An Effective Implementation of Masked and Unmasked AES Block for High Security

Mr.Sailesh S [1], Dr.Archana HR [2],

Dr. Surendra H H[3], Dr. Madhusudhan K N[4]

[1]Student, Department of Electronics and Communication Engineering,

[2,3, 4] Assistant Professor, Department of Electronics and Communication Engineering

BMS College of Engineering, Bangalore, India

Email: [1]saileshs360@gmail.com [2]archanahr.ece@bmsce.ac.in

[3] surendrahh.ece@bmsce.ac.in [4]madhusudhankn.ece@bmsce.ac.in

Abstract:

AES Encryption algorithm, also known as the Rijndael algorithm, it is a symmetric block cipher algorithm. Here we implement AES Algorithm as a normal AES design and Masked AES design, in the normal AES design we perform the round operation and a pre-round computation process, in round operation we implement sub bytes, shift rows, mixed columns and key expansion process to arrive at the cipher text, and in the masked AES design we use a random mask generator to generate random mask data and xor the masked data with the plain text and it is given as the input to the AES core, here we use masking mainly for the security purpose, and we compare the Area, delay and power of both the normal AES design and masked AES design. Then using the masked design we make an encryption and decryption of the images.

Keywords: **AES, Encryption, Decryption, Masking, Round operation, Key expansion.**

1. INTRODUCTION

Cryptography is the use of a cryptosystem or cipher to prevent users other than the intended receiver from decrypting or utilising the encrypted material, sometimes known as encryption. A message can be encoded using a cryptosystem only when the correct algorithm and keys are used to decode the message the recipient can see the encrypted content. The main application of cryptography is the transmission of confidential information through computer networks. The AES encryption technique is a block cipher that employs multiple rounds of encryption and an encryption key. The AES uses the secured double rate registers for improving the security of the data [5], along with the secret key. An encryption system known as a block cipher only encrypts one block of data at a time. The block in typical AES encryption has a length of 128 bits. The length of the key might range from 128 bits to 256 bits. The usage of a 128-bit encryption key is referred to as 128-bit encryption. With AES, the same key is used for both encryption and decryption, thus AES is a symmetric encryption algorithm.Asymmetric encryption algorithms are those that employ two distinct keys a public key and a private key in their operation.

2 . EXISTING SYSTEM

During the encryption process of AES Algorithm, random intermediate data is continuously added to the plaintexts to protect the side-channel leakage from replacement boxes that process the secret data. In this system we implement the 128 bit AES Algorithm where the plain text is given as the input and after the round operation is completed we arrive at the final encrypted cipher text, here we use the secured double rate register (SDRR) for increasing the security of the algorithm. But this system has few drawbacks, A conventional AES engine requires a large lookup table, because of which the area has increased. The speed of the AES Algorithm is significantly reduced due to the large amount of random masking data values.To overcome this issue AES algorithm is implemented using masking technique.

3. AES Design

For sensitive and intelligent infrastructures like the safe healthcare system, smart grid, fabric, and home, cryptographic designs offer protection. The fields of cryptology and cryptanalysis have a tight relationship with cryptography. There are several other algorithms for security which is known as DES, but AES is said to be faster because it can encrypt many files within a short period of time. Fig.1. shows the block diagram of the AES Algorithm, here the plain text (128 bit) is given as the input and the plain text is processed in blocks, the block size is 128 bits (4 words/16 bytes),we use a key in each and every round. In AES Algorithm the plain text is processed in 10 rounds to arrive at the cipher text. We use a separate sub key for each and every round, in each round we are going to use 4 sub key, initially we are going to perform a pre round computation, so totally we require 44 sub keys, the round function consists of four steps one is sub bytes, shift rows, mixed columns, & add round key these four steps are done for 10 rounds, but in last round the mixed column operation will not be done, here the here the key is processed in terms of words, hence we are going to use words [W0 – W3] for first round and for last round [W40 – W43]. Hence finally after performing all these round functions we arrive at the cipher text which is also 128 bit. Similarly for the decryption process we do the reverse process which is also called reverse AES where we perform the inverse sub bytes, inverse shift rows, inverse mixed column, by giving the cipher text as the input and by using keys from words [W40 – W43] to [W0 –W3] and arrive at the plain text.

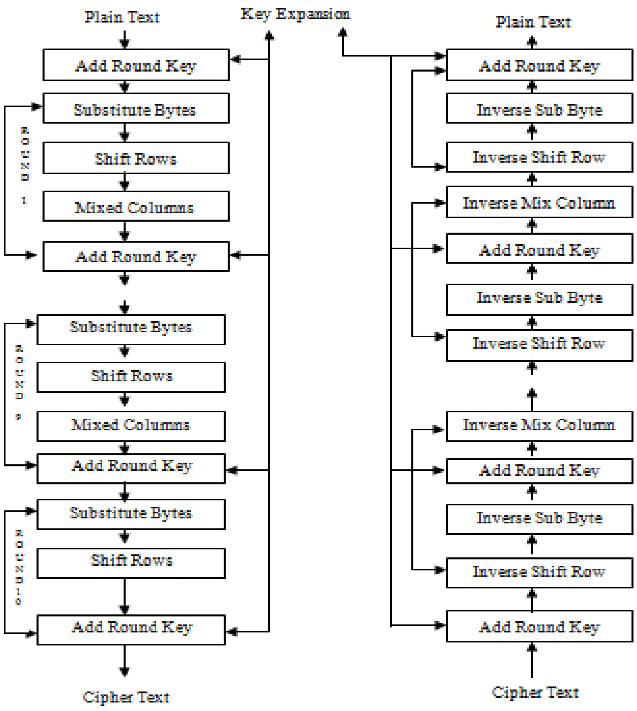


Fig 1. Block schematic of AES Algorithm

4. AES Masking

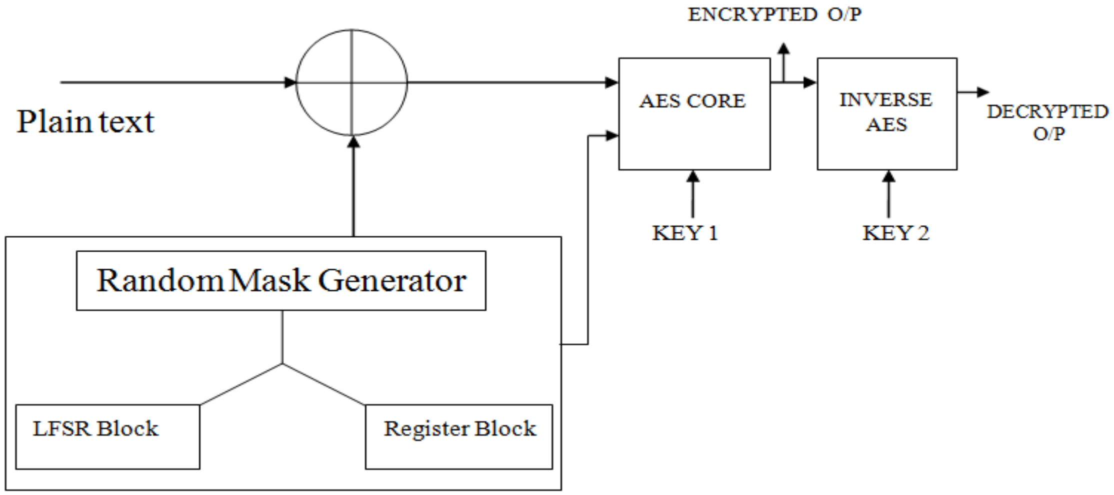


Fig 2. Block schematic of the proposed AES Masked Design

Fig.2. shows the block diagram of the masked AES design, the block consists of random mask generator, which consists of LFSR block and the register block, the register block consists of D Flip flops each of single bit so there are 128 flip flops from the 128 bit data the values are taken randomly using LFSR and perform XOR operation and give as feedback to the input hence we get the random mask data. This masked data is then XORED with the input data i,e the plain text, so we will be getting the plain text as masked plain text, this data is given as input to the AES core where we first perform the encryption using a key to arrive at the cipher text, this data is then given through the other AES core to perform the inverse AES which uses another key to arrive at the decrypted output. Here we are using two keys one is the transmitter key and other is the receiver key when both the transmitter key and receiver key are same then both the encryption and decryption will be done, if the key is different then only encryption will be done but decryption will not be done.

5. Image encryption and decryption of masked AES design

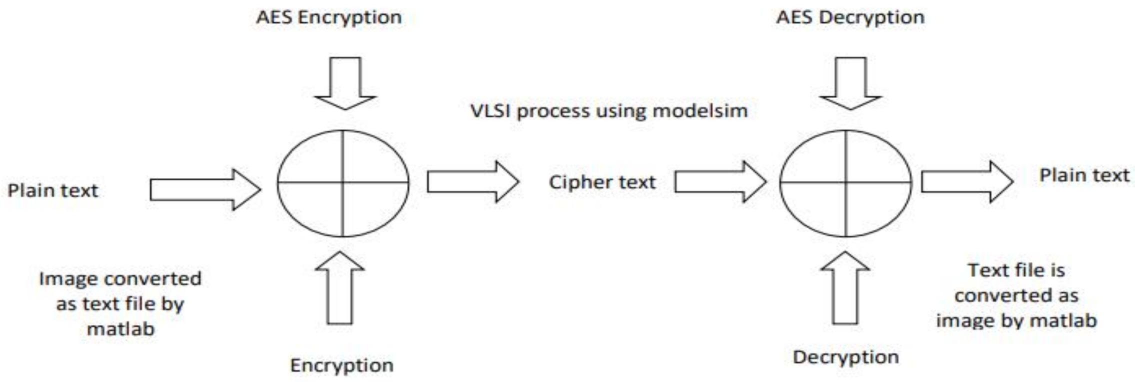
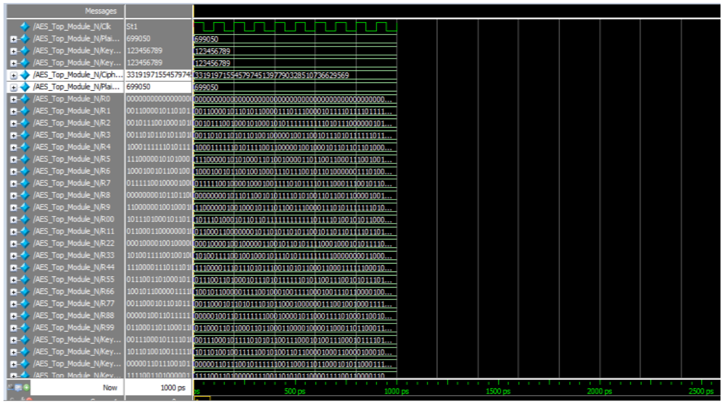

AES Encryption
AES Decryption
VLSI process using modelsim
Plain text
Cipher text
Plain text
Image converted as text file by matlab
Encryption
Decryption
Text file is converted as image by matlab

Fig 3. Image encryption and decryption using Matlab & VLSI

As shown in fig 3, we are going to make encryption & decryption based on images. We are going to merge the matlab & vlsi for this Process. Initially we give the plain text as the input, the plain text can be anything image, text. But in our case we give as an image. We take an image and convert it into pixels through matlab, pixels here are 0's and 1's. Here the pixels will be stored in the notepad in txt file. This txt file will then be read in verilog and then the encryption and decryption will be performed and the output will be converted to text file (pixels) and after this we will get the image through matlab. Here we will first read the image, then the read image is checked if it is colour image or gray image, if its gray image then it is said as the input image, if it is colour image it then converts it to gray image, then will display the image, then the we will resize the image and load the image files and convert it as text files then the converted text file is fed into the other part where we use the modelsim process here we use a key, the key can be given any name here 1 character is 8 bit so totally 128 bit, hence we can give 16 characters, then the encrypted and decrypted text file will be read and the image will be displayed.

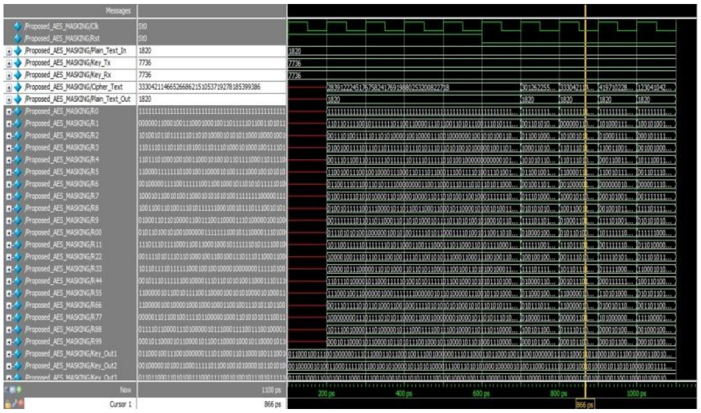
6. Results and Simulation



```
Messages
/AES_Top_Module_N/Clk      St1
/AES_Top_Module_N/Plai...  699050
/AES_Top_Module_N/Key...   123456789
/AES_Top_Module_N/Key...   123456789
/AES_Top_Module_N/Ciph...  3319197155457974
/AES_Top_Module_N/Plai...  699050
/AES_Top_Module_N/R0       0000000000000000
/AES_Top_Module_N/R1       0011000010110101
/AES_Top_Module_N/R2       0010111001000101
/AES_Top_Module_N/R3       0011010110101101
/AES_Top_Module_N/R4       1000111111010111
/AES_Top_Module_N/R5       1110000010101000
/AES_Top_Module_N/R6       1000100101100100
/AES_Top_Module_N/R7       0111110010000100
/AES_Top_Module_N/R8       0000000010110110
/AES_Top_Module_N/R9       1100000010010001
/AES_Top_Module_N/R00      1011101000101101
/AES_Top_Module_N/R11      0110001100000001
/AES_Top_Module_N/R22      0001000010010000
/AES_Top_Module_N/R33      1010011110010010
/AES_Top_Module_N/R44      1110000111011101
/AES_Top_Module_N/R55      0111001101000101
/AES_Top_Module_N/R66      1001011000001111
/AES_Top_Module_N/R77      0011000101101011
/AES_Top_Module_N/R88      0000010011011111
/AES_Top_Module_N/R99      0110001101100011
/AES_Top_Module_N/Key...   0011100010111101
/AES_Top_Module_N/Key...   1011010010011111
/AES_Top_Module_N/Key...   0000011011100101
/AES_Top_Module_N/Key...   1111001101000001
Now                        1000 ps
```

Fig 4. Simulation of AES algorithm

Fig.4 shows the simulation of AES algorithm, the transmitter key and receiver key is same, both encryption and decryption is done, when the key is not matching decryption will not be done, but encryption will be done.



```
Messages
/Proposed_AES_MASKING/Clk             St0
/Proposed_AES_MASKING/Rst             St0
/Proposed_AES_MASKING/Plain_Text_In   1820
/Proposed_AES_MASKING/Key_Tx          7736
/Proposed_AES_MASKING/Key_Rx          7736
/Proposed_AES_MASKING/Cipher_Text     333042114665266862151053719278185399386
/Proposed_AES_MASKING/Plain_Text_Out  1820
/Proposed_AES_MASKING/R0              1111111111111111111111111111111111111111111
/Proposed_AES_MASKING/R1              00000011000100111000100010011011111011001101011
/Proposed_AES_MASKING/R2              1010010110111111101101010000101010110001000010001
/Proposed_AES_MASKING/R3              11011101110110110100111011101000101000100111101
/Proposed_AES_MASKING/R4              110111010000100100110001010010110111100011011110
/Proposed_AES_MASKING/R5              11000011111110100100110000101001111000100101010
/Proposed_AES_MASKING/R6              00100000111100111111001100100010110101011111010
/Proposed_AES_MASKING/R7              10001011001010011000101010101001111111100000111
/Proposed_AES_MASKING/R8              10011001101001110101111110001001011101110010101
/Proposed_AES_MASKING/R9              01000110110100001100111001100001110100000100100
/Proposed_AES_MASKING/R00             010110100101001000000011111111001011100001110100
/Proposed_AES_MASKING/R11             1110111011110001100110001000101111101011110010
/Proposed_AES_MASKING/R22             001111010111011010000100110010011101110110001100
/Proposed_AES_MASKING/R33             101101111011111110001001001000010000000111110100
/Proposed_AES_MASKING/R44             00101110111111001000011101101010100110001110111
/Proposed_AES_MASKING/R55             11000001011001011110011000010010101000010100011
/Proposed_AES_MASKING/R66             110000001001000010001000100011001001110101101100
/Proposed_AES_MASKING/R77             00000110110010011110110000010001101010101110011
/Proposed_AES_MASKING/R88             01111011000011101000001011100011110011100100001
/Proposed_AES_MASKING/R99             0001011000010110000101100110000100010110000101
/Proposed_AES_MASKING/Key_Out1        01100010011100100000011101100011011000100111001
/Proposed_AES_MASKING/Key_Out2        00100000101001100011111011001001010000101101010
/Proposed_AES_MASKING/Key_Out3        0110110001101010011100011110010100101110101111
Now                                   1100 ps
Cursor 1                              866 ps
```

Fig 5. Simulation of AES algorithm with masking

Fig 5 shows the simulation of AES algorithm with masking, the transmitter key and receiver key is same, both encryption and decryption is done, here masking is used to increase the internal security of the data.

I. Area and Delay Comparision of normal AES and Masked AES

Method Name	Area in terms of LUT'S	Delay
Normal AES Design	29,832	110.375 ns
Masked AES Design	29,682	106.865 ns

Table 1 Area and Delay Comparision

Table 1 shows the comparision of the area and delay parameters of the normal AES Algorithm and the masked AES Algorithm here the area is expressed in terms of LUT'S in the normal AES encryption the number of LUT's is found to 29,832 and in the masked implementation of the AES encryption the number of LUT's is found to 29,682. Also the delay of the normal AES is found to be 110.375 ns and that of masked AES is 106.865 ns.

	Power (mW)	
Method Name	Logic power	Dynamic power
Masked AES Design	962	5247
Normal AES Design	10950	32747

Table 2. Power comparision table

Table 2, Shows the power comparision of normal AES Algorithm and the masked AES Algorithm, here the logic power is found to be 10,950 mW and the dynamic power is found to be 32747 mW for the normal AES Algorithm, and for the masked AES Algorithm the logic power is found to be 962 mW and the dynamic power is found to be 5247 mW.

II. Results of Masked AES design for image Encryption and Decryption

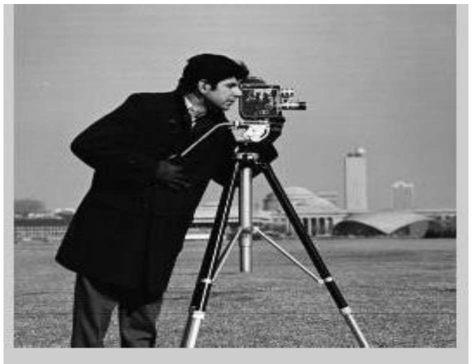


Fig 6. Input Image

Figure 6. Shows the input image which is the gray image is which is to be converted into pixels and to be stored in notepad in .txt file which is then given into the module for encryption process.

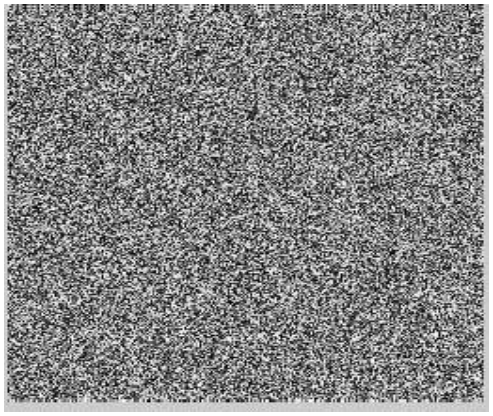


Fig 7. Encrypted Image

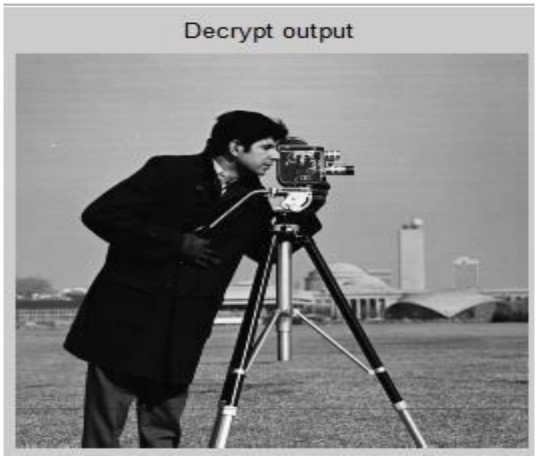


Fig.8. Decrypted Image

Figure 8. Shows the Decrypted image which is same as the input image which is the gray image which goes the encryption and decryption process and conversion of image into pixels and storing in the note pad in the .txt file and getting back the input image.

7. CONCLUSION

A unique Pipelined AES Design with masking technique for high security is implemented. Also we perform the encryption of the plain text using the pre round computation followed by the round operations. We have also designed a decryption system. This design provides a high level security by encrypting the plain text along with masking along with efficient area, delay and power parameters, and also based on the masked design we have done the encryption anddecryption of images

REFERENCES

[1]Chou, Yuan-Hsi, and Shih-Lien L. Lu. "*A High Performance, Low Energy, Compact Masked 128-Bit AES in 22nm CMOS Technology*." 2019 International Symposium on VLSI Design, Automation and Test (VLSI-DAT). IEEE, 2019.

[2]Sunil, J., Suhas, H.S., Sumanth, B.K. and Santhameena,S.,2020, November. "*Implementation of AES Algorithm on FPGA and on software*". In 2020 IEEE International Conference for Innovation in Technology (INOCON) (pp. 1-4). IEEE.

[3]Kumar, T.M., Reddy, K.S., Rinaldi, S., Parameshachari, B.D. and Arunachalam, K., 2021. "*A low area high speed FPGA implementation of AES architecture for cryptography application*". Electronics, 10(16), p.2023.

[4]Khairallah, M., Chattopadhyay, A. and Peyrin, T., 2017, December. Looting the LUTs: "*FPGA optimization of AES and AES-like ciphers for authenticated encryption*". In International Conference on Cryptology in India (pp. 282-301). Springer, Cham.

[5]Bellizia, D., Bongiovanni, S., Monsurrò, P., Scotti, G., Trifiletti, A. and Trotta, F.B., 2018. "*Secure double rate registers as an RTL countermeasure against power analysis attacks"*. IEEE transactions on very large scale integration (vlsi) systems, 26(7), pp.1368- 1376.

[6]Regazzoni, F., Wang, Y. and Standaert, F.X., 2011. "FPGA *implementations of the AES masked against power analysis attacks*". Proceedings of COSADE, 2011, pp.56-66.

[7]D'souza, Flevina Jonese, and Dakshata Panchal. *"Advanced encryption standard (AES) security enhancement using hybrid approach*." 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE, 2017.

[8] Mandal, Akash Kumar, Chandra Parakash, and Archana Tiwari. "*Performance evaluation of cryptographic algorithms: DES and AES*." 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science. IEEE, 2012.

[9] Madhusudhan, K. N., and P. Sakthivel. "*Combining digital signature with local binary pattern-least significant bit steganography techniques for securing medical images*." Journal of Medical Imaging and Health Informatics 10.6 (2020): 1288-1293.

[10] Atikah, Nur, et al. "*AES-RC4 Encryption Technique to Improve File Security.*" 2019 Fourth International Conference on Informatics and Computing (ICIC). IEEE, 2019.

[11] Cirineo, Christian C., et al. "*MarkToLock: an image masking security application via insertion of invisible watermark using steganography and advanced encryption standard (AES) algorithm*." 2017 International Conference on Applied System Innovation (ICASI). IEEE, 2017.

[12] Mahalle, Vishwanath S., and Aniket K. Shahade. "*Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm*." 2014 International Conference on Power, Automation and Communication (INPAC). IEEE, 2014.