# MESSAGE SECURITY AND INTEGRITY MAINTENANCE USING FUZZY LOGIC AND SECRET SHARING

Anurag Mohapatra[1],Madhabananda sahoo[2], Ashis Kumar Mishra[3]

**Abstract**— Sending information from one point to another is called data communication. Today the security is the main issue in data communication. Encryption can provide a fine solution for it. The encryption algorithm is the mathematical procedure for performing encryption on data. A key is used to cipher a message and to decipher it back to the original message. The implementation of these algorithms can be very intricate. After conducting a research on currently using encryption algorithms, we have identified that all these algorithms only concern about security.With the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of long route data transmission in industrial process, it is essential to protect the confidential data from unauthorized access. In this paper, we analyze the Advanced Encryption Standard (AES), and we add some modification so as to provide enhanced security along with maintaining data integrity. Here we use Fuzzy Logic along with Secret Sharing Concept so as to provide finer and enhanced way of security and data integrity maintenance.

**Index Terms**— Fuzzy Logic, Message Integrity, Message security, Encryption, AES, Secret Sharing, Fuzzification, Image Creation, Modified AES.

## 1 INTRODUCTION

Security is ubiquitous. With the advent of ecommerce and electronic transactions, the need for development of secured systems has grown tremendously. With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. Cryptography is the study of building ciphers to ensure the confidentiality and integrity of information. Cryptographic systems fall into two main categories: those that rely on secret mechanisms (such as the German World War II Enigma machine) and those that rely on public, yet hard-to-solve, mathematical problems (such as RSA). Most modern cryptographic systems are variations of the latter. This allows all of the associated algorithms to be public, since knowing the method does not allow one to break the code. However, given enough computer time, any such code can be broken. Message integrity is dealt with authorized modification and alteration of data otherwise known as plaintext which is to be send to the receiver. There are so many approaches are made over year's analysis and various implementations by crypt analysts. Till now no model has been developed which could give fault free & full security to message while storing & sharing. There has been no model proposed yet that would provide message integrity and security at the same time. A software DES implementation is not fast enough to process the vast amount of data generated by multimedia applications and a hardware DES implementation (a set-top box) adds extra costs both to broadcasters and to receivers. In order to tackle these problems systems based on advanced encryption standard (AES) where proposed. AES [3, 6, 7] is very fast symmetric block algorithm especially by hardware implementation [7].The AES algorithm is used in some applications that require fast processing such as smart cards, cellular phones and image-video encryption. However, a central consideration for any cryptographic system is its susceptibility to possible attacks against the encryption algorithm such as statistical attack, differential attack, and various brute attacks. This paper proposes new encryption schemes as a modification of AES algorithm. The modification is done by adding a key stream generator, such as (A5/1, W7), to the AES [6] image encryption algorithm inorder to increase the image security and in turn the encryptionperformance.

## 2 AES ALGORTIHM

Rijndael AES algorithm is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting anycombination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data lengths that can bedivided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [4, 6]. These rounds are governed by the following transformations:

### 2.1 SubByte Transformation

Is a nonlinear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation.

### 2.2 ShiftRows Transformation

Is a simple byte transposition, the bytes in the last three rows of the state are cyclicallyshifted; the offset of the left shift var-

ies from one to three bytes.

### 2.3 MixColumns Transformation

Is equivalent to a matrix multiplication of columns of the states. Each columnvector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

### 2.4 AddRoundKey

Is a simple XOR between the working state and the roundkey. This transformation is its own inverse.

The encryption procedure consists of several. After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-mix columns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

## 3 KNOWN AES ATTACKS

A cryptographic "break" is anything faster than a brute force-performing one trial decryption for each key. AES has a fairly simple algebraic description. In 2002, a theoretical attack, termed the "XSL attack", was announced by Nicolas Courtois and Josef Pieprzyk, purporting to show a weakness in the AES algorithm due to its simple description. On July 1, 2009, Bruce Schneier blogged about a related-key attack on the 192-bit and 256-bit versions of AES, discovered by Alex Biryukov and Dmitry Khovratovich, which exploits AES's somewhat simple key schedule and has a complexity of $2^{119}$. In December 2009 it was improvedto $2^{99.5}$. This is a follow-up to an attack discovered earlier in 2009 by Alex Biryukov, Dmitry Khovratovich, and IvicaNikolic, with a complexity of $2^{96}$ for one out of every $2^{35}$ keys. In November 2009, the first known-key distinguishing attack against a reduced 8-round version of AES-128 was released as a preprint. This known-key distinguishing attack is an improvement of the rebound or the start-from-the-middle attacks for AES-like permutations, which view two consecutive rounds of permutation as the application of a so-called Super-Sbox. The first key-recovery attacks on full AES were due to AndreyBogdanov, Dmitry Khovratovich, and Christian Rechberger, and were published in 2011. The attack is based on bicliques and is faster than brute force by a factor of about four. It requires $2^{126.1}$ operations to recover an AES-128 key. For AES-192 and AES-256, $2^{189.7}$ and $2^{254.4}$ operations are needed, respectively. With the ever expanding and increasing computational speed in today's world, as explain by Moore's Law which states that "Every 2 years the computational speed would increase by 2 times". With such fast rate of increase it is not far when this algorithm would also be broken.

## 4 MESSAGE INTEGRITY

Message integrity means validity of a transmitted message. It deals with methods that ensure thatthe contents of a message have not been tampered with and altered. The most common approachis to use a one-way hash function that combines all the bytes in the message with a secret key and produces a message digest that is impossible to reverse. Integrity checking is one componentof an information security program.

## 5 FUZZY SET THEORY

Fuzzy [8, 9] set theory is an extension of classical set theory where elements have varying degrees of membership. A logic based on the two truth values True and false is sometimes inadequate when describing human reasoning. Fuzzy [5] logic uses the whole interval between 0 (false) and 1 (True) to describe human reasoning. A fuzzy set is any set thatallows its members to have different degree of membership function in the interval [0,1].The degree of membership (or) truth is not same as probability.Fuzzy truth is not likelihood of some event (or) conditions. The fuzzy truth represents membership in vaguely defined sets.

## 6 SECRET SHARING

Secret [4] sharing was invented independently by Adi Shamir and George Blakley in 1979. Secret sharing (also called secret splitting) refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own. Secret sharing [4] schemes are ideal for storing information that is highly sensitive and highly important. Examples include: encryption keys, missile launch codes, and numbered bank accounts. Each of these pieces of information must be kept highly confidential, as their exposure could be disastrous; however, it is also critical that they not be lost. Traditional methods for encryption are ill-suited for simultaneously achieving high levels of confidentiality and reliability.

## 7 PROPOSED MODEL

Symmetric key cryptography refers to encryption methods in which both the sender and receivershare the same key (and, less commonly, in which their keys are different, but related in an easilycomputable way). The modern study of symmetric ciphers relates mainly to the study of blockciphers and stream ciphers and to their applications. A block cipher take as input


- *Anurag Mohapatra is currently pursuing bachelor's degree program in computer science and engineering in College of Engineering and Technology(BPUT),India. E-mail: mohapatra.anurag@gmail.com . His current Field of research being Computer Security and Artificial Intelligence.*
- *Madhabananda Sahoo is currently pursuing bachelor's degree program in computer science and engineering in College of Engineering and Technology (BPUT), India. E-mail: madhabananda.sahoo@gmail.com His current field of reasearch being soft-computing.*
- *Ashis Kumar Mishra is currently is a lecturer in computer science and engineering department at College of Engineering and Technology (BPUT), India. E-mail: ashiskumar.misra@gmail.com .His Current field of research is Cloud Computingand Machine learning*

a block ofplaintext and a key, and output a block of cipher text of the same size. Since messages are almostalways longer than a single block, some method of knitting together successive blocks isrequired. Several have been developed, some better security in one aspect or another than others.They are the mode of operations which must be carefully considered when using a block cipherin a crypto system. Rijndael algorithm is one of the AES (Advanced Encryption Standard)algorithm used for data encryption technique. It is a block cipher algorithm in which the blockmeans the information to be encrypted is divided into blocks of equal length. It is an integrated-block cipher, with a variable block length and variables key lengths. Internally, the AESalgorithms operations are performed on a two dimensional array of bytes called the state. Thestate consists of four rows of bytes.

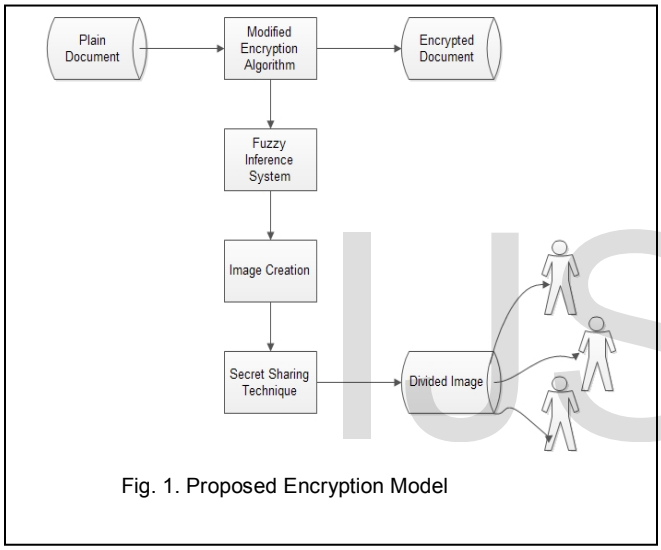


Fig. 1. Proposed Encryption Model

### 7.1 Encryption

The main steps of Rijndael algorithm [3] are:

#### 7.1.1 SubBytes Transformation

In the SubBytes step, each byte in the state matrix is replaced with a SubByte using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher.The S-box used is derived from the multiplicative inverse over GF(28), known to have good nonlinearityproperties. To avoid attacks based on simple algebraic properties, the S-box isconstructed by combining the inverse function with an invertible affine transformation. The Sboxis also chosen to avoid any fixed points (and so is a derangement), and also any oppositefixed points.

#### 7.1.2 ShiftRows Transformation

The Shift Rows step operates on the rows of the state; it cyclically shifts the bytes in each row bya certain offset. For AES, the first row is left unchanged. Each byte of the second row is shiftedone to the left. Similarly, the third and fourth rows are shifted by offsets of two and threerespectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n isshifted left circular by n-1 bytes. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. (Rijndael variantswith a larger block size have slightly different offsets). For a 256-bit block, the first row isunchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytesrespectively—this change only applies for the Rijndael cipher when used with a 256-bit block, asAES does not use 256-bit blocks.

#### 6.1.3 MixColumns Transformation

In the MixColumns step, the four bytes of each column of the state are combined using aninvertible linear transformation. TheMixColumns function takes four bytes as input and outputsfour bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher. In more general sense, each column is treated as a polynomial over GF(28) and is then multiplied modulo x4+1 with a fixed polynomial $c(x) = 0x03 \cdot x3 + x2 + x + 0x02$. The coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from GF(2)[x]. The MixColumns step can also be viewed as a multiplication by a particular MDS matrix in a finite field. This process is described further in the article Rijndael mix columns.

#### 7.1.4 AddRoundKey Transformation

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey isderived from the main key using Rijndael's key schedule; each subkey is the same size as thestate. The subkey is added by combining each byte of the state with the corresponding byte of thesubkey using bitwise XOR.

The above discussed steps are present in a general AES algorithm.The general AES algorithmtakes nearly 10 rounds to complete the encryption. After encryption has been done we are to thenpass itthrough a Message Digest message to provide integrity.

## 8 MODIFICATIONS

Here in this proposed model we want to provide better security as well as integrity maintenanceto the message by doing a little modification to the AES algorithm and introducing into it fuzzy[1]application as well as image creation techniques. The

new steps would be as follows:

### 8.1 Fuzzy Inference System

In this technique we define fuzzy inference system through which an intermediate cipher textformed after the initial first threeround is passed. The cipher text is passed through this in block form.Each block is of size 1024bits. The input to the FIS would the difference in number of zero'spresent to the number of one's present in the block.

FIS input = No. of Zero's in block – No. of one's in block

The output of the FIS would be color codes for Red, Green and Blue values of pixel. This would go into next round of image creation to produce each pixels of the image from the color code.

### 8.2 Image Creation

The outputs from the above FIS would be taken as the RGB values for each pixel. According toRGB values each pixel color would be set. These pixels would be then set to create a color-image. The size of the color image would depend upon the size of the message. It may vary from256*256 to 1024*1024. This image acts as the hash function image for the text to be used to giveintegrity of the message.

### 8.3 Secret Sharing

Secret Sharing technique is mostly used in distributing sensitive information among specific people except no one else should see the information. We would like divide our image formed in previous round so as to distribute among concerned people or between several servers for an individual. By doing this we protect the information from being seen by people other than the people concerned. The secret sharing technique would provide us a way to emphasize security upon the image rather than the whole document as the image is much lighter than the document and we can send the heavier actual encrypted document through an insecure and faster route without fear of being read or decoded.
As we can see in fig1 by creating an image using fuzzy as hash function we would use this particular image for decryption in the future as well as image comparison so as to check the integrity of the received data.

## 9 Conclusion

From our proposed model we have planned introducing a little modification to the current flow of encryption so as to provide both message integrity as well as security of sensitive data that would and could only be read or decoded by the person concerned. By proposing this model we are trying to reduce attack possibilities in security as the modification introduce would shift the emphasis of security from heavier encrypted document to lighter image document formed from it.

## Acknowledgment

The authors wish to thank my parents, teachers and my friends as well as my partners for helping me in this paper.

## References

[1] Fuzzy Logic: An Introduction [online] http://www.seattlerobotics.org

[2] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994

[3] Dr. Brian Gladman, Rijndeal (by Joan Daeman& Vincent Rijmen), "A Specification for the
AES Algorithm", 15 April 2003.

[4] M. Naor and A. Shamir, "Visual cryptography," in Proc. Eurocrypt'94, LNCS 950.1995, pp.
1–12.

[5] Hexiong Yang, Chongwen Li, Fuzzy Mathematics and Its Application, Tianjin: Tianjin Science & Technology Publishing House, 1990.37-101.

[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", IJCSE Volume 1 Number 1.

[7] R. C.-W. Phan, "Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)", Information processing letters 91(2004) 33-38.

[8] ArindamSarkar, J.K Mandal, " Secured Wireless Communication using Fuzzy Logic based High Speed Public-Key Cryptography (FLHSPKC)" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[9] "Fuzzy Sets and Applications: Selected Papers by L.A. Zadeh", ed. R.R. Yager et al. (John Wiley, New York,1987).