Highly Secure Advanced Encryption Standard Using Vedic Mathematics and Visual Cryptography

[1]Snehapriya M, [2]Manju Devi,
[1]Final year MTECH, [2]Professor and HOD,
[1]Dept of ECE,
[1]The Oxford College of Engineering, Bommanahalli, Bangalore, India

Abstract: Cryptography is a well known data security algorithm which is used till date. Cryptography is a science of converting message into unrecognizable form and provides resistance for stealing the information. Advanced encryption standard is a highly secure algorithm is widely used in network security and communication. The most commonly used encryption standard is AES. Even though this is the standard algorithm, hackers are able to break the algorithm and retrieving the hidden data. There are mainly four steps in AES, which include add-round key, sub-bytes, shift-rows, mix-columns. This paper mainly concentrates on mix-columns. Thus, we intend to develop highly secure encryption algorithm that combines AES with another form of encryption known as visual cryptography. And also perform multiplications involved in AES, vedic mathematics approach will be incorporated to increase the algorithm's efficiency with respect to area. The analysis and simulation is done using MATLAB, modelsim tools. This method of implementing AES using vedic-mathematics improves the performance in terms of speed, power and area.

IndexTerms **- cryptography, vedic mathematics, AES, visual cryptography.**

I. INTRODUCTION

In digital communication systems, the information is transmitted wirelessly and it should be secure. The cryptographic algorithms encrypt the data at the transmitter and decrypt the data at the receiver side. The advanced encryption standard is a subset of much larger encryption algorithm known as Rijndael. The cryptographic algorithms involves encrypting the data to be transmitted or shared by means of unique keys, for encryption and decryption, which are known only to the authorized parties, thereby ensuring data security. Several cryptographic algorithms have been discovered and researched upon in the recent times ,giving importance to the problem of vulnerability of the algorithms especially in applications which demand high security i.e. for smart cards, ATMs, WWW servers etc. Among these, the Advanced Encryption Standard (AES) algorithm is one of the highly preferred algorithms as it has higher immunity towards attacks. However, when considering the hardware implementation of the design, the AES is losing, since it involves several complex operations implemented in the Galois Field .Also, these complex operations are iterative in nature which in turn disturbs the speed of the encryption system and therefore increases the vulnerability. In this paper, an area efficient architecture for performing the various operations involved in the Advanced Encryption Standard (AES) method of cryptography is introduced.

Vedic mathematics is an archaic style of mathematics which subsisted in India in 1500 B.C, and was later on brought to limelight by a famous scholar Sri Bharathi Krishna Tirthaji between 1911 and 1918.He systemized it into 16 simple sutras, which are used by most of the researchers and mathematicians due to its ease of use. Out of the 16 formulae available in Vedic Mathematics, the Urdhwa Tiryakbhyam Sutra was utilized in order to address the flaws observed in the conventional mix columns architecture utilized in AES. Visual cryptography is one other technology which is included that increases the effectiveness of the AES algorithm.

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in specific a way that decryption becomes a mechanical operation that does not require a computer. The idea was about producing image shares of a given secret image in a way that the image shares appear meaningless. Recovery of the image can be done by superimposing specified number of share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is a little more advantageous for implementation, while compared to conventional cryptography schemes, since the decryption process does not need any computation. Further, the image based information becomes more secure, since only the intended recipient can reveal the true meaning of the decrypted image.

II. EXISTING SYSTEM

The AES is algorithm is a symmetric block cipher which has different block lengths and key lengths specified to be 128, 192, 256 bits. The AES parameters depend on the key length. The four different stages of AES are add round-key, substitution-bytes, shift-rows and mix-columns. A 4×4 matrix is known as a state array. Each byte in a state array is a component within a galoi's field 2^8. Depending on the size of the key, the number of rounds are 10, 12, 14 for 128, 192, 256 bits respectively. In every round all the four steps of AES are performed. The existing method depends on the look table approach.

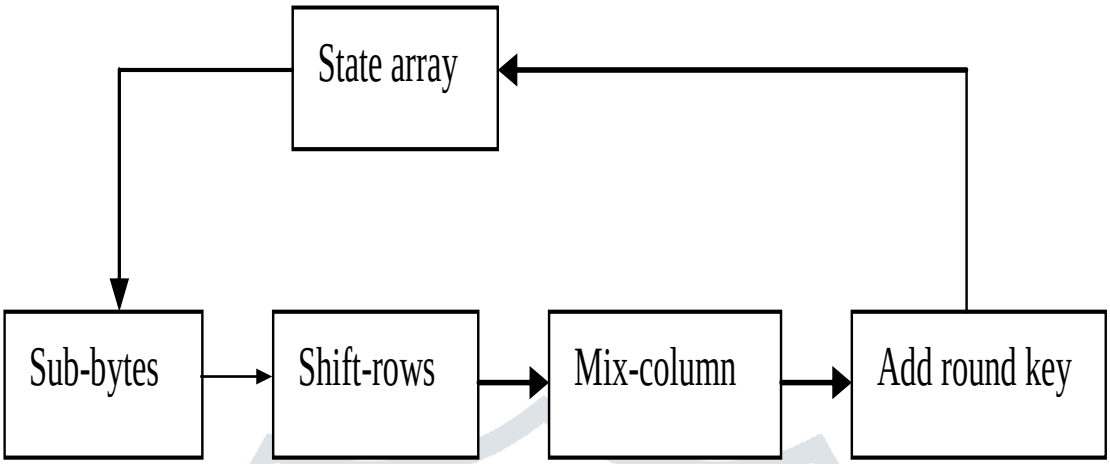

Fig 1: steps involved in AES

Each round of AES include

(1) ADD ROUND KEY

Add round-key step involves bit-XORing round key which is generated randomly with the state array matrix. This is performed by the key expansion algorithm.

(2) SUB-BYTES

The data obtained by the Add round-key is then modified by sub-byte transformation. This step uses a table of pre-defined value called S-BOX table. It performs byte by byte substitution of each byte of the state array matrix. The inverse of this step is performed at the decryption which uses Inverse S-BOX table.

(3) SHIFT-ROWS

It is cyclic shift of elements to the left by one position for the matrix obtained by the sub-bytes step. The first row elements remain the same as the sub-byte matrix. The shifting of elements is done row wise.

(4) MIX-COLUMNS

Mix-columns are implemented by performing matrix multiplication using galio's field i.e GF(2^8). For the mixed columns step to perform requires a pre-defined look up table for both encryption and decryption. All the 256 values has to be stored to perform multiplication. A state matrix for encryption and decryption are defined for mix-columns.

The state matrices are:

A= for encryption. B= for decryption.

In AES, the most critical and hardware-consuming transforms are MixColumn / inverse MixColumn and Sub- Byte / inverse SubByte, and our module includes the integration of all these transforms into one unit for both the encryption and decryption, while the remaining transforms are just involving the routing and logical XOR operation and, if we include them, will not have a significant impact on the performance of design.

In fig 2 the flow of different steps are included in AES are shown. First the input data is given in galoi's field. For the given numbers we take the values in 'L' table which is already predefined. Then the values are added and stored in other variable. If the answer exceeds the value 'FF' which is equal to 255 in decimal then answer must be subtracted with 255 until it reaches the value equal to less than 255. If the answer is less than 'FF' then it directly reads the values from the 'E' table.

Table 1 shows the number of rounds for different lengths of key and block lengths on which AES can perform.

Table 1: table for key and block lengths

Bit pattern	Key length(words)	Block length(words)	No. of rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

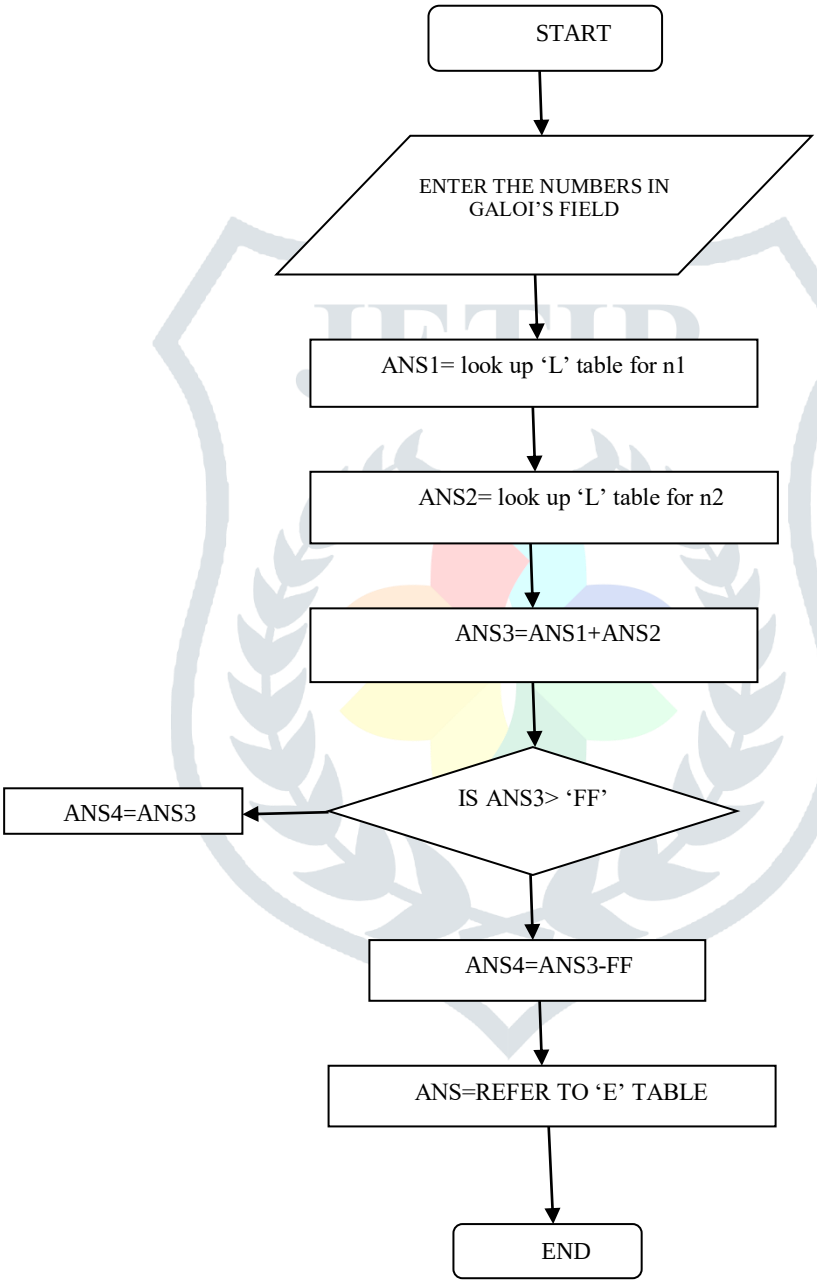

Fig 2: flow chart of existing system

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	4385	14752	29%
Number of 4 input LUTs	8688	29504	29%
Number of bonded IOBs	256	376	68%

Fig 3: the area used by the Look up table approach

This table shows the resultant area that is utilized by the 'look up table' approach. Almost 29% of the area is utilized by this approach. And other 29% is utilized by the 'LUT' which is look up table values. And 68% is utilized by the IOB's.

III. PROPOSED SYSTEM

Vedic mathematics is constructed with 16 sutras (formulae) and 16 Upa sutras (sub formulae) after extensive research in Atharva Veda. The very word „Veda" has the derivational meaning i.e. the fountainhead and illimitable storehouse of all knowledge. Vedic mathematics is the name given to the ancient system of mathematics or, to be precise a unique technique of calculations based on simple rules and principles with which many mathematical problems can be solved, be it arithmetic, algebra, geometry or trigonometry. The system is based on 16 Vedic sutras or aphorisms, which are actually word formulae describing natural ways of solving a whole range of mathematical problems. The beauty of Vedic mathematics lies in the fact that it reduces the otherwise cumbersome-looking calculations in conventional mathematics to a very simple one. This is so because the Vedic formulae are claimed to be based on the natural principles on which the human mind works. This is a very interesting field and presents some effective algorithms which can be applied to various branches of engineering such as computing and digital signal processing.

The proposed Vedic multiplier is based on the "Urdhva Tiryagbhyam" sutra (algorithm). These Sutras have been traditionally used for the multiplication of two numbers in the decimal number system. In this It is based on a novel concept through which the generation of all partial products can be done with the concurrent addition of these partial products. The algorithm can be generalized for n x n bit number. Since the partial products and their sums are calculated in parallel and the multiplier is independent of the clock frequency of the processor. Due to its regular structure, it can be easily layout in microprocessors and designers can easily circumvent these problems to avoid catastrophic device failures. The processing power of multiplier can easily be increased by increasing the input and output data bus widths since it has a quite a regular structure. Due to its regular structure, it can be easily layout in a silicon chip. The Multiplier based on this sutra has the advantage that as the number of bits increases, gate delay and area increases very slowly as compared to other conventional multipliers.

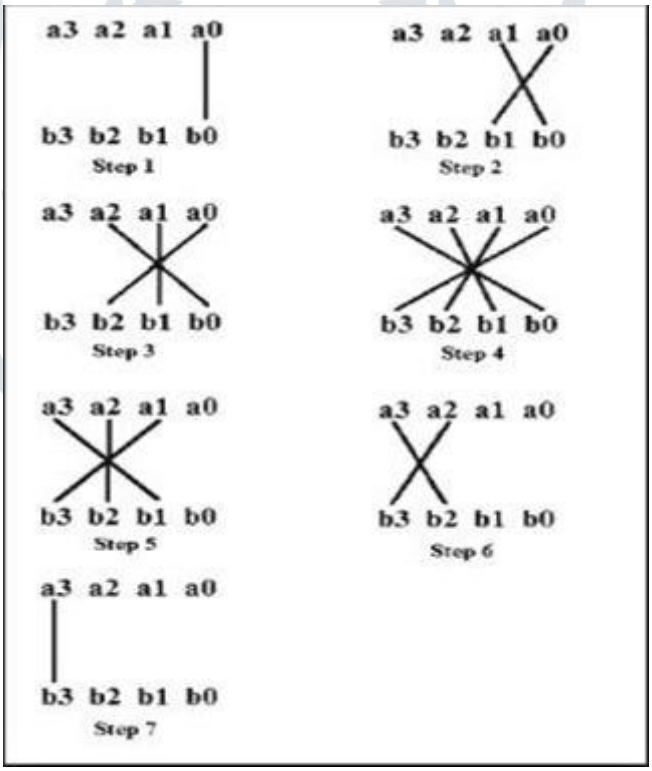

Fig 4: steps of vedic mathematics

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	25	14752	0%
Number of 4 input LUTs	43	29504	0%
Number of bonded IOBs	32	376	8%

Fig 5: area utilized by vedic mathematics

Fig 5 shows the area utilization result obtained from ISE XILINX tool. From 'vedic mathematics' approach the area utilized is almost reduced when compared to that of 'look up table' approach. The area used us very minimal and hence it is shown as 0%. From about 14752 slices only 25 slices are used. Hence this proposed approach is comparable faster

and reduces the amount of area consumed. Hence the proposed system is better compared to the existing system. The time delay of the existing system is 18.87 ns and the time delay of the proposed system is 7.160 ns.

IV. VISUAL CRYPTOGRAPHY

Visual cryptography is a technique used for data hiding in wireless networks. The user input data is encrypted, and is divided into N no.of shares. Then these shares are decrypted at the receiver end. The user name and the passwords at the encryption side are converted into images which are predefined by the developer. These image formats are only known by the developer and cannot be known to the hackers.

SHARE ENCRYPTION:

To encrypt the shares, the input is considered as a share. Hence, the shares are taken that is converted into block matrices. During the encryption process, the shares are undergone to the basic AES procedure and the output is the encrypted share. In this process, the shares and AES algorithm binds together to give the resultant shares which are called as encapsulated shares.

SHARE DECRYPTION:

Figures which are created during the encryption process all are decrypted and stacked together to retrieve the secret data. If any one of the share of the original image is missing, it is impossible to retrieve the original text or image. In the decryption, the pixel array is computed from the reconstructed image and xor with the same key used in encryption. Decrypted image is exactly equal to the original image or the text remains the same as that of the encryption.

V. EXPERIMENTAL REULTS

Results of proposed vedic mathematics approach

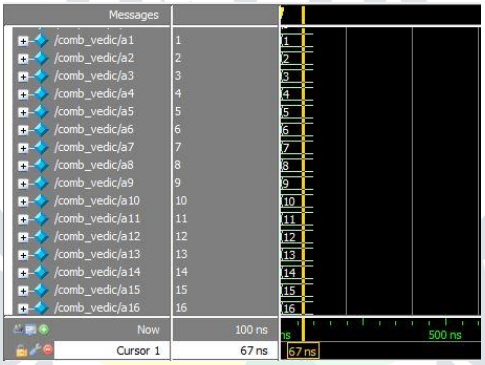

Fig 5: input waveform

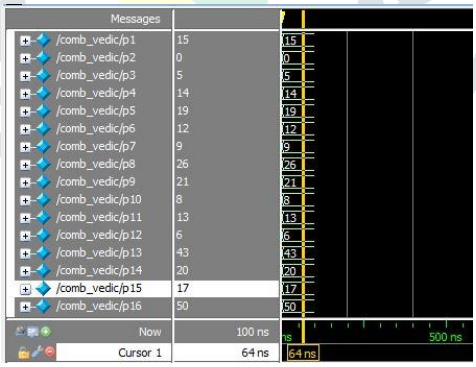

Fig 6: output waveform

Results of visual cryptography

Images of User name: sn

Password is: pr

Fig 7: S

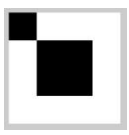

Fig 8: N

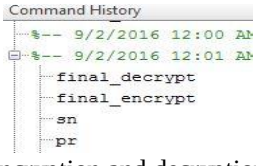

Fig 9: Encryption and decryption results

CONCLUSION

In this paper encryption is performed using 128 bit key with the use of vedic mathematics. This network security algorithm has wide applications in communication security. The code can be optimized for efficient area and time consumption parameters and used for high end applications.

REFERENCES

[1] Nidhi Gaur, Anu Mehra, SPIN, IEEE 2018, Enhanced AES architecture using extended set ALU at 28nm FPGA, International conference on signal processing and integrated networks.

[2] Sheetal U Jonwal, Prathibha P Shingare, IEEE, 2017, Advanced encryption standard implementation on FPGA with hardware in loop, International conference on trends in electronics and informatics, ICEI.

[3] Sonam Negi, Satendra Kumar Chauhan, 2018, Implementation of AES employing systolic array and pipeling approach, IEEE.

[4] Ambika R, C S Mala, Nov 2013, FPGA implementation of AES using vedic mathematics" International journal of innovative research in science and engineering, IJIRSE.

[5] Soumya Sadanandan, Anjali V, July 2014, Design and implementation of advanced encryption standard using vedic mathematics, Internation journal of innovative research in advanced engineering, vol-1,issue-6.

[6] Amit Kumar, Manoj Kumar, 2017, "Implementation of AES algorithm using VHDL", International conference on computing methodologies, ICCMC, preceedings of IEEE.

[7] S.R. Rupanagudi et al, 2016, A novel and highly secure encryption methodology using a combination of AES and visual cryptography, ICACCI.