption of an image using AES algorithm and tested on image and results are shown.

Security of image data has become increasingly important for many applications like video conferencing secure facsimile, medical, military applications etc. It is hard to prevent unauthorized people from eavesdropping in any communication system including internet. Cryptography provides a method for securing an

authenticating the transmission of information over insecure channels. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. Thus, image information transmission has increased rapidly, and image encryption technology has drawn more attention. Images are generally the collection of pixels. Encryption (sometimes called as Encipherment) is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment).With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Transmission of sensitive data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity, and non- reproduction of exchanged information.

1.1CRYPTOGRAPHY

Cryptography is the method of using mathematics to encrypt and decrypt data. It enables us to store sensitive information or transmit across insecure networks, so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data cryptanalysis is the method of analysing and breaking secure communication. Classical cryptanalysis invokes an interesting combination of analytical reasoning, application of mathematical tools, determination, and luck. Cryptanalysis also called as attackers. Cryptology embraces both cryptography and cryptanalysis. Cryptography can be strong or weak, its strength is measured in the time and resources, and it would require recovering the plaintext. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. A cryptographic algorithm is a mathematical function used in the encryption and

decryption process. It works in the combination with a key-a word, number, or face- to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is thus entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. Cryptography includes the following process such as Encryption and Decryption.

1.2 AES ALGORITHM

1.2.1 AES Encryption and Decryption

For each round of AES, 128bit input data and 128-bit key is required i.e., it needs 4 words of key in one round thus the input key must be expanded to the required number of words depending upon the number of rounds. The output of each round serves as input to the next stage. In AES system, same secret key is used for both encryption and decryption, thus simplifies the design. For both its cipher and inverse cipher, the AES algorithm uses a round function i.e., composed from four different byte-oriented transformations:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The above four transformations are looped Nr-1 times. In the last round Mix column is not performed.

The tenth round Mix columns stage is not included. The nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

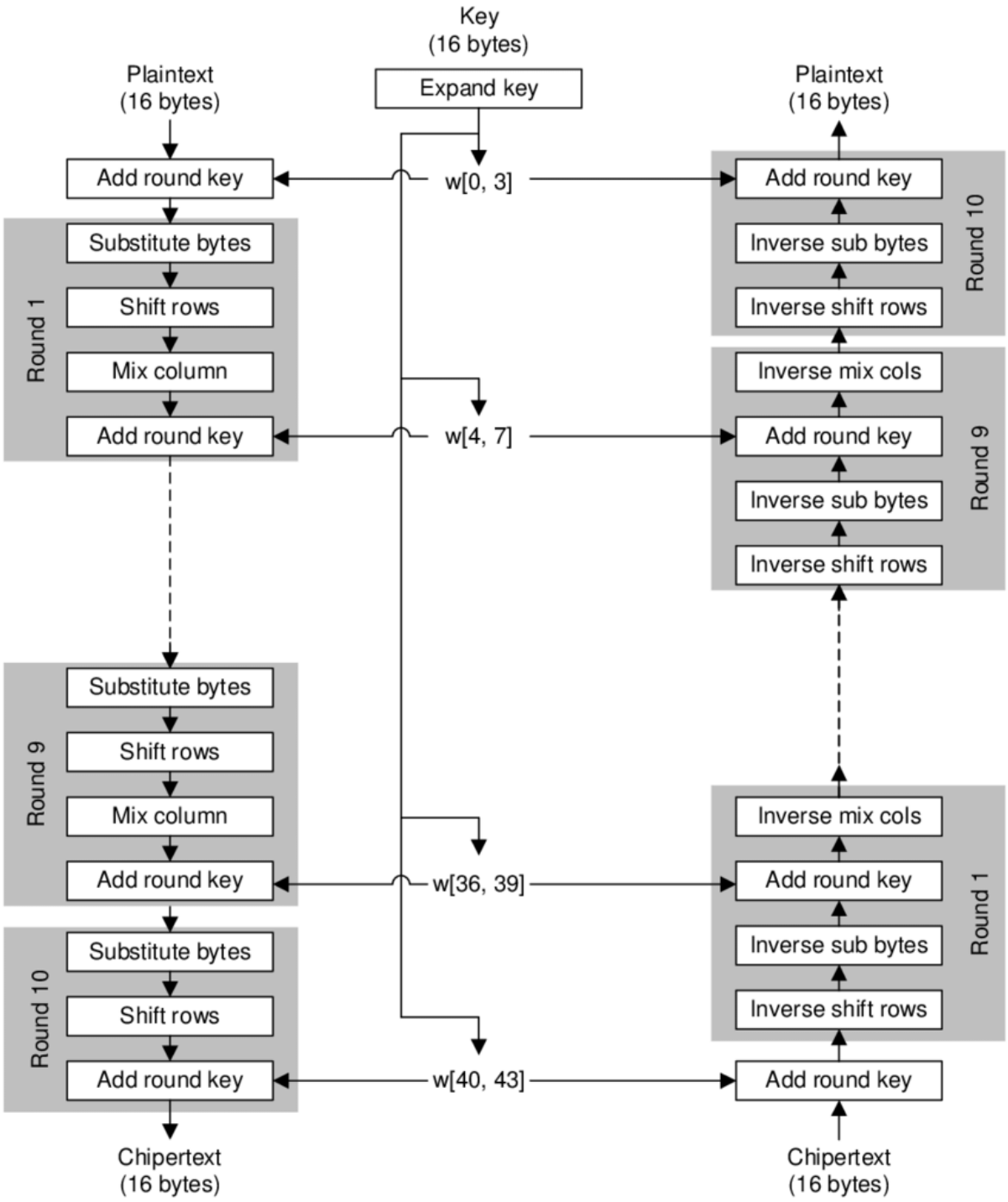


Fig 1.1 AES Encryption and Decryption.

1.2.2 AES Transformation

Substitute Bytes

It is a nonlinear byte substitution, using a substation table (S-box) each byte from the input state is replaced by another byte. The substitution is invertible and is constructed by the composition of two transformations as described below. The substitute bytes operation is as shown in Figure 2.

Inverse Substitute Bytes

It is the reverse operation of the Substitute Bytes transformation, in which the inverse S-box is applied to each byte of the state. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (28).

Shift rows

Shift rows operate on individual rows of the state. It provides diffusion throughout the AES algorithm. In the Shift Rows transformation, the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the left, respectively .

Inverse Shift rows

It is the inverse of the shift rows; the first row of the state array remains unchanged. The bytes in the second, third and fourth rows are cyclically shifted by one, two and three bytes to the right, respectively.

Mix columns

In the Mix Columns transformation, every column of the state array is considered as polynomial over GF (28). After multiplying modulo x4+1 with a fixed polynomial a(x), the operation of Mix Column is as shown in Figure 4.

Inverse Mix columns

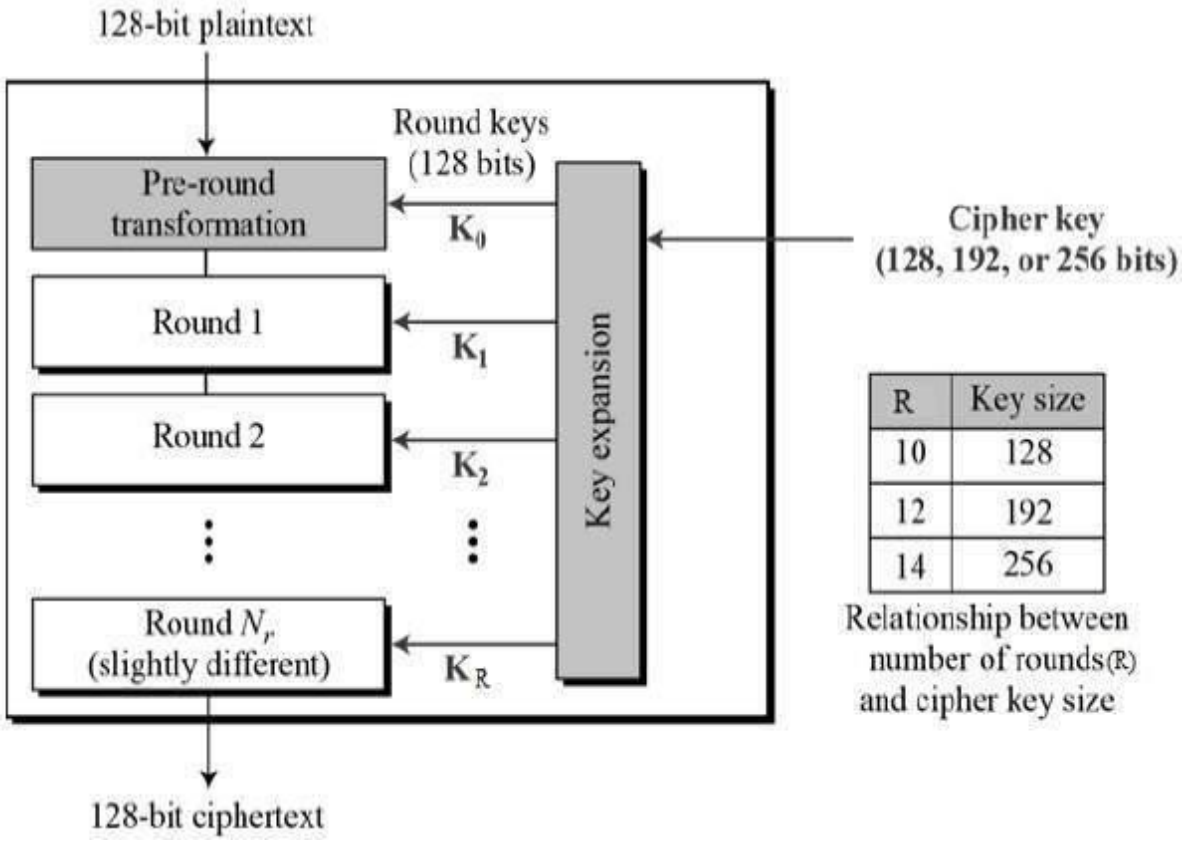
In the Inverse Mix Columns transformation, every column of the state array is considered a polynomial over GF (28). After multiplying modulo x4+1 with a fixed polynomial

b(x), b(x) =0B*x3 + 0D*x2 +09*x + 0E

The result is the corresponding column of the output state. As it is not so straightforward hardware implementation as Mix column, so if we compare both, Inverse Mix Column requires more logic resources for implementation.

Add round key

The Add Round Key operation is as shown in Figure, which is a simple XOR operation between the State and the Round Key. The Round Key is derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element: b (i, j) = a (i, j) k (i, j) Where a is the current State, b the next State and k is the round key.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

FIG 1.2 AES TRANSFORMATION

1.3 FEATURES OF AES ALGORITHM

- SP Network: It works on an SP network structure rather than a Feistel cipher structure, as seen in the case of the DES algorithm.
- Key Expansion: It takes a single key up during the first stage, which is later expanded to multiple keys used in individual rounds.
- Byte Data: The AES encryption algorithm does operations on byte data instead of bit data. So, it treats the 128-bit block size as 16 bytes during the encryption procedure.
- Key Length: The number of rounds to be carried out depends on the length of the key being used to encrypt data. The 128-bit key size has ten rounds, the 192-bit key size has 12 rounds, and the 256-bit key size has 14 rounds.

1.4 APPLICATIONS OF AES ALGORITHM

- Wireless Security: Wireless networks are secured using the Advanced Encryption Standard to authenticate routers and clients. Wi-Fi networks have firmware software and complete security systems based on this algorithm and are now in everyday use.

- Encrypted Browsing: AES plays a huge role in securing website server authentication from both client and server end. With both symmetric and asymmetric encryption being used, this algorithm helps in SSL/TLS encryption protocols to always browse with the utmost security and privacy.

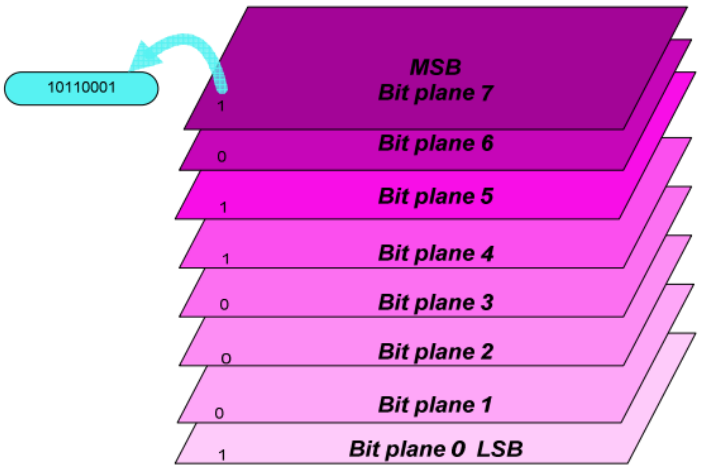
- General File Encryption: Apart from corporate necessities, AES is also used to transfer files between associates in an encrypted format. The encrypted information can extend to chat messages, family pictures, legal documents, etc.

- Processor Security: Many processor manufacturers enable hardware-level encryption using the likes of AES encryption to bolster security and prevent meltdown failures, among other low-profile risks.

1.5 BIT PLAN CODING

Low contract of image enhanced by the image enhancement method. But this method brighten all the pixels of given image so this drawback is overcome in the bit-plane. In Bit-Plane Slicing image is sliced into eight binary planes[7].The bits which are presents in the bit plane 0 is the least significant bit and the bits which are present in the bit plane 7 are the most significant bits. It is clear that

the intensity value of each pixel can be represented by an 8-bit binary vector (b7, b6, b5, b4, b3, b2, b1, b0) where i is from 0 to 7 and each bi is either “0” or“1”. In this case, an image may be considered as an overlay of eight bit-planes. Each bit-plane can be thought of as a two tone image and can be represented by a binary matrix.



CHAPTER 2
LITERATURE SURVEY

Shady Mohammed Soliman, Baher Magdy and Mohamed A. Abd El Ghany had proposed the “Efficient implementation of the AES Algorithm for Security Applications” in 2016. They designed 2 AES encryptions based on the idea of integrating between iterative looping and pipelining to optimize between area, throughput, and power to provide a competitive design to use in low power enabling technologies. FPGA is used to calculate the dynamic power consumption. The AES-128 algorithm applications implemented on low power modules such as Xbee and Bluetooth low energy (BLE) which are the most recommended modules for internet of things (IOT) applications. They attained the competitive throughput of 34 Gbps, and efficiency of 65.42 and 50.58 Mbps/slice respectively.

B.V. Varun, A. M.V., A.C. Gangadhar and P.U in 2019 had proposed the progress of mobile communication and VLSI technology in development of smart devices. The AES and RSA algorithms are proposed to secure the data from vulnerable attacks. It also used to improve the performances of smart devices and helps for better human-machine interaction. As large amount of data is generated on daily basis from most of the devices and it also stored as well as transmitted through various users. Several attacks have been discovered which makes these algorithms vulnerable for threats.

R. Yu et al in 2017 had proposed a protocol and authentication with Block-chain algorithm to protect the user privacy information in the social community detection. Considering user with high closeness, they use authentication mechanism based on the block-chain and encrypt the relationship with Hash function for better security. Then, they use the text encryption protocol in the text recommendation process to ensure the security of information.

R. Ueno in 2020 had proposed highly efficient round-based Advanced Encryption Standard (AES) hardware architectures that support encryption and both encryption and decryption. The proposed Datapath utilizes new operation-reordering and register-retiming techniques to unify critical components with fewer additional selectors. The Datapath has the lowest critical path delay compared to the conventional ones with tower-field S-boxes. A new technique for optimising matrices for linear operations named multiplicative offset is presented. It can improve the efficiency of AES hardware architecture by approximately by 9% without any overhead. The synthesis results suggest that the proposed architecture was more efficient than the best conventional architecture in terms of throughput per area. In addition, because of gate-level timing simulations with back-annotation, they confirmed that encryption and decryption can perform with the lowest power or energy consumption.

Issam Hammad in 2010 had proposed the technique using composite field arithmetic byte substitution, where higher efficiency is achieved by merging and location rearrangement of different operations in the steps of encryption. The previous designs focused on improving the encryption stage and replicate it to implement the multistage encryptor, this work took advantage from the repeated

operations in each stage of the encryptor to achieve resources merging and sharing.

Nur Afifah, Aris Fanani, Yuniar Farida and Putroue keumala Intan in 2018 had proposed to design a data security application is cryptography in which there are many methods can be used to encrypt a data. The AES method is applied to encrypt an image. But in decryption process the plaintext can be restored. The AES method is resistant to cropping attacks and is not resistant to blurring attacks and enhancements.

B. Koziel, R. Azarderakhsh and M.M. kermani in 2018 had proposed a high-performance and scalable architecture for isogeny-based cryptosystems. A high-performance field arithmetic unit, efficient scheduling methodology, and achievable parallelization schemes in isogeny evaluations and Fp arithmetic. When applied to the super singular isogeny Diffie-Hellman key exchange protocol, our architecture on FPGA is 2 times faster than a Haswell software implementation and 1.36 times faster than the fastest other FPGA implementation. Overall, isogeny-based cryptography appears to be a strong candidate for standardization since it utilizes small keys and this work demonstrated that hardware accelerators are indeed viable and can achieve a high degree of parallelization.

P. Jindal, A. Kaushik, and K. Kumar in 2020 had proposed the design and implementation of advanced encryption standard algorithm on 7^{th} series programmable gate array. The implementation of traditional AES algorithm has been accomplished on Artix7 and kintex7 FPGA, Xilinx VIVADO tool has been used to simulation. It is found that Kintex7 FPGA consumes less area in

comparison to Artix7 FPGA. The implementation can also be done on ultra-scale and ultra-scale+ FPGAs for enhanced performance. Also, these can be converted into ASIC designs for high speed and throughput.

Mustafa Nasri et al. in 2010 “FPGA-based Implementation of elliptic curve cryptography” proposed an elliptic curve cryptosystem mellow by programming Spartan3E FPGA kit and analysed by implementing the Elgamla encryption plan on it. It contributes the same level of the security that other surrogates contribute, it performs processing in less time, less memory and fewer computations and less power consumption. It is pertinent for resource constrained devices in the IoT. Hardware implementation of the elliptic curve cryptography using FPGA boost the system performance and a lot of protected than the software implementation.

Nouha Oualha et al in 2013 “Lightweight Attribute-based Encryption for the Internet of Things” proposed CP-ABE scheme using effective pre-computation techniques. The key concept behind pre-computation techniques is to pre-compute and cache set pairs collected with commonly exorbitant cryptographic operations. Pre-computation techniques based on the generator, the pre-processing algorithms of the generator are executed by the hardware devices or trusted authority. The pre-computation technique reduces the cost of the CP-ABE encryption, the pre-computation technique used less computation and less energy drain than original schema.

CHAPTER 3
SOFTWARE DESCRIPTION

Python language is versatile and flexible, and it runs the code efficiently. As the name indicates, it is used for many purposes nowadays. Most of the organizations uses python programming as it has several improved applications.

3.1 PYTHON

Python is the language used to implement since it has many advantages. Python has all the features of object-oriented languages like C++ and java. In python the code is easier, simple, and easy to debug. Hashing functions, signature algorithms and verification algorithms are used here to secure the medical data. So, the DSA algorithm can be implemented by using python language easily. In python there are several libraries to digitally sign the data.

Python is simplified, object oriented and high-level programming language with dynamic symbolism. Python is the only language that helps in connecting two languages. There are two main features in using python language. Python language does not need any compilation process before the program is being executed and another advantage is that the code can be reused. Wherever coding is required, the code can be written easily since it consists of modules and packages.

3.1.1 PYTHON IMPLEMENTATION

Python was deliberately intended to be a direct, simple, and for the most part lightweight programming language that would require negligible code to achieve undertakings contrasted with different dialects.

The truth of the matter is that Python frequently takes considerably less code than that might some way or the other expected for other programming

languages, like C or Java. The idea of Python's direct construction implies a more limited expectation to absorb information for anybody working with the language, particularly those new to programming.

3.1.2 DEBGUGGING PROCESS

The way of construction of Python makes it simpler to learn and carry out, yet that essential nature has different advantages. The direct plan of Python and convenience additionally builds its coherence increased, likewise makes investigating code undeniably clearer, which implies that even lower level or novice developers can investigate and troubleshoot their own code quite successfully.

3.1.3 PYTHON IS EASY SOURCE

Python was created as an open-source programming language, like Linux. It is an open-source working framework. The open-source nature of Python fits a solid local area of designers that help the language and push it ahead. Since it is open source, there is a lot of data accessible, and utilizing the language is free.

3.1.4 PYTHON IN CYBERSECURITY

The advantage of this language is that it's utilized in many fields. Network safety experts find a good pace rapidly. Python’s convenience implies that any accomplished online protection proficient that has developed a moderately solid specialized foundation can get familiar with the essentials of the Python language and begin programming and execute their code rapidly protection has become more significant.

3.2 MATLAB

MATLAB is a software program package for excessive-performance mathematical computation, visualization, and programming surroundings. It affords an interactive surrounding with masses of integrated features for technical computing, pics, and animations. It stands for Matrix Laboratory. It became a simple technique to implement matrix software program developed by means of the LINPACK (Linear machine bundle) and EISPACK (Eigen gadget bundle) projects. MATLAB is a current programming language environment, and it has subtle information structures, including built-in enhancing and debugging equipment, and helps item-orientated programming. It is a multi-paradigm. So, it may work with a couple of varieties of programming strategies, together with Functional, Object-Oriented and Visual Besides surroundings. MATLAB is likewise a programming language. It lets in several forms with manipulations with matrix, set of rules implementation, information and capabilities plotting, and can engage with applications written in different programming languages. MATLAB has considerable centres for showing vector and matrices as graphs, as well as annotating and printing graphs. It includes excessive stage structures for two dimensional and three-dimensional records visualization, image processing, animation, and presentation pix. It includes low-degree structures that permit us to customize the show of pictures completely as well as to build complete graphical user interfaces on our MATLAB applications.

3.2.1ADVANTAGES OF MAT LAB

EASE TO USE

The program can be used as a scratchpad to evaluate expressions typed on the command line, or it is used to execute massive prewritten packages. Applications can be written and modified with the integrated development environment and debugged with the MATLAB debugger, Because the language is so simple to

apply, it is most fulfilling for the quick prototyping of recent packages. Many software improvement gear is supported to make this system smooth to apply. They include editor/debugger, online documentation and manuals, a workspace browser, and good-sized demos.

3.2.2 PLATFORM INDEPENDENCE

MATLAB is supported on any kind of systems, imparting a tremendous measure of platform independence. The language is provided on Windows 2000/XP/Vista, Linux, diverse variations of UNIX and the Macintosh. Applications written on any platform will run on the opposite complete platform and records documents written on any platform may be studied apparently on some other platform. As a result, packages written in MATLAB can shift to new structures while the wishes of the user alternate.

MATLAB comes with a large library of predefined functions that gives tested and prepacked solutions to many primary technical tasks. For instance, assume that we're writing an application that ought to evaluate the records associated with an enter statistics set. In most languages, we might want to write our subroutines or functions to put in force calculations along with the arithmetic suggest, general deviation, median, and so on. Hundreds of different offerings are constructed properly into the MATLAB language, making your task much comfortable. In addition to the considerable libraries of offerings constructed into the basic MATLAB language, there are numerous unique-purpose toolboxes relevant to assist complicated problems in particular regions. For example, a user can purchase preferred toolkits to clear up troubles in signal processing, manipulate systems, communications, photograph processing, and neural networks, etc. There is likewise a broad compilation of unfastened user-contributed MATLAB packages which might be shared through the MATLAB web page.

3.2.3 DEVICE-INDEPENDENT PLOTTING

MATLAB has many basic plotting and imaging commands. The plots and photos may be displayed on any graphical output device supplied by the laptop on which MATLAB is going for walks. This facility makes MATLAB a first-rate device for visualizing technical facts.

3.2.4GRAPHICAL USER INTERFACE

MATLAB carries a device that lets in a programmer to interactively layout a Graphical User Interface (GUI) for software. With this capability, the programmer can design refined records-analysis packages that may be operated by means of extraordinarily inexperienced customers.

3.2.5 MATLAB COMPILER

MATLAB's adaptability and platform independence are produced by means of compiling MATLAB packages into a machine-impartial p-code and then decoding the p-code education at runtime. This method is closely related to that used by Microsoft's Visual Basic language. Unfortunately, the resulting applications can every now and then execute slowly because MATLAB code is interpreted in preference to compiled. This compiler can assemble MATLAB applications into an actual executable code that runs faster than the interpreted code. It is a tremendous technique to transform a prototype MATLAB program into an executable suitable for sale and distribution to users.

3.3 MODELSIM

Model sim is a multi-language environment by mentor graphics for the simulation of the hardware languages such as VHDL, Verilog and System C and includes a built in C debugger. Model sim can be used independently, or in conjunction with Intel Quartus Prime, PSIM, Xilinx ISE or Xilinx Vivado. Simulation is performed using the graphical user interface (GUI) or automatically using scripts.

Model Sim eases the process of finding design defects with an intelligently engineered debug environment that efficiently displays design data for analysis and debug of all hardware description languages.

CHAPTER 4

EXISTING METHOD

AES algorithm is of three types i.e., AES-128, AES-192 and AES-256. This classification is done on the bases of the key used in the algorithm for encryption and decryption process. The numbers represent the size of key in bits. This key size determines the security level as the size of key increases the level of security increases. The AES algorithm uses a round function that is composed of four different byte-oriented transformations. For encryption purpose four rounds consist of:

- Substitute byte
- Shift row
- Mix columns
- Add round key

While the decryption process is the reverse process of the encryption which consists of:

- Inverse shift row
- Inverse substitute byte
- Add round key
- Inverse mix columns

There is a number of round present of key and block in the algorithm. The number of rounds depends on the length of key use for Encryption and Decryption.

	Key Length (in word/byte/bits)	Block Size (in word/byte/bits)	Number of rounds
AES - 128	4/16/128	4/16/128	10
AES – 192	6/24/192	4/16/128	12
AES - 256	8/32/256	4/16/128	14

AES algorithm uses a round function for both its Cipher and Inverse Cipher. This function is composed of four different byte-oriented transformations.

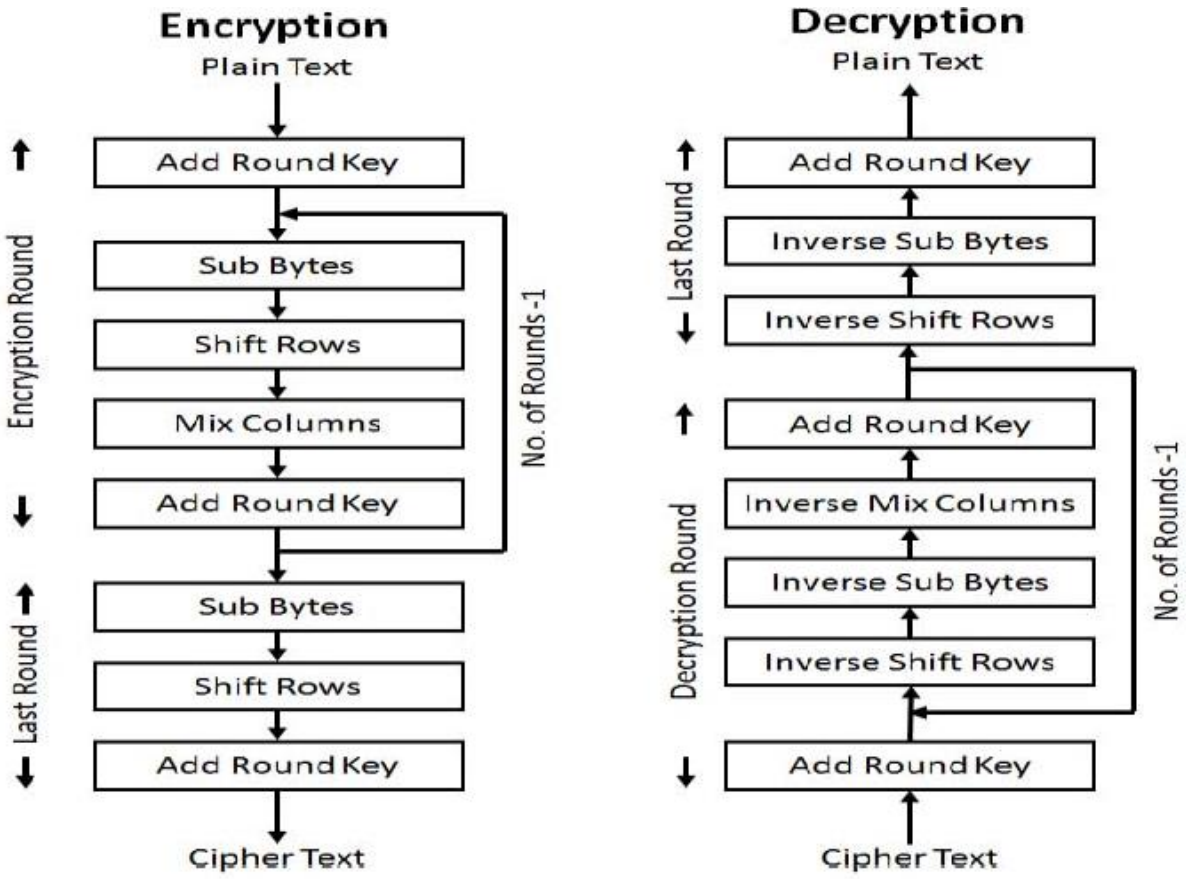


Fig Block Diagram of AES Algorithm

4.1 Encryption process

4.1.1Substitute byte transformation

The Substitute bytes transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table S-box. The operation of substitution byte is shown as image below.

y

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6c	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	Fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	60	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	18	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	of	b0	54	bb	16

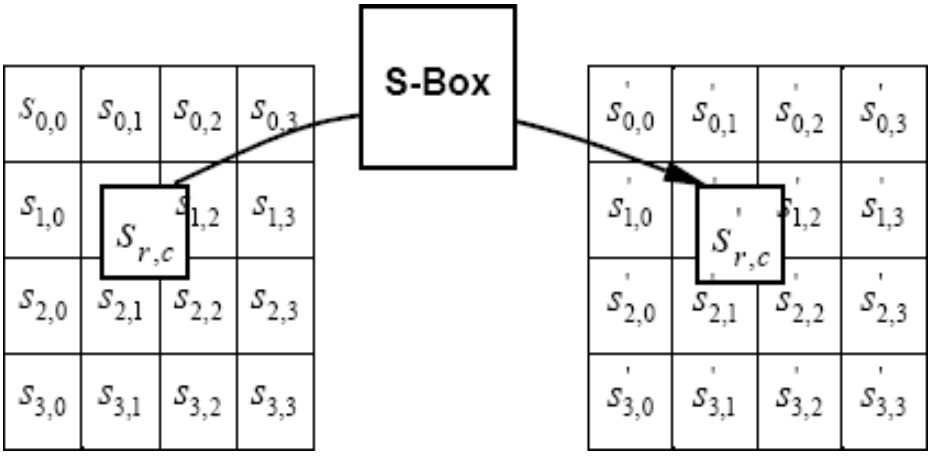


Fig 4.1 Operation of substitution type.

4.1.2 Shift rows transformation

In the Shift Rows transformation, the bytes in the last three rows of the State are cyclically shifted over different numbers of bytes. The first row, r = 0, is not shifted.

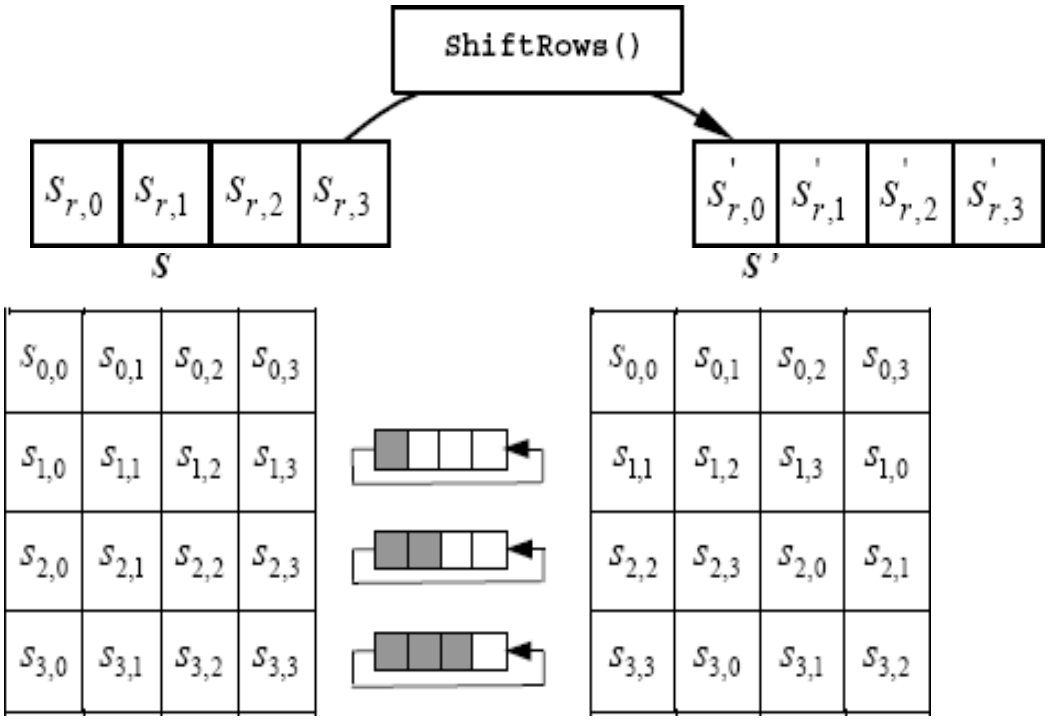


Fig 4.2 Cyclic shift row operation.

4.1.3 Mix Column Transformation

The Mix Columns transformation operates on the State column-by-column, treating each column as a four-term poly- nomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x 4 + 1 with a fixed poly- nomial a(x), given by

a(x) = {03}x ^3 + {01}x^ 2 + {01}x + {02} .

The resultant columns are shown in the figure below. This is the operation of mix columns

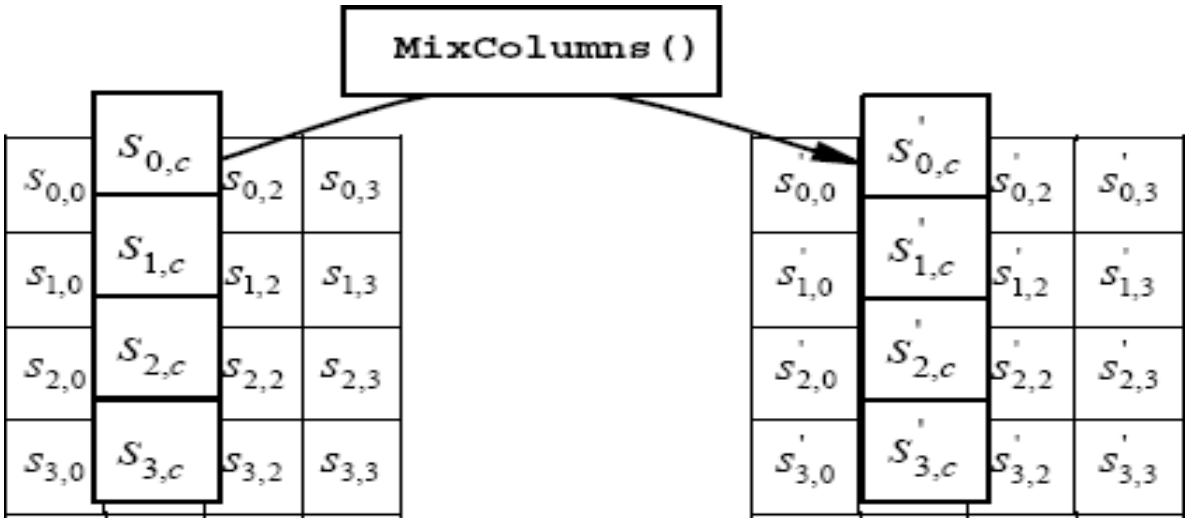


Fig 4.3 Mix Column operation

4.1.4 Add Round Key Transformation

In the Add Round Key transformation, a Round Key is added to the State by a simple bitwise XOR operation. The Round Key is derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element:

$$b(i, j) = a(i, j) \oplus k(i, j)$$

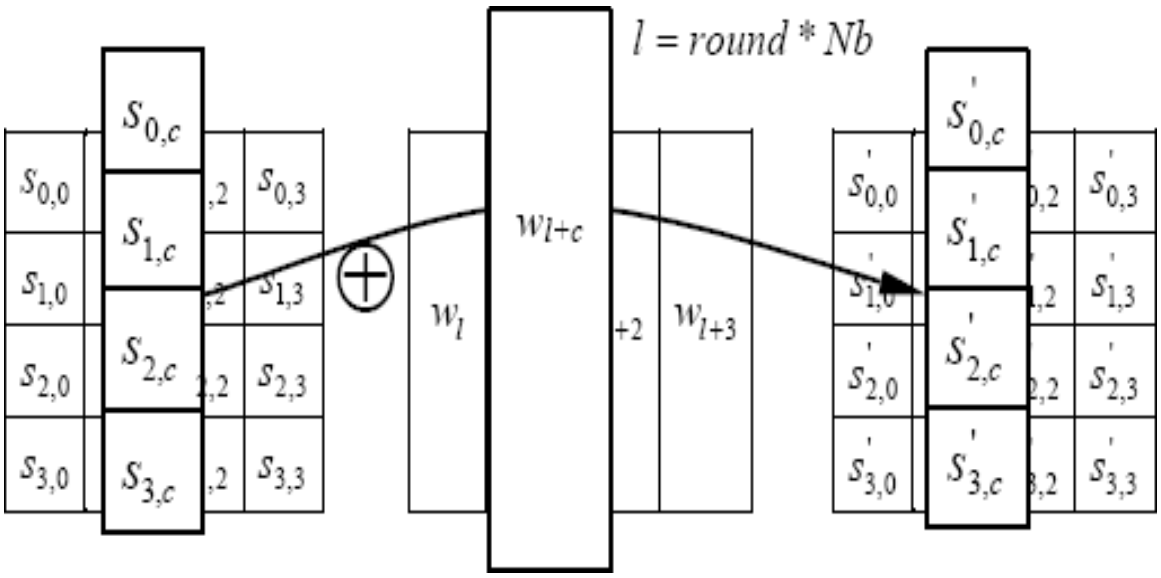


Fig 4.4 Add Round Key Operation.

4.2Decryption Process

4.2.1 Inverse shift row transformation

Inverse Shift Rows is the inverse of the Shift Rows trans- formation. The bytes in the last three rows of the State are cyclically shifted over different numbers of bytes. The first row, r= 0, is not shifted. The bottom three rows are cyclically shifted by Nb-shift (r, Nb) bytes, where the shift value shift(r,Nb) de-

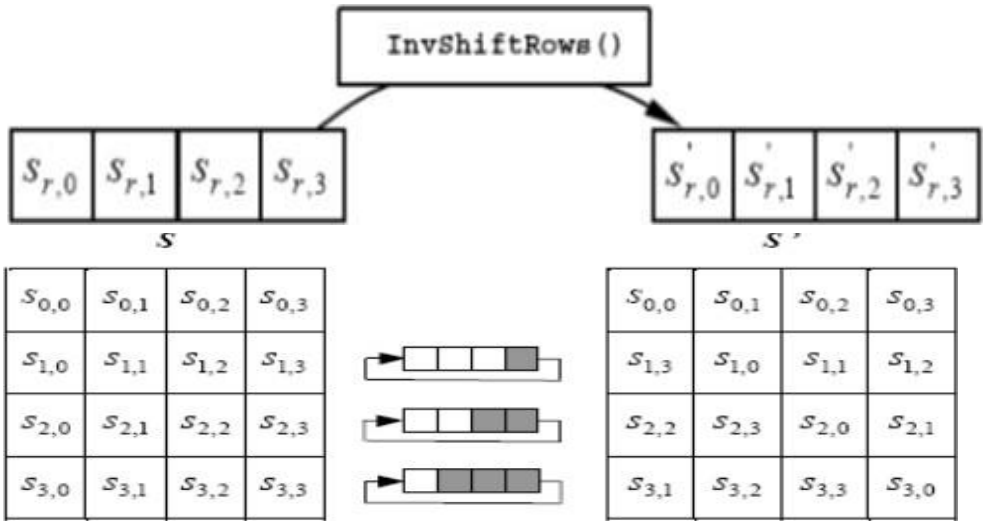


Fig 4.5 Inverse Shift Row Operation.

4.2.2 Inverse Substitute by Transformation

Inverse Substitute Bytes is the inverse of the byte substitute-transformation, in which the inverse S-box is applied to each byte of the State. It is reverse process of Substitute byte transform. This is obtained by applying the inverse of the fine transformation followed by taking the multiplicative in – verse in GF (2^8). There is an inverse s-box table for substitute the value.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Fig 4.6 Inverse S-box: substitution values for the byte xy

4.2.3 Inverse Mix Columns Transformation

Inverse Mix Columns is the inverse of the Mix Columns trans- formation. Inverse Mix Columns operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF(2^8) and multiplied modulo x^ 4 + 1 with a fixed polynomial $a^{-1}(x)$, given by

$$a^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

4.3. IMPLEMENTATION

4.3.1 ENCRYPTION ALGORITHM

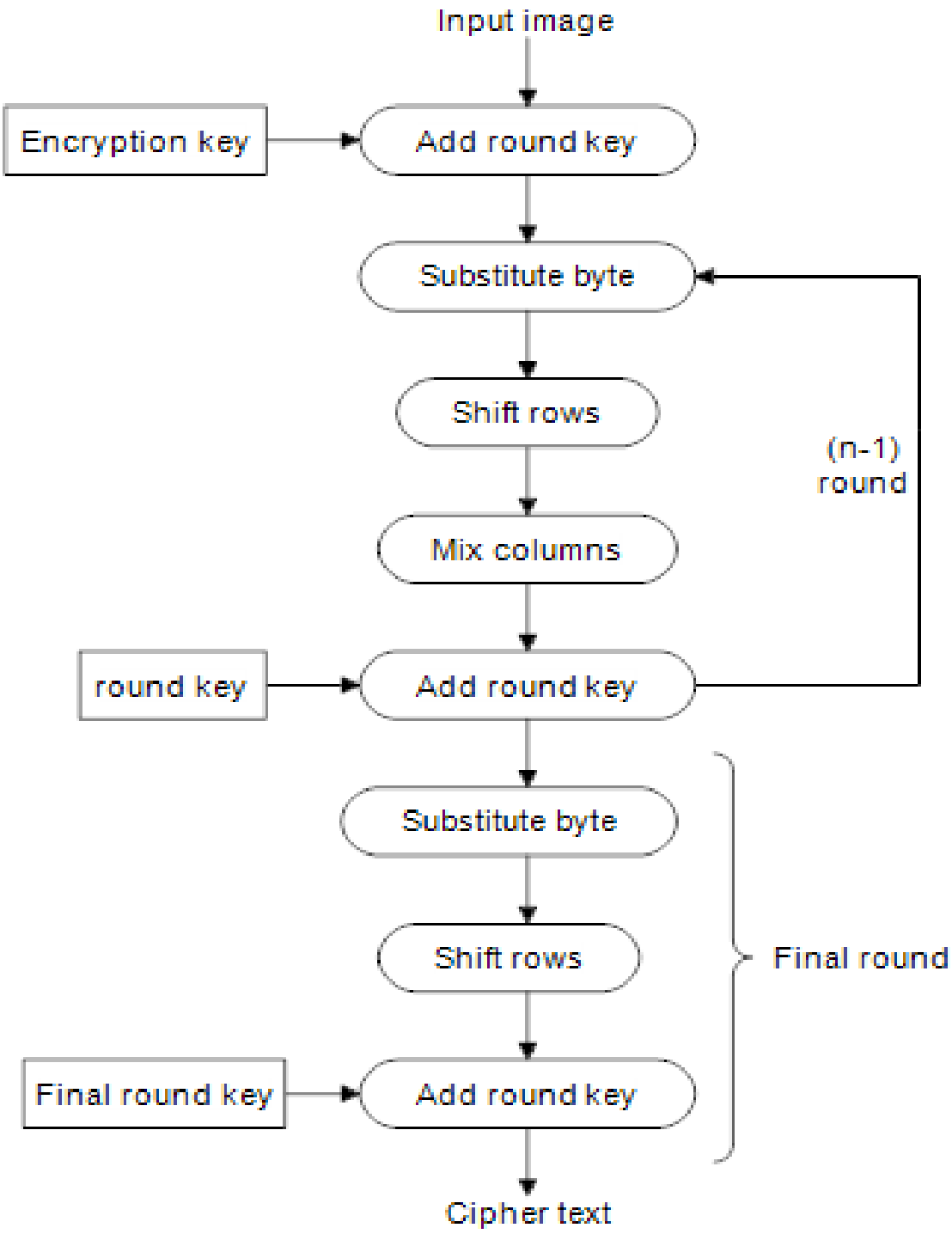


Fig 4.7 Flowchart of AES Encryption Algorithm.

The implementation of the AES – 128 encryption and decryption algorithm with the help of the MATLAB Software is done. In which the input is an image and the key in hexadecimal format and the output is the same as that of input image. For encryption process first, dividing image and making it 4*4-byte state i.e., matrix format. Calculate the number of rounds based on the key Size and expand the key using our key schedule. And there are (n-1) rounds performed which are substitute byte, shift rows, mix columns and add round key. The final round "n" does not consist of mix column in the iteration.

4.3.2 DECRYPTION ALGORITHM

The AES decryption process is the revers process that of the encryption process. The above figure shows flow of the AES decryption algorithm. Which consist of cipher text as the input, the key is same for decryption process which for encryption. In case of decryption the inverse substitute byte, inverse shift rows and the inverse mix columns are to be implemented. While the add round key remains the same.

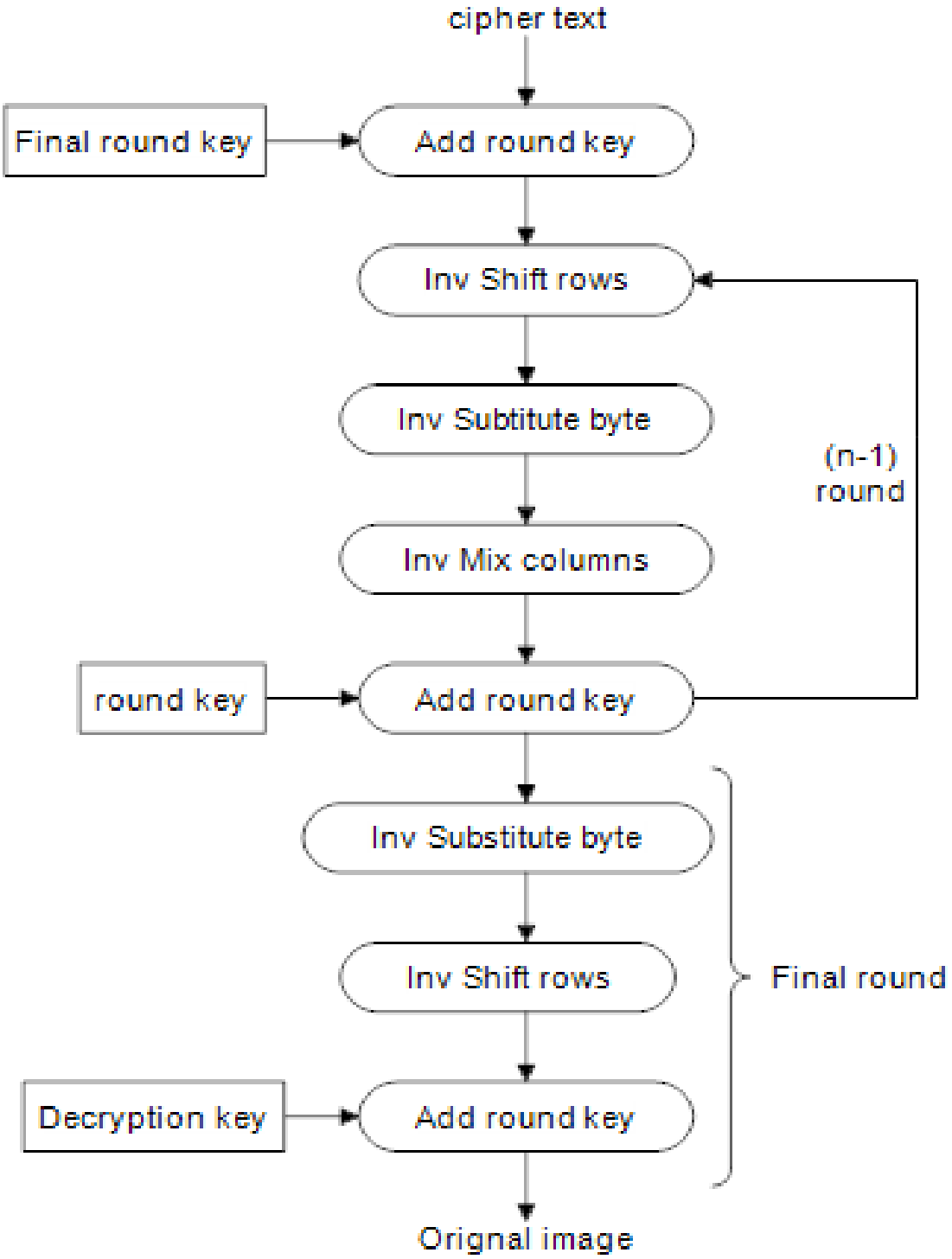


Fig 4.8 Flowchart of AES Decryption Algorithm

CHAPTER 5

PROPOSED SYSTEM

5.1 PROPOSED METHOD

In the existing method we have done the following encryption and decryption for image. In our project we have done the encryption and decryption for images using aes algorithms and also, we have explained about the extraction of bit planes images which is nothing but it is based on the concept of decomposing a multilevel Image into a series of binary images and compressing each binary image via one of several well known binary compression methods from the least significant bit (LSB) and the most significant bit (MSB).

5.2 BLOCK DIAGRAM

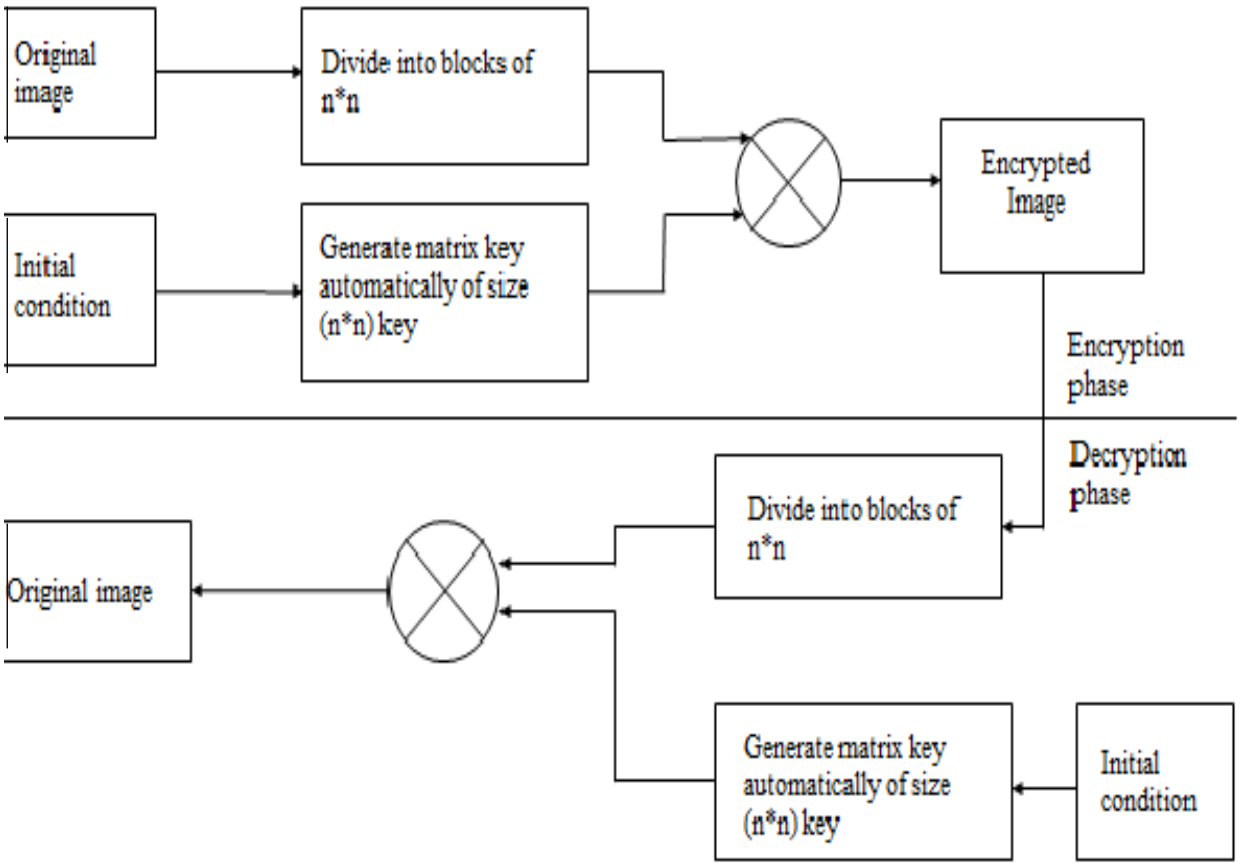


Fig 5.1 Block Diagram of AES

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key size of lengths 128,192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively.

5.3 BOUNDARY EXTRACTION OF IMAGE

The boundary of the image is different from the edges in the image. Edges represent the abrupt change in pixel intensity values while the boundary of the image is the contour. As the name boundary suggests that something whose ownership changes, in the image when pixel ownership changes from one surface to another, the boundary comes into the picture. Edge is basically the boundary line, but the boundary is the line or location dividing the two surfaces.

5.3.1 TYPES OF BOUNDARY EXTRACTION TECHNIQUES

There are two types of boundaries in binary images.

- **Innerboundary**

  It is the difference between the original image and the eroded image. The eroded image is the shrunk image when erosion is applied to the original image. On taking the difference between the original image and the eroded version, we get the inner boundary of the image. The inner boundary is the part of the main surface separating the other surface. Erosion shrinks the white portion thus the boundary is the part of the white surface itself.

- **Outer boundary**

  It is the difference between dilated image and an original image. The dilated image is the expanded image when dilation is applied to the original image. Dilation increases the white portion of the image. On taking the difference between dilated and original versions of the image we get the boundary which is the lost art of the black surface.

Description

- **BW = im2bw(I,level)** converts the grayscale image `I` to binary image `BW`, by replacing all pixels in the input image with luminance greater than `level` with the value `1` (white) and replacing all other pixels with the value `0` (black).This range is relative to the signal levels possible for the image's class. Therefore, a `level` value of `0.5` corresponds to an intensity value halfway between the minimum and maximum value of the class.
- **BW = im2bw(X,cmap,level)** converts the indexed image `X` with colormap `cmap` to a binary image.
- **BW = im2bw(RGB,level)** converts the truecolor image `RGB` to a binary image.

5.4 EXTRACT BIT PLANE IMAGE FROM MATLAB

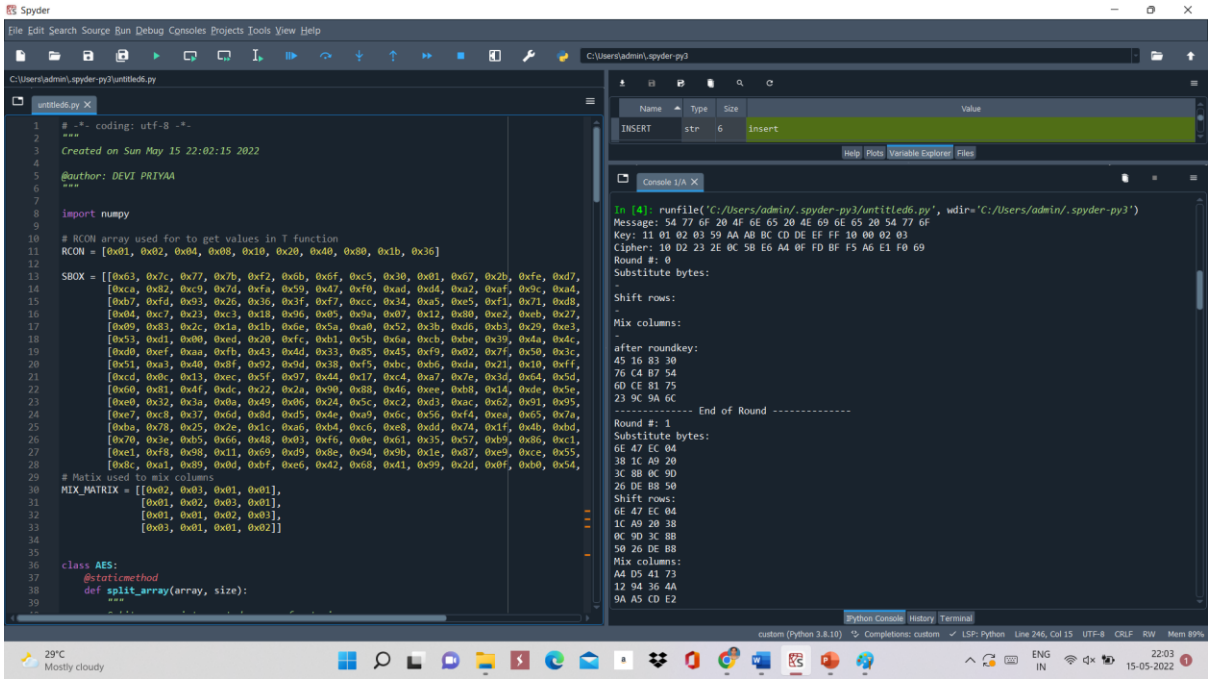
Image is basically combination of individual pixel (dots) information. When we write that image is of 620 X 480 size, it means that image has 620 pixel in horizontal direction and 480 pixel in vertical direction. So, altogether there is 620 X 480 pixels and each pixels contains some information about image.

Grayscale image are basically those images which we say black and white image. Each pixel of grayscale image has a value lies in between 0 – 255 which decides at which position, the image will be black and at which position, it will be white. If pixel value is 0, it means that pixel colour will be fully black and if pixel value is 255, then that pixel will be fully white and pixel having intermediate value will be having shades of black and white.

CHAPTER 6

RESULTS

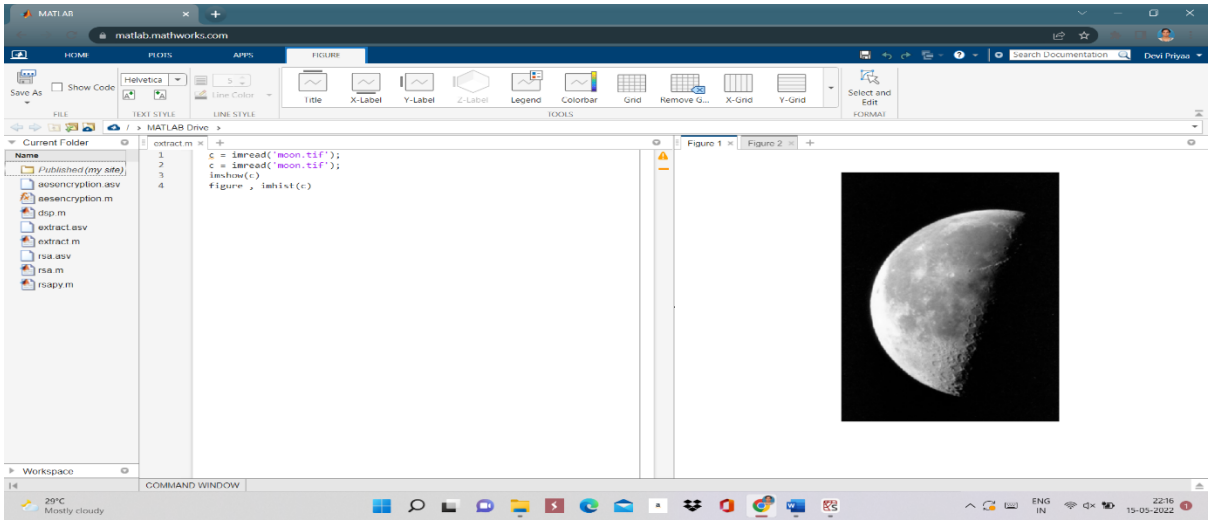
6.1 AES ALGORITHM



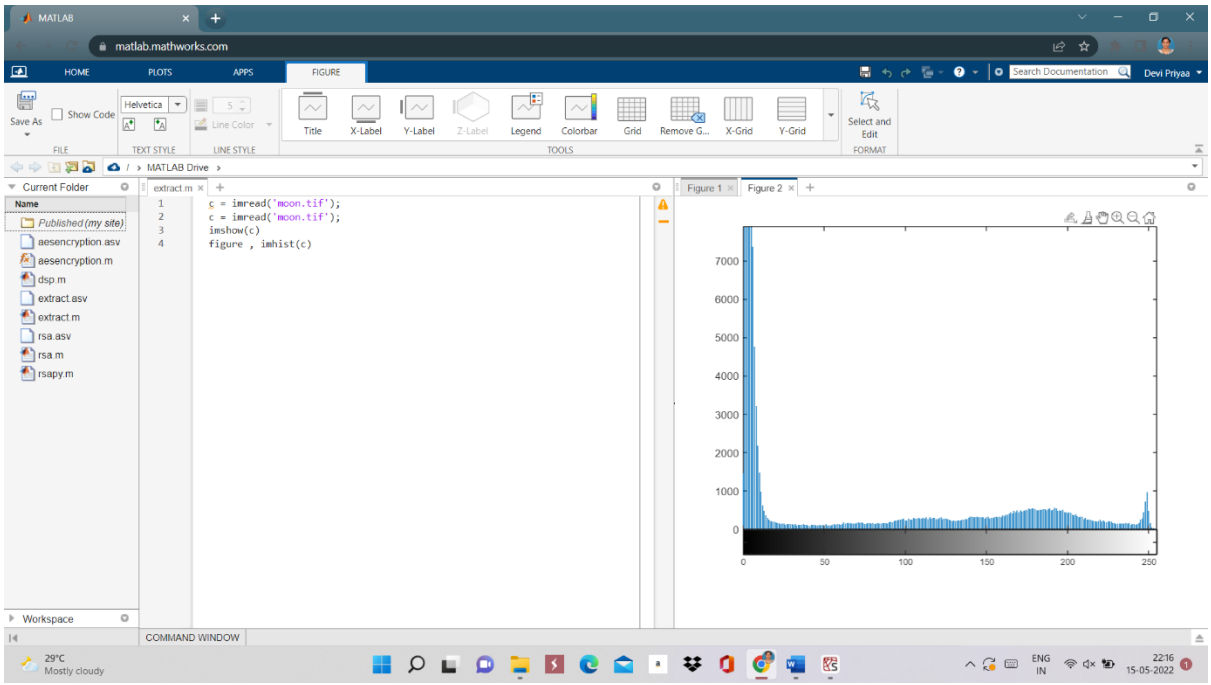
This output shows the substitute keys, round keys, shift rows and mixed columns.

6.2 EXTRACTION OF IMAGE USING BITPLANES

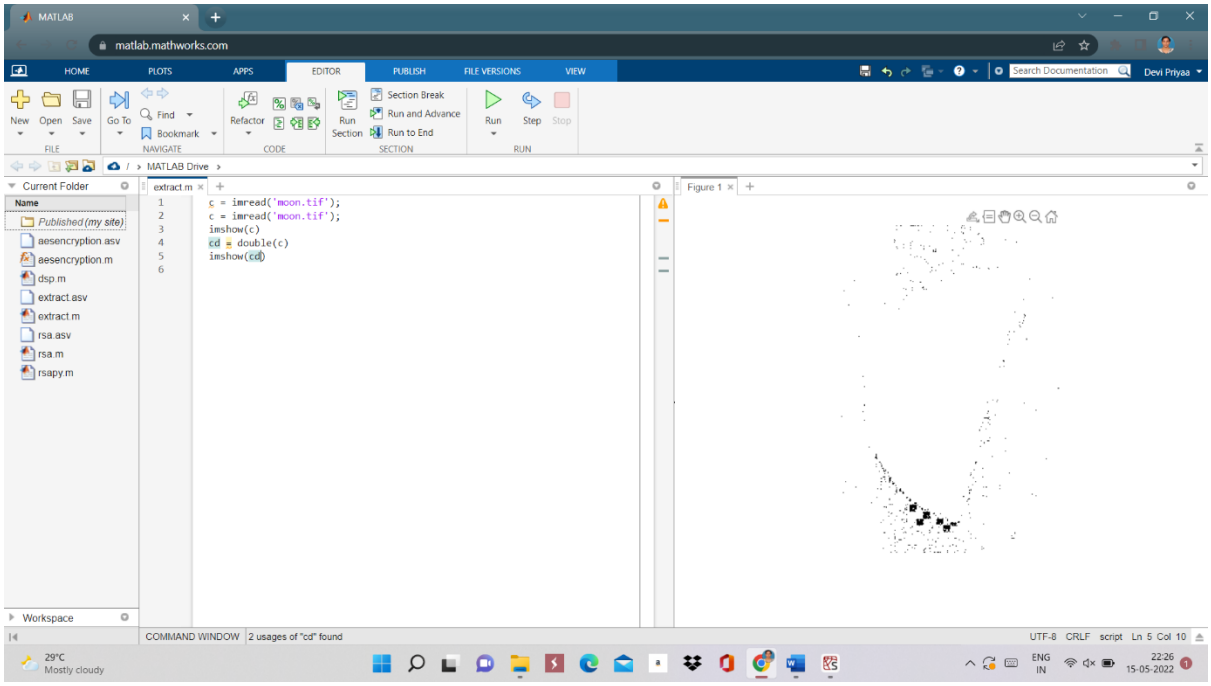
The image can be extracted using the bit planes according to the Least Significant Bit (LSB) and the Most Significant Bit (MSB).



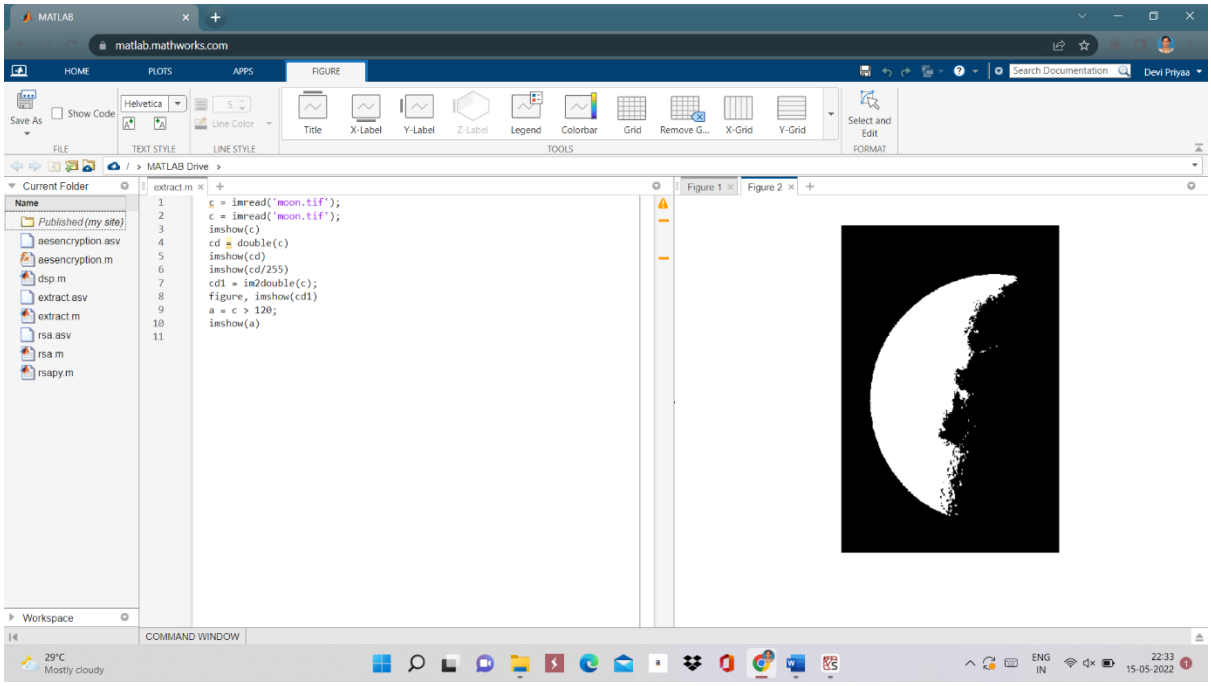
In this image, we displayed the original image of a moon using MATLAB. The image in the MATLAB can be viewed only on .tif format. i.e., Tag Image File Format.



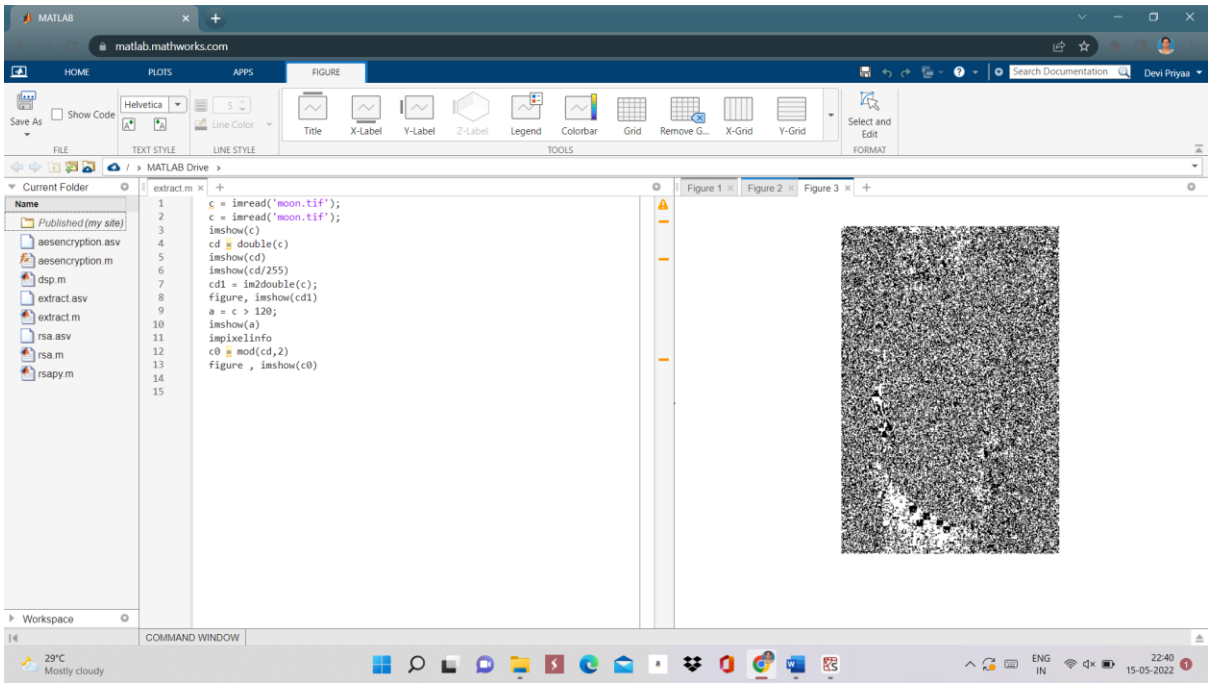
Here, the histogram of the greyscale image is displayed.



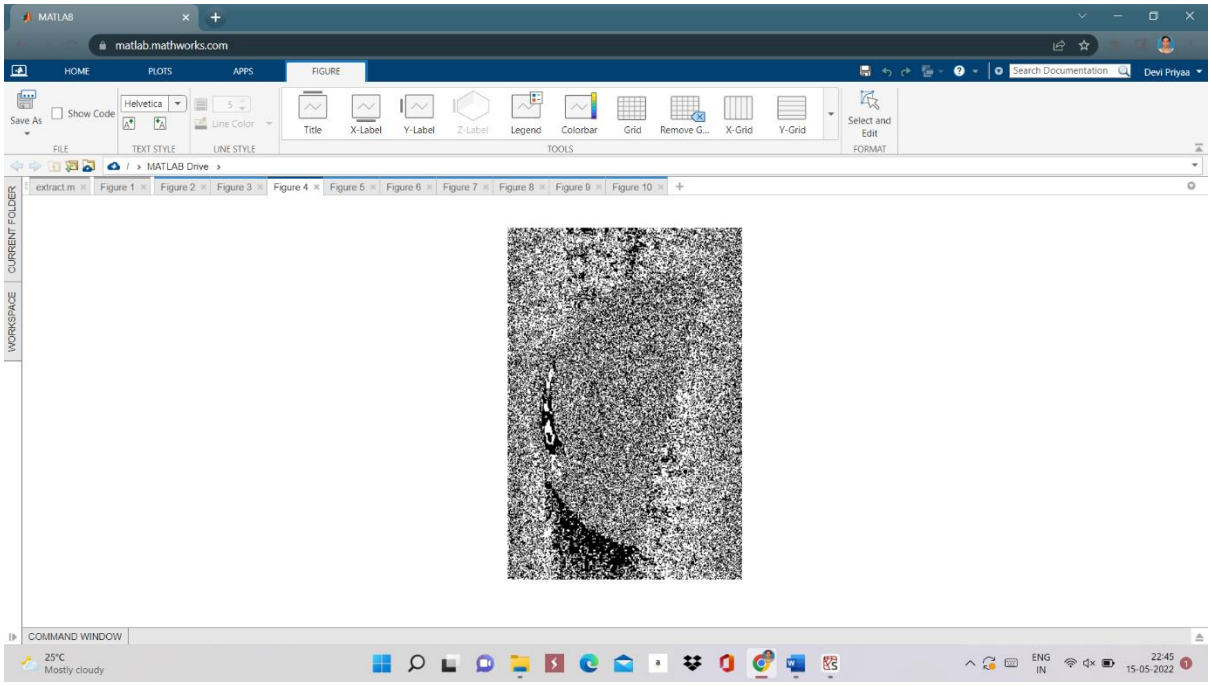
In this image, we have doubled the original image in which we type casted the original image. While we double the image, we can see only the white screen. Only when we convert it into the uint8 (unsigned integer) because the images accept the values between 0 and 1. By dividing the image by 255, we can get the values between 0 and 1 and can get back an original image.



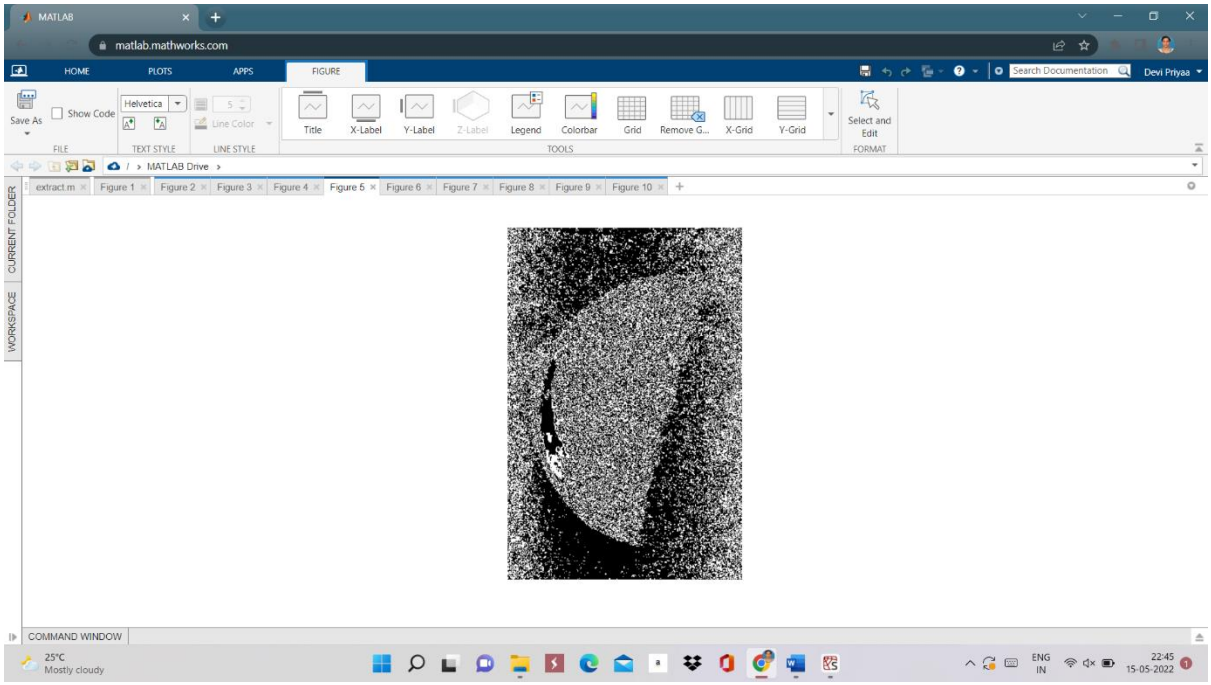
In this figure, for the image should be converted into a binary image we applied a threshold value 120 for images. So whatever the pixels of the image which is more than 120 the value is stored as 1 and which is less than 120 it will be stored as 0.



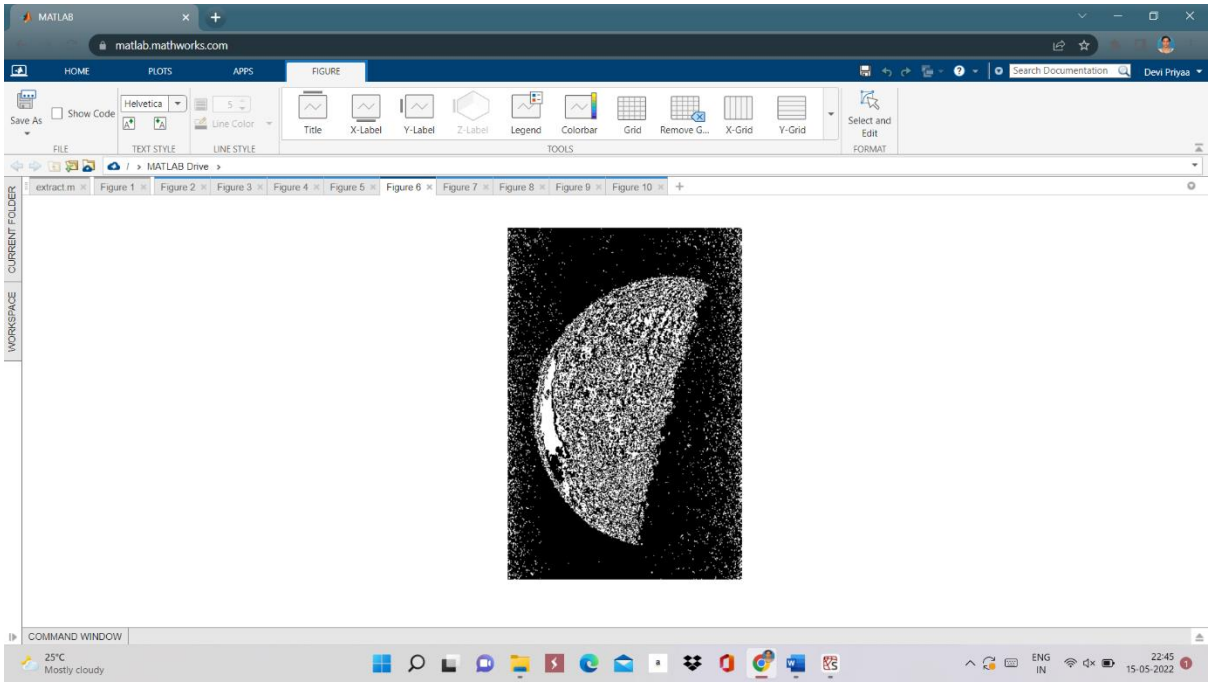
Here, the least significant bit (LSB) of the image is obtained using the binary value 0. The image has 8 bits. The value of LSB is 0 and the MSB is 7. By using this concept, we will extract the images in each bit plane to see the binary value configuration.



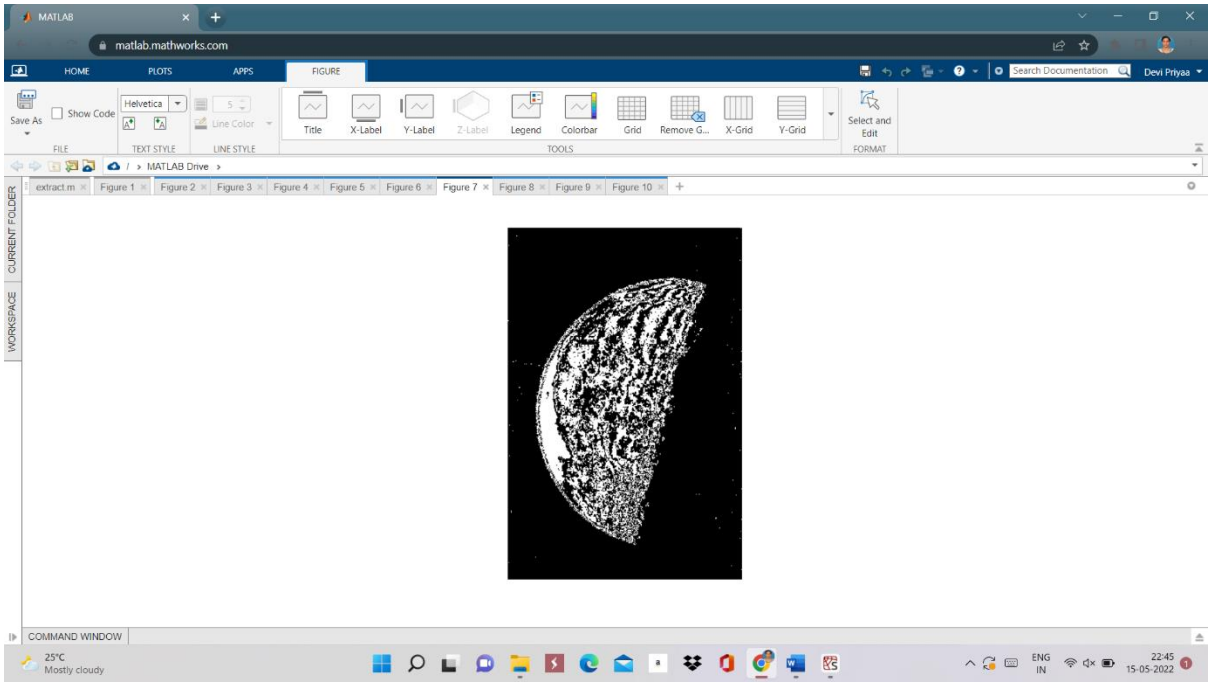
1st Bit plane



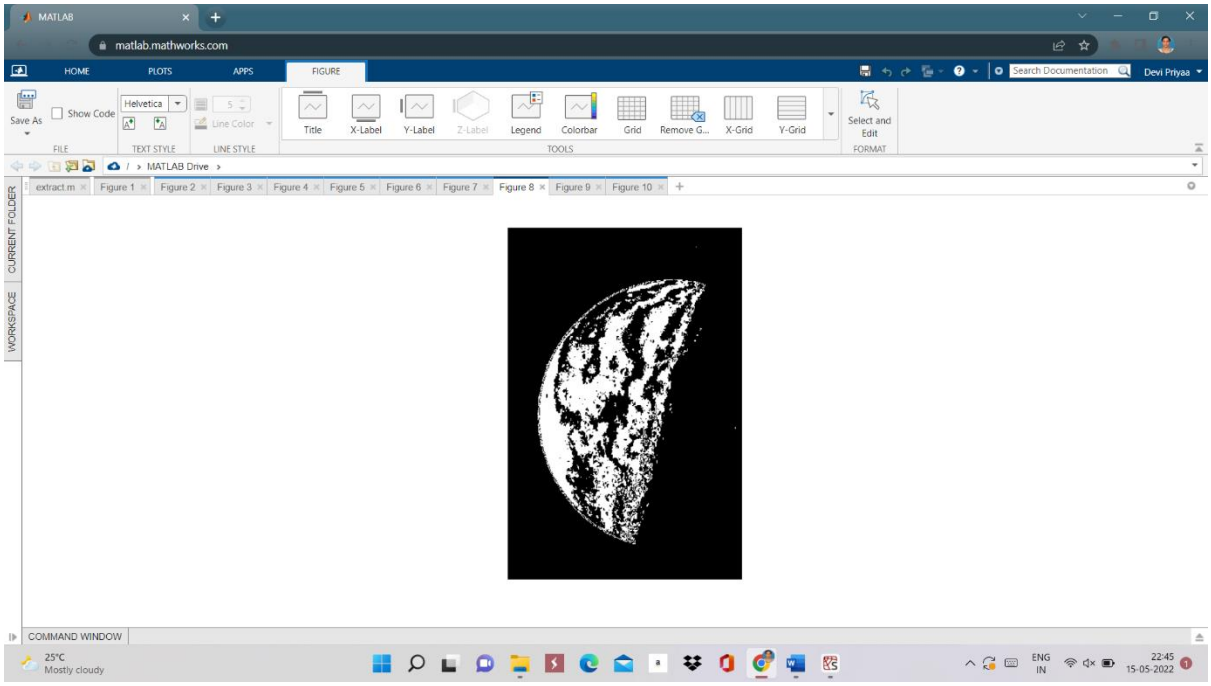
2nd Bit plane



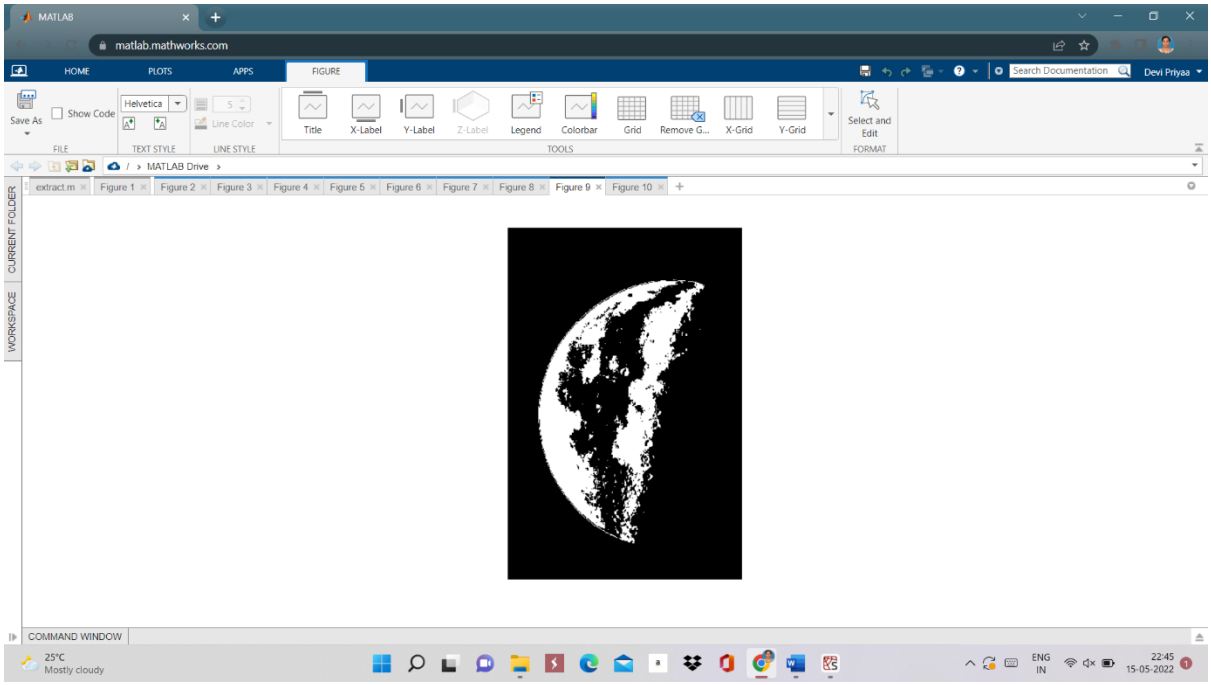
3rd Bit plane



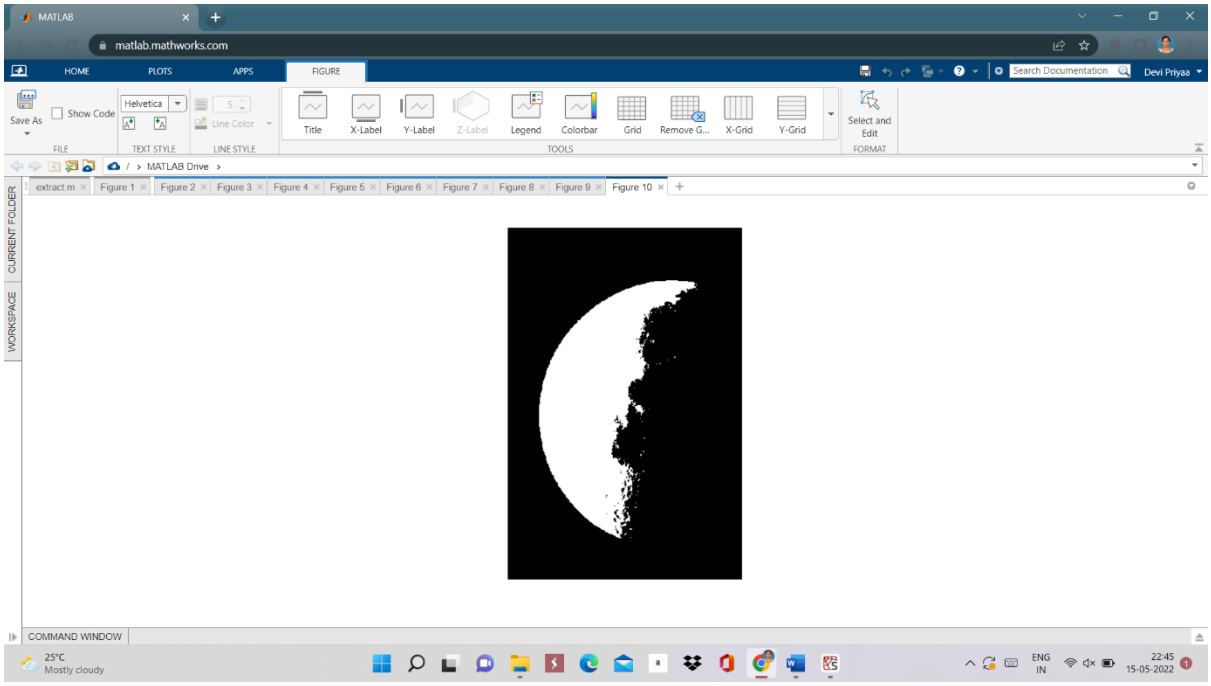
4th Bit plane



5^{th} Bit plane

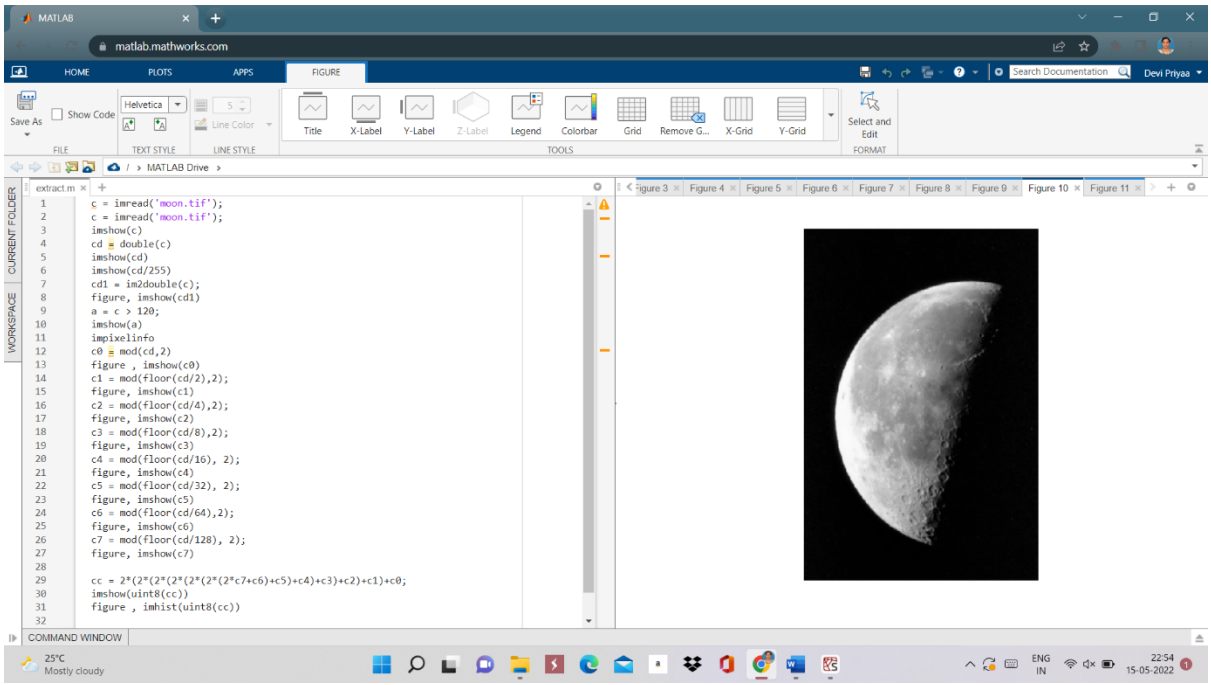


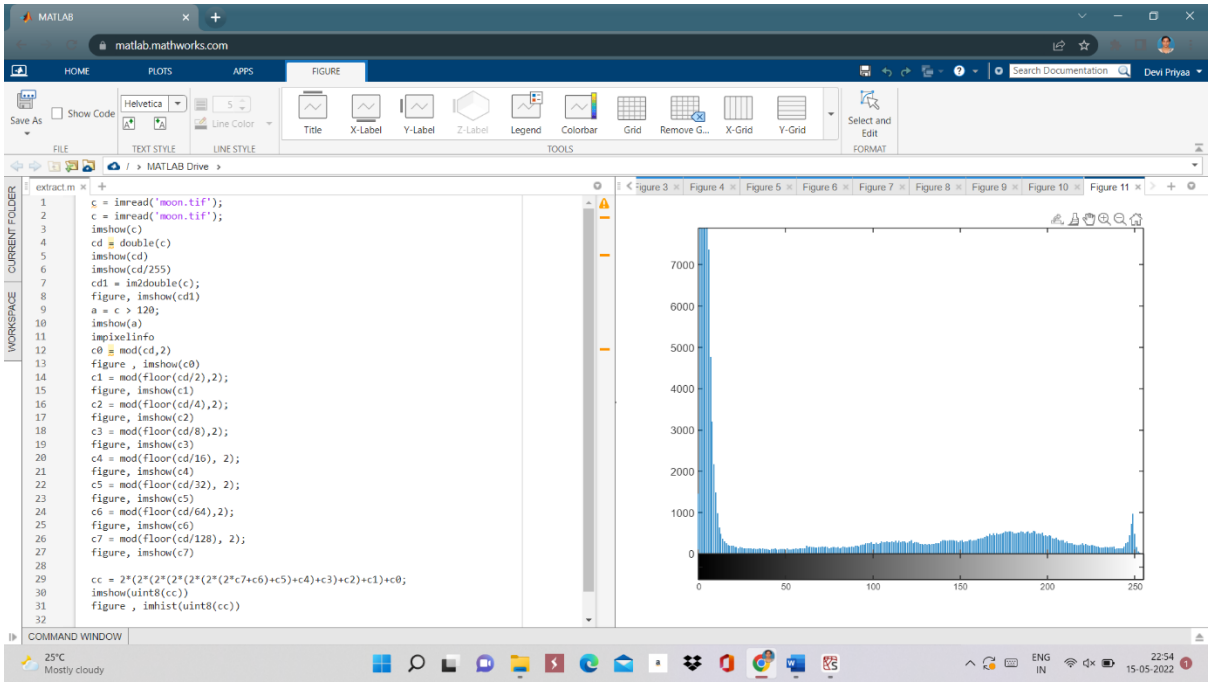
6^{th} Bit plane



7th Bit Plane

From these, bit plane images, we can't get back the clear original image. For this, we have to convert the binary format to the integer format, then only the original image is retained.

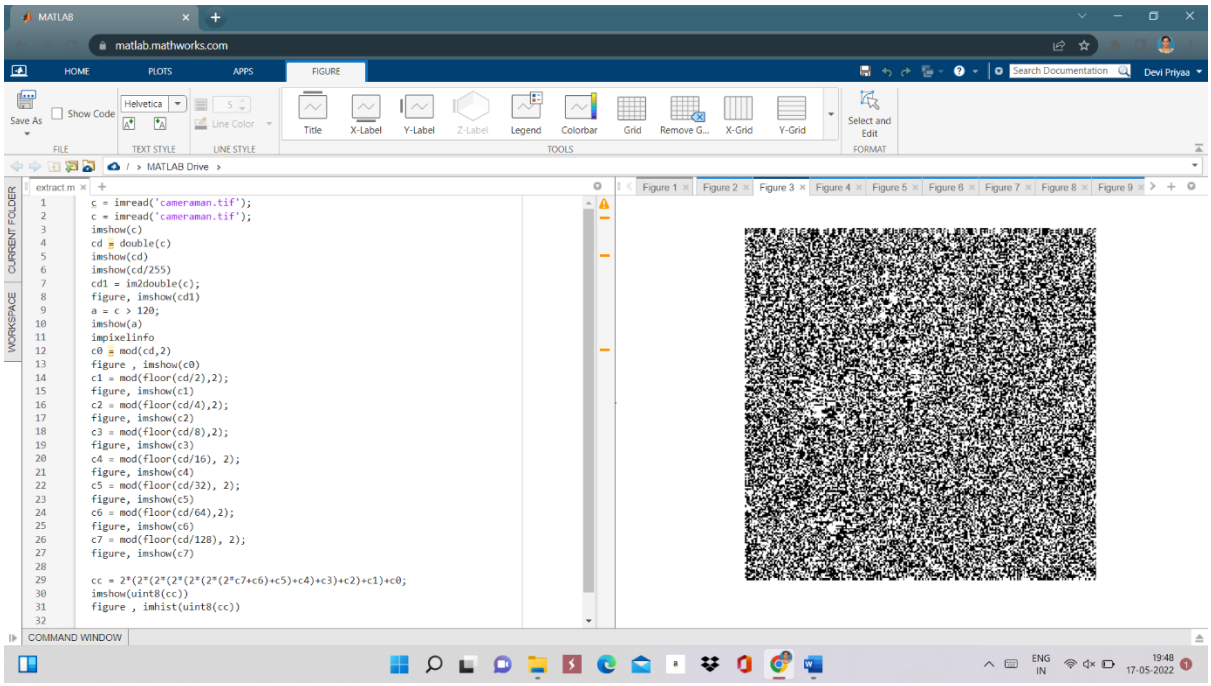




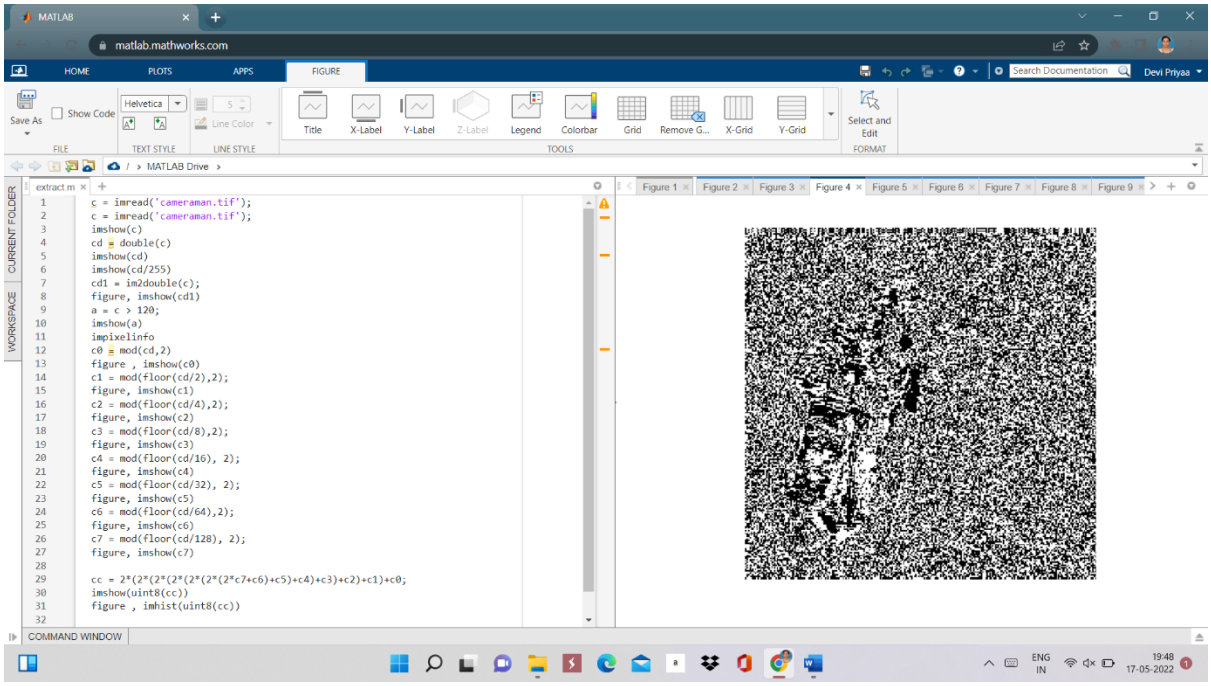
Hence, here we can get back the original image after binary conversion and bit plane extraction.

6.3 EXTRACTION OF IMAGE USING BIT PLANES

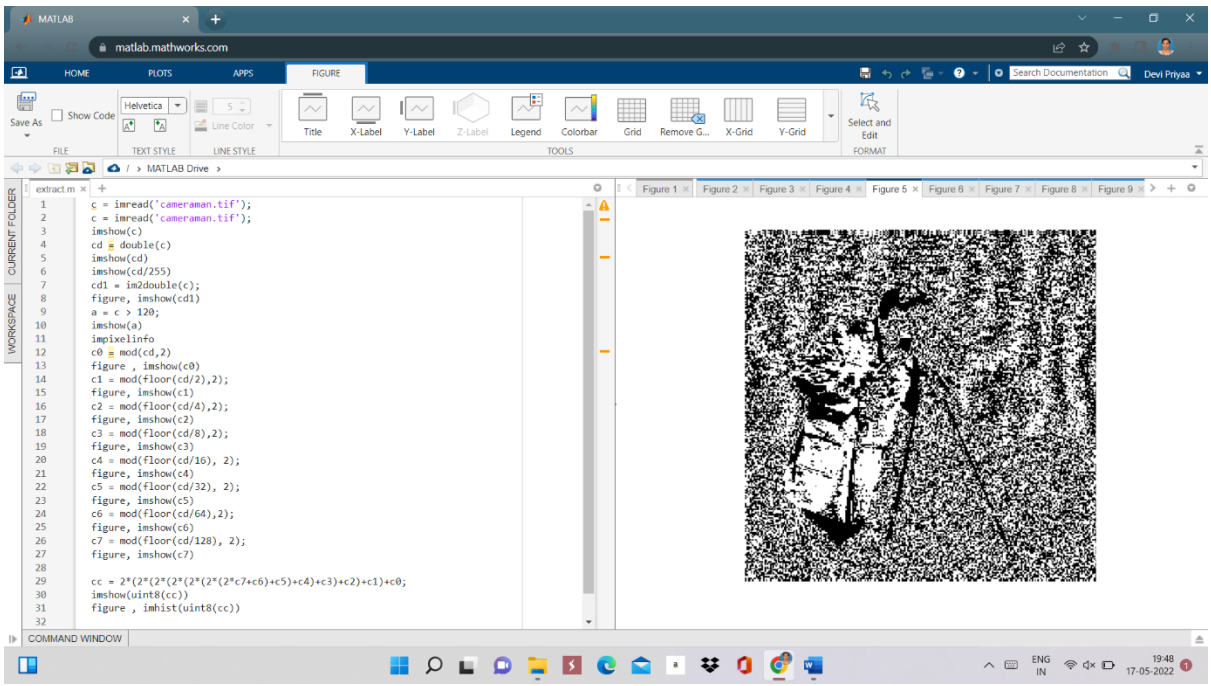
For Cameraman image



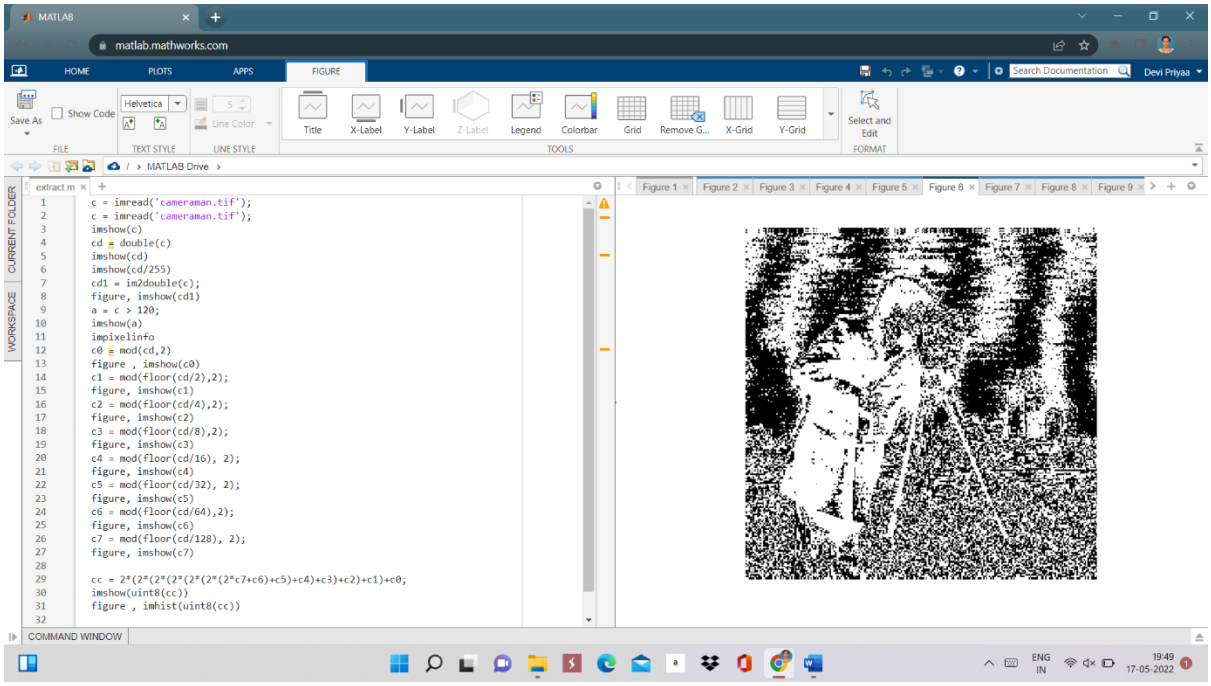
1st Bit Plane



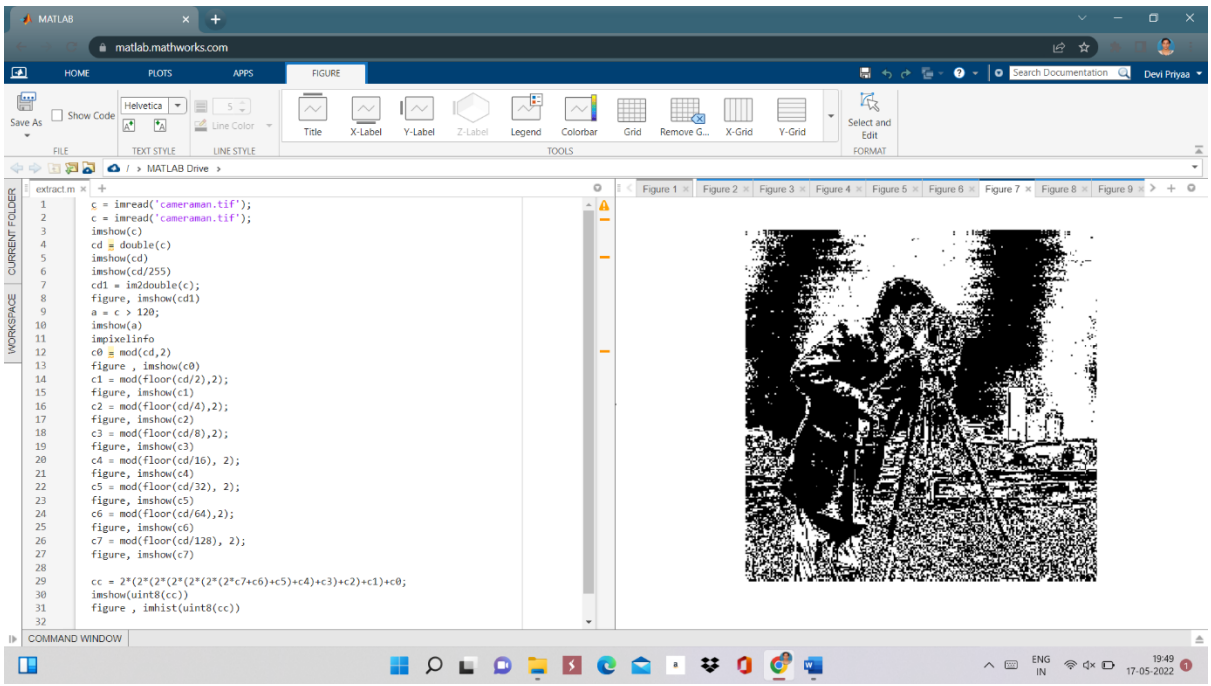
2nd Bit Plane



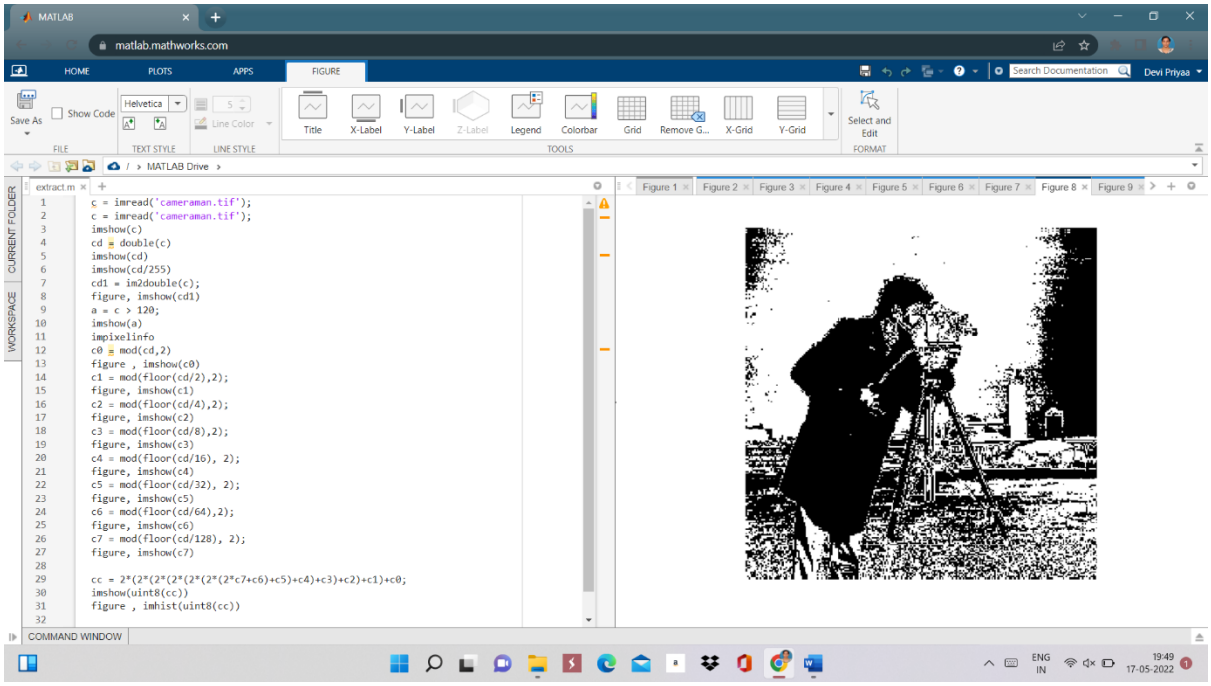
3rd Bit Plane



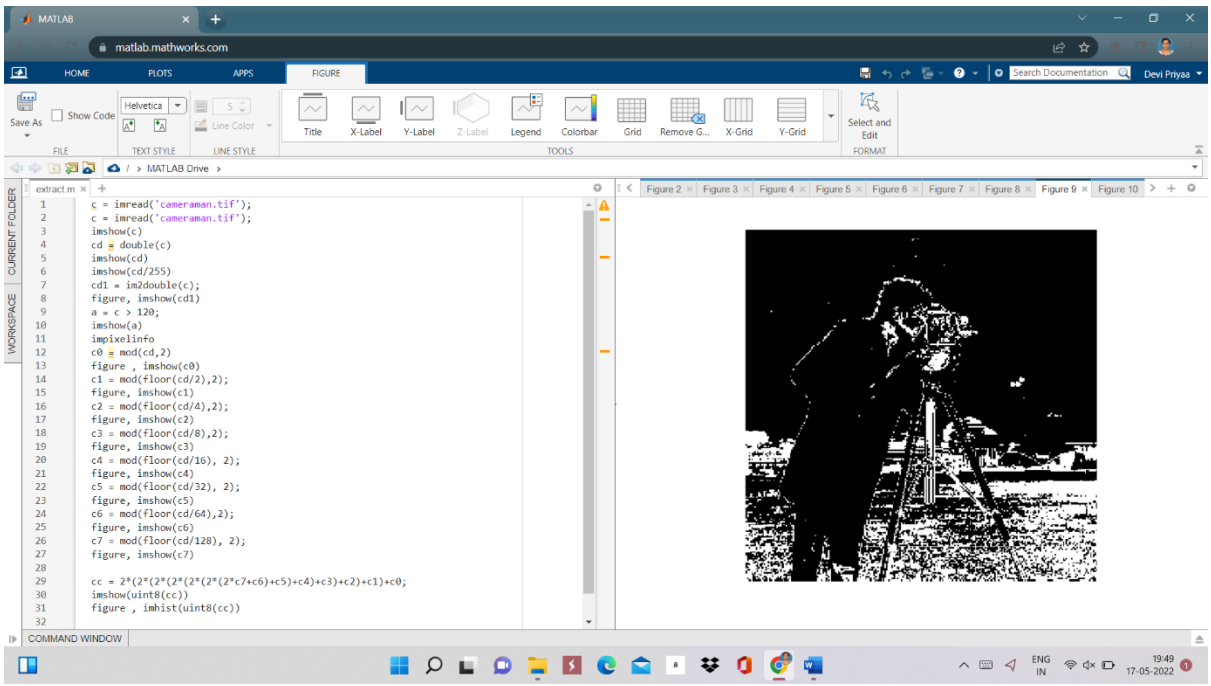
4th Bit Plane



5th Bit Plane

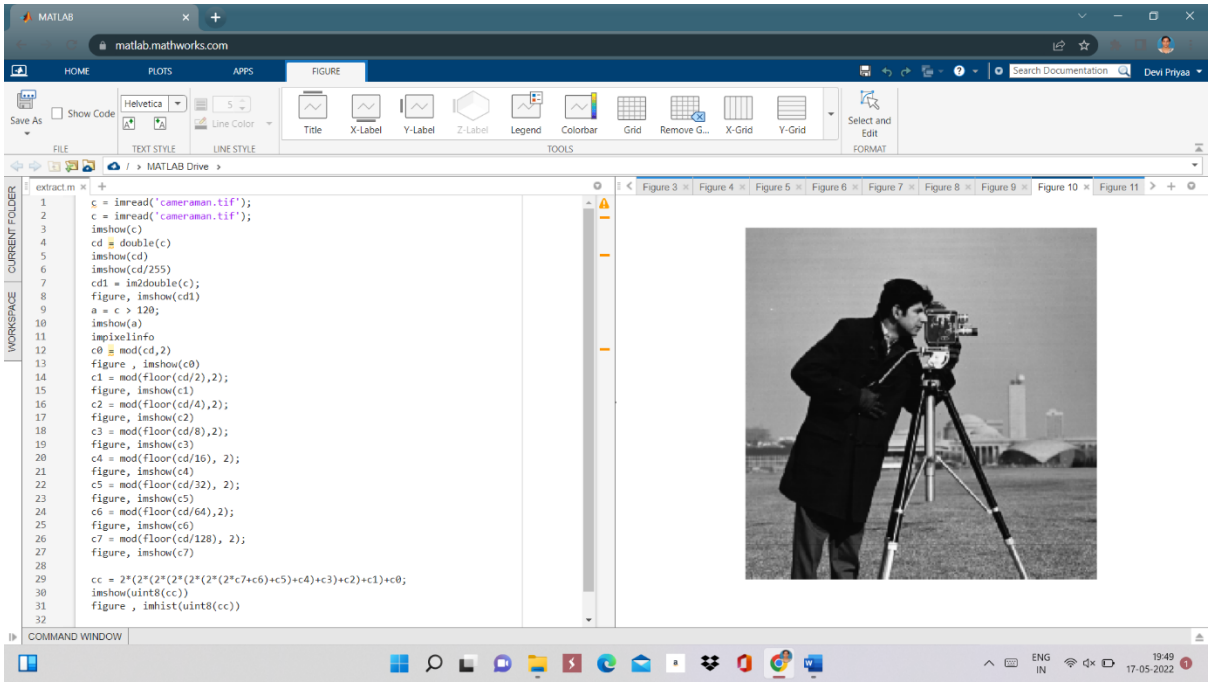


6th Bit Plane



7th Bit Plane

we are converting the binary format to the integer format, then only the original image is retained.



6.4 MATLAB IMAGE OUTPUT

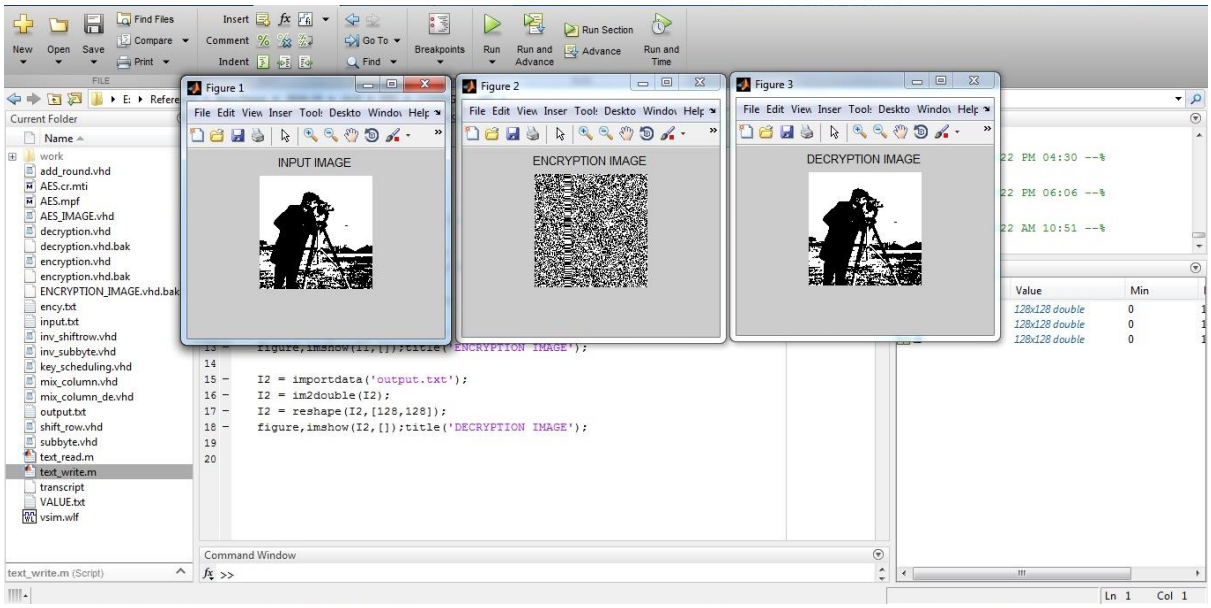


Fig 6.1 Encryption and Decryption of Images

6.5 MODELSIM OUTPUT FOR TEXT

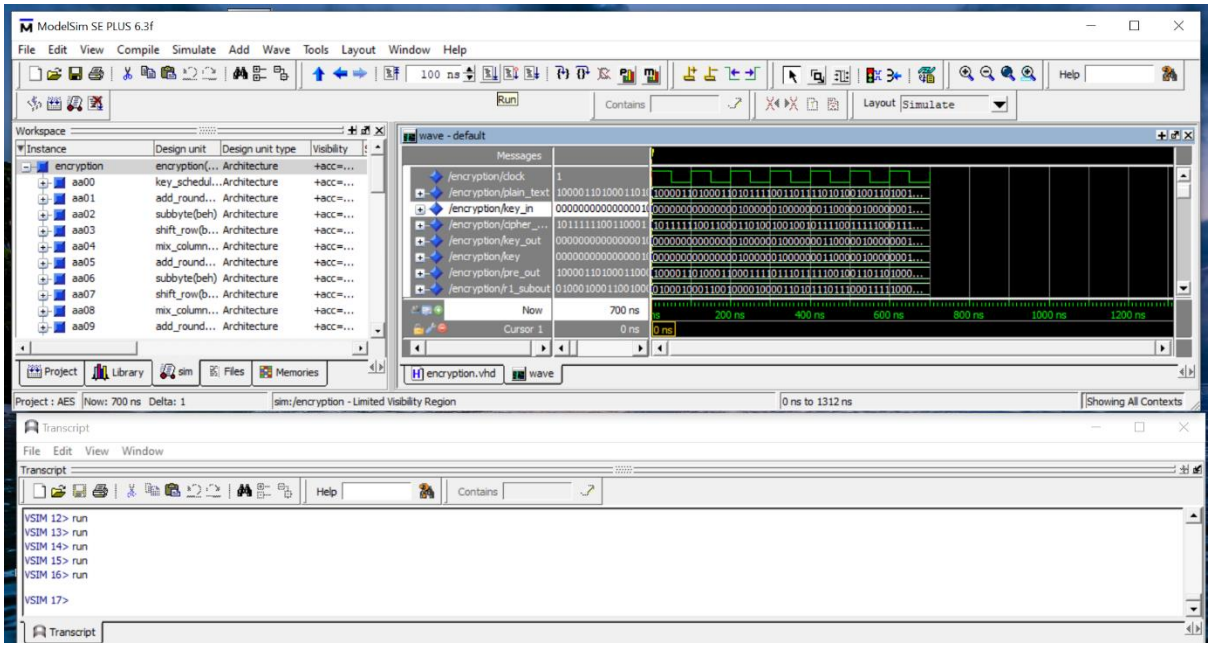


Fig 6.2 Encryption for text

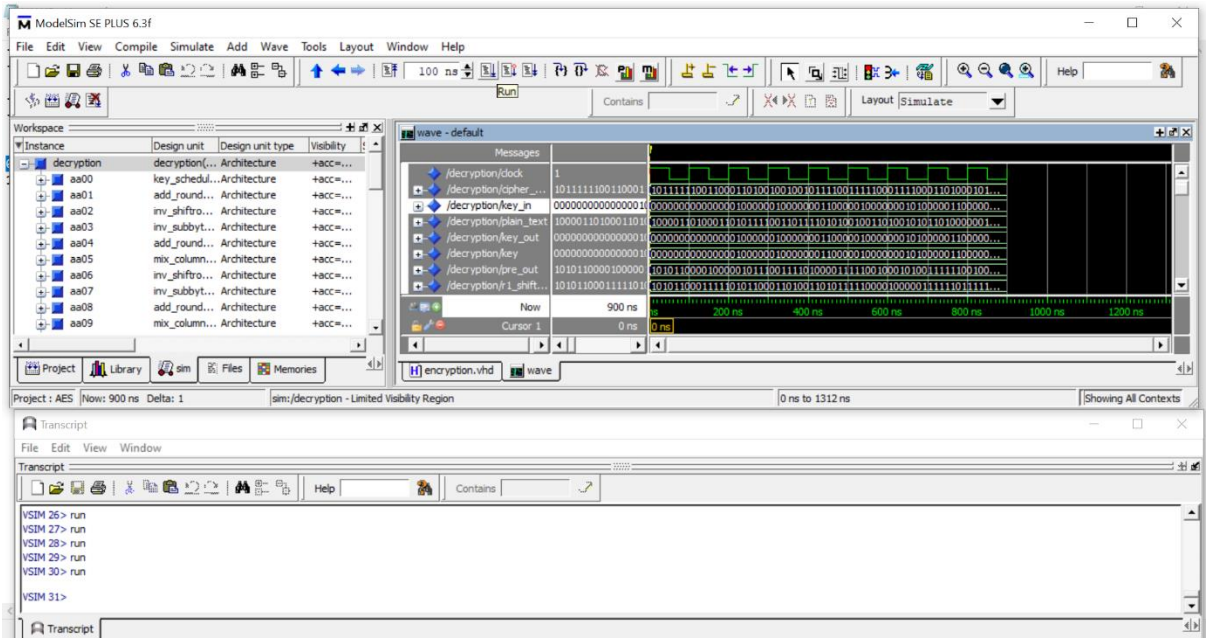


Fig 6.3 Decryption for text

6.6 MODELSIM OUTPUT FOR IMAGE

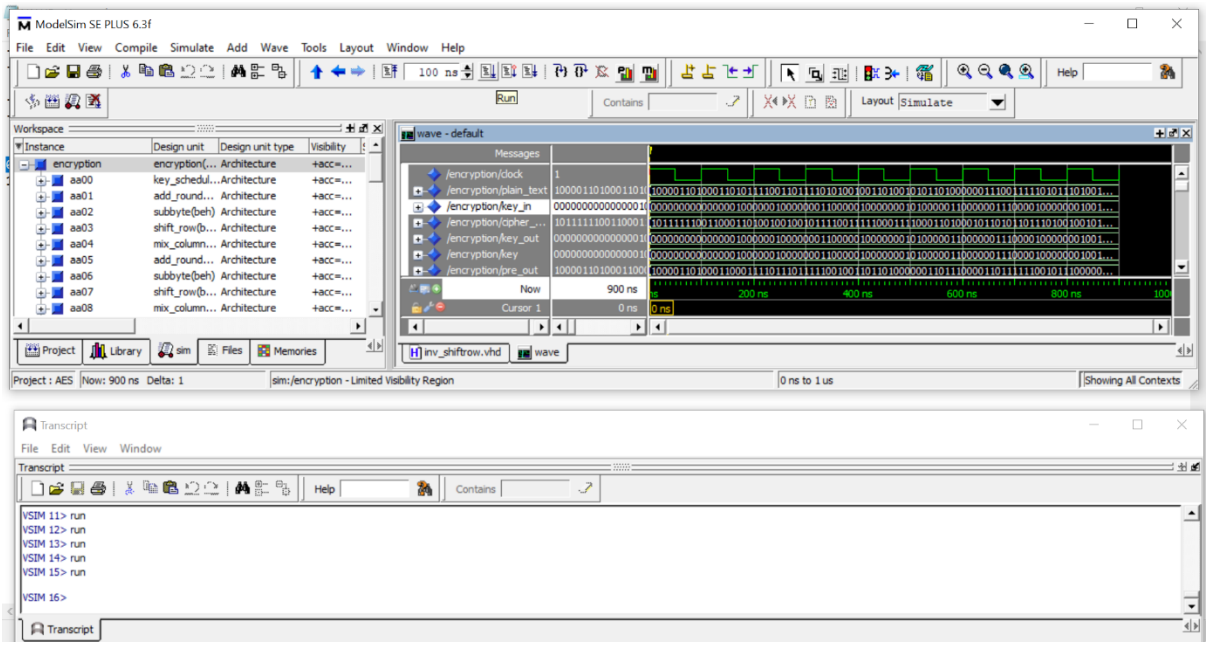


Fig 6.4 Encryption for Image

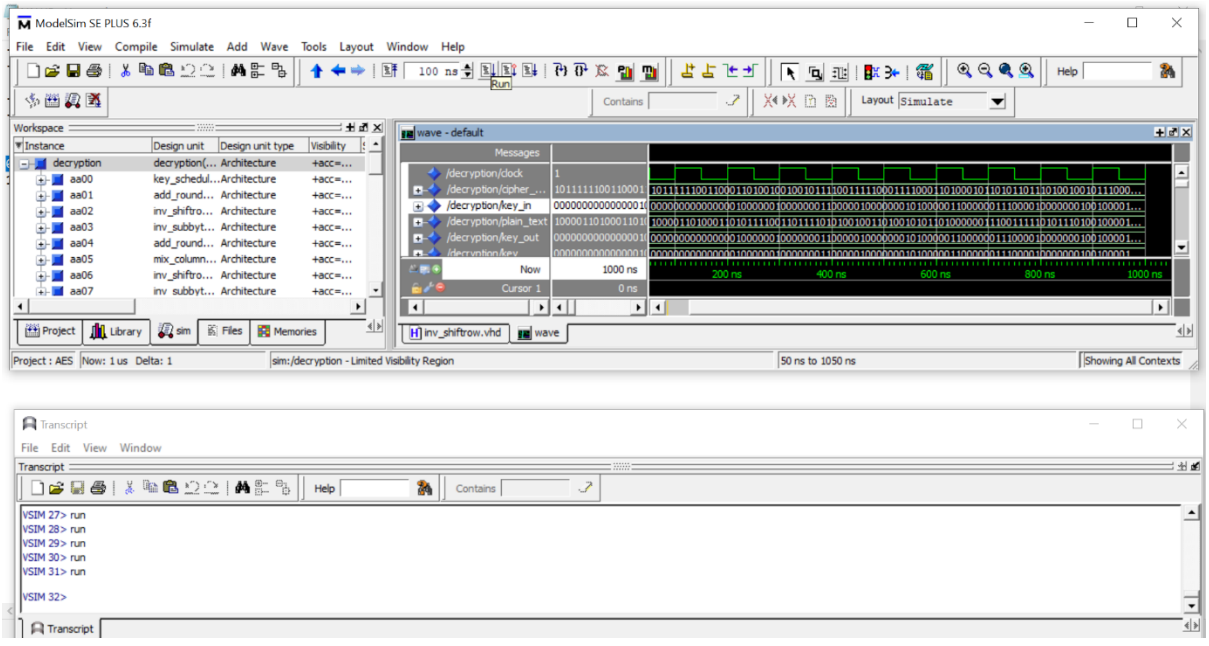


Fig 6.5 Decryption for Images

DATA USED

Encryption

Input:
1000011010001101011110011011110101001001101001010110100000011100111110101110100100010001010110101010001001100000000101110100000

Key:
0000000000000001000000100000001100000100000001010000011000000111000010000000100100001010000010110000110000001101000011100000111

Output:
1011111100110001101001001001011110011111000111100011010001011010110111010010010111000100011101111111011001010110110011010010111

Decryption

Input:
1011111100110001101001001001011110011111000111100011010001011010110111010010010111000100011101111111011001010110110011010010111

Key:
0000000000000001000000100000001100000100000001010000011000000111000010000000100100001010000010110000110000001101000011100000111

Output:
1000011010001101011110011011110101001001101001010110100000011100111110101110100100010001010110101010001001100000000101110100000

CHAPTER 7
CONCLUSION

Using internet and network are increasing rapidly. Everyday a lot of digital data have been exchanging among users. Some of data is sensitive that need to protect from intruders. Encryption algorithms play vital roles to protect original data from unauthorized access. Various kind of algorithms are existed to encrypt data. Advanced encryption standard (AES) algorithm is one of the efficient algorithms and it is widely supported and adopted on hardware and software. This algorithm enables to deal with different key sizes such as 128, 192, and 256 bits with 128 bits block cipher. In this paper, explains a number of important features of AES algorithm and presents some previous research that have done on it to evaluate the performance of AES to encrypt data under different parameters. According to the results obtained from research shows that AES has the ability to provide much more security compared to other algorithms like DES, 3DES etc.

Image Encryption and Decryption using AES algorithm is implemented to secure the image data from an unauthorized access. A Successful implementation of symmetric key AES algorithm is one of the best encryption and decryption standard available in market. With the help of MATLAB coding implementation of an AES algorithm is synthesized and simulated for Image Encryption and Decryption. The original images can also be completely reconstructed without any distortion. It has shown that the algorithms have extremely large security key

space and can withstand most common attacks such as the brute force attack, cipher attacks and plaintext attacks.

REFERENCES

[1] Jha Y, Kaur K, Pradhan C., "Improving image encryption using two-dimensional logistic map and AES" in 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, pp. 0177 – 0180.

[2] S.M. Soliman, B. Magdy and M.A. Abd El Ghany, "Efficient implementation of the AES algorithm for security applications" IEEE 2016 29th International System-on-chip Conference (SOCC), 2016, pp.206-210.

[3] B.V Varun, A. M.V., A.C. Gangadhar and P.U., "Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices," 2019 IEEE 19th International Conference on Communication Technology (ICCT),2019, pp. 1391-1395.

[4] R. Yu et al., "Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network," in IEEE Access, vol.5, pp. 24944-24951, 2017.

[5] R. Ueno et al., "High Throughput/Gate AES Hardware Architectures Based on Datapath Compression," in IEEE Transactions on Computers, vol. 69. No. 4, pp. 534-548, 1 April 2020.

[6] Issam Hammad, Ezz El-Masry., “High Speed AES Encryptor with Efficient Merging Techniques” in IEEE embedded system letters, 2010, pp.67-71.

[7] Nur Afifah, Aris Fanani, Yuniar Farida and Putroue keumala Intan, “Image Cryptographic Application Design using Advanced Encryption Standard (AES) Method in Built Environment, Science and Technology International Conference 2018.

[8] B. Koziel, R. Azarderakhsh and M.M. Kermani, “A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography,” in IEEE Transactions on Computers, vol.67, no. 11, pp. 1594-1609, 1 Nov. 2018.

[9] P. Jindal, A. Kaushik, and K. Kumar, “Design and Implementation of Advanced Encryption Standard Algorithm on 7th Series Field Programmable Gate Array,” in IEEE 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1-3.

[10] E.R Naru, H. Saini, and M, Sharma, “A recent review on lightweight cryptography in Iot,” 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),2017, pp. 887-890.

[11] M. Dworkin, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST Spec. Publ., Gaithersburg, MD, USA, 2007.

[12] Y. Hori, A. Satoh, H. Sakane, and K. Toda, “Bitstream encryption and authentication with AES-GCM in dynamically reconfigurable systems,” in Proc. Int. Conf. Field Program. Logic Appl. (FPL), 2008, pp. 23–28

[13] Norouzi B et al, “A simple, sensitive ad secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process”, 2019., pp-1469 – 1497.

[14] Sourabh Singh, Anurag Jain, “An Enhanced Text to Image Encryption Technique using RGB Substitution and AES”, in 2013 International Journal of Engineering Trends and Technology (IJETT) vol. 4, issue – 5, pp. 2108-2112.

[15] R. Gopinath, M. Sowjanya, “Image Encryption for Color Images Using Bit Plane and Edge Map Cryptography Algorithm”, in 2012 International Journal of Engineering Research and Technology (IJERT) volume 1, issue-8, pp. 1-4.