Modified AES Algorithm Integrating IBDP (Image Block Displacement Procedure) for Data Encryption

Anukirti
PG Student
Department of Computer Science & Engineering
MIET Meerut, India

Vishal Jayaswal
Assistant Professor
Department Computer Science & Engineering
MIET Meerut, India

ABSTRACT

Today sharing of a digital images over network is growing in huge numbers. The security of network is becoming more significant as the quantity of data being exchanged on the internet rises. Apart from this, the data that is relevant for the image is also transmitted with it. Therefore, the privacy and data integrity entails protecting against illegal access and utilization. Thus these actions have resulted in enormous growth of the field of securing the data. Information ciphering is a method which is utilized for hiding data in the digital files likes- audio, images and video etc. This method is also referred to as steganography. Here the data is hidden in the image. The data may be the information about the image.

To calculate and estimate the performance of the proposed algorithm, a set of test were done which were quite successful and promising. These assessments were comprised of histogram analysis, correlation analysis, differential analysis, information entropy. Results of assessments displayed that the new integration method has a promising security features and it is more efficient than AES algorithm alone, without the shifting technique which enables it becoming a decent method for ciphering the digital data. The results exhibited that histogram of a ciphered image made a uniform distribution which is quite unique different from the histogram of the plain image and the correlation of pixels of the image was dramatically decreased by utilizing the integration method, thus higher entropy results were achieved.

General Terms

AES Algorithm, NIST, SNR, PSNR, MSE, RMSE.

Keywords

PFAK, Data Encryption, Modified Algorithm PCA, Noise, Block Cipher, NC, Noise.

1. INTRODUCTION

A digital picture can be thought of as a 2D function f (x, y) where x and y are coordinates of a plain and the amplitude of, f is described as the intensity of grey level at any pair of coordinates (x, y). When x and y and the amount of intensity all are distinct and limited then we call an image a digital image. A digital image is comprised of fixed number of pixels and each of them has a distinct location and value. These elements are known as picture elements, pixels. Pixel is a term mostly used to signify the elements of a digital image. The most advanced of a human is vision, so it is not a surprising thing that images play a vital role in human perception. Though, contrasting humans, who are limited to the visual band of an electromagnetic spectrum, imaging machines cover complete electromagnetic spectrum which ranges from gamma waves to radio waves. Machines can operate on the images on which humans cannot operate. These include electron microscopy, ultrasound and images generated by computer. Consequently, processing of a digital image encompasses a varied and wide range of applications.

Ciphering the data improves the security of the information by distorting it. To cipher the data the correct code (key) is needed and the correct code (key) to decipher information too. This is most effective method to hide the information where transmitter and receiver keep the secured code (key) to decipher the information. Ciphering is similar to transmitting undisclosed messages between senders and recipient, - if someone tries to snoop without the legitimate secured code (key) then intruder won’t be able to comprehend the communication.

Two techniques are available for ciphering: symmetric ciphering and asymmetric ciphering. Symmetric ciphering which is also called secret key ciphering. In this technique transmitter and the receiver have the same secret code (key) to cipher and decipher a communication. Another method is asymmetric key ciphering, in this approach there is a pair of keys. One for encrypting the message and another is for deciphering the message.

The AES algorithm works in 2 parts; ciphering and deciphering. In proposed method the modification are done in the encryption phase. As we know that the encryption in AES works in 4 parts: (i) Substitute bytes (ii) Change Rows (iii) Merge Columns (iv) Add Round Secret code (key). The proposed technique works on shift row phase to make improve the parametric values of the existing AES algorithm.In cryptography, the AES is also known as Rijandael [1].

2. REVIEW OF LITERATURE

Ashwini R. Tonde et.al (2014) investigated and implemented this work [1]. The deployment of high speed AES technique which is grounded on FPGA is presented, to develop the protection of the communication while transmitting. Ciphering method, mathematical principle, process of ciphering and logic structure of AES are described. Parallel processing and pipelining techniques were utilized to attain better computing speed. The virtual outputs present that high speed AES ciphering system was implemented in a right way. Design was tested on Xilinx Virtex-5 FPGA. Allpractices including virtual working and deployment were done on Model Sim ISE 13.3 development platform. Outputs show that system can finish the complete procedure in a right way in 200 MHz clock-rate.

E. Kavitha et.al (2016)in this research work [2] hardware deployment of improved area block encryption, AES by utilizing FPGA. The core comprises of the secret key schedule storage and expansion, the cipher and decipher and eight bit I/O information interfaces with complete regulation. The scheme is grounded on augmented field by utilizing time distribution of resources and duplication manner. In this paper, AES algorithm is studied and modelled in VHDL targeting for optimized area in FPGA. The design is functionally simulated in Modalism. The area optimization is verified by implementing this design on FPGA using Xilinx ISE synthesis tools.

Langfang Hebei, et.al, (2011) in this research paper [3] storage systems charged with taskof handling and storing data, centralized storage of a immense amount of information shared for multiple operators. Distortion or disclosure of such data will be a reason business problems. Old time database systems' safeguard is creating a secured PIN or privilege distribution etc., these approaches have many security problems- the administrator of the database has the access of the complete information without any constraint. The solution to this problem is to cipher the information which will ensure safeguard of the data even if the data is leaked as it will be in encrypted format.

Archana Mishra et.al, (2016) presented in this paper [4]AES which is based on VLSI which deals espionage and cybercrimes. This is widely used symmetric block encryption procedure which alters data into obscure information grounded on secret code defined modification set. Moreover, this approach doesn't compromise with data properties as the amount of input and output information is exactly similar, and it can utilized in vast range of applications. Here the writers bound their focus on 128bit AES ciphering and deciphering actions over VHDL coded alterations which needs secret key for positive accomplishment of information safeguard. With growth in multiple suggested methods for deployment of information safeguard, now it is more dynamic and crucial for a feasibility study of any hardware is very much required to check ciphering and deciphering steps of the suggested 128bit AES technique. In virtual deployment results, the authors analyse the each of the modification which is incorporated for coding on Field Programmable gate Array using Xilinx ISE tool.

Ahmed Fathy, et.al, (2012)emphasizes in this paper [6],that the implementation of AES on Field Programmable gate Array atmosphere andfocusing on newly introduced methods for improving the ciphering pace and reducing the needed deployment area. Because of their inelegance, machine learning algorithms are also vital candidates for competent AES cryptanalysis procedure and expansion.

3. BASIC THEORY

The image ciphering is to transmit the image safely over the communication channel so that no intruder could decipher the communication. Image- video ciphering have usage in several areas like-transmission, defense communication etc. The growth of ciphering is going ahead into a future of infinite opportunities. The image has unique features like- high redundancy, bulk capability and high correlation among pixels. Ciphering methods are very resourceful instruments to secureclassified data. Ciphering described as converting simple text into encrypted text which is not useful for the people not having decipher code. Deciphering is the contrast of ciphering, it is the procedure of altering the ciphered text into simple useable format. Ciphering of information has now turned as a vital way to safeguard the information obtainable on intranet or internet. Ciphering is a method of deploying exceptional mathematical techniques and secured codes (keys) to modify the information into ciphered data before making them travel over any network. The primary target of safety supervision is to give reliability, exactness, verification of operators and safeguarding of information. Safeguarding of images is a crucial requirement and process, because attack on the communication by transferring digital commodities over unrestricted network takes place often. Ciphering methods that are described and analyzed well to uplift the overall enactment of these ciphering techniques. Recently suggested image ciphering KA systems is very resourceful method as in this image information is altered into text mode as per ASCII code. So, if an intruder attempts to decode the information he won't be able to get the information as whole data is transmitted in text format. Different cryptographic methods are applied on image and on text too.

AES is Symmetric Key Algorithm that Encrypts and Decrypts the information. AES is not only for text data but also applicable for images. Its original name is Rijandael. Grounded on Rijandael encrypting method devised by 2, Joan Daemen and Vincent Rijmen. Rijandael is a group of of cipher with distinct key and size of block. For Advanced Encryption System, NIST chose three members of Rijandael group, with the block size of 128bits ,but three separate key length- 128_192_256 bits. AES has been accepted by the Government of USA and right now it is being utilized globally.

The AES technique is proficient in utilizing cryptographic keys of 128,192 and 256 bits to cipher and decipher information in chunks of 128 bits. This standard is grounded on Rijandael technique. AES method used with 3 distinct key size these 3 separate sizes are called as AES-128, AES-192, AES-256. Ciphering consists of 10 iterations of progression. for 128bits key, 12 iterations for 192bits keys and 14 iterations for 256bits keys. All other iterations are similar except last round. Each iteration of processing comprises of 1 byte based replacement steps: column wise mixing phase, row wise permutation phase andtotalling of the round key. The order of the four steps are separate for ciphering deciphering.

Permutations, substitution in algorithm AES permits fast deployment of method. For ciphering process, everyiteration comprises of 4 stages. **(i)**Replace bytes **(ii)** Shift rows **(iii)**Merge columns **(iv)**Add round key For Decryption, each round comprises of these 4 discussed steps. **(i)** Inverse move rows **(ii)** Inverse replace bytes **(iii)** Add iteration key **(iv)**Inverse mix column.

4. PROPOSED METHODOLOGY

Here shifting technique [15] is described which makes an altered table, this table would be utilized to make new modified image. The proposed method works as below,

(i) Feed the original image and fragment this into several chunks with equal number of pixels. Image is disintegrated into chunks and every single of them has finite number of pixels. Afterwards, blocks are moved to different places.

(ii) Form the shifted table of ciphering to consolidate secure cipher code and hash function, which would be utilized to shift the columns and rows of the picture. The hash function and cipher code of this technique is utilized to play vital role in construction of shifted table, which will be utilized to yield the ciphered picture with altered chunks. The shifting procedure refers to maneuver of distinguishing and displacing an arrangement of actual picture.

(iii) The primary indication is that an image can be ciphered by moving the columns, rows of the actual picture and not to alter the locations of the blocks, but by moving all rows n number of times dependent on shift table and then similar number of times for columns to organize the blocks.

The size of the block should be small for better ciphering because less number of pixels pixles would be alike to their adjacent pixel.

(iv)In this scenario, the correlation will be reduced and thus it becomes challenging to guess the value of any given pixel from the values of its neighbors.

(v) The correlation will be reduced in this situation, so it will become puzzling to approximate the value of pixel by considering value of neighboring pixels.

This perceivable data can be condensed by lessening the correlation among picture pixels employing the shifting process or some other method.

(vi)On the acceptor's end the actual image is attainable by inverse of the shifting of blocks. A detailed flow diagram of the discussed procedure is drawn below.

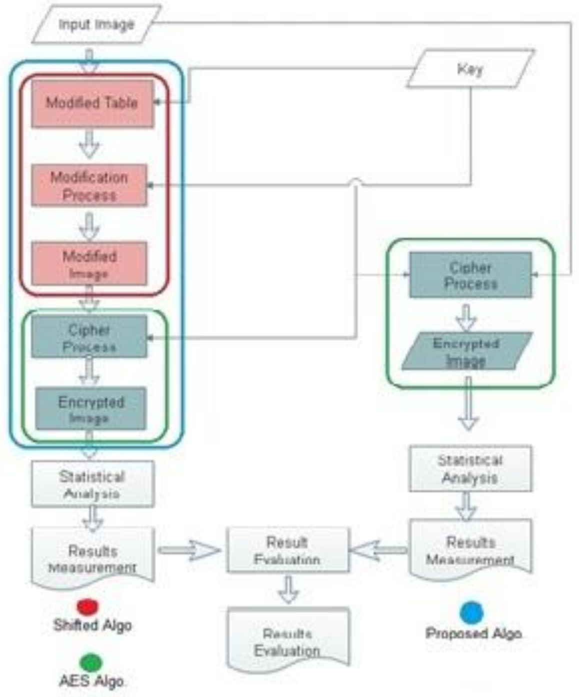

Fig 1: Flowchart of Modified AES Algorithm with IBDP Method.

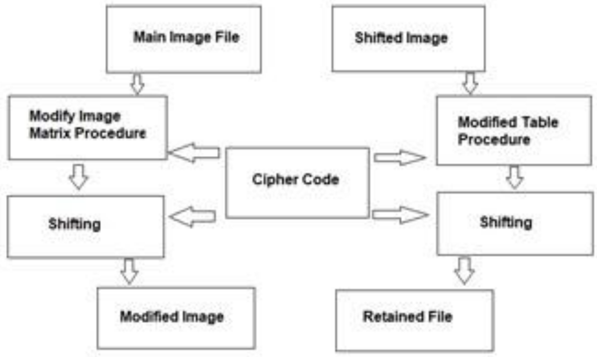

Fig 2:Working of Image Block Displacement Procedure.

5. EXPERIMENTAL RESULTS

The various images are used for the research process and to find the results. The data for image were highly dimensional, and 5 attributes have been finally considered on the basis of requirements. The image is loaded using MATLAB and processed it with existing algorithm and proposed algorithm one by one and compare the results of both algorithm.

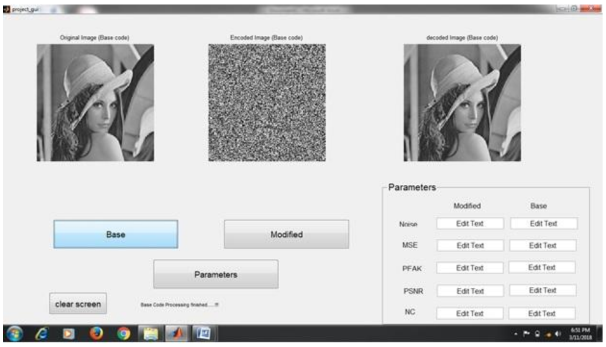
project_gui
Original Image (Base code)
Encoded Image (Base code)
decoded Image (Base code)
Parameters
Modified
Base
Noise
MSE
PFAK
PSNR
NC
Edit Text
Base
Modified
Parameters
clear screen
Base Code Processing finished.....!!!
6:51 PM
3/11/2018

Fig 3:Encrypted and Decoded Image, After Running image with AES Algorithm.

After selecting the image, we have decoded the selected image with base code, as shown in the Figure 2, above the input image has been deformed, distorted and retained back after decryption. In above screenshot the distorted image before decryption is also presented.

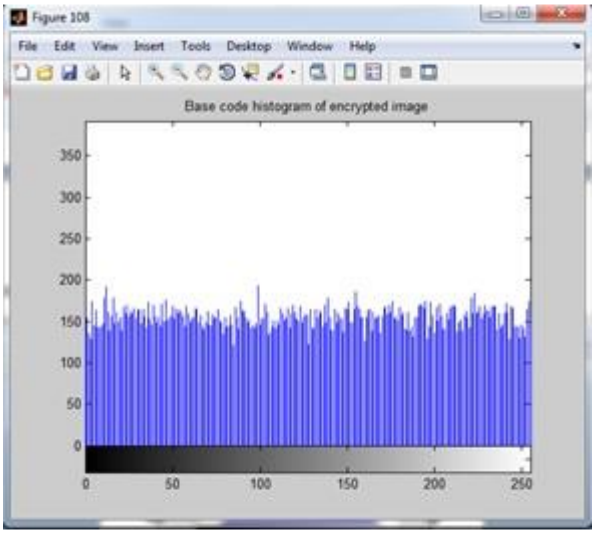

Fig4: Histogram of Encrypted Image after running with AES Algorithm.

In the Figure 3, shown above,the window is showing the Histogram of input image after distortion when it was run with base code.

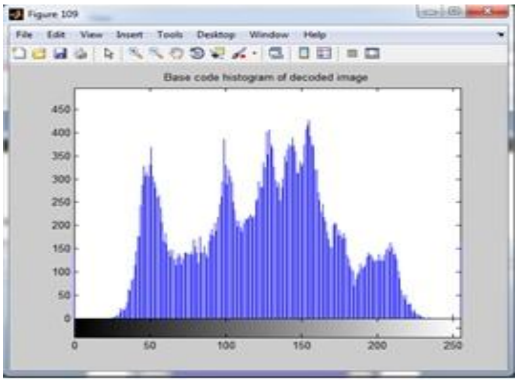

Fig5:HistogramofDecrypted Imageafter running with AES Algorithm.

The aboveFig 4, is showing the histogram of decrypted image after running with AESAlgorithm.

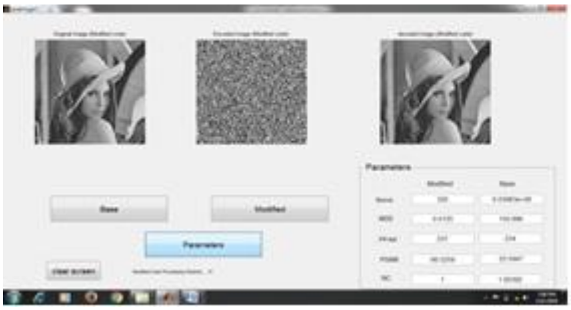

Fig 6: Parameters' Results afterRunning Image with Modified AES Algorithm (Proposed Algorithm).

For modified AES, separate histograms are generated. In Fig 6, the input image isciphered anddecrypted afterrunning with modified AES Algorithm.

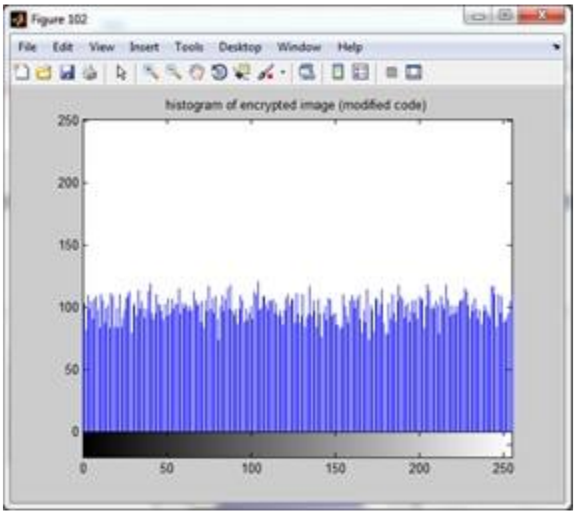

Fig7: Histogram of Encrypted Image after running with Modified AES.

In Fig 7, this histogram is generated for decrypted image when run with modified code.

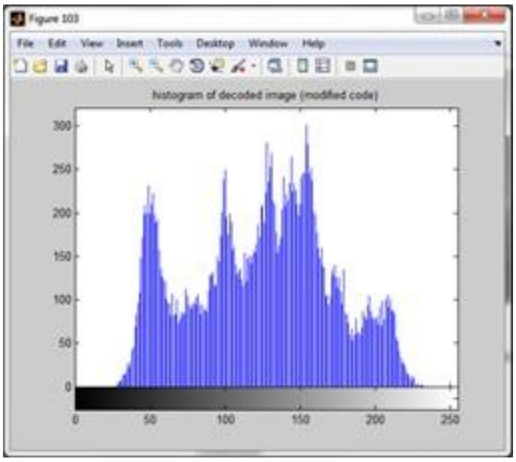

Fig8: Histogram of Encrypted Image when after running Modified AES.

In the Figure 8, histogram is generated by modified code for the decrypted image.

5.1 Result

As it can be seen in the table 1 and table 2 shown below that there is a big improvement among all parameters Noise, MSE, PFAK, PSNR and NC of existing AES algorithm and Modified AES algorithm which is a proposed work. And with this proposed work the parameters are improved drastically. So it can be said that the proposed modification in the existing AES Algorithm will give a huge improvement to the Image encryption techniques. In this modified AES method we are altering the image matrix which we called image block displacement and with this change we have achieved better results than original AES algorithm in the form of execution time and entropy.

Table 1: Comparison AES and Modified AES

Parameters	AES Algorithm	Modified AES Algorithm
Noise	6.03983e+06	320
MSE	150.996	0.0125
PFAK	234	237
PSNR	25.5947	66.5259
NC	1.00392	1

Table 2: Result Analysis (Execution Time and Entropy)

Parameters	AES Algorithm	Modified AES Algorithm
Execution Time	41.4573	18.9419
Entropy	4.931	3.427

6. CONCLUSION

An image ciphering procedure alters the primary picture in to a different image which is hard to detect as actual one. Keeping the picture trustworthy among its users is the sole target as security is a concerning issue after rapid growth of multimedia applications. Thus ciphering is the best means to keep the information intact.

Right now it is not easy to produce a block cipher which is very secure and fast executing. Most of the encryption are secure after multiple iterations, however they are very slow executing after many rounds. Although improvements have been done at the cost of performance.

In our approach length of the key of moderate size. And the advancements that can be made in our proposed approach may include the faster execution speed without compromising the robustness of the algorithm

Mostly cipher techniques are produced in "Trial-and-Error" environment. Cryptography will exist for very long duration. There will be modification on this platform, as length of the key, which will give a tough time to intruders. In short ciphering methods will also get strong along with time and intruder's approach.

In this work we present image encryption using Modified Advanced Encryption Standard. Encryption is a method to protect data from an unauthorized attack by using special algorithm, here modification to the Advanced Encryption Standard (AES) is done which show a high level security and excellent image encryption.

This work deal with Encryption of image using MAES. It provide great security for digital image. The image to encrypt is converted in to a matrix of scale values. The matrix is separated into small sub matrices which are shuffled in a random order. This random order is serves as the shared secret between the two communicating person and then it is transmitted on a secure channel using Encryption techniques. On the receiver side sub matrices are shuffled back to original positions.

Round of the algorithm can vary from 10 rounds up to 14 rounds. The number of rounds is dependent on length of the key and size of the block. Probably, less rounds is a reason why analysts criticizeRijandael. But if ever this is faced as a difficulty, by putting little extra efforts the length of the key and the size of the block can be increased to vanish it.

Right now it isn't likely to deduce a block encryption which is secure and quick. Many ciphering methods are safe after countless number of rounds but they are very low at speed. Augmentations have been introduced but at the expense of performance. Most of the approaches as Rijandael are established in trial-error atmosphere. Ciphering will be nearby for a long time several deviations may be introduced as- key lengths which will prevent the information from intruders.

7. FUTURE SCOPE

The enhancements which can be introduced in this approach are – this algorithm will be able to deal with videos and PDF files etc. as well. As a future work of this approach the idea may be to enlarge suggested technique to include different hash functions, signatures algorithms, block ciphers.

Following are the various possibilities which can be done in future

1. In this modified AES algorithm, the larger size of the key can be implemented to make the algorithm more robust. As this effort will have great utilizations in multimedia communications.
2. Application Specific Integrated Circuits (ASIC) based implementation can be performed on the proposed architectures and accurate power consumed for a particular technology can also be computed.
3. Various attacks can be tried on the AES Algorithm by invasive and non- invasive methods. A monitoring circuit can be designed which can detect and communicate any attacks on the encryptor.
4. Different modes of operations other than ECB mode can be applied to AES algorithm and a comparative study on the parameters can be made.
5. Moreover, MAES can be applied in regulatory requirements and email privacy, to give user more mobility, expanding enterprise control vs. 3rd party supply of information and storage solutions.

8. ACKNOLEDGEMENT

I am extremely obliged and beholden to my parents and my colleague for being pillars of strong point, for their reliable moral support, and inspiration. I treasure their blessings and good wishes and dedicate this hard work to them. I thank one and all who have been instrumental in serving me to complete this dissertation work.

9. REFERENCES

[1] Ashwini R. Tonde Ȧ, Akshay P. DhandeȦ "Implementation of Advanced Encryption Standard (AES) Algorithm Based on FPGA" IJCET , Vol 4 , No. 2 , April -2014

[2] E.Kavitha, "FPGA implementation of area optimized AES Algorithm for secure communication applications" (IJARCET), Volume 5, Issue 4, April 2016

[3] Nan Li, "Research of Database Encryption Based on Fast AES Algorithm Implementation" Springer-Verlag Berlin Heidelberg Part III, CCIS 216, pp. 31–35, 2011

[4] Archana Mishra*, Sourabh Sharma, "Design and Implementation of High Speed AES Algorithm for data security" (IJESRT), 5(8): August, 2016

[5] https://en.wikipedia.org/wiki/Image_compression

[6] Ahmed Fathy, Ibrahim F. Tarrad, Hesham F.A. Hamed, Ali Ismail Awad,"Advanced Encryption Algorithm:Issues and Implementation Aspects", Springer-Verlag Berlin Heidelberg AMLTA 2012, CCIS 322, pp. 516–523, 2012

[7] S. Kahu, and R. Rahate, "Image compression using singular value decomposition", International Journal of Advancements in Research & Technology, vol. 2, no. 8, pp. 244-248, 2013

[8] https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[9] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[10] S. SrideviSathyaPriya, P. Karthigai Kumar, N.M. Siva Mangai, and P.T. Vanathi, "Survey on Efficient, Low-Power, AES Image Encryption and Bio-cryptography Schemes" Smart Computing Review, vol. 2, no. 6, December 2012

[11] http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[12] http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

[13] https://in.mathworks.com/help/matlab/learn_matlab/product-description.html?requestedDomain=true

[14] https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryption

[15] Ahmed Bashir Abugharsa, AbdSamad Bin Hasan Basari, HamidaAlmangush,"A New Image Encryption Approach using The Integration of A Shifting Technique and The Aes Algorithm", IJCA Vol-42 No.9, March-2012

[16]