



DATA MINING USING ID SYSTEM: ADVANCED INTRUSION DETECTION SYSTEM

Raghavendra Rao .B,

Research Scholar / Department of CSE,
Bundelkhand Institute of Engineering & Technology,
Bundelkhand Univeristy, Jhansi
eliterbk@gmail.com

Dr.K.C.Roy

Director & Research,
Bundelkhand Institute of Engineering & Technology,
Bundelkhand Univeristy, Jhansi

Manuscript History

Number: **IRJCS/RS/Vol.07/Issue07/JLCS10083**

DOI: **10.26562/IRJCS.2019.JLCS10083**

Received: 22, June 2019

Final Correction: 30, June 2019

Final Accepted: 02, July 2019

Published: July 2019

Citation: Rao & K.C.Roy (2019). Data Mining Using ID System: Advanced Intrusion Detection System. International Research Journal of Computer Science (IRJCS), Volume VI, 668-674. doi://10.26562/IRJCS.2019.JLCS10083

Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Copyright: ©2019 This is an open access article distributed under the terms of the Creative Commons Attribution License, Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract— For every communication system data security is the primary concern. Because of the unceasingly intense growth of internet and communication has made extensive use of images unavoidable. For the effective security of communication AES Algorithm for encryption and decryption has been introduced. It is based on AES Key Expansion where encryption process is bitwise exclusive or operation of a set of image pixels using 128 bit keys which changes for every pixels set. The Advanced Encryption Standard can be programmed both in software as well as in pure hardware. It is a most effective way of protecting sensitive information as it is stored on media or transmitted through the communication paths.

Index Terms— Data mining; pixels; IDS; AES Algorithm; Intrusion; System

I. INTRODUCTION

There has been a need of secure transmission and storage of data to protect it from unauthorized access. Encryption is one of the common techniques to validate image security. Encryption of Images and Videos has a very wide application in various field which includes internet connection, Multimedia systems, the Industrial process, for transmitting medical images, Tele-Communication and military communication ,legal images that could contain a lot of confidential information. In the previous times Vector Quantization was used for the protection of images as an image encryption technique. In VQ image can be decomposed into vectors, which is then encoded and decoded vector by vector. Chaotic Algorithm was also used for the image cryptography. A chaotic map was created by symmetric block encryption Algorithm for permutation and diffusion of data. For encryption by using chaotic maps iteratively, multiple times is applied to the image. National Institute of Standard and Technology (NIST) defined the AES Algorithm.AES Algorithm makes uses of identical keys for the sender and receiver, for the encryption of message text and for the decryption of the cipher text. Over times many Algorithms have come from over the world for the Data Encryption but Rijndael Algorithm has been considered best for the purpose of security, Performance, Efficiency, implementing ability and flexibility. Rijndael has been defined as a block cipher that is developed by Joan Daemen and Vincent Rijmen. The algorithm is very smooth in supporting any combination of different datas and key size of 128, 192, and 256 bits. Though, AES hardly allows for a 128 bit data of length that could be divided into four most basic operation blocks. These blocks can operate on an array of bytes and can also be organized as a 4×4 matrix that is known as the state. For encrypting it fully, the data has to be passed through Nr rounds (Nr = 10, 12, 14) [4, 6].

These rounds can be governed by the given transformations:

- i. Byte sub transformation: It is known as a non linear byte Substitution, by using substitution table (s-box), that is constructed by multiplicative inverse and using affine transformation.
- ii. Shift rows transformation: It is a simple byte transposition, in which the given bytes presented in the last three rows of the state are shifted cyclically; the offset in the left shift also varies from one byte to three bytes.
- iii. Mix columns transformation: It is equivalent to a matrix multiplication of columns of the states. Each column vector is being multiplied by a fixed matrix. It is to be noted that the bytes has to be treated as a polynomials not as the numbers.
- iv. Add round key transformation: It is a simple XOR present between the working state and the round key. Its own inverse is its transformation

AES algorithm is considered as an efficient scheme for hardware and software both the implementations. But if we compare to software implementation, hardware implementation results in providing a greater security and very high speed. Hardware implementation has also been successful in providing wireless security like military communication and mobile communication where there is a bigger impact on the speed of communication. A lot of work that is shown has been presented on hardware implementation of AES by using FPGA.

II. LITERATURE REVIEW

A. Image Encryption using a new parametric switching chaotic system,2016

By- Yicong Zhou, Long Bao , C.L Philip Chen

It introduced the new parametric switching chaotic system known as PSCS and its correspondent transforms for encrypting images. The presented parametric switching chaotic system has a very simple structure and integrates the logistic, tent maps and sine into one individual system. It can be implemented in both software and hardware. The 1D and 2D transforms are being proposed for coherent scrambling data streams and images.

B. Image Encryption using P-Fibonacci transform and decomposition,2017

By-Karen Panetta, Yicong Zhou, Sos Aagain

In the given paper they present a modern approach to move forward the security level of bit-plane decomposition based encryption calculations. a unused picture encryption calculation by combining two well-known approaches has been presented: picture bit-plane decomposition and the picture pixel stage utilizing recursive sequences. The p-Fibonacci sequence has been chosen as an case of recursive groupings and the Fibonacci P-code bit-plane decomposition as a decomposition case which incorporates the conventional picture bit-plane deterioration (i.e. $PD = 0$). The displayed PFE algorithm, on the other hand, has illustrated a unused application of the Fibonacci P-code and its bit-plane decomposition for picture encryption. The PFE calculation comprises of five forms: decomposition prepare, a bit-plane rearranging handle, a bit-plane resizing prepare, an encryption handle and a information mapping process. Both of the decomposition and encryption processes are parameter subordinate.

C. Image Encryption Using Affine Transform and XOR Operation, 2018

By-Amitava Nag,Jyoti Prakash Singh, Srabani Khan,D.Sarkar

They proposed a two stage encryption and decryption calculations that is based on rearranging the image pixels utilizing relative change and they encrypting the coming about picture utilizing XOR operation. They redistribute the pixel values to diverse area using affine change strategy with four 8-bit keys. The transformed picture at that point separated into 2 pixels x 2 pixels blocks and each piece is scrambled utilizing XOR operation by four 8-bit keys. The add up to key estimate utilized in algorithm is 64 bit. Their comes about demonstrated that after the affine change the relationship between pixel values was essentially diminished.

D. Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it, 2019

By- Kuldeep Singh and Komalpreet Kaur

In this paper we have compared four diverse chaotic maps Cross chaotic, Calculated, Ikeda and Henon outline. Through the recreation comes about, histogram analysis and relationship examination we have found out that cross chaotic outline appeared best comes about than other three chaotic maps. It is sensitive to the secret keys, it has larger key space, and it gives best encrypted picture. This appears that cross chaotic outline is best reasonable for the picture encryption. Moreover, cross chaotic outline stand up to most of the known attacks such as statistical attack, differential attack and thorough assault. We have moreover appeared the impact of different commotions on the picture. In spite of the fact that the quality of picture corrupts due to the impact of noise but not to an extend that picture cannot be recognized.

E. A Digital Image Encryption Algorithm based composition of two logistic Maps,2019

By-Ismael Amr Ismail,Mohammad Amin, and Hossam Diab

The introduced an efficient chaos-based stream cipher , that is composed of two logistic maps and a quite large external secret key for the image encryption.In the propound image encryption method, an external key that is of 104 bit and two chaotic logistic maps were used that confused the relationship between the normal plain image and cipher image. And for making the cipher more robust against any attack, the private key is modified once the encryption of each pixel of plain image is done.The vitality of the proposed algorithm,makes the encryption of each plain pixel dependent on the key, the cipher text value, and the output of the logistic map.

F. Image Encryption using DCT and Stream cipher, 2019

By-Lala Krikor, Sami Baba, Thawar Arif, Zyad Shaaban

The proposed encryption strategy employs the Particular Encryption approach where the DC coefficients and a few particular AC coefficients are scrambled, consequently the DC coefficients carry critical visual information, and it's troublesome to anticipate the specific AC coefficients, this allows a tall level of security in comparison with strategies specified over. The calculation will not scramble bit by bit the whole image but as it were particular DCT coefficients will be scrambled, and additional security has been included to the resulted scrambled pieces by utilizing Piece Rearranging strategy depending on two prime numbers, where these two primes will produce groupings or push and column numbers to be utilized in rearranging. The algorithm is considered as a quick picture encryption calculation, due to the particular encryption of certain portion of the picture (the DC and a few AC coefficients).

G. Image Encryption Using Advanced Hill Cipher Algorithm, 2018

By-Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda

A cipher algorithm has been proposed which has used an Involuntary key matrix for encryption. They used distinctive pictures and encrypted them by making use of original Hill cipher calculation and their proposed AdvHill cipher algorithm. And it has been clearly noticeable that the original Slope Cipher cannot encrypt the images properly on the off chance that the picture comprises of expansive range covered with same colour or gray level. But their proposed algorithm works for any pictures with distinctive gray scale as well as colour images.

H. Image Encryption Using Block-Based Transformation Algorithm, 2018

By-Mohammad Ali Bani Younes and Aman

They presented a block-based transformation calculation that is based on the combination of image transformation and one of the much known encryption and unscrambling algorithm known as Blowfish. The original image can be isolated into blocks, which were modified into a transformed image using a transformation algorithm, and at that point the transformed image was encrypted by making use of the Blowfish algorithm. Their conclusion also shows that expanding the number of pieces by using smaller piece sizes comes about in a lower relationship and higher entropy.

I. Modified AES Based Algorithm for Image encryption, 2018

By-M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki

In this paper a modern modified version of AES, to plan a secure symmetric picture encryption method, has been proposed. The AES is expanded to back a key stream generator for picture encryption which can overcome the problem of finished zones existing in other known encryption algorithms. Detailed analysis has appeared that the unused scheme offers high security, and can be realized effortlessly in both hardware and program. The key stream generator has an important impact on the encryption execution. We have shown that W7 gives superior encryption comes about in terms of security against factual examination assaults.

III. ADVANCED ENCRYPTION STANDARD

A. IDS Structure

Data block of 4 columns of 4 bytes is state key is expanded to array of words has a 9/11/13 round in which state undergoes:

- Byte Substitution (1 S-box Used On Every Byte)
- Shift Rows (Permute Bytes Between Groups/Columns)
- Mix Columns (Subs Using Matrix Multiply Of Groups)
- Add Round Key (Xor State With Key Material)
- View As Alternating Xor Key & Scramble Data Bytes

Initial Xor Key Material & Incomplete Last Round with fast XOR & table lookup implementation

B. Operation of IDS

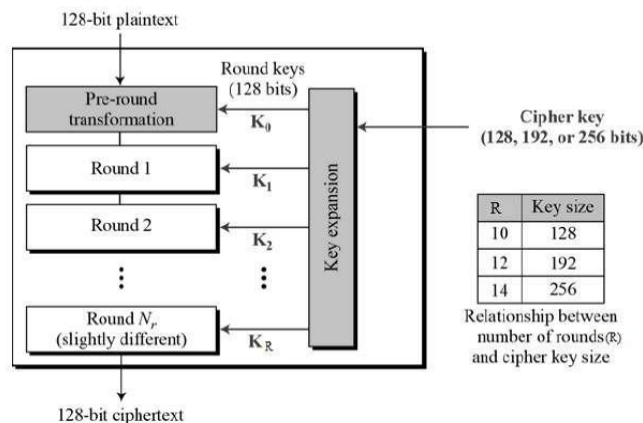


Fig 1. Schematic of ID Structure

AES is an iterative rather than Feistel cipher. It is based on 'substitution-permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key

C. Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below:

1) Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns

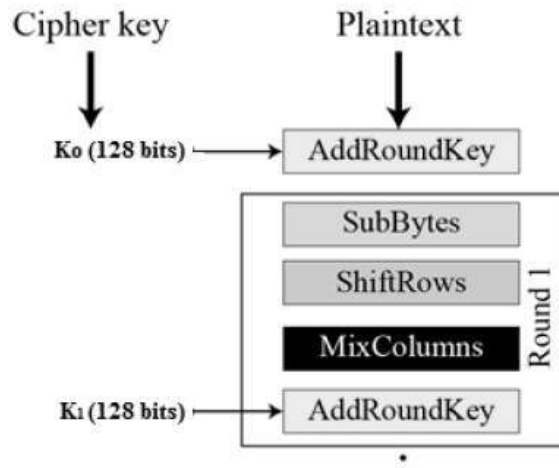


Fig 2. Round Operation

2) Shift rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3) MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4) Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XOR ed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

D. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order

1. Add round key
2. Mix columns
3. Shift rows
4. Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithm needs to be separately implemented, although they are very closely related.

IV. IMPLEMENTATION

A. Programming Language :-

Python 2.7

B. Library :-

- Open Cv 3.1 :- For Image Manipulation
- Numpy :- matrix operation

C. File Details :-

- dev_AES.py :- Contain Base AES algorithm
- dev_main.py :- Input output operation for image and image manipulation
- base image: - a.jpg
- after encryption :- encrypt-img.p
- output image after decryption :- OUTPUT.bmp

D. Input files /operation :

- input_file :- a.jpg
- call Function enc() in dev_main.py

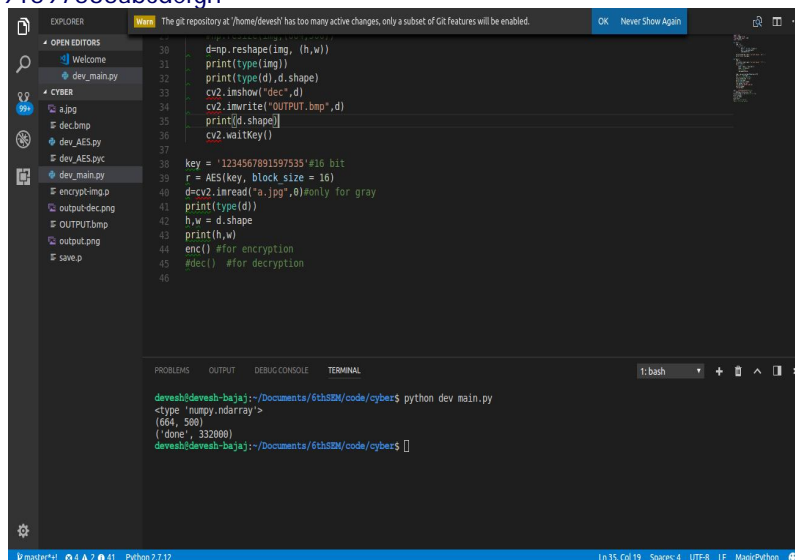
E. Output :

- encrypt-img.p (encrypted Image)

V. RESULT

A. For 128 bit Key

Key Used:- 1234567891597535abcdefg



```
30 d=np.reshape(img, (h,w))
31 print(type(img))
32 print(type(d),d.shape)
33 cv2.imshow("dec",d)
34 cv2.imwrite("OUTPUT.bmp",d)
35 print(d.shape)
36 cv2.waitKey()
37
38 key = '1234567891597535' #16 bit
39 r = AES(key, block size = 16)
40 d=cv2.imread("a.jpg",0)#only for gray
41 print(type(d))
42 h,w = d.shape
43 print(h,w)
44 enc() #for encryption
45 #dec() #for decryption
46
```

```
devesh@devesh-baja:~/Documents/6thSEM/code/cyber$ python dev main.py
<type 'numpy.ndarray'>
(664, 506)
('done', 332800)
devesh@devesh-baja:~/Documents/6thSEM/code/cyber$
```

Fig 3. Encryption

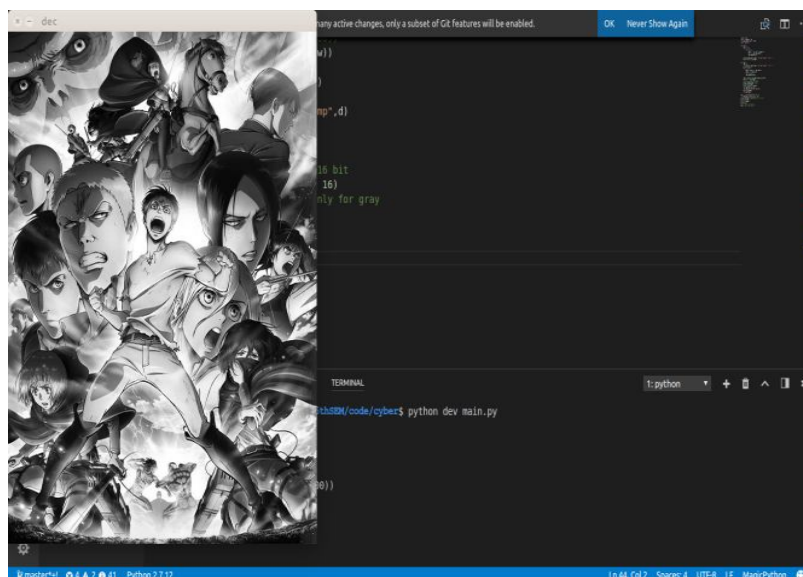
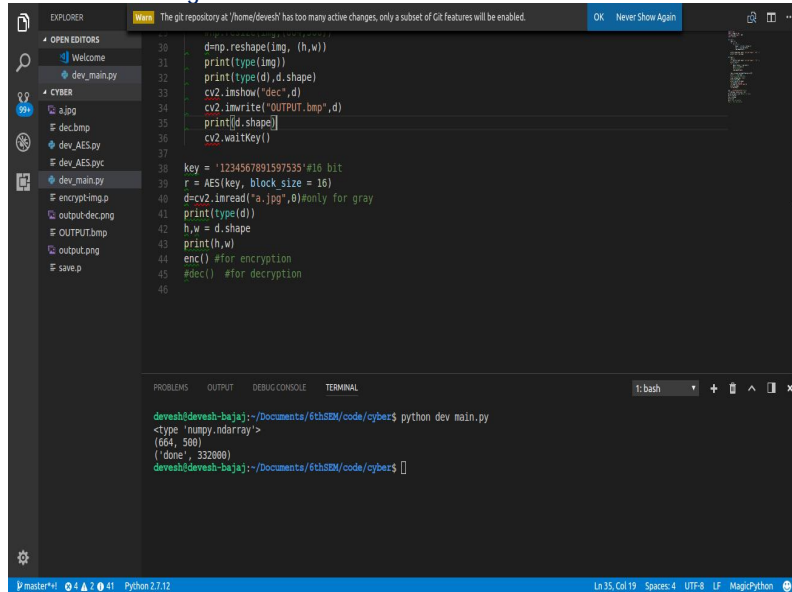


Fig 4. Decryption

B. For 192 bits

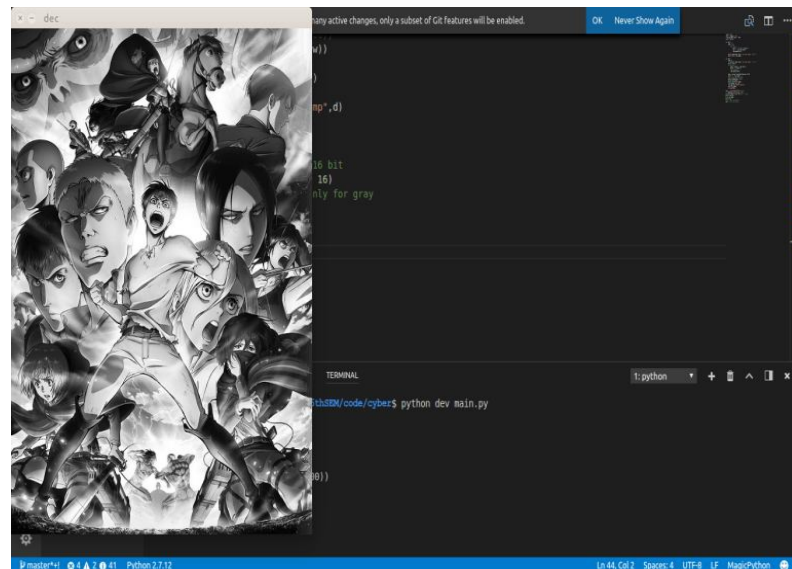
Key Used:- 1234567891597535abcdeefgh



```
30 dmp.reshape(img, (h,w))
31 print(type(img))
32 print(type(d), d.shape)
33 cv2.imshow("dec", d)
34 cv2.imwrite("OUTPUT.bmp", d)
35 print(d.shape)
36 cv2.waitKey()
37
38 key = '1234567891597535'#16 bit
39 r = AES(key, block_size = 16)
40 d=cv2.imread("a.jpg",0)#only for gray
41 print(type(d))
42 h,w = d.shape
43 print(h,w)
44 enc() #for encryption
45 #dec() #for decryption
46
```

```
devesh@devesh-bajaj:~/Documents/6thSEM/code/cyber$ python dev main.py
<type 'numpy.ndarray'>
(664, 500)
('done', 332000)
devesh@devesh-bajaj:~/Documents/6thSEM/code/cyber$
```

Fig 5. Encryption



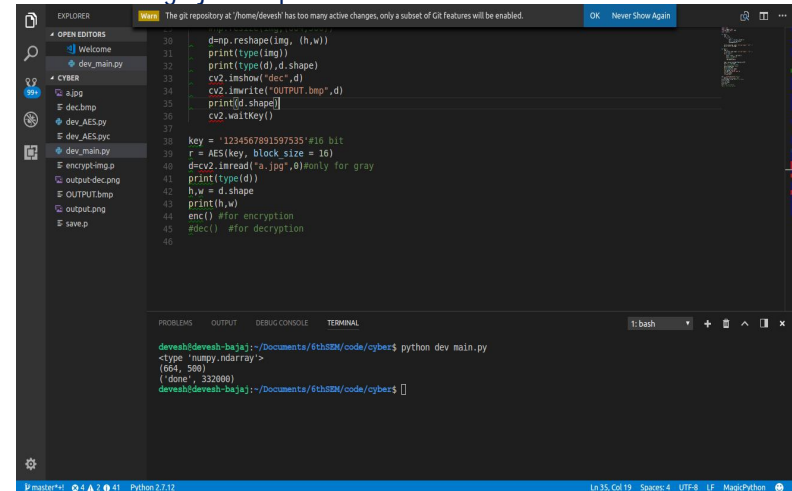
```
30 dmp.reshape(img, (h,w))
31 print(type(img))
32 print(type(d), d.shape)
33 cv2.imshow("dec", d)
34 cv2.imwrite("OUTPUT.bmp", d)
35 print(d.shape)
36 cv2.waitKey()
37
38 key = '1234567891597535'#16 bit
39 r = AES(key, block_size = 16)
40 d=cv2.imread("a.jpg",0)#only for gray
41 print(type(d))
42 h,w = d.shape
43 print(h,w)
44 enc() #for encryption
45 #dec() #for decryption
46
```

```
devesh@devesh-bajaj:~/Documents/6thSEM/code/cyber$ python dev main.py
<type 'numpy.ndarray'>
(664, 500)
('done', 332000)
devesh@devesh-bajaj:~/Documents/6thSEM/code/cyber$
```

Fig 6. Decryption

C. For 256 bits

key_32= 1234567891597535abcdeefghijklmnop



```
30 dmp.reshape(img, (h,w))
31 print(type(img))
32 print(type(d), d.shape)
33 cv2.imshow("dec", d)
34 cv2.imwrite("OUTPUT.bmp", d)
35 print(d.shape)
36 cv2.waitKey()
37
38 key = '1234567891597535abcdeefghijklmnop'#32 bit
39 r = AES(key, block_size = 16)
40 d=cv2.imread("a.jpg",0)#only for gray
41 print(type(d))
42 h,w = d.shape
43 print(h,w)
44 enc() #for encryption
45 #dec() #for decryption
46
```

```
devesh@devesh-bajaj:~/Documents/6thSEM/code/cyber$ python dev main.py
<type 'numpy.ndarray'>
(664, 500)
('done', 332000)
devesh@devesh-bajaj:~/Documents/6thSEM/code/cyber$
```

Fig 7. Encryption

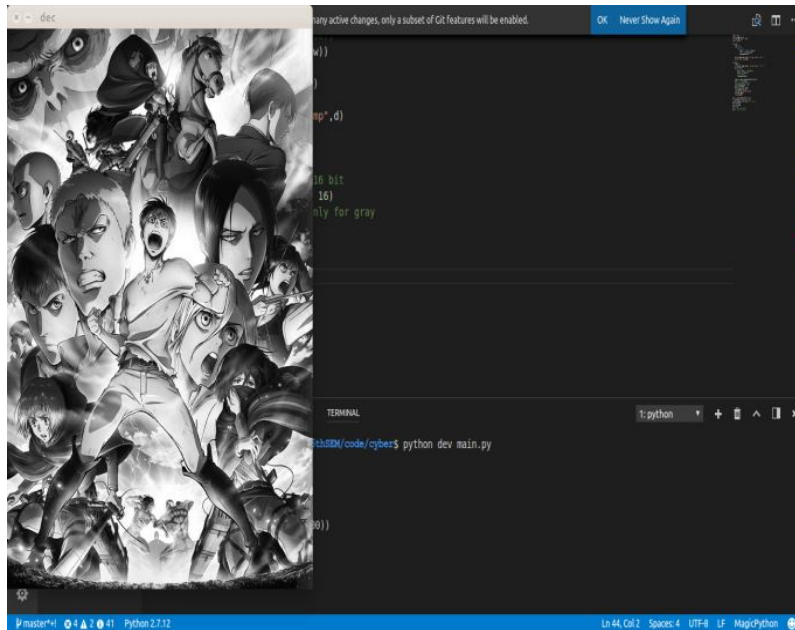


Fig 8. Decryption

VI. PERFORMANCE MEASURES

S. No	Size of Encryption Key	Time For Encryption (sec)	Time For Decryption (sec)
1	16 (128 bit)	18.69	20.25
2	24 (192 bit)	25.45	29.37
3	32 (256 bit)	28.56	32.42

REFERENCES

1. Zhou, Yicong, Long Bao, and CL Philip Chen. "Image encryption using a new parametric switching chaotic system." *Signal processing* 93, no. 11 (2013): 3039-3052.
2. Zhou, Yicong, Karen Panetta, Sos Agaian, and CL Philip Chen. "Image encryption using P-Fibonacci transform and decomposition." *Optics Communications* 285, no. 5 (2012): 594-608.
3. Nag, Amitava, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, and Partha Pratim Sarkar. "Image encryption using affine transform and XOR operation." In *Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on*, pp. 309-312. IEEE, 2011.
4. Singh, Kuldeep, and Komalpreet Kaur. "Image encryption using chaotic maps and DNA addition operation and noise effects on it." *International Journal of Computer Applications (0975-8887) Volume* (2011).
5. Ismail, Ismail Amr, Mohammed Amin, and Hossam Diab. "A digital image encryption algorithm based a composition of two chaotic logistic maps." *IJ Network Security* 11, no. 1 (2010): 1-10.
6. Krikor, Lala, Sami Baba, Thawar Arif, and Zyad Shaaban. "Image encryption using DCT and stream cipher." *European Journal of Scientific Research* 32, no. 1 (2009): 47-57.
7. Acharya, Bibhudendra, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda. "Image encryption using advanced hill cipher algorithm." *International Journal of Recent Trends in Engineering* 1, no. 1 (2009).
8. Bani Younes, Mohammad Ali, and Aman Jantan. "Image encryption using block based transformation algorithm." (2008).
9. Zeghid, Medien, Mohsen Machhout, Lazhar Khriji, Adel Baganne, and Rached Tourki. "A modified AES based algorithm for image encryption." *International Journal of Computer Science and Engineering* 1, no. 1 (2007): 70-75.