IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Special Issue-1, Jun 2017 E-ISSN: 2347-2693

AES Based Digital Data Security System

R. Jadhav[1], S. S. Redake[2], P. R. Patil[3], S. V. Patil[4], K. R. Jain[5*]

[1] Dept. Of Electronics and Telecommunication, A. C. Patil College of Engineering, University of Mumbai, Mumbai, India.
[2] Dept. Of Electronics and Telecommunication, A. C. Patil College of Engineering, University of Mumbai, Mumbai, India.
[3] Dept. Of Electronics and Telecommunication, A. C. Patil College of Engineering, University of Mumbai, Mumbai, India.
[4] Dept. Of Electronics and Telecommunication, A. C. Patil College of Engineering, University of Mumbai, Mumbai, India.
[5*] Dept. Of Electronics and Telecommunication, A. C. Patil College of Engineering, University of Mumbai, Mumbai, India.

*Corresponding Author: komalrj710@gmail.com, Tel.: +91-9766134232

Available online at: www.ijcseonline.org

***Abstract*—** Financial records, health records, government documents, business documents and quality control information often start out in paper form. While this paper-based records and documents are gradually digitized, security concerns about how such electronic data is stored and transmitted have increased. The prevention of unauthorized modification and loss of records is highly important in the all this sectors. It is hard to keep track of who has used or copied which paper documents. Paper documents are often maintained with very low security control. Therefore, a secured system is not only required but also important. This paper presents system for the management of paper document securely in the digital form. Document digitization refers to the process of capturing the image of a paper document and turning it into digital form. A document scanner is usually used for capturing the document image. While saving the digitized document it is encrypted first and then saved or direct transmitted as per the need. In this paper, we use the AES encryption algorithm to secure data.

***Keywords*—**AES, Encryption, Decryption

I. INTRODUCTION

Organizations delivering customer centric services like Bank, Financial records, health records, government and business etc., involve extensive handling of documents. These documents are critical for effective service delivery. With increasing number of documents generated every day, storing and retrieving documents become an operational challenge. These challenges can be broken down into accessibility, productivity and security. Constant handling of Documents makes them prone to damage and chances are high that you may lose critical documents or documents related to the organizational legacy. Due to more papers, one can experience difficulty in locating records, sorting documents and identifying key pieces of information. According to a study by Cooper and Lybrand, "7.5% of all documents get lost and 3% of the remainder is misfiled." This suggests that out of every one hundred documents, ten documents are sitting on the wrong desk, being removed from the office, etc. Some documents cannot be reproduced if lost. This dramatically increases the risks and costs associated with paper filing systems. Also paper documents are often maintained with very low security control. Most old paper records can realistically be discarded. However, some items such as contracts, deeds, powers of attorney, partnerships, or wills, may need to be kept in their original paper form. For reducing the storage and security purpose, we can convert these documents into images through scanning. This is called as digitization of paper documents. Once the digital copies have been created, they can easily be stored in multiple servers at multiple geographic locations by companies that provide advanced security and cost-effective storage. With a document imaging system, personnel can retrieve documents directly from their desktop PC within seconds. There is no re-filing necessary after using the document.

The goal of Document Digitization is to significantly reduce the dependence on the original paper documents without adversely affecting operational efficiency, security, control. The scanned copy of the original document provides a fall back option in case the papers are lost or damaged. Therefore, digitizing the paper documents increases the need of security. Digital documents are saved in secured environments like servers, databases, encryption etc., and can be accessed only by authorized users, which provides more security compared to a paper-based system, where a misplaced or mishandled document is a common problem.

© 2017, IJCSE All Rights Reserved

In this paper, customer paper documents are digitized and saved securely by using the encryption algorithm. We use the encryption technique before it saved digitized image. So it can accessible to only authorised person.

II. METHODOLOGY

The Advanced Encryption Standard (AES) specifies a Federal Information Processing Standards (FIPS)-approved cryptographic algorithm that can be used to protect electronic data.[6] The AES algorithm is a symmetric block cipher that can encrypt and decrypt the information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. This standard specifies the Rijndael algorithm that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.[1] The input and output for the AES algorithm each consist of sequences of 128 bits.

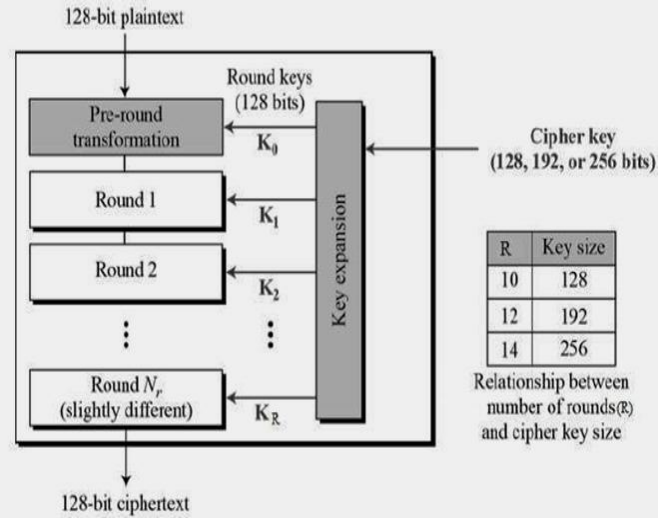

Figure 1. Flow of AES 128-bit Algorithm

The figure.1 shows flow of encryption process of AES algorithm, having main block of key expansion. The AES algorithm involves following steps:

1) Key Selection- The sender and receiver agree upon a 128-bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k [0], k [1] ...k [15]. Where each block is 8bits long (8*16=128 bits).
2) Generation of Multiple keys- The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one-time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

A. *Encryption process in AES*

In each round following steps involves:

1. Sub byte- The Substitute byte transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table S-box[1]. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation.

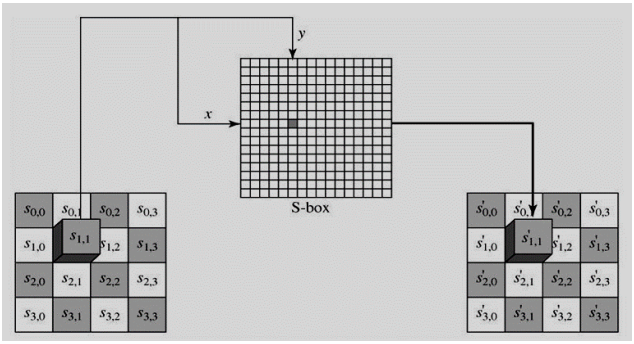

Figure 2. SubByte Substitution

2. Shift Rows- 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. This has the effect of moving bytes to "lower" positions in the row while the "lowest" bytes wrap around into the "top" of the row.

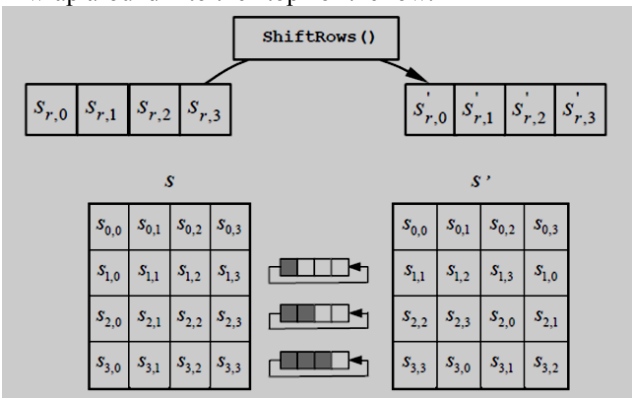

Figure 3. Shift Row

3. Mix Columns- The Mix Columns transformation 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(x), given by

a(x) = {03}x3 + {01}x2+ {01}x + {02}.

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

© 2017, IJCSE All Rights Reserved

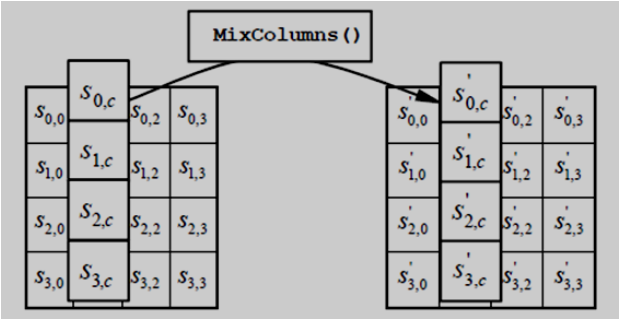

Figure 4. Mix column

4. AddRoundKey- 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 AddRoundKey are of the same size and to obtain the next State an XOR operation is done per element:

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

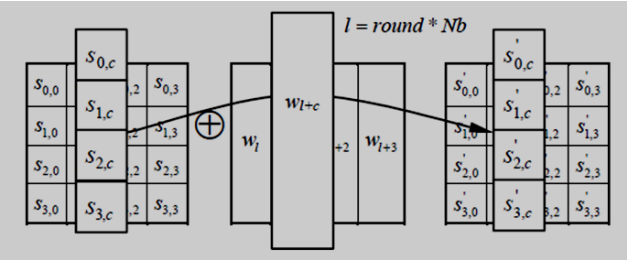

Figure 5. AddRoundKey

B. Decryption process in AES

1. Inverse Shift Row Transformation - Inverse Shift Rows is the inverse of 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. The bottom three rows are cyclically shifted by Nb-shift (r, Nb) bytes, where the shift value shift (r, Nb) depends on the row number.

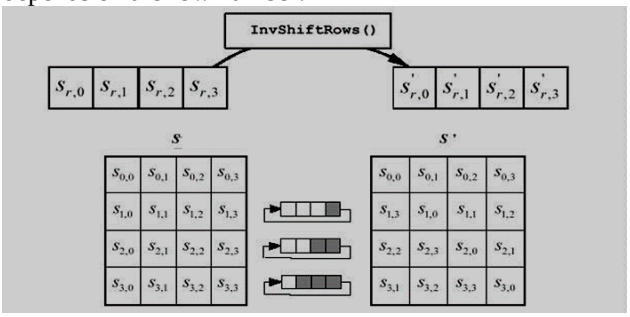

Figure 6. Inverse Shift Row Transformation

2. Inverse substitute byte transformation- Inverse Substitute Bytes is the inverse of the byte substitution 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 affine transformation followed by taking the multiplicative in-verse in GF (28). There is an inverse s-box table for substitute the value.
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 (28) and multiplied modulo x4 + 1 with a fixed polynomial a-1(x), given by

$$a\text{-}1(x) = \{0b\}x3 + \{0d\}x2 + \{09\}x + \{0e\}$$

C. Key process in AES

Pseudo code for AES Key Expansion: The key-expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x(Nr+1) words, where Nr is the number of rounds.[7] The process is as follows:

I. The first four words are made from the cipher key (initial key). The key is considered as an array of 16 bytes (k0 to k15). The first four bytes (k0 to k3) become w0, the four bytes (k4 to k7) become w1, and so on.
II. The rest of the words (wi for i=4 to 43) are made as follows: If (i mod 4)! = 0, wi=wi-1 XOR wi-4.
If (i mod 4) = 0, wi=t XOR wi-4. Here 't' is a temporary word result of applying SubByte transformation and rotate word on wi-1 and XORing the result with a round constant.

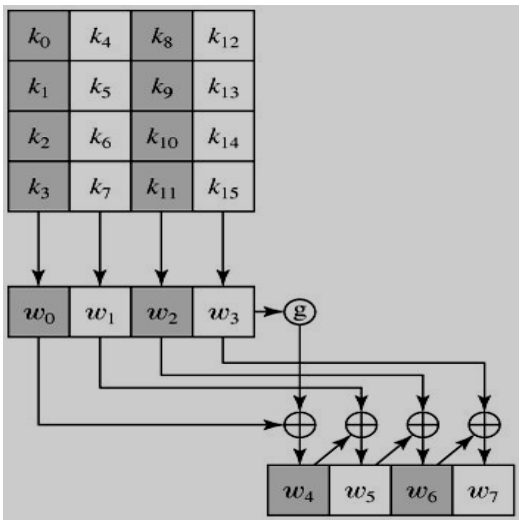

Figure 7. Key expansion in AES

III. RELATED WORK

The figure.8 shows the flow diagram of working system. As shown in figure, system consists of first the document that

© 2017, IJCSE All Rights Reserved

we need to secure. This document is captured using camera. Once it is captured an effective encryption algorithm is applied to this captured image. As mentioned above we have used AES-128 algorithm to secure (encrypt) the captured document. The encryption will be applied before the document gets saved.

The reason why AES algorithm is applied before captured document get saved is that, the person who is capturing (or scanning) the important or confidential documents may not be always authorized person.

This system thus, give access to captured original document which is already get encrypted before get saved to the authorized person having valid key. The people who wish to open the document don't having valid key will not be able to access original document.

This makes the digitization of paper document along with the security which is main aspect.

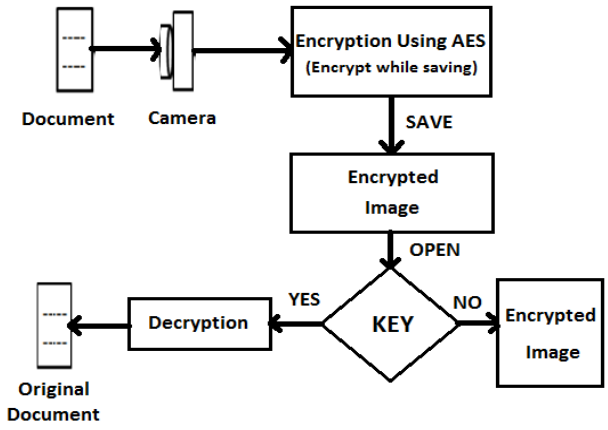

Figure 8. Implementation

IV. RESULTS AND DISCUSSION

The output of GUI given below clearly indicates the implemented result of algorithm designed.

1. We start with taking picture of paper document which we want to encrypt. For this we just click on the "Capture image" button.

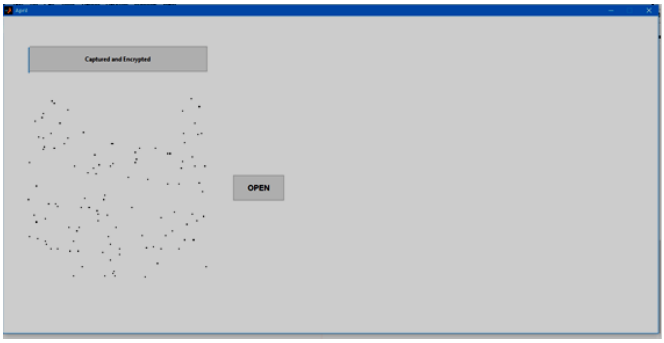

Figure 9. Encryption of Document

The Figure 9 shows the output after clicking the "Capture image" button. It shows the encrypted image as processed through the AES algorithm.

2. After typing appropriate key, user get the decrypted image i.e. original picture of paper document.

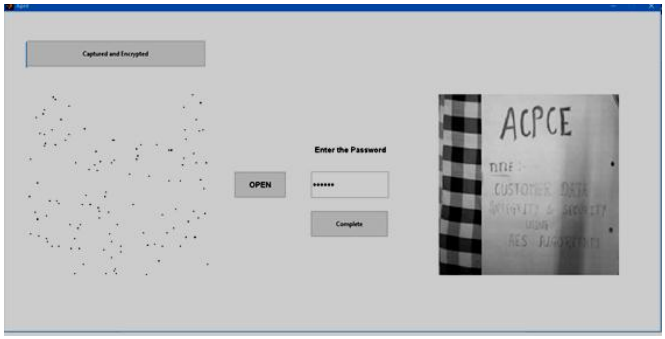

Figure 10. Decryption by Authorized Person

The Figure 10 shows the output after giving the appropriate key. The encrypted image is processed through decryption algorithm taking the user key.

3. If user types the key 6 characters but key is wrong, then it gives us encrypted image as shown in Figure 11.

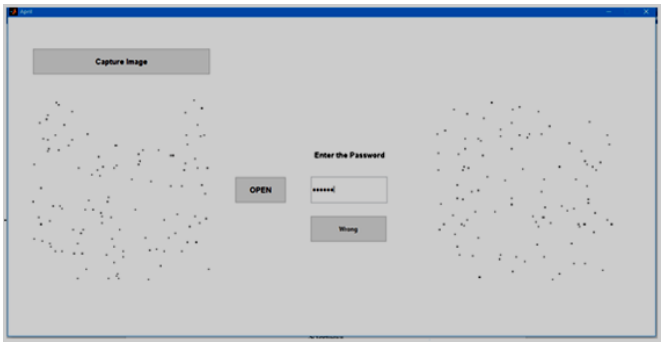

Figure 11. Decryption by Unauthorized Person

To get a measure of how similar two images i.e. original images and decrypted images are, we find the histogram of two images.

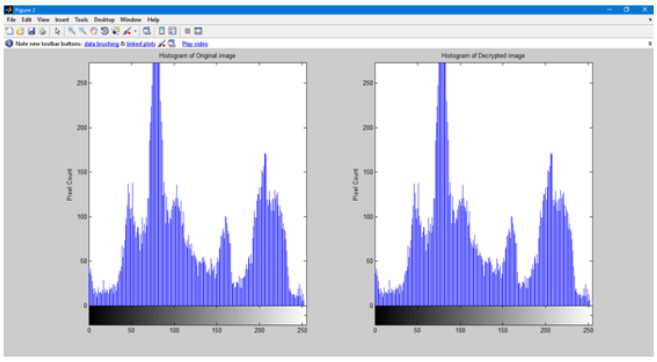

Figure 12. Histogram of Original and Decrypted image

© 2017, IJCSE All Rights Reserved

From figure 12 we can see that histogram of two images are identical. It means after decryption we get the original image without distortion.

The following are some parameters for quality measurement between the original and the processed image i.e. decrypted image:

Table 1. Result

Parameters	Value	Description
Peak signal-to-noise ratio (PSNR)	Infinity	If you compare two identical images, the PSNR is infinity.
Mean squared error (MSE)	0	When there is no difference between original and the processed image vale of MSE is zero.
Structural Similarity Index (SSIM)	1	Gives image quality degradation caused by processing, if value of SSIM is 1, it means no degradation in original image.

V. CONCLUSION AND FUTURE SCOPE

Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to an application, we should have knowledge regarding performance, strength and weakness of the algorithms. The memory required for implementation is largest in RSA. DES and AES require medium size of memory. Therefore, if the demand of any application is the smallest memory size, the AES and DES is the best option. But if cryptographic strength is a major factor in the application, AES is the best suited algorithm. So for bank customer data security we are using AES algorithm.

The proposed system using AES algorithm offers high encryption quality. Even AES-128 offers a sufficiently large number of possible keys, making an exhaustive search impractical for many decades. Encryption and decryption encryption by AES Algorithm is less than the time required by DES Algorithm. 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.

The focus shall be to implement the system which reduces time required to encrypt and decrypt the image of paper document. Also it will be not affect the quality of image. We also try to replace camera with scanner to encrypt and decrypt the more number of images at a time. Using scanner, image acquisition process can be faster. So we can use our system to secure the business documents and similar large industries having more storage of paper documents.

REFERENCES

[1] S. Mewada, P. Sharma and S. S. Gautam, *"Exploration of efficient symmetric AES algorithm,"* 2016 Symposium on Colossal Data Analysis and Networking (CDAN), *Indore, 2016, pp. 1-5.*

[2] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[3] Surbhi Sharma, "*Embedding more security in digital signature system by using combination of public key cryptography and secret sharing scheme*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.3, pp.111-115, 2016.

[4] P. Thakkar, H.K. Mishra, Z. Shaikh, D. Sharma, "Image Encryption and Decryption System Using AES for Secure Transmission", International Journal of Computer Sciences and Engineering, Vol.5, Issue.5, pp.109-114, 2017.

[5] Sachin sharma and Jeevan Singh Bisht, "*Performance Analysis of Data Encryption Algorithms*", International Journal of Scientific Research in Network Security and Communication, Vol.3, Issue.1, pp.1-5, 2015.

[6] William Stallings, "*Advance Encryption Standard*," in Cryptography and Network Security, 4th Ed., India: PEARSON, pp. 134–165.

[7] Behrous Forouzen, "*Cryptography and Network Security*", Tata Mc Graw –Hill Education 2011

Authors Profile

Ms. Apurva Ramdas Jadhav pursuing Bachelor of Engineering in Electronics and Telecommunication from Mumbai University, Mumbai. She has secured "Best Paper Award" in 4th National Conference on "Advances in Technology & Management "on March 23-24, 2017.

Ms. Shubhangi Sambhaji Redake pursuing Bachelor of Engineering in Electronics and Telecommunication from Mumbai University, Mumbai. She has secured "Best Paper Award" in 4th National Conference on "Advances in Technology & Management" on March 23-24, 2017.

Ms. Pranali Ramesh Patil pursuing Bachelor of Engineering in Electronics and Telecommunication from Mumbai University, Mumbai. She has secure d "Best Paper Award" in 4th National Conference on "Advances in Technology & Management "on March 23-24, 2017.

Ms. Shivali Vivek Patil pursuing Bachelor of Engineering in Electronics and Telecommunication from Mumbai University, Mumbai. She has secured "Best Paper Award" in 4th National Conference on "Advances in Technology & Management "on March 23-24, 2017.

Ms. Komal R. Jain pursued Bachelor of Engineering in Electronics and Telecommunication from North Maharashtra University, Jalgaon in 2004 and currently working as Assistant Professor in Department of Electronic and Telecommunication, University of Mumbai, Mumbai since 2004. She has secured "Best Paper Award" in 4th National Conference on "Advances in Technology & Management "on March 23-24, 2017.

© 2017, IJCSE All Rights Reserved