*IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*
*Volume 10, Issue 4, Ser. I (Jul. - Aug. 2020), PP 08-19*
*e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197*
*www.iosrjournals.org*

# Review on Image Encryption/Decryption using AES Algorithm for Hardware Accelerator Design and Implementation

Deeksha P[1], Suchitra M[2], Mokshith B[3], Sharath Kumar K[4], Ayaz Jaffar[5]
[1 3 4 5](UG Student, Department of Electronics and communication, Vidyavardhaka College of Engineering, India)
[2](Associate Professor, Department of Electronics and communication, Vidyavardhaka College of Engineering,India)

***Abstract:*** *In the growing information era, information distribution and transferal has amplified exponentially. Images extremely donate to communication during this age of the multimedia. Safety, integrity, privacy, and verification services are the most significant factors in information security. Encryption is a method used to preserve image privacy. This paper presents a comprehensive study of various techniques for image encryption. The existing technology is analyzed with respect to algorithm, type of implementation, memory management, and mathematical computations. The main aim of this paper is to obtain a hybrid solution for the existing drawbacks and develop an enhanced system for image encryption and decryption. Many researchers' developments on improvingalgorithm's performance are reviewed in this paper. The proposed system in this paper focuses on design of hardware accelerator by using Cadence tools.*

***Keywords:*** *Algorithm, Cryptography, Decryption, Encryption, Image, Information Security, Public key, Simulation*

---

Date of Submission: 12-08-2020 Date of Acceptance: 28-08-2020

---

## I. Introduction

An accumulative expanse of data is transferred in the web, counting not just text but along with it audio, software files and image. Images are broadly used in day-to-day life, and, as an outcome, the safety of image information is a significant condition [1]. When either communication bandwidth or storing is restricted, information are often compacted. In specific, when a wireless communication system is working, low-bit-rate compression algorithms are needed as outcomes of bandwidth limits. The major resolution of cryptography is to make definite confidentiality, truthfulness and convenience through the appliance of encryption methods [2]. Basically, it comprises design of procedures based on the grounds of mathematics, electricaland computer science engineering domain to encode as well as decrypt the data in the form of information and images. However, maximum encryption approaches need hardware based visual arrangements and include complicated mathematical processes. The efficiency and performance parameters are mapped. The paper concludes by presenting a comparative study of all existing techniques for image encryption and highlighting further challenges. The best results have been extracted for a better design in this paper. Cryptography is normally classified into two inclusive groups: symmetric key encryption and asymmetric key encryption. The former group, symmetric key encryptioncustoms the similar key at both the source as well as destination. The latter group, asymmetric key encryption uses dissimilar keys at both the source anddestination. Through the utilization of an algorithm, image is formed into meaningless cipher text and requires the utilization of a key to rework the info back to its original form. In this paper, the complete flow of encryption is divided into the elements and characteristics of encryption technique based on:

i. Algorithm
ii. Implementation
iii. Mathematical Computation
iv. Encryption techniques

The literature survey of various existing methodologies and characteristics for image encryption developed by Researchers have been studied in this paper. The main goal for developing an ASIC is to focus on 3 major parameters- Area, Power, and Time. The RTL simulation results are discussed and verified in this paper. The flow of ASIC design is proposed from RTL to GDSII.

## II. Literature Review

Based on the encryption algorithm, the speed and time taken for encryption varies. There are many algorithms which differ from each other they are listed in this paper.

**Based on Algorithm**

1. Rivest-Shamir-Adleman (RSA): RSA algorithm was designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. The authors' [3] represented their work in paper. RSA algorithm is used as a tool for encoding the information and also an additional coating of safety to the whole encryption procedure that has been applied. Image encryption approach for data verification by means of FTM (Fourier Transform Method) grounded phase recovery algorithm and RSA open key method. The effectiveness of the projected method against possible outbreaks is also analyzed Also in the paper reviewed by the author [4] similar work is carried out using RSA algorithm. The challenge faced here is to optimize the speed and time. Security level is observed to be less because the encryption used here is asymmetric type. Since this algorithm uses greater than 1024 bits key length it consumes greater power and it's a comparatively slower process. Hence mathematical modifications are carried out to meet the speed and time constraints. RSA algorithm has its own flaws as observed by the author therefore it's not preferred for commercial use.

2. Data Encryption Standard (DES):DES is utmost extensively accepted. It was developed by IBM in 1980s and later it was adopted by National Institute of Standards and Technology (NIST). The key length used for encryption in DES algorithm is 56 bits. The key size being too small with a cipher block size of 64 bits. The power utilization is quite lesser. Brute forces can be attacked; hence it has issues with the security. The DES algorithm was modified and obtained new algorithms as stated.

3. Triple DES:Another algorithm adapted from DES algorithm is Triple DES, which uses 3 keys simultaneously. Key 1 is used to encrypt for first time, key 2 is used to decrypt and key 3 is used to encrypt for second time. The key length is more. The attacks are minimized. As discussed by the author in paper [6] they have used Triple DES algorithm as encryption algorithm. In the paper the author first converts image into bytes which are then converted to bits. The triple DES algorithm outstands in security as it uses 3 keys instead of 2. But time will be increased for triple DES process. It provides better quality but reflects to be poor in performance. Multimedia data video and audio files cannot be processed.

4. Simplified Data Encryption Standard (S-DES):The S-DES is a simplified algorithm than DES algorithm. It uses symmetric key algorithm which supports multimedia files, texts, images etc. In the paper [5] authors have used S-DES algorithm for enhanced encryption technique. In this paper the procedure used is position scrambling which scrambles the plain text obtained with current cryptanalytic methods like differential, linear and linear-differential cryptanalysis. In this type of encryption/decryption similar key is used. It was observed that it's hard to implement both in relations of safety and effectiveness. Only either of the parameter can be optimized.

5. Chaos Technique:Chaotic technique is highly optimized encryption algorithm which uses two techniques i.e. substitution and permutation methods. The author in the paper [7] reviewed that the algorithm uses a set of chaotic system. One was to create chaotic order that was then, with the aid of a verge function, converted to a binary symbol. The further was to construct the permutation matrix. Encryption is carried out by using these two systems. The author reflects a new process of encryption by means of creating binary stream for key input, arbitrarily modifying the image pixel standards. Then by using permutation matrix the modified image was encrypted.

6. Block Based Transformation:Block based image encryption technique is a unique type of encryption algorithm of dividing the image into blocks and encrypts the data using a well-known encryption algorithm. The authors in paper [8] produce an algorithm with enhanced level of security by diving the whole image into parts and then encrypting each part separately. The authors explain it to be a mixture of image alteration and encryption using existing algorithm. The algorithm used by the authors in this paper is Blowfish encryption algorithm. Creating the sub-blocks from the whole image, with the help of transformation hence rearrangement takes place. On each rearranged block the Blowfish algorithm is used for encryption. In this paper the authors obtained results which presented that the correlation parameter among image elements was found to be reducing. Observation made by authors reflected that the increase in blocks number with blocks of smaller sizes which caused greater entropy and reduced correlation. Author also observed that the level of security obtained was relatively higher.

7. RC4:It is an encryption stream, which means that each digit or character is encrypted one at a time. A cipher is a message that has been encoded. In the paper [9] the author have propounded that the algorithm used relies on RC4 and Chaotic logic map. There are 3 stages involved; in the initial stage external key is converted into early value by the system. In the following stage for producing the pseudo random number the early value is applied to the chaotic
map. Later, in the final stage system brings out XOR operation between the pseudo random number and plain image. This process is a symmetric type of algorithm. The author analysis the algorithm and the results generated by using this algorithm. Observation was made that it was an easy encryption algorithm with fast computer implementations. The outstanding factor that author witnessed was using this algorithm optimized the time. The speed of processing was very fast and the speed did not depend upon the key size.

**Based on Transforms**

1. Fourier Transforms: A new technique based on the type of transform was presented by Ran Tao et al, by means of a multi-order Fourier transform. The encoded image was gained from outline diverse instructions of the Opposite Distinct Fourier Transform (IDFR FT) the inserted sub-image. Technique involved a superior key and the number of keys would be set larger than twice the quantity of the pixels in the unique image. The author combined the planned technique with additional image encryption approaches to improve the safety of the system in the paper [10]. An image encryption procedure was suggested based on the fractional Fourier transform. The information at the inhabited part of the multifaceted purpose is enhanced.

2. Wavelet Transform:Chaos-Based image encryption algorithm using Wavelet Transform was proposed by Zhu Yu et al .The algorithm habits the wavelet breakdown focused and the image information in the sub-band high frequency and later it is encrypted in functional for that generated sub-band image. Then the image is encoded to feast part throughout the whole image and it is represented by a wavelet. An additional encoding procedure is implemented to complete the encryption procedure. The author has described the same process in the paper [11]. The author also highlights the theoretic study and tentative results that this procedure has a clear increase in efficiency as well as fulfilled safety.

**Implementation Techniques**

1. FPGA Implementation: The authors describe an image encryption and decryption algorithm applied AES 128-bit core in the paper [12]. In this process the image info was transformed into a hexadecimal arrangement and the plain hexadecimal generated information for encryption was transferred to FPGA through UART. The synthesis and simulation was carried out via Spartan-3E FPGA which uses Xilinx ISE. As observed by the authors, the experimental observations were made and compared in terms of area, power, and time. The author clearly represented a quantitative analysis of these three parameters in the paper. Similar work was carried out for decryption. FPGA is general purpose hence using a FPGA based technique is costlier as it involves many verification stages involved.

2. Realization using MATLAB:MATLAB is a multi-paradigm mathematical calculating environment and branded language advanced by Math Works. There is also a need for partial image encryption during image encryption so that the execution time is decreased and thus efficiency improves. This form of partial image encryption can be done using Selective image encryption technique introduced by the authors in paper [13]. This main aim was to propose a study and execution of Discriminating image encryption technique by using MATLAB. The authors focused on controlling the computational time and computational resources. The core idea was chosen because of software implementation using MATLAB which required more number of cycles for processing the image.

**Image Encryption Techniques**

1. Permutation Technique:The author presented an algorithm such as permutation of random pixels. The values used in encryption are preserved in the form of the 64-bit key. The author's incentive was to maintain the feature of the image [14]. This scheme involved three phases of encryption. The first phase included splitting of an image into blocks then the block of images was permuted. In the second stage, the key is generated by values used in the encryption process. And the third stage of the numbering of shares is done that is generated from a secret image. The author analyzed the technique and found that it provided confidentiality two-color image with fewer computations. This method was quoted as unique as it encrypts the image first then generates the key. But it's a time-consuming process as it involves more mathematical computation. The memory management was observed to be inefficient.

2. Steganography Technique:The author proposed effective steganographytechnique with hash-lsb (hash – least significant bit HLSB) along with rc4 algorithm also including shuffling algorithms for encrypting the pixels in

paper [16]. With the help of hash-lsbby using hash function which cultivates a method to introduce RGB pixels data bits of the cover image in the LSB bits. Author analyzed the results which stated that greater resemblance existed among the cover image and the stego image. Similarly it was for furtive images and removed image. The author also stated that these algorithms can be realized by using MATLAB program.

3. Based on Bit-plane Decomposition and Random Scrambling:In the paper [15] the author modified the general method and proposed a new technique which had stable scrambling degree as compared to the traditional method Arnold transform. Initially the original image was decomposed into several bit-plane sub images. These sub images
were shuffled among themselves with the help of a random scrambling algorithm. Followed by this the scrambled sub images were merged with initial levels of bit planes. Hence an encrypted image was obtained. Since each bit is scrambled with a random scrambling sequence the position after the encryption of the sub image bits might not be the same coordinates as that of the original sub image bit plane position. Both position and grey level scrambling can be carried out at a time this was reflected by the author.

4. Compression Friendly Encryption Scheme (CFES):The authors in this paper [17] had deeply witnessed the algorithms and clearly gave a comparison between two encryption procedures i.e. Compression Friendly Encryption Scheme (CFES) and Advanced Encryption Standard (AES) The authors studied and estimated the AES algorithm along with CFES for digital images and also their safeguard against brute-forces, and other attacks. Authors observed that the weaknesses by using this technique were connected to little entropy and flat association, the authors have also mentioned that the image obtained after encryption by using CFES had an association in the straight direction and AES encrypted image had lesser connection in all the directions. It was observed that the algorithm with fewer correlation values indicates higher security.

5. Based on Bitwise Operation:This paper uses a secured symmetric scheme for image encryption. The authors in the paper [18] proposed a secure technique for encryption of numerical images; it is valid for any digital file. The bitwise XOR and fluctuating process were performed to encrypt a block of secret bytes and then shuffling occurs with the size of secret key places i.e. referred to as N places. The key for encryption is very large providing security against spells such as brute-force attack. The authors analyzed on the basis of, arithmetical study and differential attack study also on key sensitivity analysis, which proves high acceptability of the suggested algorithm.

6. Using Relative Displacement (RDC) and Dynamic Base Transformation (DBTC):The authors focused on a different technique of encryption which did not include a predefined key [19]. The input image was split up into parts, each part coded with a dissimilar algorithm. To obtain higher level of security the key was generated by using two firm keys. The significant piece of this algorithm was that, each part was operated with the help of conversion at the base, the second sub part of image was distorted with the switching place and the amount of recurrences are increased, and in residual fundamentals, modest operation were performed. Hence, this algorithm was complex blend without any complex design.

7. Stream Encryption Scheme:The stream encryption scheme was based on infinite key generation; it helps in encrypting one bit or byte one at a time. The author in the paper used this type of scheme because of its low memory requirement making it as more advantageous for encryption technique. In the paper [20] the technique used a 2D chaotic map was generalized to 3D for a real-time symmetric encryption which was based on 3D chaotic map. First shuffling of image pixel positions occur the another chaotic map is used to confused the connection of cipher images hence the author observed that resistance against attacks was increased. A gray-level encryption technique based on exclusive (XOR) operation along with an encoding method was implemented by the author [21]. Initially slicing of gray-level image occurs by forming binary images then encryption takes place by using XOR operation with a binary random image. . The authors combined the XORed image and binary random image into an encrypted image and a key image. Using this scheme produced gray-level encrypted data with key data during a space domain.

8. Block Encryption Scheme:The encryption scheme used involves breaking up of plain text tofixed length blocks. At a time only one block encryption occurs. The key feature of this scheme was it provided integrity protection along with confidentiality. Chaotic maps are used to transform these blocks. In this paper[22] the author suggested a chaotic block cipher scheme for image encryption systems that encrypts bits instead of pixel fragments. According to the proposed scheme plain-image was encrypted into a cipher-image with eight registers of 32-bits. Author observed that primitive operations with a non-linear transformation were applied for encryption, which produced a more competent chaotic system.

**Image Type**

1. Windows Bitmap (BMP):The bitmap is a file format of an image with pixel value of 8 bits. The number of bits maybe 16 or 32, it is dependent on the applications. A gray scale image was decomposed to form eight binary layers of image. The bitmap format is dependent on only two parameters i.e. information content and the number of pixels. Author in the paper [23] uses this type of image file format while working with AES algorithm novel based encryption. The AES algorithm is operated with the Feedback mode. While transmitting the image, a problem arose regarding the size of the image or resolution; in this case compression of images occurs.

2. Color Image Protecting:In order to protect digital color image's information, a color image encryption algorithm built on Lorenz chaos sequence and its decryption technique defensive from shearing attack was presented by the authors in paper [24]. Firstly, 3D Lorenz chaotic sequences are improved to be with ideal pseudo-randomness. Then, the RGB components image's pixel positions are shifted and the pixel value was altered based on the 3D sequence so that the image will be scrambled and encrypted. While doing the decryption, a method was provided depending on the neighboring pixels' values. The experimental result indicated that algorithm had a good efficiency and is safer..

## III. Proposed System

After surveying the existing systems we choose a hybrid solution in terms of algorithm and implementation technique. We choose to design a hardware accelerator for Image Encryption and Decryption using AES Algorithm, the reason we opted for AES Algorithm is because it meets our main constraints such as Time and Power. As we have reviewed the papers based on algorithms, RSA[3] has the highest security where it uses 512 bits key length but the computational cycle is more compared to AES Algorithm so it consumes more time. Similarly with DES algorithm it is considered to be mitigating the issue of increasing execution time but the major drawback is its security. It is easily attacked by brute forces. While considering the power the software implementation in FPGA using MATLAB consumes more power for simulation and also time consuming as it involves more number of computational cycles where in Hardware implementation power consumption is very less. The AES algorithm encrypts the data into 128-bit fragments. Three key sizes are used, 128 bits, 192 bits and 256 bits, respectively, in three variants, with three separate Nr rounds 10, 12 and 14 depending on the application for which we design the system. As we are designing our system for commercial use the key size is 128 bits with 10 rounds. There are 9 rounds of SubBytes, ShiftRows, MixColumns followed by AddRoundKeys transformations with an initial Roundkey addition transformation. No transformation of MixColumns occurs in the last round (10th round).The design optimization has been done by considering the main three parameters that are Area, Power and Time. In our system, we have considered power and time as major factor to optimize by skewing down area parameter while designing of ASIC for image encryption/ decryption.

**The Proposed Design Flow**

The flow of the VLSI design from RTL to logic synthesis then Physical layout generation and finally GDSII stream out stage is shown in Figure.1. The RTL stage consists of blocks for performing encryption/decryption written in Verilog code. The behavior and design function are defined in Hardware Description Language (HDL) form during this stage. The RTL consists of main block for AES core and four sub-blocks for performing AES operation which consists of s-box implementation, shiftrows, mixcolumns and addround keys. All these sub-blocks are instantiated in the main block. Next stage being logic synthesis, it is a method of translating the verilog codes of RTL into optimized netlist generation at gate-level.Verification of generated netlist is carried out. Physical design is a stage where the translation of the configured netlist at the gate-level into a graphical representation of the specification known as layout is carried out. Before streaming out the GDSII file for fabrication various verifications are carried out at each step including RTL verification, Logic gate level netlist verification and layout verification. GSDII file is binary format of file containing cell geometry and cell references parameters. Graphical Database System (GDSII) file contains all named documents, cell geometric shapes and other information about the model.

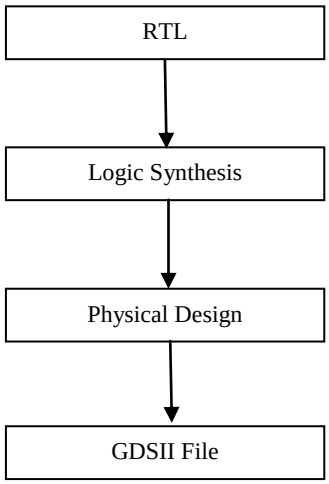


**Figure.1.** Proposed Design Flow

## IV. AES Algorithm Architecture

**Subbytes/Inverse Subbytes Transformation**

SubBytes and the Inverse SubBytesare the first transformation block in the Encryption and Decryption respectively. The SubBytes substitution is a nonlinear byte Substitution operating separately for every byte of a State.To perform SubByte transformation, take the multiplicative inverse in the finite field GF (28) and affine transform. For Decryption Inverse SubByte is performed by finding Inverse affine transform and then multiplicative inverse of that byte.

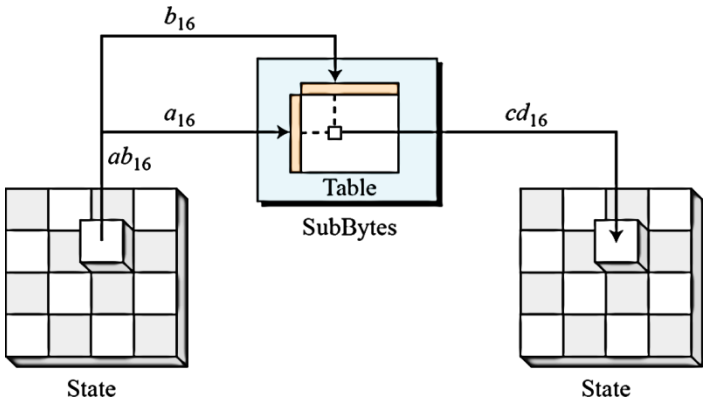


**Figure.2.** SubBytes Transformation

Figure.2 illustrates how to handle the change. There are two hexadecimal digits a and b in first order, the row is represented by the left digit (a) and the column is represented by the the right digit (b) of the substitution table. Such two digits are the intersection of new bytes.

Similarly, transformation of Inverse SubBytes is the reverse of transformation of SubBytes, however the table used to map the byte is distinct. Substitution can be achieved by using table S-BOX or using the arithmetic composite field. There are two separate tables for SubBytes and the inverse SubBytes; Table 1 is used for regeneration of SubBytes and Table 2 is used in inverse.

**Table.1.** SubBytes Transformation Table

| | | b | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| a | 0 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| | 1 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| | 2 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| | 3 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| | 4 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| | 5 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| | 6 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| | 7 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| | 8 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| | 9 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| | a | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| | b | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| | c | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| | d | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| | e | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| | f | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

SubBytes table is termed as S-box and inverse SubBytes table is termed as Inverse S-box. There are two components of the affine transformation and its reverse; a fixed matrix is multiplied in the multiplication component with the data and then a constant vector is added to the additional part resulting in multiplication.

**Table.2.** Inverse SubBytes Transformation Table

| | | b | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| a | 0 | 52 | 09 | 6a | d5 | 30 | 36 | a5 | 38 | bf | 40 | a3 | 9e | 81 | f3 | d7 | fb |
| | 1 | 7c | e3 | 39 | 82 | 9b | 2f | ff | 87 | 34 | 8e | 43 | 44 | c4 | de | e9 | cb |
| | 2 | 54 | 7b | 94 | 32 | a6 | c2 | 23 | 3d | ee | 4c | 95 | 0b | 42 | fa | c3 | 4e |
| | 3 | 08 | 2e | a1 | 66 | 28 | d9 | 24 | b2 | 76 | 5b | a2 | 49 | 6d | 8b | d1 | 25 |
| | 4 | 72 | f8 | f6 | 64 | 86 | 68 | 98 | 16 | d4 | a4 | 5c | cc | 5d | 65 | b6 | 92 |
| | 5 | 6c | 70 | 48 | 50 | fd | ed | b9 | da | 5e | 15 | 46 | 57 | a7 | 8d | 9d | 84 |
| | 6 | 90 | d8 | ab | 00 | 8c | bc | d3 | 0a | f7 | e4 | 58 | 05 | b8 | b3 | 45 | 06 |
| | 7 | d0 | 2c | 1e | 8f | ca | 3f | 0f | 02 | c1 | af | bd | 03 | 01 | 13 | 8a | 6b |
| | 8 | 3a | 91 | 11 | 41 | 4f | 67 | dc | ea | 97 | f2 | cf | ce | f0 | b4 | e6 | 73 |
| | 9 | 96 | ac | 74 | 22 | e7 | ad | 35 | 85 | e2 | f9 | 37 | e8 | 1c | 75 | df | 6e |
| | a | 47 | f1 | 1a | 71 | 1d | 29 | c5 | 89 | 6f | b7 | 62 | 0e | aa | 18 | be | 1b |
| | b | fc | 56 | 3e | 4b | c6 | d2 | 79 | 20 | 9a | db | c0 | fe | 78 | cd | 5a | f4 |
| | c | 1f | dd | a8 | 33 | 88 | 07 | c7 | 31 | b1 | 12 | 10 | 59 | 27 | 80 | ec | 5f |
| | d | 60 | 51 | 7f | a9 | 19 | b5 | 4a | 0d | 2d | e5 | 7a | 9f | 93 | c9 | 9c | ef |
| | e | a0 | e0 | 3b | 4d | ae | 2a | f5 | b0 | c8 | eb | bb | 3c | 83 | 53 | 99 | 61 |
| | f | 17 | 2b | 04 | 7e | ba | 77 | d6 | 26 | e1 | 69 | 14 | 63 | 55 | 21 | 0c | 7d |

**Shiftrows/Inverse Shiftrows Transformation**

This operation is the second transformation block for Encryption and Decryption respectively, in which each rows are shifted to the left in a cyclical manner. The count of shifting is determined by the number of rows in the state matrix. Initially the first row is ideal where there is no change, second row is shifted left by one byte, third row is shifted left by two bytes and fourth row is shifted left by three byte. Similarly in the decryption, InvShiftRows transformation is performed by right shifting the each row in a cyclic way and the number of shifting depends on the number of rows. Figure.3 shows the Cyclic ShiftRows transformation for AES algorithm.

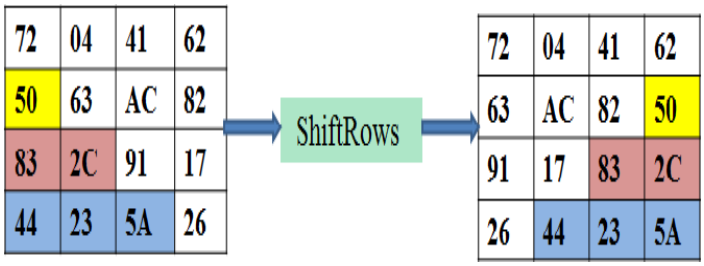


**Figure.3**.ShiftRows Transformation for AES Encryption

**Mixcolumns/Inverse Mixcolumns Transformation**

MixColumns transformation is used in the cycle of encryption, here each column is considered as a polynomial for four terms. Inverse MixColumns is the reverse process of MixColumns that is used for cipher text in decryption. The columns are deemed as polynomials over GF (28) and multiplied modulus x4 + 1 with a fixed polynomial A (x), expressed in equation (1),

A(x) = {03} x3 + {01} x2 + {01} x + {02}.(1)

Multiplication and addition in GF (28) is involved in the algorithmforMixColumns and Inverse MixColumns. The MixColumns multiplies the column of the state by row in a constant matrix and the resulted column is replaced in the original state. Figure.4 describes the operation of this transformation.

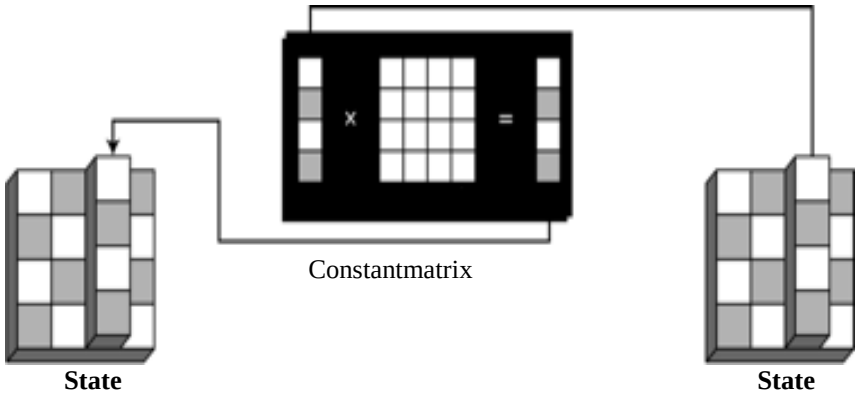


**Figure.4**. MixColumns transformation of AES Encryption

**AddRoundKey Transformation**

The AddRoundKey adds every column of the state matrix with the round key word. The AddRoundKey precedes one column at a time. In this transformation the cipher key will be included. Thefinal state matrix as shown in Figure.5 will be generated by doing XOR operation among column of the Stateand the key matrix which is generated by key generator.

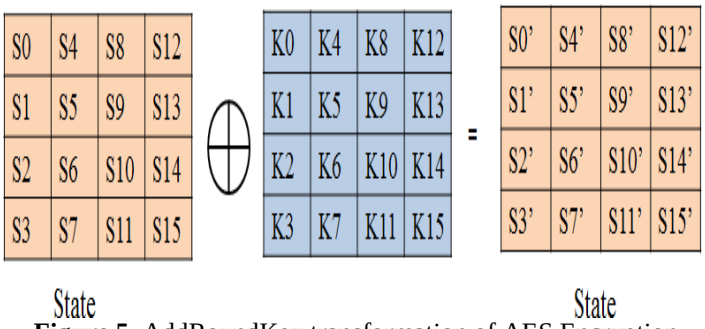


**Figure.5.** AddRoundKey transformation of AES Encryption

**Key Expansion**

The procedure for obtaining all Round Keys from the original input key is defined by the key expansion. In the encryption the original keys are the initial round key and in the decryption the original keys will be the last group generated by the key expansion. Before the iterations start encryption or decryption the inputs are added with the initial round key. The key size is 128 bits, the size of the round keys will be 16 bits which consists of 10 groups. The round keys are generated word by word. Round key can be generated by using some similar encryption transformations.

**Galois Field**

In cryptography, the Galois field (GF) or Finite Field with a finite number of elements is commonly used. Field order is defined as the total number of elements that are present in GF. A GF is of the form $p^n$, where n is a positive integer and p is a prime number sometimes called the Galois field characteristic.

Between them there are plenty of cryptographic algorithms that use GF, the one that uses the GF ($2^8$) by AES algorithm. A polynomial representation of GF ($2^8$) is used to represent the data Byte. In Equation 2, the polynomial representation of data bytes in Finite Fields is shown,

$a(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0$ (2)

In Galois field Arithmetic operation varies entirely from standard arithmetic algebra;, modulo is the multiplication product of polynomials. The polynomial that can't be factorized by two or more is called irreducible polynomial, bit-wise XOR operation can be found with an addition.

Based on the Galois Field following operations including addition, multiplication and multiplicative inverse are performed. These operations are used at each encryption transformation stages in AES algorithm.

1. Finite Field Addition

The finite field addition elements is accomplished by using the coefficient values of the polynomial representation for corresponding powers, this addition is performed in Galois Field GF ($2^8$), i.e. Modulo 2, so that 1 + 1 = 0. Subsequently, both addition and subtraction operation on bytes representing field elements are identical to an Exclusive-OR (XOR) operation.

Polynomial:(x6 +x4 +x+1)+(x7 +x6 +x3 +x)=x7 +x4 +x3 +1
Binary: {01010011} + {11001010} = {10011001}
Hexadecimal: {53} + {CA} = {99}

2. Finite Field Multiplication

The finite field Multiplication is a complex polynomial of reduction which defines the finite field in module multiplication. (I.e., multiplication followed by division using the polynomial reduction as the divisor — the rest is the product.) The "•" symbol can be used to denote multiplication in a finite field.

3. Multiplicative Inverse

In mathematics, the multiplicative inversion of a number (a) is the number that yields 1 or (a · x) = 1 when multiplied by x.

## V. Design Methodology of AES Algorithm

In AES algorithm there are two architecture designs,
i. AES Encryption Algorithm
ii. AES Decryption Algorithm

**AES Encryption Algorithm Architecture**

Using this design, cipher text is constructed from plain text. The AES algorithm is a block cipher with a private key. It encrypts 128 bits of block size data. It uses three main sizes, in three variants, 128 bits, 192 bits, and 256 bits. AES uses three separate round operation types, i.e. 10,12 and 14 respectively, but the final round key is 128 bits in each version. Figure.6 shows AES block diagram.

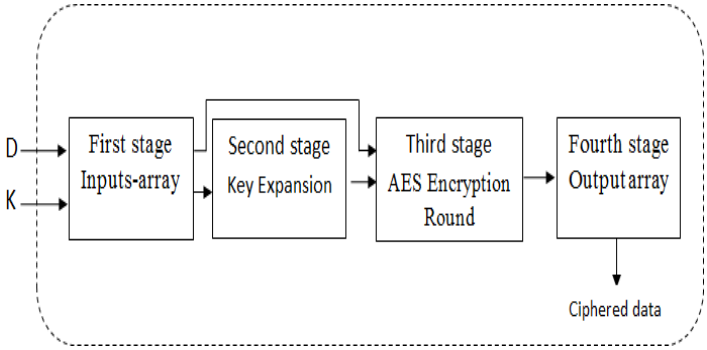


**Figure.6.** AES Encryption block diagram

In the first stage 128 bit data is entered and 128 bit key was also entered, in the second stage 128 bit key array is obtained from the first stage and this key array is modified to create new keys to be used in the AES Encryption rounds. In the third stage state array is received from the first stage and the key array.In the fourth stage the cipher text is created from the state array, consisting of 128 rows each rows consists of1-bit.

**AES Decryption Algorithm Architecture**

This design used the cipher text to retrieve the plain text. The AES algorithm is a block cipher with a private key. This decrypts 128 bits of block size cipher text. Figure.7 shows AES Decryption Block Diagram

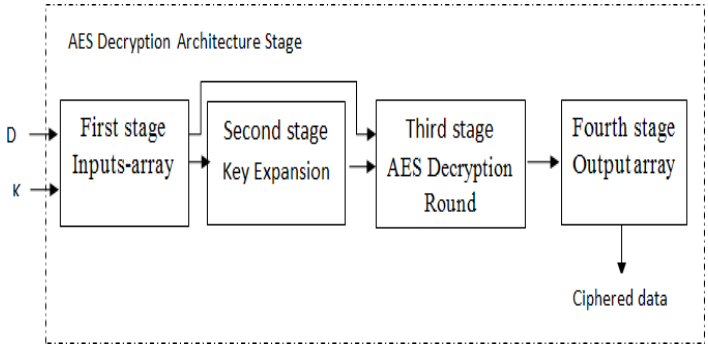


**Figure.7**. AES Decryption block diagram

Following the block diagram, first stage input array reads a 128 bit data which forms an array called as state array. The state array reflects the cipher-text that the original data is being processed to obtain.

**VerilogImplementation**

Verilog HDL is a standard language for hardware classification by IEEE. This is broadly adopted in the design of integrated digital circuits. Verilog is intended for use in simulation verification, timing analysis, test analysis and logic synthesis. Verilog HDL enables developers to design atvariouslevelsofabstractionlikeregistertransferlevel,gate level and switch level. Verilog is used as an input for synthesis programs that will produce a summary of the gate level for the circuit. We use the Cadence Genus tool to run the Verilog code and we receive the different reports regarding the required area, power, time and number of gates.

**Simulation results using Cadence nclaunch**

The RTL code is simulated by using Cadence nclaunch which produces waveform for the inputs, outputs and other ports individually for encryption and decryption. These values generated from the waveform in hexadecimal values are verified using the online AES calculator which ensures that the result obtaining using the waveform is correct. This verification of RTL is very important as it allows us to know the correctness of the RTL code generated for encryption and decryption.

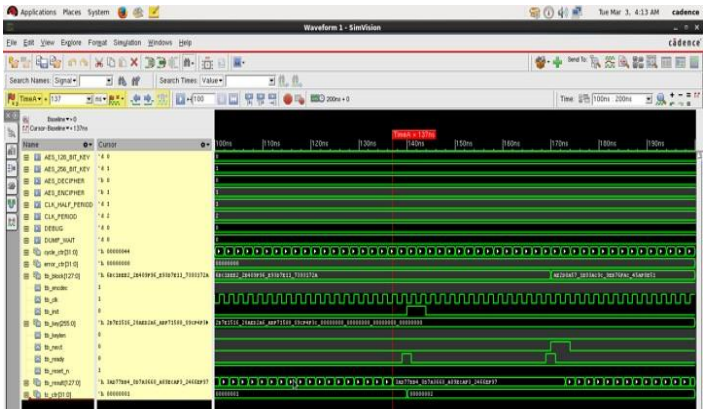

**Figure.8** Simulation Result of Encryption

Figure.8 shows the simulation result of Encryption using nclaunch for AES-128 bit by considering the following inputs.

Plain Text –6BC1BEE22E409F96E93D7E117393172A

Key Input – 2B7E151628AED2A6ABF7158809CF473C

The obtained Encrypted output is as shown below.

Cipher Text – 3AD77BB40D7A3660A89ECAF32466EF97

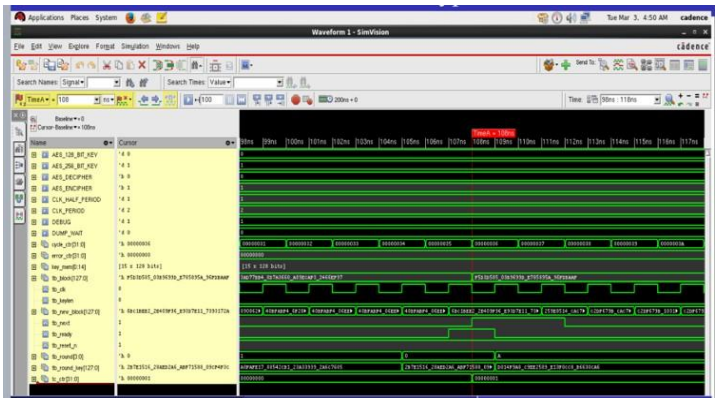

**Figure.9** Simulation Result of Decryption

Figure.9 shows the simulation result of Decryption using nclaunch for AES-128 bit by considering the following inputs.
Cipher Text – 3AD77BB40D7A3660A89ECAF32466EF97
Key Input – 2B7E151628AED2A6ABF7158809CF473CThe obtained Decrypted output is as shown below.
Plain Text – 6BC1BEE22E409F96E93D7E117393172A

## VI. Conclusion

In this paper, various important algorithms, image encryption techniques, different encryption schemes, type of image used and various types of mathematical computations have been existing and examined in order to get acquainted with the other encryption algorithms used in encoding the image which has been transmitted over link. The major goals of meeting up with area, time and power constraints are checked with various algorithms and techniques individually as well as when combined together. Based on the application and optimization required we combine the methods and operate to get the desired results. In this paper we also review some of the latest encryption methods and suggest using the AES algorithm for encryption/decryption which is survey to be as fast in nature. Further implementations can be carried out by developing an ASIC for image encryption which reduces the computational cycles hence optimizes the time and speed. By choosing the best hybrid of algorithm and technique which is compatible with the technology used for ASIC development security level and performance can be enhanced. RTL code for image encryption and decryption is simulated by using Cadence nclaunch and is verified by using the online AES calculator, as the encrypted data is obtained in terms of hexadecimal value.

## References


[1]. AnkitaAgarwal, "Secret Key Encryption Algorithm Using Genetic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012
[2]. Mustafa Emad Hameed1,2, Masrullizam Mat Ibrahim1 , NurulfajarAbdManap1, "Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security", Journal of Telecommunication, Electronic and Computer Engineering, Jan 2018
[3]. AmitChatterjee, JitendraDhanotia, Vimal Bhatia, SantoshRana, ShashiPrakash, "Optical Image Encryption using Fringe Projection Profilometry, Fourier Fringe Analysis, and RSA Algorithm", 978-1-5386-4318-1/17/$31.00 ©2017 IEEE.
[4]. Shankha Mukherjee, Shankha Mukherjee, SouvikSinha, TamalMukhopadhyay, "A meticulous implementation of RSA Algorithm using MATLAB for Image Encryption", 978-1-5386-1703-8/17/$31.00 ©2017 IEEE.
[5]. SandeepSrivastava, Sanjay Kumar, "Image Encryption using Simplified Data Encryption Standard (S-DES)", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.2, October 2014.
[6]. Anup&Suchithra, "Image Encryption using Triple DES Algorithm", Imperial Journal of Interdisciplinary Reasearch (IJIR), Vol-3, Issue-5, 2017.
[7]. JianchengZou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number, "Proceeding of the IEEE Inter Symposium On Circuits and Systems, Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.
[8]. GuoshengGu ,Guoqiang Han, "An Enhanced Chaos Based Image Encryption Algorithm",
[9]. RiahUkurGinting, Rocky YefrenesDillak, "Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map" @2013 IEEE
[10]. N Singh, A Singh- Optics and Lasers in Engineering, "Optical image encryption using fractional Fourier transform and chaos", Elsevier 2008
[11]. Farnaz Arab, SalwaniMohdDaud, SitiZaitonHashim, "Discrete Wavelet Transform Domain Techniques" 2013 IEEE
[12]. M.P. Priyanka, E. Lakshmi Prasad, Dr. A. R. Reddy "Fpga Implementation Of Image Encryption And Decryption Using AES 128-Bit Core", In proceeding of IEEE explore 2017.
[13]. UpendraBisht, 2 ShubhashishGoswami, "Analysis and Implementation of Selective Image Encryption Technique Using Matlab", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3, Ver. III (May-Jun. 2014)
[14]. IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.
[15]. Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding", Microwave and Optical

Technology Letters Vol. 21, No. 5, 318-322 , June 5 1999
[16]. H.Abood, "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms". Annual Conference on New Trends in Information & Communications Technology Applications-(NTICT'2017) 7 - 9 March 2017 IEEE.
[17]. Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04, 2012
[18]. S. Kaur et al , "A Review of ImageEncryption Schemes Based on the Chaotic Map," International Journal of Computer Technology &Applications,vol. 5, Issue. 1, PP. 144-149, 2014.
[19]. N. Kandele, S. Tiwari, "A New Combined Symmetric Key Cryptography CRDDBT Using - Relative Displacement (RDC) and Dynamic Base Transformation (DBTC)," International Journal of Engineering Research & Technology, vol. 2, Issue.10, www.ijert.org, October - 2013.
[20]. Guanrong Chen, Yaobin Mao, Charles k. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", chaos, Solitons and Fractals 2004
[21]. Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", chaos, Solitons and Fractals 2005
[22]. Mohammed Amin, Osama S. Fragalah, Ahmed A. AbdEl-latif, "A chaotic block Cipher algorithm for image Cryptosystem", Elsevier B.V 2009
[23]. Sadhana Singh, AshishAgrawal and PriyankaPradhan "Advanced Text to Image Encryption by Using Selective Encryption Technique with C# (AES Encryption and CFB Mode)", International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2016.
[24]. X.F.Zhang, J.L.Fan, B.S.Kang, "Digital image encryption algorithm protection from shear transformation attack, August 2006

Deeksha P, et. al. "Review on Image Encryption/Decryption using AES Algorithm for Hardware Accelerator Design and Implementation." *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, vol. 10, no. 4, 2020, pp. 08-19.