ISSN : 0973 - 8355

www.ijmmsa.com

INTERNATIONAL JOURNAL OF MATHEMATICAL, MODELLING, SIMULATIONS AND APPLICATIONS

IJMMSA

E-MAIL
editor.ijmmsa@gmail.com
editor@ijmmsa.com

INTERNATIONAL JOURNAL OF MATHEMATICAL, MODELLING, SIMULATIONS AND APPLICATIONS
IJMMSA

ISSN 0973-8355www.ijmmsa.com
Vol 7,Issuse 2.June 2019

Implementing Digital Data Security System Using AES Algorithm

[1]MD.Asim, [2]B.Devananda Rao ,[3]R.Samaiah

ABSTRACT

It is common for many types of papers, such as financial records, health data or government documents, to begin life on paper. Growing security concerns about electronic data handling and transmission have accompanied the digitization of more and more paper-based documentation. There is a lot of focus on data security in these areas. It is tough to keep track of who is copied or utilized paper documents. It is usual for paper documents to be in a vulnerable condition. As a result, a secure system is not only necessary, but also essential. Study documents may now be safely stored digitally, thanks to a technology described in this paper. A paper document may be "digitized" by taking a photo of the original and then converting it to digital form. Capturing a picture of a document is often accomplished via the use of a document scanner. This process is followed by either saving or directly transmitting the digital document. To keep data safe, we will be using the AES encryption technique.

1.INTRODUCTION

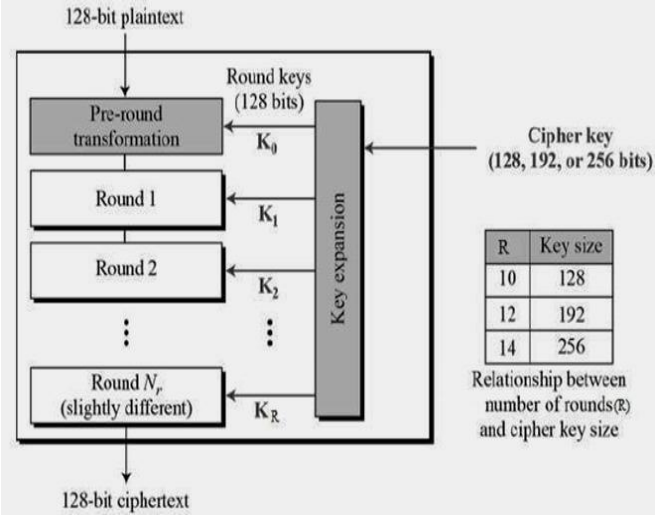
Providing customer-centric services, such as banking, financial records, health records, government and business, requires a great deal of document management. These papers are essential for delivering high-quality customer service. Storage and retrieval of documents has become an operational concern as the quantity of documents created each day grows. These issues may be split down into three main categories: accessibility, productivity, and security. The constant handling of papers makes them more susceptible to deterioration, which increases the risk of losing important records or documents that tell the story of your organization's history. Having a lot of paperwork might make it harder to find records, categorize documents, and identify important information. Research by Cooper & Lybrand shows "7.5% of papers are lost and 3 percent of the remaining are misfiled." [3]. This means that out of every hundred papers, 10 are sitting on the incorrect desk, being thrown out of the office, etc. If a document is lost, it cannot be reconstructed. A paper filing system's danger and expense just went through the roof because of this. Paper documents, on the other hand, are commonly kept in a state of minimal security control. The majority of obsolete paper records may be disposed of. In other cases, however, documents such as contracts, deeds, powers of attorney and partnerships, as well as wills, may need to be retained in their paper form. To save space and improve security, we may scan these papers into images[2]. Digitization of paper documents is a term for this. Companies that offer high-level security and cost-effective storage may readily store the digital copies after they have been made on several servers across different geographic regions. With a document imaging solution, employees may recover documents from their desktop computers in seconds. It is not essential to re-file after utilizing the document.

[1,2,3]Assistant Professor
[1,2,3] Department of Computer Science & Engineering,
[1,2,3]Dr.K.V.Subba Reddy College Of Engineering For Women

2.METHODOLOGY

Document Digitization aims to dramatically decrease reliance on original paper records without compromising operational efficiency, security, or control. In the event that the original documents are lost or destroyed, the scanned copy serves as a back-up. Digitizing paper documents raises the bar for data security[4]. It is more secure than a paper-based system since digital records are stored in safe settings like servers, databases, encryption, and so on, and can only be viewed by authorized individuals. The encryption technique is used to digitize and securely store client paper documents. It is encrypted before it is preserved as a digital picture. So that only those who are authorized to access it may do so.

In order to safeguard electronic data, the Advanced Encryption Standard (AES) provides a cryptographic algorithm authorized by the Federal Information Processing Standards (FIPS)[7]. Strictly speaking, AES is a block cipher that may be used to encrypt as well as decode data, making it a symmetrical algorithm. To put it another way: Encryption transforms data into an incomprehensible form called ciphertext, while decryption transforms the ciphertext back into plaintext. Data blocks of 128 bits may be processed using the Rijndael algorithm with cipher keys of 128, 192, or 256-bit lengths. [1] 128-bit sequences are used for both input and output in the AES algorithm.



"Figure1.Flowof AES128-bitAlgorithm"

Figure 1 depicts the AES algorithm's encryption process, which includes the key expansion block. Follow these procedures to learn how to use the AES algorithm:

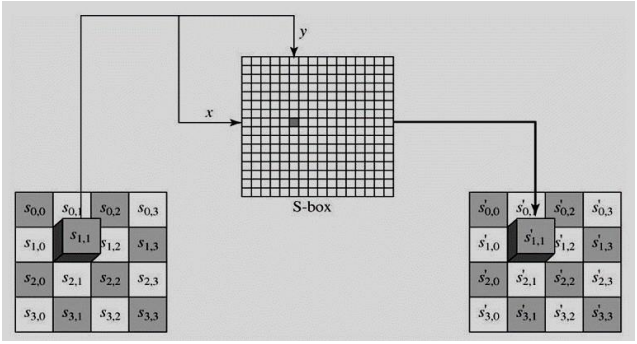
1) Key Selection- An agreed-upon 128-bit key is used for transmission. Images may be encrypted and decrypted using this key. In order to use this encryption method, they must share the key in a safe way. Blocks k [0], k [1], and k [15] represent the key. There are 128 blocks of 8bits apiece.

Generation of Multiple keys- With the above-described Modified AES Key Expansion approach, both the transmitter and the receiver may now produce the keys necessary for the procedure independently. Using these extended keys for subsequent communications may be done as many times as necessary until they lose their original key value.

A. "EncryptionprocessinAES

Ineachround followingstepsinvolves":

1. Sub byte- Each byte of the State may be treated as an independent unit in the non-linear substitution process known as the Substitute Byte Transformation (S-box). Combining an invertible affine transformation with the inverse function protects the S-box against assaults based on basic algebraic features.



"Figure2.SubByteSubstitution"

2. ShiftRows-The bytes in the State's final three rows are shifted cyclically by various amounts of bytes using the Shift Rows transformation. Row r=0 is left untouched. Because the arrangement of the bytes within the row has changed, the "lowest" bytes have moved to the "top" of the row.

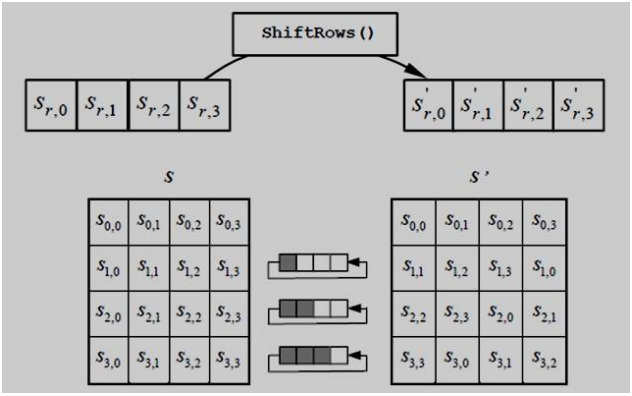


Figure3. ShiftRow

3. Mix Columns- Section-by-section, the Mix Columns alteration applies to the State's four-term polynomial. A appropriate polynomial, a(x), is used to enhance the segments' polynomials over GF (28) modulo x 4 + 1.

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

Figure 1 shows the resulting columns. A mix column's functioning is shown in this way.

- AddRoundKey- A bitwise XOR adds a Round Key to the State in the Add Round Key transformation. The key scheduling technique is used to get the Round Key from the Cipher Key. The elements of the State AddRoundKey
- (r, Nb)

have the same size, hence an XOR operation is performed on each one to get the following State:

"b(i,j) = a(i,j)⊕k(i,j)

2) DecryptionprocessinAES"

- This is the inverse of the Shift Rows transformation, which is called the Inverse Shift Rows. Three rows of bytes in the State's last section are randomly distributed across varying quantities of bytes. The initial row, r = 0, does not shift. r, Nb-shift (r, Nb) bytes are applied to the bottom three rows, where the row number determines the shift value

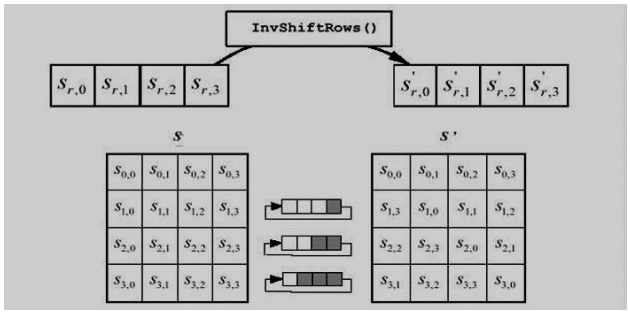


Figure6.InverseShiftRowTransformation

- "It is the reverse of the byte replacement change, in which the contrary S-box is applied to every byte of the state." Inverse substitution byte change Substitute byte change is the opposite of this. The multiplicative in-stanza in GF is used to reverse the relative change and get this result. The value may be substituted using a reverse s-box table.
- In reverse blends, the ingredients are reversed. This is the reverse of the change in Mix Columns. State segments are treated as four-term polynomials when using Reverse Mix Columns. a-1(x) is a good polynomial over GF (28) and is used to increase the segments modulo x4 + 1 using the polynomial a-1(x).

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

B. Keyprocessin AES"

"Pseudo code for AES Key Expansion: Word-by-word, the key-expansion procedure generates round keys, each consisting of four bytes. 4x(Nr+1) words are generated in this process, where Nr is the number of iterations."[7]Theprocessisasfollows:

1. The encryption key is used to form the first four words (initial key). Arrays of 16 bytes are used to represent the key (k0 to k15). Four bytes (k1-K7) are used to create the first two bytes (w0), and so forth.
2. To complete the sentence, substitute the following words (wi for i=4–43): Wi is equivalent to wi-1 XOR wi-4 in this scenario. If (I mod 4) is zero, then wi=t XOR wi-4; otherwise, wi-4 XOR wi. SubByte transformations on wi-1, followed by word rotation, result in the short-lived word "t," which may be used in programming.

3.RELATEDWORK

Figure.8 depicts the functioning system's flow diagram. First, the document that we need to protect is depicted in the figure. This document was made possible thanks to the use of a digital camera. Once the picture has been acquired, an effective encryption procedure is employed. In order to protect (encrypt) the scanned document, we employed the AES-128 technique, as previously described. The document will be encrypted before it is saved.As a result, the AES algorithm is used before the recorded document is stored in order to ensure that only authorized individuals are capturing (or scanning) the critical or secret information.As a result, authorized users with a valid key may see the original document that was collected using this technology. Because they do not have a valid key, anyone who want to open the document will not be able to access the original document.Digitizing paper documents and ensuring their security becomes possible as a result.

4.RESULTSANDDISCUSSION

The results of the algorithm's implementation are shown in the GUI output shown below.

1. An encrypted paper document is first photographed digitally. "Capture photo" button is all you need to do this.

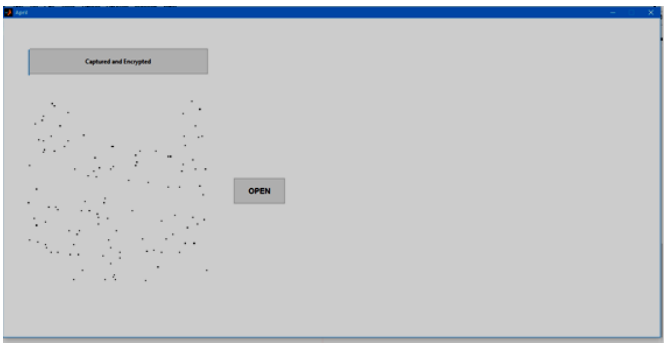
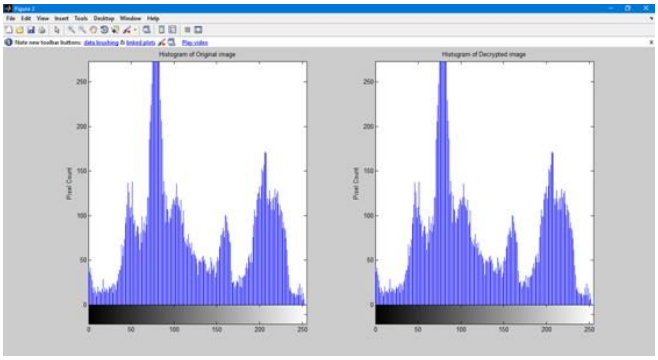


Figure9.EncryptionofDocument



“Figure12.HistogramofOriginalandDecryptedimage

5. CONCLUSIONANDFUTURE SCOPE”

Encryption methods differ in that each has advantages and disadvantages. We need to know about the performance, strengths, and weaknesses of various cryptography algorithms before we can use them effectively in a given application. In RSA, the amount of memory needed for implementation is the biggest. For DES and AES, the amount of RAM required is medium. The AES plus DES is the ideal choice for any application that requires the minimum memory footprint. AES, on the other hand, is the ideal algorithm to use if security is a top priority. We are using the AES algorithm to protect bank client data.

The suggested system employs the AES algorithm, which provides excellent security. An comprehensive search will be unfeasible for decades, even with AES-128's vast number of potential keys AES Algorithm encryption and decryption takes less time than DES Algorithm encryption and decryption. Symmetric key implementation that works In terms of encryption and decryption, AES is among the finest. A MATLAB code version of an AES method for image encryption and decryption has been synthesized and simulated. It is also possible to rebuild the original photos in their entirety and without any artifacts.

Reduce the amount of time it takes for picture encryption and decryption by using the technology currently being considered for implementation. It will also have no effect on the quality of the picture. Cameras may be replaced with scanners so that more pictures can be encrypted and decrypted at once. Scanners may expedite the picture capture process. Because of this, we may use our technology to protect corporate records and other huge enterprises that store a lot of paper documents.

REFERENCES

1. P.Thakkar,H.K.Mishra,Z.Shaikh,D.Sharma,"Image EncryptionandDecryptionSystemUsingAESforSecureTransmission", International Journal of Computer Sciences andEngineering, Vol.5, Issue.5,pp.109-114,2017.
2. Sachinsharma and Jeevan Singh Bisht, "*Performance Analysis ofData Encryption Algorithms*", International Journal of ScientificResearchinNetworkSecurityandCommunication,Vol.3,Issue.1, pp.1-5,2015.
3. A.Sharma,RSThakur,S.Jaloree,"*InvestigationofEfficientCrypticAlgorithmforimagefilesEncryptioninCloud*",International Journal of Scientific Research in Computer ScienceandEngineering,Vol.4, Issue.5,pp.5-11,2016.
4. Surbhi Sharma, "*Embedding more security in digital signaturesystembyusingcombinationofpublickeycryptographyandsecretsharingscheme*",InternationalJournalofComputerSciencesandEngineering,Vol.4, Issue.3,pp.111-115,2016.
5. WilliamStallings,“*AdvanceEncryptionStandard*,”in Cryptography and Network Security, 4th Ed., India: PEARSON,pp.134–165.
6. BehrousForouzen, “*Cryptography and Network Security*”, TataMc Graw –HillEducation2011.
7. S.Mewada,P.SharmaandS.S.Gautam,*"Explorationo fefficientsymmetricAESalgorithm,"* 2016SymposiumonColossal Data Analysis and Networking (CDAN), *Indore, 2016,pp.1-5.*