Journal of Science and Technology
ISSN: 2456-5660 Volume 6, Issue 2, March-April 2021
www.jst.org.in DOI: *https://doi.org/10.46243/jst.2021.v6.i2.pp118-122*

Study of Signal Image Processing by Implementing a Secure Software of Nonlinear Advanced Encryption Standard

G.Madhavi
Assistant Professor, Department of ECE, MGIT, Hyderabad
Corresponding Author: gmadhavi_ece@mgit.ac.in

To Cite this Article
G.Madhavi *"***Study of Signal Image Processing by Implementing a Secure Software of Nonlinear Advanced Encryption Standard***", Journal of Science and Technology, Vol. 06, Issue 02, March-April 2021, pp.:118-122.*

Article Info
Received: 08-04-2021 *Revised: 10-04-2021* *Accepted: 13-04-2021* *Published: 15-04-2021*

ABSTRACT:
It was designed to withstand linear or differential cryptanalysis (i.e., AES) assaults, which are the most common types of cryptanalysis. It is crucial that the S-box used in the AES be chosen carefully. There may be a flaw in the S-box architecture of the AES algorithm based on the new attack techniques. Linearity issues in the S-box are to blame for the setbacks. A novel performance approach for increasing nonlinear transformation complexity in the S-box structure is offered after a thorough examination of the AES algorithm. An additional layer of security was added by employing a biometric approach for both encryption and decryption in order to fend off new threats and perform AES with verilog-protected encryption and decryption. For encryption and decryption, Verilog's novel nonlinear version of AES S-Box offers increased security with adequate performance.

AES, Non-linear S-Box, Biometric Image are some of the keywords.

I. Introduction

As consumers spend more time online, the need for network security grows. Compromise of physical or local security is rare, but compromise of a network's security is much more prevalent. All aspects of computers and information processing are covered by computer security. A company's data is seen as a valuable asset in industries that rely heavily on computer systems and networks to do business. Anti-virus software is used to protect computers from unwanted access. In order to keep unauthorised people from accessing any component of your computer system, you may use prevention measures. In order to establish whether or not someone tried to get into your system, whether or not they were successful, and what they may have done, you need detection.
Electronic data may be encrypted using the Advanced Encryption Standard (AES) from the National Institute of Standards and Technology (NIST). Digital information, including financial, telecommunications, and government data, is intended to be encrypted using this method. Data Encryption Standard (DES) was replaced by AES (DES).

II. Advanced Encryption Standard

It stands for Advanced Encryption Standard, or AES. In lieu of the Data Encryption Standard (DES), AES is a symmetric key encryption method (DES). NIST picked AES as a Federal Information Processing Standard because of its high level of encryption. The AES algorithm has three key sizes: 128,192, and 256-bit. The method behaves somewhat differently depending on the size of the encryption key, therefore as key sizes rise, the complexity of the cypher algorithm increases as well. In the AES algorithm, four fundamental transformations are depicted:
Using a substitution table, this transforms each byte of the State one at a time (Sbox).

2. Row Transformation:

- Depending on the row, a certain amount of bytes are shifted to the left.
- The transformation of the mix columns is the third step.
- It's possible to map a column's four bytes into a new value for each byte in the column.
- Round Key Transformation may now be added.
- The 128 bits of State and the 128 bits of the round key are bitwise XORed.

III. Existing System

Modem cryptography has focused on the security of sensitive information communicated via the Internet. The Advanced Encryption Standard (AES) is based on the Rijndael algorithm (NIST). This is the first open encryption algorithm that protects sensitive information. There are certain drawbacks to using DES due to its short key length, the complementary feature, and the presence of weak and semi-weak keys; a stronger encryption algorithm should be used in its place. When utilising the AES, the goal is to ensure that only the intended recipient with a certain key may access the original data. However, malicious flaws may be inserted into non-secure situations. The S-current box's encryption algorithm is linear and vulnerable to cryptanalysis. As a result, the suggested DES system is not as secure as DES claims to be. The essential size of the fascinating system will not be little, therefore the area will expand.

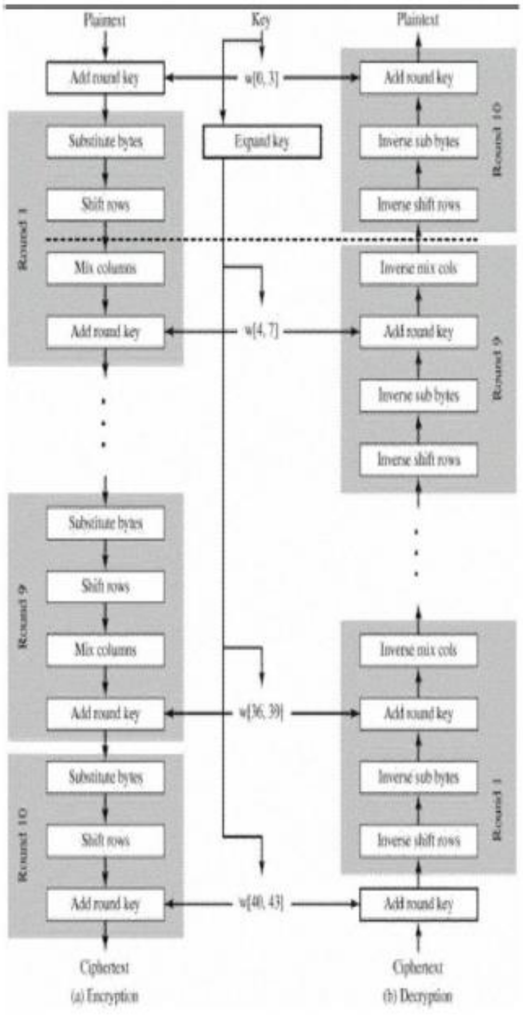

Fig.1.Block diagram of AES Algorithm

IV. Proposed System

We know from Rijndael algorithm research that a non-linear S-box transformation layer is essential to the overall method's robustness. There's no doubt that the AES's cryptographic strength relies on the S-selection. box's Many cryptographers have found a flaw in the design of the current S-box. Our strategy combines a dynamic nonlinear transformation method with a linear function to increase the complexity of the S-box structure. For example, a high quality s-box can easily withstand assaults such as differential cryptanalysis and linear cryptanalysis. Both Substitution Bytes and Inverse Substitution Bytes are protected by S-boxes, which are used in the AES. The nonlinear and linear transformation models need to be rethought in the design of the S-Box in order to increase its complexity.

4.1 Non-linearity:

The Substitute Bytes step in AES serves the purpose of non-linearity. The RijndaeI S-box, an 8-bit substitution box, is used to update each byte in the array in the Sub Bytes phase. S-boxes convert one bit of input data into another bit of output data. S-boxes that perform well have the ability to modify half of the output bit by changing one input bit. As a result, every single output bit will rely on the input bits. An S-box that is extremely resistant to all known threats will be designed here. The key is safeguarded because the S-box is nonlinear. The dynamic formulation of the s-box prevented the attackers from knowing the key. As a result, there will be more security.

4.2 Biometrics:

Each time a person's biometrics are analysed, the results are somewhat different. Due to the fact that the initial biometric and a subsequent untreated measurement of the same biometric would not match, they cannot be saved in untreated form as passwords. There must be a safe method of storing biometrics that cannot be exploited by an attacker to impersonate a legitimate user for biometrics to be widely accepted. Because of S-nonlinear Box's nature, the encryption and decryption processes are very secure, although biometrics are used to enhance authentication. The fingerprint is encrypted using AES and then decrypted to increase its complexity. When paired with biometric authentication, this creates a comprehensive application.

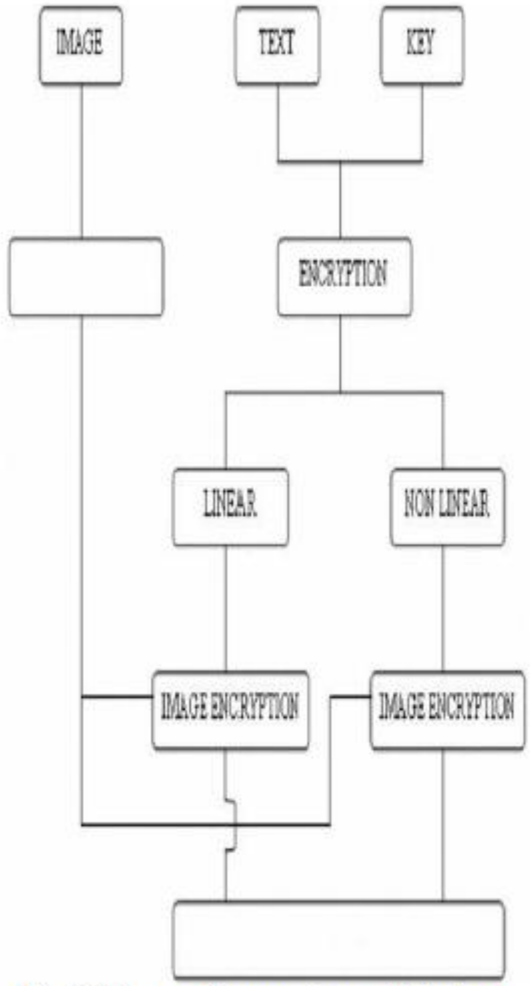

Fig.2. Proposed encryption architecture

V. IMPLEMENTATION

Construction becomes more difficult by changing the S-linear box's structure into a nonlinear one. By replacing a random hexadecimal number, you may obtain the nonlinear structure. During the encryption process, the suggested structure generates a random hexadecimal number for each S-box value that is called. Three S-Boxes are employed in the nonlinear implementation. To construct the virtual S-Box, the input value is first mapped to the original AES S-Box, called Default S-Box (Pre-defined S-Box), and then XORed with the new derived S-Box, called the l's complement of the real S-Box. As a result, the virtual S-Box will be constructed on-the-fly for every possible value of the input. Similar to the decryption procedure, the inverted virtual S-Box will be used for both processes. A virtual S-Box will be built, and the encrypted value will be mapped to this virtual S-Box to produce the encrypted output. Decryption begins with a mapping of the input value to the S-Box, and this value is then mapped to the virtual S-Box to yield the decrypted original value.

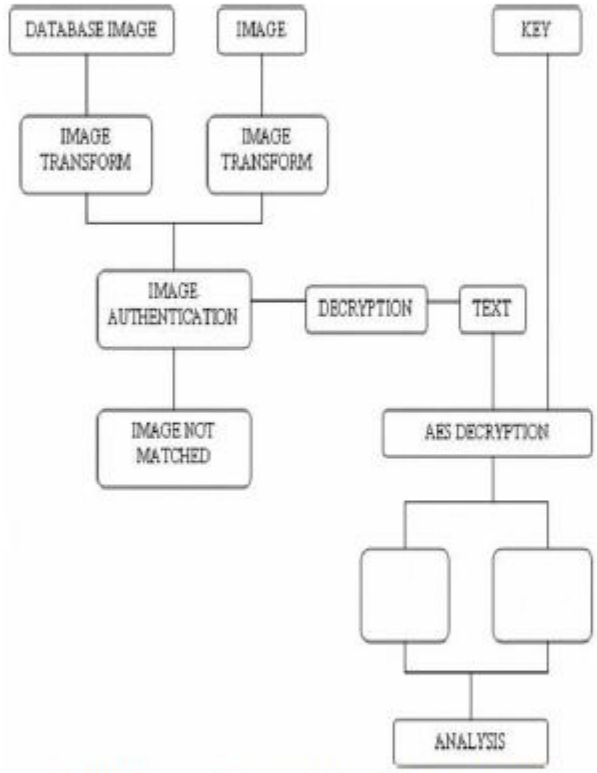

Fig.3.Proposed decryption architecture

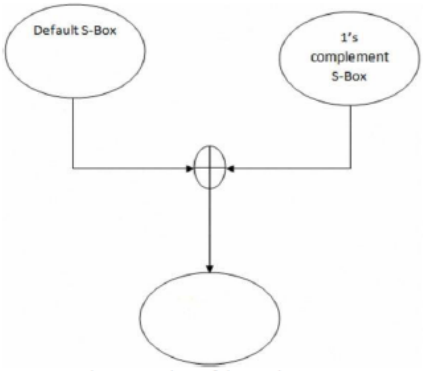

Fig.4.Creation of dynamic S-Box

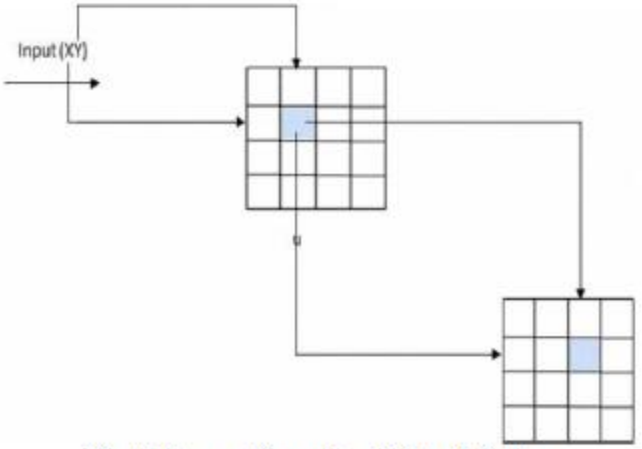

Fig.5.Decryption using Virtual S-Box

An encrypted picture is created by repeatedly swapping the rows and columns of an input image using the fuzzy vault technique, which uses an input image as input. A database of fingerprint images is used to compare the user's input to those saved in the database. In this case, authentication is granted and the decryption procedure begins.

VI. CONCLUSION

The new attack techniques clearly demonstrate that the S-design box's has some flaws. The S-box and key schedule have a linearity issue, which is its primary flaw. In order to guard against new attacks, nonlinear transformations in the S-box and key schedule design must be improved. In our implementation strategy, we increased the complexity of the nonlinear transformation of the S-box to counter new threats. In this implementation approach, the uniqueness of the AES algorithm is not harmed, but it is made more dynamic and non-linear, making it unbreakable. An acceptable speed of data encryption and decryption may be achieved using the Verilog implementation approach. Using a new nonlinear transformation for AES S-box, this implementation increases the S-box structure's complexity. Strong and increased security is provided by the S-improved box's construction. Additional security is provided by the biometrics approach being aligned with the AES algorithm.

References

[1] National Institute of Standards and Technology (NIST), "Recommendation for Block cipher modes of operation," Dec.2001.

[2] "A New Mutable Nonlinear Transformation Algorithm for S-box" Atsushi WATANABE, Hiroshi HARUKI,Shun SH1MOTOMAI, Takeshi SAITO, Tomoyuki NAGASE

[3] "A Research and Improvement based On Rijndael Algorithm" Van chun, Yanxia GUO

[4] NIST, "Advanced Encryption Standard," FIPS PUB 197, pp. I-51, November 2001

[5] "AES Proposal: Rijndael", Joan Daemen, Vincent Rijmen, Springer- Verlag, Berlin Heidelberg, 2002.

[6] Claude Carlet "Lower bounds on the higher order nonlinearities of Boolean functions and their applications to the inverse function"

[7] Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard Mehran Mozaffari- Kermani, and Arash Reyhani-Masoleh.

[8] "Efficient method for simplifYing and approximating the S-boxes based on power functions" by A. F arhadian and M.R. Aref in the year 2009.

[9] "A High speed FGPA implementation of the rinjdael algorithm" by Refik Sever A., Neslin Ismailoglu, Yusuf C.Tekmen, Murat Askar anc Burak Okcan.2004

[10] "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" by Md. Nazrul.