ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 7, July 2017

Security Enhancement usingcounter block based Advance Encryption Standard (AES-CBC256) in Image Processing

ShikhaVerma

Email id: csengg.shikha@gmail.com ,

Surbhi Agrawal

Department of computer science &Engg

Subharti University (UP), INDIA

ABSTRACT

Recently more and more attention is image encryption based data security, since it maintains the excellent property that the image data is encrypted while protecting the image content'sconfidentiality. In this paper we propose a counter based block code AES (Advanced Encryption Standard)-256, operations in image encryption and decryption which overcome distorted quality after decryption process and processing time of our approach as compare with normal AES-128 technique. The encrypted cipher images always display the uniformly distributed RGB pixels for 4x4 block size based decryption position The proposed method can achieve real time confidentialityand image recoveries are free of any distorted pixel,which simulated using MATLAB 2014Ra Version.

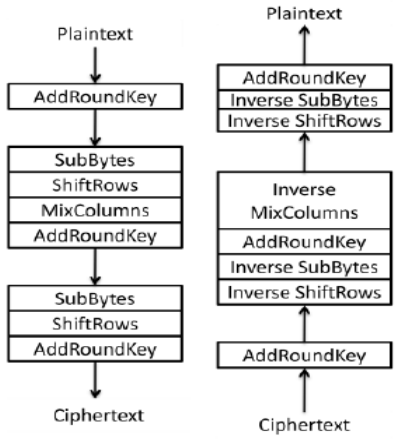
Keywords: Image Encryption, Image encryption key, Stream Cipher, RC4 algorithm, Data Encryption Key, Image Decryption, Data Decryption etc.

I.INTRODUCTION

1.1. Advance encryption standard basics

The AES is basically a crypto graphical algorithm designed for the purpose of security. The NIST (National Institute of Standards and technology) issued a request for AES to replace DES in September 1997. The 15 candidate's algorithms were selected and a year later only 5 finalist were announced in August 1999.These five algorithms are MARS, RC6, Rijndael, Serpent and Twofish. The Rijndael algorithm, developed by Joan Daemen and Vincent Rijmen was selected as the winner of the AES development process in October 2000. The FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197(FIPS 197) specifies an algorithm called Advanced Encryption Standard (AES) in Nov-26-2001.

AES has advantages as it provides combination of security, performance, efficiency and flexibility. For any security system Key size is very important, it determines the strength of security, area optimization and power consumption. As AES is derived from Rijndael it is also called as Rijndael in cryptography to protect sensitive data by converting it into unintelligible form called as a cipher text means coded text.



(a) Encryption process (b) Decryption process

Fig.1. AES Encryption/Decryption process

The AES algorithm is a symmetric block cipher that can encrypt as well as decrypt information. Encryption converts data into an unreadable form known as cipher-text. Encryption of the cipher-text converts the data back into its original readable form,

which is called plain-text. AES as well as most encryption algorithms, are reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order.
The AES algorithm operates on bytes, which makes it simpler to implement and describe. The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption which is the symmetric type of cryptography. The data block length is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. In addition, the AES algorithm is also an iterative algorithm.

For encryption, each round consists of the following four steps:
1) Sub bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key.
For decryption, each round consists of the following four steps:
1) Inverse shift rows, 2) Inverse bytes, 3) Add round key, and 4) Inverse mix columns.

1.2. **Image Encryption**
Encryption is a process which changes image into a stream of coded data which makes it difficult to understand by unauthorized user. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

II.RELATED WORK

Praveen.H.L , H.S. Jayaramu, M.Z.Kurian [1] Has developed a model which can easily encrypt the images obtained from satellites. Even If faulty data occurs then satellite needs not to wait for long time to receive next data. To prevent this error free encryption scheme is proposed in On-Board. They also states that AES provides an error-free encryption system and error is much more reduced even in radiation in satellites.

Ahmed Bashir Abugharsa, AbdSamadBin Hasan Basari and HamidaAlmangush [2] has also used AES algorithm to encrypt image, they have first rotated the plain image to generate another image with the help of magic cube. The original image is divided into six sub-images and these sub-images are divided amongst a number of blocks and attached to the faces of a Magic Cube and to confuse the relationship between the plain image and the encrypted image, the rotated image is fed into an AES algorithm which is applied to each pixel of the image to encrypt the image even further.

Jawad Ahmad and Fawad Ahmed [3] have compared two encryption algorithms namely Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES). They have explored the security estimations of AES and CFES for digital images against brute-force, statistical, and differential attacks, the results they have calculated to test the security of these algorithms for digital images shows some weaknesses in CFES. These weaknesses were mainly related to low entropy and horizontal correlation in encrypted images, the authors also states that the image encrypted by CFES has correlation in horizontal direction while AES encrypted image has very less correlation in all directions. The algorithm which has less correlation values indicates that it has higher security.

Manoj. B, Manjula N Harihar[4] also states that Image Encryption and Decryption using AES can be designed and implemented to protect the confidential image data from an unauthorized access the authors found that Successful implementation of AES algorithm is one of the best encryption and decryption standard available in market.
Seyed Hossein Kamali, Reza Shakeria (2010) [5] proposed a new encryption scheme as a modification of AES algorithm based on both ShiftRow Transformations. In this if the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes.. Experimental result shows that that MAES gives better encryption results in terms of security against statistical attacks and increased performance.

Hai Yu, Zhiliang Zhu (2009) [6] An efficient image encryption algorithm is proposed, based on image reconstruction using some adjacent pixel characteristics**.** According to the different characteristics of different bit level binary images, the proposed encryption scheme reconstructs the image at the bit level. Two parts of information, the significant one and the unimportant one, are treated differently and processed separately. Simulations and cryptanalysis both show that the proposed image encryption scheme is more efficient and yields better level of security.

K.C.Ravishankar,M.G. Venkateshmurthy(2006) [7] The proposed technique segments the image into regions of fixed size. These regions act as units for processing the image. Selective Encryption makes it possible to encrypt only a part of the image leaving the rest of the image unaltered. Here, the regions covering the part of the image are considered for encryption. Selective Reconstruction deals with decrypting only a part of the encrypted image. Both the methods give a fair amount of reduction in the encryption time.Once the segmentation and permutation of regions is completed, the regions are encrypted independently.

Qiu-Hua Lin, Fu-Liang Yin, and Yong-Rui Zheng (2004).[8] In this paper, an image encryption method is proposed by using the linear mixing model of blind source separation *(BSS).* It can simultaneously encrypt multiple images with the same size by mixing them with the same number of statistically independent key images, the size of which is equal to that of the images to be encrypted. Since these multiple images cover mutually through mixing among them while the key imnges cover them, and there is not any restriction on the key space, the proposed method has high level of security.

Ruiliu, Xiaoping tian (2012) [9] proposed a new algorithm for color image encryption using chaotic map and spatial bit-level permutation (SBLP).Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix and permute the matrix at bit-level by the scrambling mapping generated by SBLP. then use another Logistic chaotic sequence to rearrange the position of the current image pixels. Experimental results show that the proposed algorithm can achieve good encryption result and low time complexity, This makes it suitable for securinvideo surveillance systems, multimedia applications and real-time applications such as mobile phone services.

Bibhudendra Acharya Saroj Kumar Panigrahy, SaratKumarPatra, and Ganapati Panda (2009) [10] This paper proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involuntary key matrix for encryption. They have taken different images and encrypted them using original Hill cipher algorithm and their proposed AdvHill cipher algorithm. and in the results it is clarified that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. But their proposed algorithm works for any images with different grayscale as well as color images.

III. PROPOSED IMPLEMENTATION

3.1. Hybrid AES-CBC-256Algorithm

The Block-CBC is usesprocessesfrom mixed(orthogonal)arithmeticalcollectionsXOR,ADDa ndSHIFT. Adoubleshiftsourcesallbitsof theinformationandkeytobemixed recurrently.

Thekeyprogramprocedureis modest;the128-bit keyKisdividedintofour32-bitblocksK=(K[0],K[1],K[2], K[3]).CBC (Tiny encryption algorithm)appearstobeextremelyresilientto differencecryptanalysis(Bihamet al.,1992)andattainscomplete diffusion (where a one bit alteration in the simple text will cause about 32bit changes inthe cipher text).
Apart from that an AES encryption key is constructed as follows. The AES-128 encryption process involves 10 rounds of encryption along with an initial round for the 128 bit data encryption. To begin with, the 128-bit key is expanded into a set of eleven 128-bit round keys using the Key expansion routine. Each of this key is used for the rounds, finally resulting in the cipher text output. The initial round in the AES Encryption comprises of the Add Round key step in which the plain text is XOR'ed with the Cipher Key.

The 128-bit input block of data is processed byte-by-

byte and mapped into a 4x4 byte matrix for processing convenience as per the AES standard. Each block of input and the intermediate inputs between the different rounds is mapped into a 4x4 state matrix as shown in the fig. below:

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Figure 3.1: 4x4 state matrix

In the 10th round, the above steps are repeated excluding the Mix Columns step. Following sections explain each of them in detail. The overall process of AES encryption is illustrated in the figure below:

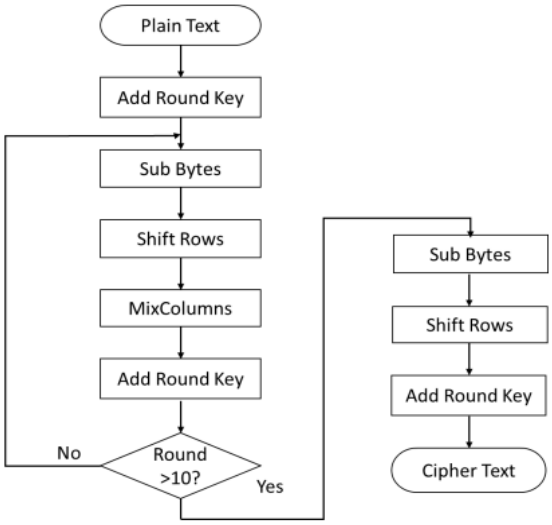


Fig. 3.2: AES Encryption Block diagram

3.2 Add Round Key Conversion

In this transformation, the Round key is added to the State by bitwise XOR operation. The Round key for each round has to be produced from the Key Development which is explained in the coming sections.

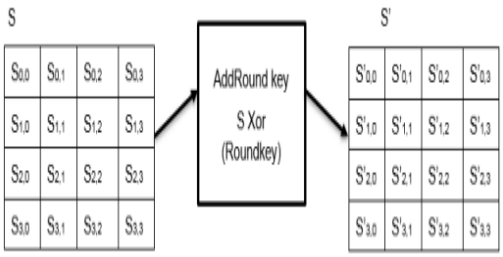


Figure 3.3: Add Round Key Transformation

IV. ROPOSED FLOW DIAGRAM

The Sub Bytes transformation applies S-Box to each byte in the public. Fig. shows the S-Box substitution values for the AES-128 Encryption.

The proposed system can be categorized into two portions: the sender's view and the receiver's view as shown in Figure 1 and Figure 2:

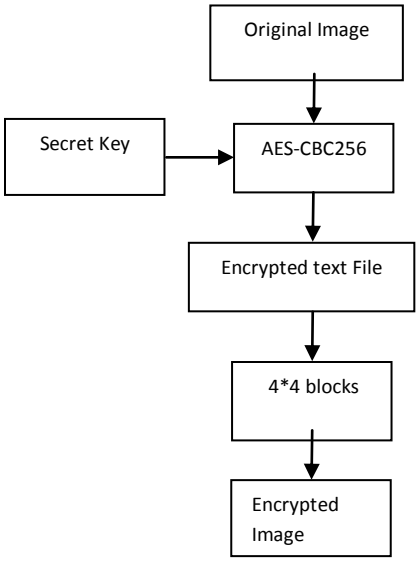


Figure 4.1.Block diagram from the sender's view

The secret txt is encrypted by AES-CBC256 encryption algorithm with the help of secret key at the sender's side. Then the encrypted text is embedded into a 4*4 blocks by counter block code(CBC) algorithm and it can produce the minimum response for sender's

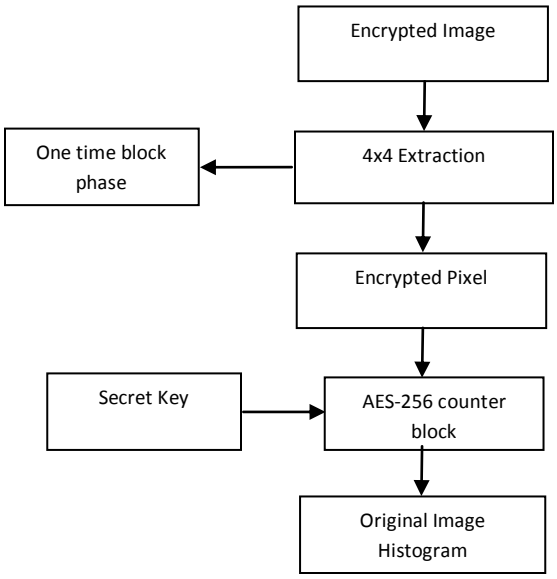


Figure 4.2. Block diagram from the receiver's view

The encrypted text is extracted from the tiny blocks by using s-box extraction algorithm at the receiver's side. The extracted secret image is decrypted by the AES CBC256 algorithm with the shared secret key and the original message/packet is then produced.

V. Experimental Results

The results evaluation for message can only be deciphered through the information that has the decryption key, recognized as the private key.This type of encryption has a quantity of advantages over usual symmetric Ciphers.

It means that the recipient can create their public key approximately available- someone deficient to send them a communication usage the procedure and the receiver's public key to do so. A viewer may have both the procedure and the public key, but will still not be capable to decode the text. Individual the receiver, with the private key can decrypt the message. Confidential Data using AES-256CBC and Block-based Encryption :

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

Figure 5.1: S-box matrix

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

Figure 5.2 Inverse S-Box

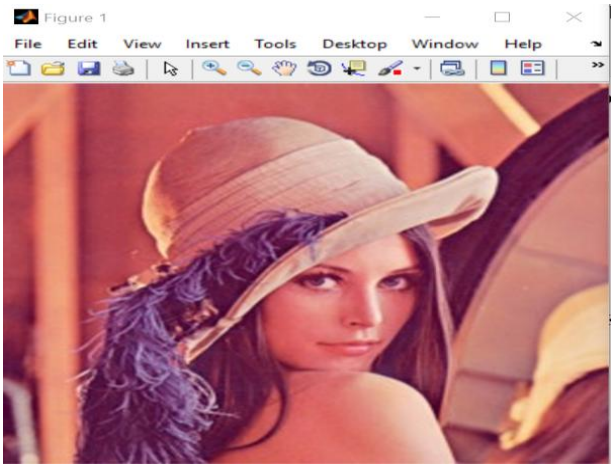


Figure 5.3: Input image for encryption process

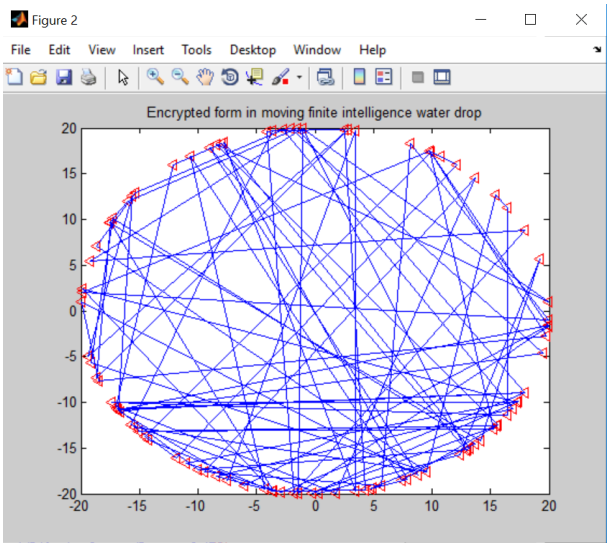


Figure 5.4 : Input image scrambling process for encryption for block based assignment in s-box

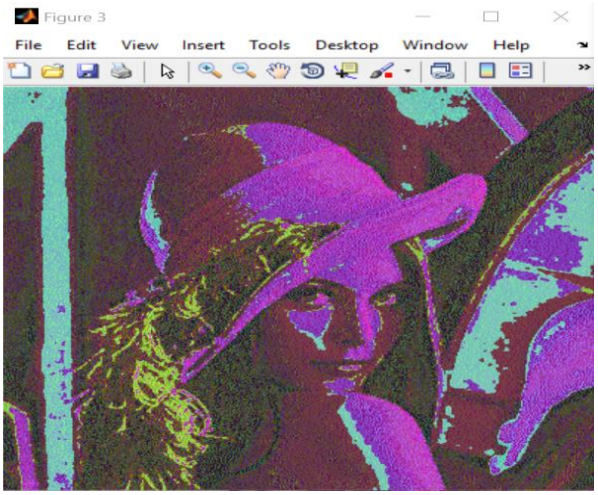


Figure 5.5 : Encrypted image scrambling process for encryption for block based assignment in s-box counter based block assignment encryption AES

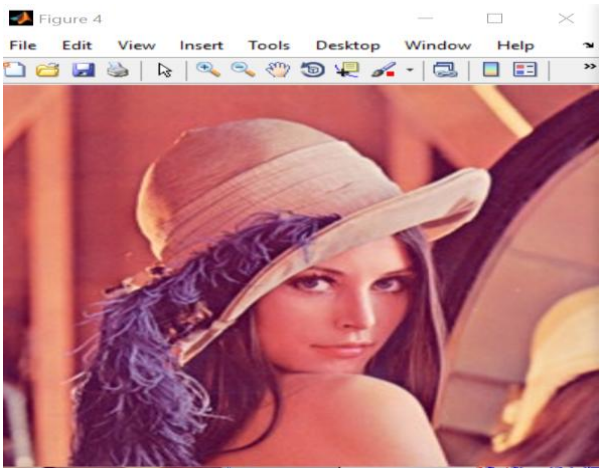


Figure 5.6: Decrypted image after inverse scrambling process for decryption for block based assignment in s-box counter based block assignment

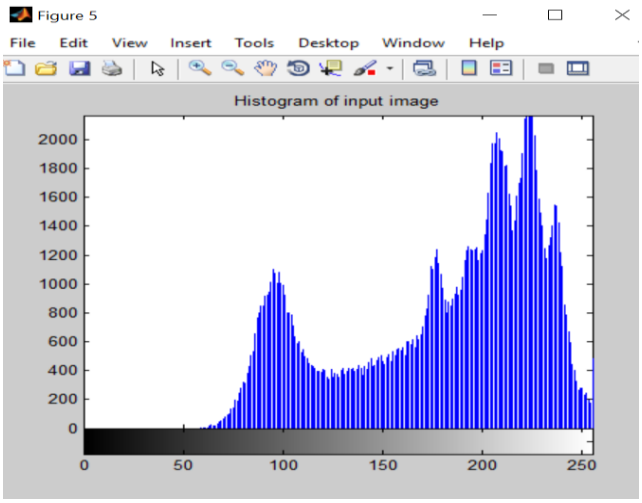


Figure 5.7: Input image after before scrambling process for decryption for block based assignment

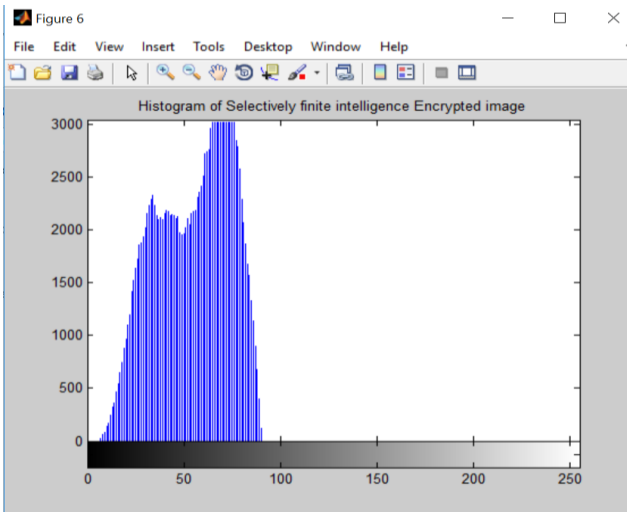


Figure 5.8 : Encrypted image histogram after scrambling process for decryption for block based assignment for s-box

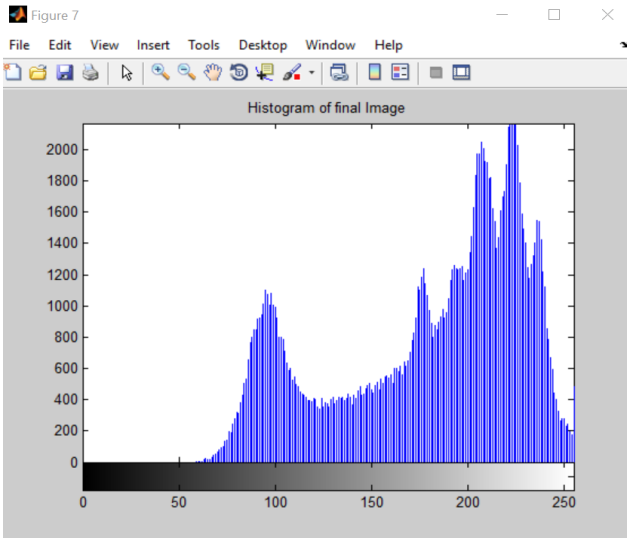


Figure 5.9: Decrypted image histogram after scrambling process for decryption for block based assignment for s-box .

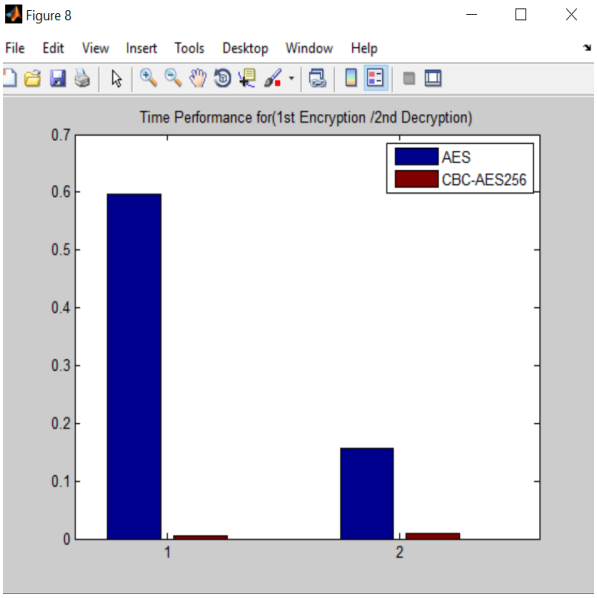


Figure 5.10: Processing time for before and after scrambling process for encryption- decryption for block based assignment for s-box for our proposed technique.

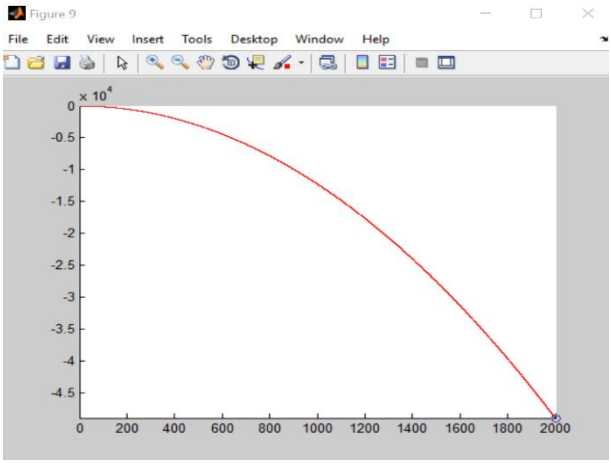


Figure 5.11: Error minimization process for before and after scrambling process for encryption-decryption for block based assignment for s-box for our proposed technique.

This planned scheme effort on the secure approach of light weight cryptographic procedure. AES 256CBC Encryption Algorithm to adjust with countless real time restraints like memory space. The proposed scheme uses block based CBC to produce the random key creation it safer for delicate data transmission in numerous real-time submissions.

VI.CONCLUSION

This work proposes a key ideas last our suggestion deceits which take text encryption ended the assumed commutative algebraic systems as the underlying work structure for constructing cryptographic schemes. By doing so, we can efficiently obtain better result for the given algebraic schemes. The security supposition is that the projected AES-Block based CBC256 image encryption over the given non-commutative algebraic systems is intractable.We have proposed two novel examples for the building of group-theoretic one-way purposes for key exchange. The primary plaintext image may be recuperated with no mistake. attributable to the two's similarity plots, during this means, the collector could take away a bit of put in data within the disorganized area, and concentrate another piece of inserted data and recoup the primary plaintext image within the plaintext space.

REFERANCES

[1] Praveen.H.L , H.S Jayaramu, M.Z.Kurian "Satellite Image Encryption Using AES" International Journal of Computer Science and ElectricalEngineering (IJCSEE), Vol-1, Iss-2, 2012.

[2] Ahmed Bashir Abugharsa, AbdSamadBin Hasan Basari and HamidaAlmangush "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm" International Journal of Computer Science Issues (IJCSI); Vol. 9 Issue 4,p41 Jul2012.

[3] Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal ofVideo & Image Processing and Network Security IJVIPNS-IJENS Vol:12No:04.

[4] Manoj.B, Manula N Harihar "Image Encryption and Decryption using AES" International Journal of Engineering and Advanced Technology(IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[5]. S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[6]. H. Yu, Z. Zhu "An Efficient Encryption Algorithm Based on Image Reconstruction" 2009 International Workshop on Chaos-Fractals Theories and Applications.

[7]. K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 ©2006 IEEE.

[8]. Q.Hua Lin, Fu-Liang Yin, and Y.R. Zheng" Secure image communication using blind source separation*" 2004 IEEE.*

[9] .R. liu, X. tian "New algorithm for color image encryption using chaotic map and spatial bit level permutation "Journal of Theoretical and Applied Information Technology 15 September 2012. Vol. 43 No.1 © 2005 - 2012 JATIT & LLS.

[10]. B. Acharya, S.K.Panigrahy, S.K.Patra, and Ganapati Panda,‖ Image Encryption Using AdvancedHill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.