Journal of Theoretical and Applied Information Technology
15th July 2021. Vol.99. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DEVELOPMENT OF IMPROVED SPEED AES BASED ON KEY DEPENDENT INTRA-ROUND OPERATIONS

SANDEEP K. SHELKE[1], SANJEET K SINHA[2], GOVIND SINGH PATEL[3]

[1,2]Schoolo of Electronics & Electrical Engineering, Lovely Professional University, Punjab, India.
[3]iIMT College of Engineering Greater Noida, UP, India

E-mail: [1]sandeepshelke18@gmail.com,[2]sanjeetksinha@gmail.comand [3]govindpatel1104@gmail.com

ABSTRACT

The modern day technological evolution in field of communication, improves our life to significant extent. Most of recent evolution, in communication field is governed by internet; on the other hand, the use of internet puts big concern for data security. The crucial applications like surveillance, medical or military; demands secured image transmission & storage. In order to provide security to the images during its transmission, multiple techniques have been developed, in last few decades. AES (Advanced Encryption Standard) is commonly used technique for image security. This work introduces, the development of AES; by making all the intra-round transformations (Sub-byte, Shift row & Mix column); as a key dependent transformations, this key dependency of intra-round transformations, results modification in the values of propagation & correlation as, 2^{-150} and 2^{-75} respectively; these value ensures protection against differential & linear attacks. For the development of proposed algorithm, c to VHDL compilation framework based on loop unrolling technique is used. This loop unrolling technique provides higher degree of parallelism for reconfigurable architecture causing the significant increase in the speed of image encryption & decryption. So the proposed AES provides high degree of security, that too at high speed but with cost of larger area requirement.

Keywords: *Linear Attacks; Differential Attacks; Image Security; Advanced Encryption Standard; Loop Unrolling Technique.*

1. INTRODUCTION

Image Processing is extensively used in multiple applications like automotive [1], aerospace [2] medical [3-4] and satellite [5-6]. Image processing application involves capturing the image, compressing the captured image & latter provide the security to image before transmitting the image. During the process of image data sharing or storing, the security of image data is the major concern, hence the cryptography plays the very vital role in digital image data protection. The rise of internet causes the great threat of information getting stole, during its transmission over the communication channel; hence the security of image data is very crucial aspects of image processing system. Cryptography is one of the method used to provide security to data, lot of other methods are also developed to provide security to data. Sometimes the existence of message is kept secret, if not possible to keep the message content secret; this type of image security technique is called as steganography. The basic difference between cryptography and steganography is that, cryptography ended up with providing the security to message content, whereas steganography provides security to message existence. Steganography can also be treated as non-visible communication, as the art of modern science.

Image cryptography model is used to secure the data transmission. In this process the image data is encrypted and transmitted to the destination. This encrypted data is then decrypted at receiver end and the secret information is extracted. Cryptography is one of important data security technique and it provides four important information security features as:

- **Confidentiality** – It is the ability to protect data from outside attackers.
- **Authentication** – The cryptographic methods like digital signatures and MAC can guard information from forgeries and spoofing.
- **Data Integrity** – The data integrity is provided by hash functions of cryptography.
- **Non-repudiation** – The non-repudiation is the ability to protect the data, against the consequences that may appear after denial of data transmission by transmitter.

All these features provided by cryptography gives the protection against attackers, so as to carry smooth business over the computer network.

The cryptography deals with encrypting message, so as to give protection against attackers. For image cryptography, the image first of all need to convert in to the text form. This plain text is applied to the cryptography tools to have an encrypted form of plain text, called as cipher text. This cipher text is obtained from plain text by using some encryption key. The plain text is in readable format whereas, cipher text is in non-readable form. The method of breaking the cryptography security system & getting access to content of encrypted message, without encryption key; is called as cryptanalysis. These cryptanalysis attacks are classified in to four types as;

- **Cipher text only attacks** – In this attack, only the cipher text is available for attacker to get the Orignal plain text.
- **Known plain text only attack** – In this attack, the attacker will try to decrypt the current cipher text, from some earlier combinations of plain text and cipher text.
- **Chosen plain text attack** – In this attack, the attacker can have access to sender's computer, so that the attacker can apply any random plain texts & generate their corresponding cipher texts. The attacker then uses these pair of plain texts & cipher texts, to decrypt the current plain text.
- **Chosen cipher text attack** - – In this attack, the attacker can have access to receiver's computer, so that the attacker can apply any random cipher texts & generate their corresponding plain texts. The attacker then uses these pair of plain texts and cipher texts, to decrypt the current plain text.

An efficient technique for image security is very essential to avoid any one of the above attacks.
Figure 1 shows the detail general model of image encryption and decryption. The main goal of encryption is to provide the security to the data [7-9]. Advanced Encryption standard (AES) is one of the widely & commonly used technique for image security. The Advanced Encryption Standard have been evolved over the period of time for better performance. In this work AES is developed with key dependent intra-round operations, so as to have more security against differential & linear attacks.

Encryption using software platforms provides an access to multiple advanced resources, and hence performs computationally more complex arithmetic operations in association with microprocessors. However, it is not convenient to use a microprocessor in standalone applications, like mobile devices, to provide secure communications because of the huge area penalty. Unlike software implementations, encryption using hardware platforms provides an efficient and effective solution for simple yet secure encryption requiring less on-chip area and small power consumption. In addition, a dedicated chip for encryption results much higher speeds in data processing than a microprocessor running software.

The algorithms need for the development of modern applications of image processing & computer vison, getting more & more complex day by day; along with this increasing complexity, rapid technology scaling; together demands faster & efficient computing resources.
Modern intelligent processing system relies on, how effectively 2-dimensional or 3-dimensional data is handled and hence, these modern intelligent processing systems takes more time for processing & extracting critical information; hence for better system performance there is need of several multicore CPUs, several GPUs, one or more FPGAs or ASICs. Nowadays FPGAs are getting more & more popular for real time data acquisition & processing specifically images with high resolution. FPGAs are intensively used for real time applications because of its several advantages as; first, low maintenance & manufacturing cost of FPGA, as compare to that of CPUs or GPUS. Second, FPGAs are highly parallel devices, hence supports high level optimizations, this kind of optimization is not possible with CPU & GPU. Third, FPGAs supports, input and output interfaces configurations at electrical circuit level, so that there is no need of dedicated hardware for various input output interfaces. Fourth, the availability of low cost FPGAs developed along with multicore CPUs, on the common package, ultimately results in better performance with heterogeneous processing. In the past, this facility was instantiated by using multiple discrete circuits, but the advancement in technology, permits integrating them as a single component, this brings several advantages in terms of low cost, small size, less power consumption, low hardware complexity. In this work, AES with key dependent round operation is developed using loop unrolling technique, so as to enhance the image encryption & decryption speed. The proposed approach is implemented using

FPGA based systems where we have simulated the proposed model with Xilinx for spartan 6 board.

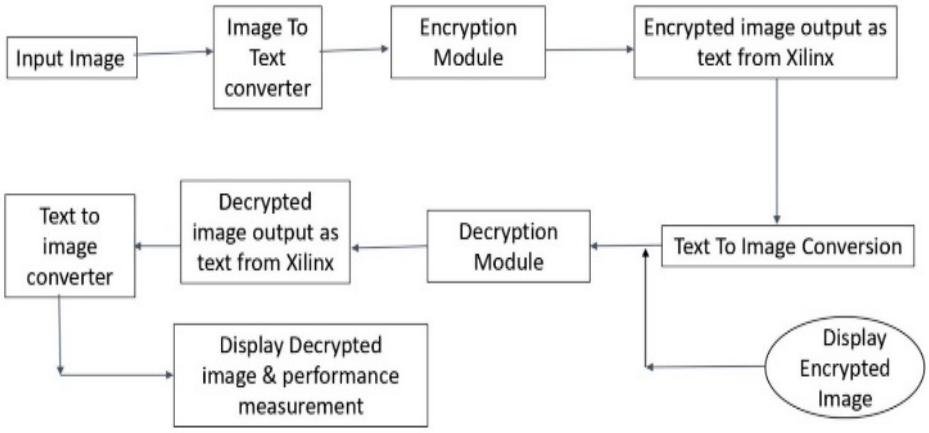

Figure 1. Image encryption & decryption

.

Rest of the manuscript is organized in following subsections: section 2 presents literature review about recent approaches of image security, Section 3 presents proposed solution for image security, section 4 presents the experimental and comparative analysis of proposed model, finally section 5 presents the concluding remarks

2. LITERATURE REVIEW

Ramalingam et al. [10] proposes, a transform domain hybrid integer encryption system based on permutation & diffusion, using haar integer wavelet transform (HIWT) & combine chaotic maps. Here HIWT is used to transform plain image and combine chaotic map is used to encrypt four sub-band coefficients of image. In order to obtain better chaotic behavior, two one dimensional chaotic maps are com-bine, so as to have huge unpredictable sequence, which is actually used for image encryption.

Srividya et al. [11] proposes, FPGA based hardware design for hybrid selective encryption & selective error correction. As the structure of FPGA allows multiple parallel operations, FPGA are very well suited for implementation in image processing. In this algorithm both encoding and encryption operations are executed in a single step, so as the basic aim of highest reliability & security is achieved. This method does not affect error correcting capability & security but still increases the speed of encryption & encoding. Kishore et al. [12] proposes an algorithm in order to meet four requirements as; first, to save the bit rate; second, to be compatible with FPGA file format; third, to provide security; fourth, less complex with faster implementation to support real time applications. This algorithm uses symbol and block scrambling for novel image encryption. Ramalingam et al. [13] presents, random adaptive image steganography algorithm based on image wavelet transform (IWT) using reconfigurable hardware architecture. In this algorithm various sub-bands like LL,HH,LH & LLH are differentiate using IWT in association with Moore & Hilbert space filtering curve scan patterns. Ledesma-Carrillo et al. [14] discussed various different approaches for image encryption, but most of them suffer from computational & time issue constraints, forced to restrict its use for real time applications. In this work orthogonal functions are used for online encryption & decryption of images based on generic FPGA-based reconfigurable architecture. The implementation of this algorithm is more feasible with FPGA, as this algorithm uses simple arithmetic operations like addition and subtraction. Leong et al. [15] implemented algorithm for image encryption using FPGA platform. Here at first image data is sent to development board, then image data is transferred with the help of SOPC builder to Altera QuartusII, then the configuration files are generated & downloaded to the board. For the decryption purpose inverse transform method is used. Yan et al. [16] proposes Abs (Analysis by synthesis) framework, so as reconstruction error will be push to high frequency band. This is a very flexible framework, as it can be very easily used in any threshold VC (Visual Cryptography) algorithm, so

as to raise visual quality without compromising security. Here the author has designed two algorithms based on AbS framework as, AbS based vector VC & AbS based probabilistic VC. Out of these two algorithms AbS based vector VC algorithm have several advantages over the available competing algorithms like almost gives zero DC component, low residual variance and better fidelity performance. Gupta et al. [17] proposes NSS (Natural Scene statistics) based model for both distorted & natural X-ray images. This NSS-based model captures consistencies of X-ray images and also provides efficient and effective tool to calculate the image degradation effect. According to author [17], there is a great scope in determining the image degradation geometrically on visual task performance in multi-view X-ray images. Altigani et.al [18] develop polymorphic Advance Encryption Standard using cipher, which works in 128 various ways. This approach increases security but there is no significant improvement in performance in terms of speed of encryption, rather the speed is reduced little bit with this approach. The significant work have been carried out for image security based on Advanced Encryption Standard. Although AES is implemented with modified hybrid ciphers [17-20] and dynamic ciphers {21-23], for better performance in terms of security, this improved performance is achieved without significant improvement in speed, rather this improvement may hamper the speed of encryption Table 1 shows comparative analysis of various image security techniques.

Table 1. Comparative Analysis of various image security techniques.

Ref.	Objective	Issues Addressed	Encryption Type	Remarks
[10]	Image Encryption	Speed & Power consumption	Cryptography	Images are first transformed using haar wavelet & encrypted using large random sequences.
[11]	Image Encryption	Selective encryption & selective error correction	Cryptography	Encoding & Encryption are performed in single step.
[12]	Image Encryption	Bit rate & JPEG file format compatibility	Cryptography	Provides security at low bit rate but increases hardware requirements
[14]	Image Encryption	Computational Complexity & time issue	Various image encryption techniques	FPGA based implementation using orthogonal functions.
[16]	Image Encryption	Reconstruction error and visual quality	Cryptography	Analysis by synthesis framework for visual cryptography.
[26]	Image Encryption	Low cost implementation	AES	Incorporated arbitrary arithmetic on composite field.
[27]	Image Encryption	Operating frequency	Cryptography	Encryption by synchronization; as a matrix approach
[28]	Image Encryption	Security	AES	FPGA Implementation of 128-Bit AES

Ramalingam et al. [10] proposes, the image security technique using haar wavelet & random sequences, the authors identified that, there is a trade-off between power & area. Novel approach proposed by Kishore et al. [12], provides compatibility with JPEG file format without affecting bit rate; but this is achieved with hardware compromise. Ledesma-Carrillo et al. [14] discussed various different approaches for image encryption, but most of them suffer from computational & time issue constraints. AES is the most widely used standard for image security, developed by US-NIST (National institute standards & technology). Significant amount of work have been done for betterment of system performance .Authors [26], [28-29] have implemented; the AES algorithm with certain modifications. Several techniques for FPGA based implementation of AES algorithm have been proposed for high speed encryption, but there is trade-off between speed & area [31-35]. Also AES is most secured algorithm, but with advancement of technology, AES algorithm could be attacked successfully in coming future; so it is important to increase the security of AES algorithm, hence in this work we focused on, increasing the speed of encryption along with improvement in security. The next section 3 illustrates the development of key dependent AES algorithm using loop unrolling technique, so as to have more secure AES algorithm with high speed operation

3. SYSTEM DEVELOPMENT

The AES stands for advanced encryption standard. AES is a symmetric key block cipher, as it uses same key for encryption & decryption. The AES can be implemented by using 3 different key size with different round of operations [12]. The combination of different key size & the corresponding number of round of operations is depicted in following table2.

Table 2. Key size

Rounds	No. of bits in the key
10	128
12	192
14	256

Thus smaller key operates with less number of rounds, whereas larger key operates with more number of rounds. The General Architecture for Advanced Encryption standard is as shown in figure 2

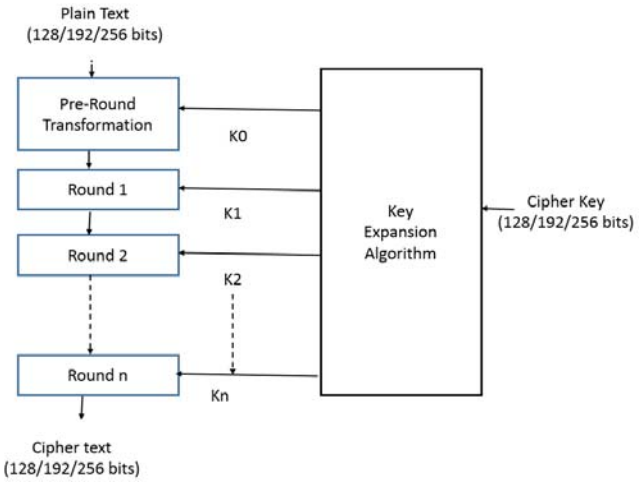

Figure 2. General architecture for AES

As shown in figure 2, the cipher key (128bits/192bits/256bits) is applied to key expansion algorithm, so that the 'n+1'sub-keys (K_0, K_1……. K_n; n=number of rounds) are generated. For 128 bits cipher key, there are 10 rounds, hence for 128 bits cipher key, the value of n=10 & hence for 128 bits cipher key total n+1=11 sub-keys are generated; similarly for 192 bits 13 sub-keys and for 256 bits cipher key 15 sub-keys are generated. As shown in figure 2, the input of 128 bits plain- text is applied to Pre-round transformation. This input is applied in the form '4 X 4' matrix with each of input state matrix is loaded with 1 byte, hence there will be total 16 bytes & as each column having 4 shells that is each column contains 1 word. After applying the input in the form of matrix each round will give output in the form of state matrix [30] as given below in figure 3.

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

Figure 3. State Matrix

Each shell of state matrix is loaded with 1 byte represented by S_{mn}, where 'm' indicates byte & 'n' indicates particular word.

The process of encryption starts with selecting cipher key size. Depending on the size of the selected cipher key, the number of rounds & the block size of plain text is decided. For uniformity, the further discussion is made by considering 128 bits cipher key, so that there will be total 10 rounds

& the block size of the plain text is 128 bits. The key expansion algorithm will generate 11 different sub keys. The encryption process starts with Pre-round transformation, this Pre-round transformation is a simple Ex-OR operation between 128 bits block of plain text & first key from key expansion algorithm, so as to get the output in the form of state matrix as shown in figure 3. This state matrix propagates through 10 rounds & finally gives the 128 bits cipher text.

Each round performs some internal operations as shown in figure 4, these internal operations are identical for each round, except the last round does not includes mix column operation[30].

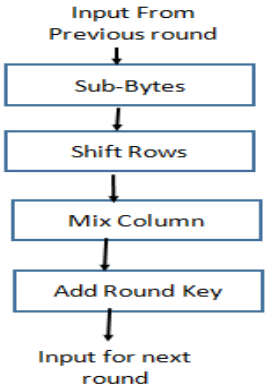

Figure 4. Operations performed in each round

Table 3. Modified round operations

Round Operation	Key Length	Modified operation
Sub byte	16 bytes	Bits of every byte of state matrix shifted circularly left by 3
	24 bytes	Bits of every byte of state matrix shifted circularly left by 5
	32 bytes	Bits of every byte of state matrix shifted circularly left by 7
Shift Row	16 bytes	No change to row 0; Circular left shift of row 1 by 1 byte. Circular left shift of row 2 by 2 byte Circular left shift of row 3 by 3 byte
	24 bytes	No change to row 2; Circular left shift of row 3 by 1 byte. Circular left shift of row 2 by 1 byte Circular left shift of row 3 by 0 byte
	32 bytes	No change to row 3; Circular left shift of row 2 by 1 byte. Circular left shift of row 2 by 1 byte Circular left shift of row 3 by 0 byte
Mix Column	16 byte	Column 0,1,2,3 of constant matrix is modified as column 1,0,2,3
	24 byte	Column 0,1,2,3 of constant matrix is modified as column 3,2,1,0
	32 byte	Column 0,1,2,3 of constant matrix is modified as column 3,0,1,2

As shown in figure 4, each round generally includes 4 operations. The proposed algorithm supports different keys of lengths as 16 bytes, 24 bytes or 32 bytes. The proposed algorithm makes the intra-round operations like sub-byte, shift row & mix column; as a key dependent. This key dependency of intra-round operations increases the security of proposed algorithm to the significant extent. The modified key dependent intra-round operations are shown in table 3.

3.1. Sub-Byte

For the consistency, it is consider that the key length is 16 bytes (128 Bits) in rest of the discussion. Sub-Byte is a substitution operation, in sub-byte operation the content of State Matrix is replaced by the content in S- Box [30] as shown in figure 5

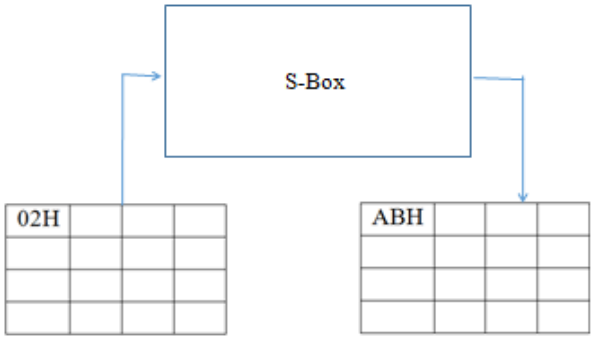

Figure 5. Sub Byte operation

The S-Box is a '16 X 16' data matrix and each location is loaded with 1 byte represented in Hexadecimal form. Now consider that, in state matrix the shell is loaded with 02 H , then the State matrix will check the row '0' and column '2' for S-box and the data of the said location of S-Box, for our case AB H will be updated in state matrix [30]. The sub byte operation is modified in proposed algorithm by circular shifting of bits of every byte in the state matrix to left side by 3. This circular shifting is done after looking up the content of S-Box

3.2. Shift Row

The shift row operation is followed by Sub Byte operation. In this shift row operation, the input is received from sub-byte stage in the form of State Matrix, then rows of the state matrix undergo specific shifting operation as shown in below table 4.

Table 4. Row wise shifting operation

Row 0	**No shifting**
Row 1	1 Byte Shift Left
Row 2	2 Byte Shift Left
Row 3	3 Byte Shift Left

Consider the state matrix received from Sub-Byte operation loaded with particular values as shown in figure 6.

22	B2	12	45
AC	3D	55	67
4A	67	74	3A
33	44	69	93

Figure 6. State matrix from sub byte stage

The state matrix undergoes shift row operations, as per table 4, so as to have modified state matrix as shown in figure 7 below.

22	B2	12	45
3D	55	67	AC
74	3A	4A	67
93	33	44	69

Figure 7.State matrix after shift row operation

3.3. Mix Column

The Mix column operation is followed by shift row operation. In the mix column operation stage, each column of state matrix received from shift row operation is individually applied to '4 X 4' fix matrix, so as to have modified version of the respective column. This process is repeated for each column of state matrix, so as to have modified state matrix. This process is illustrated in following figure 8.

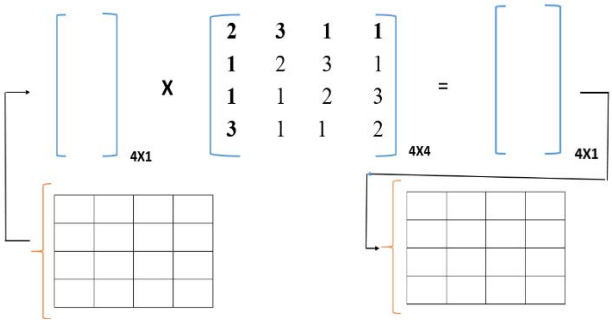

Figure 8. Mix Column operation

3	**2**	**1**	**1**
2	1	3	1
1	1	2	3
1	3	1	2

Figure 9. Modified constant matrix

The mix column operation in proposed algorithm is modified by altering the column 0, 1, 2, 3 of constant matrix as column 1, 0, 2, 3 for 16 byte key; as shown in below figure 9. Depending the key size this '4 X 4' fix matrix will be changed.

3.4 Add Round Key

The last stage of each round is the Add Round Key operation. In this stage, the state matrix received from Mix Column operation is EX-OR with the round key obtained from key expansion algorithm, so as to obtain the modified state matrix, this updated state matrix is then applied to the next round & the state matrix obtain from the last round is the cipher text.

All the four proposed operations involved in Advanced Encryption Standard is developed in c to VHDL compilation framework using loop unrolling techniques. Higher degree of parallelism is achieved for reconfigurable architecture using this compiler technique of loop unrolling. Loop unrolling technique reduces the number of iterations required to execute particular operation, so as to have significant improvement in the speed of that particular operation, however loop unrolling increases the area requirement. The genitalized example of loop unrolling technique is given as in figure 10.

After detailed discussion about modified algorithm for Advanced Encryption Standard based on key dependent intra-round operation developed using loop unrolling technique, next section brief about result & discussion.

Consider the loop as
For (i:=1000; I ;= 0; i--)
A[i] = A[i] + s

After unrolling

For (i:=1000; I ;= 0; i = i-2)
A[i] = A[i] + s
A[i-1] = A[i-1] + s
Because of this loop

Figure 10. Loop unrolling technique

4. RESULT & DISCUSION

The 14 round Advanced Encryption Standard, with key dependent intra-round operation is developed with loop unrolling technique, so as to improve the encryption & decryption speed. Also key dependency of intra-round operation ensures the significant security against linear & differential attacks.

4.1 Encryption

The Proposed algorithm with a standard test input image of size '256 X 256' is simulated with Xilinx tool on sparten 6 environment. The waveform generated after the encryption is shown in figure 11. The obtained result of proposed algorithm is compared in terms of operating frequency and the resource (LUT & Slice) utilization, as shown in table5

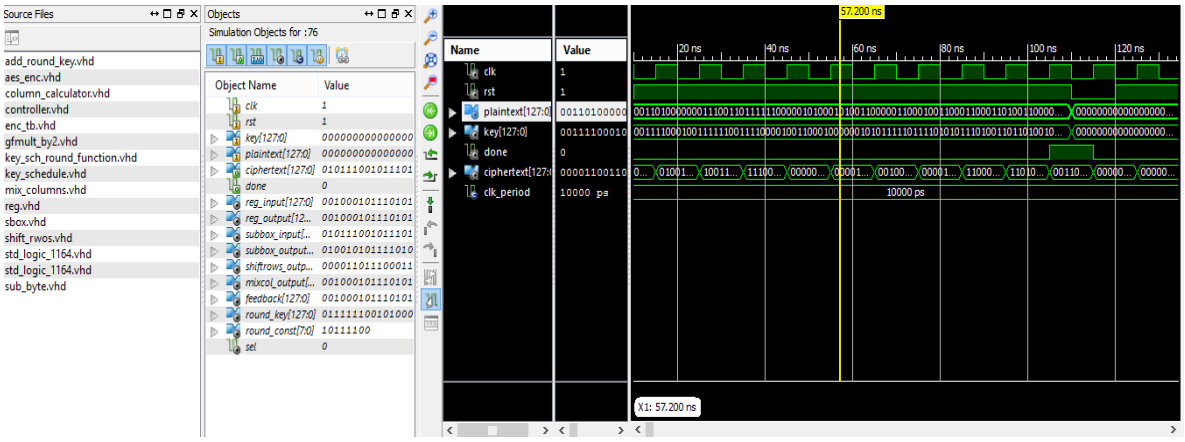

Figure 11. AES Encryption resul

LUT (Look up Table) -FPGA LUTs are the reconfigurable memory blocks with address lines as input & data line as output. The hardware logic written in a HDL (Hardware Description Language) is synthesized in to the truth table & later LUTs are used for boolean logic implementation.

Table 5. Comparative Analysis Of AES Implementation

Design	LUTs	Slices	Operating Frequency
Bilgin et al. [31]	1198	475	127MHz.
Gross et al. [32]	595	366	103MHz.
Cnudde et al. [33]	1191	553	181MHz
Meyer et al. [34]	293	162	103MHz.
Wegener et al. [35]	230	108	120MHz.
This work	242	112	132MHz.

Slices – Each Slice – In FPGA hardware design number of occupied slices is the metric of size. Lesser the occupied slices indicates smaller size. Each slice includes LUTs, logic gates & registers.
Operating frequency – Operating frequency indicates the speed of operation. Higher the operating frequency indicates high speed operation. In FPGA implementation, there is a Trade-off between speed & area. High speed can be achieved with cost of increased area.

4.2 Decryption

The encrypted image is decrypted using the proposed decryption algorithm on the Xilinx platform figure 12 shows the generated waveform. The image is encrypted using proposed algorithm as depicted in figure 11. The encrypted image is decrypted at the receiver end, the decryption is depicted in figure 12. From these waveforms of encryption and decryption, it is cleared that the Orignal image is successfully restored at receiver end.
The comparative analysis of proposed work with earlier techniques as shown in table 5, clearly indicates that the proposed algorithm is 10% faster than best of earlier algorithm, with compromise of 5.21% increase in LUTs.
In order to check the degree of security that is provided by the proposed algorithm, a special analysis technique named cryptanalysis is used.
The cryptanalysis is used to break cryptography security systems to get access to the content of encrypted messages without cryptography key. The cryptanalysis is classified as differential cryptanalysis & linear cryptanalysis. The differential cryptanalysis is carried out depending on difference propagation. The linear crypt analysis is carried out depending on input output correlation [30]. The S-Box of proposed AES is same as that of conventional AES; having the difference propagation value as 2^{-6} and input output correlation value as 2^{-3} [18]. With proposed AES minimum number of S Boxes up to the fourth round are 25, thus the propagation & correlation value updated as 2^{-150} and 2^{-75}; these values are large enough to avoid any differential & linear attacks. Thus the proposed algorithm gives the improvement not only in terms of significant security but also in terms of high speed operation, with little bit area compromise

.

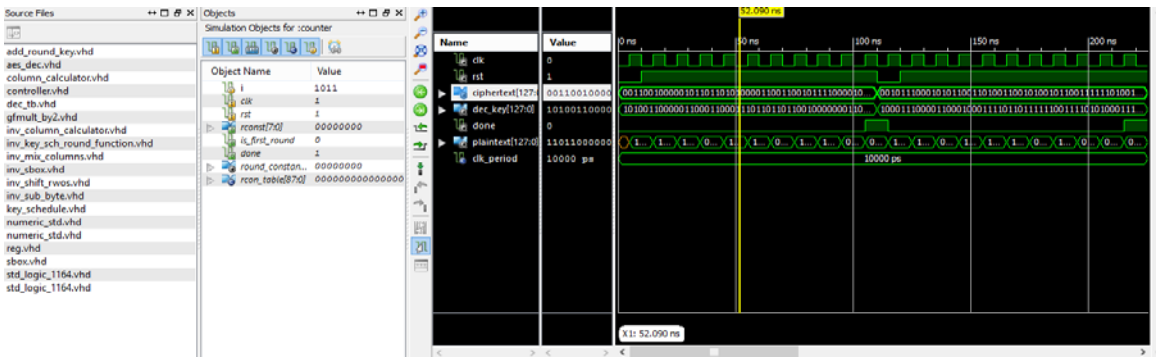

Figure 12. AES Decryption result

5. CONCLUSION

In this paper, Advanced Encryption Standard (AES) is developed with key dependent intra-round operations in c to VHDL compilation framework using loop unrolling techniques. Higher degree of parallelism is achieved for reconfigurable architecture using this compiler technique of loop unrolling. Loop unrolling technique reduces the number of iterations required to execute any particular operation, so that the frequency of proposed algorithm is increased by 10% over the previous best algorithm, with compromise of 5.21% increase in LUTs. In addition to this high speed operation, the key dependency of intra-round operations results significant improvement in degree of security, so as to avoid any differential & linear attacks.

ACKNOWLEDGEMENT

I express my sense of gratitude towards my supervisor Dr. Sanjeet K. Sinha and co-supervisor Dr. Govind Singh Patel for thier valuable guidance at every stage of my research work, also their contribution to solution of every problem at each stage.

I am also thankful to Department of Research Program, Lovely Professional University, Phagwara, Punjab, India for their very valuable and vital support in my research work.

Finally, I would like to thank all my dear friends for their valuable support and suggestions Lastly, I would also like to my family members for their unconditional support.

REFERENCES

[1] Schwiegelshohn F, Gierke L, Hübner M. FPGA based traffic sign detection for automotive camera systems. In2015 10th international symposium on reconfigurable communication-centric systems-on-chip (ReCoSoC) 2015 Jun 29 (pp. 1-6). IEEE.

[2] Taher F, Zaki A, Elsimary H. Design of low power FPGA architecture of image unit for space applications. In2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS) 2016 Oct 16 (pp. 1-4). IEEE.

[3] Li C, Balla-Arabé S, Yang F. Embedded multi-spectral image processing for real-time medical application. Journal of Systems Architecture. 2016 Mar 1;64:26-36.

[4] Pal C, Kotal A, Samanta A, Chakrabarti A, Ghosh R. An efficient FPGA implementation of optimized anisotropic diffusion filtering of images. International Journal of Reconfigurable Computing. 2016 Mar 1;2016.

[5] Elmannai H, Loghmari MA, Naceur MS. Nonlinear separation source and parameterized feature fusion for satelite image patch exemplars. In2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS) 2015 Jul 26 (pp. 405-408). IEEE.

[6] Quemada M, Hively WD, Daughtry CS, Lamb BT, Shermeyer J. Improved Crop Residue Cover Estimates from Satelite Images by Coupling Residue and Water Spectral Indices. InIGARSS 2018-2018 IEEE International Geoscience and Remote Sensing Symposium 2018 Jul 22 (pp. 5425-5428). IEEE.

[7] Ali I, Sabir S, Ullah Z. Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309. 2019 Jan 9.

[8] Liu J, Kato N, Ma J, Kadowaki N. Device-to-device communication in LTE-advanced networks: A survey. IEEE Commu

[9] Ahmadian AM, Amirmazlaghani M. A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms. Signal Processing: Image Communication. 2019 May 1;74:78-88.

[10] Ramalingam B, Rengarajan A, Rayappan JB. Hybrid image crypto system for secure image communication–A VLSI approach. Microprocessors and Microsystems. 2017 May 1;50:1-3.

[11] Srividya BV, Akhila S. Implementing a Hybrid Crypto-coding Algorithm for an Image on FPGA. InInternational Conference on Information and Communication Technology for Intelligent Systems 2017 Mar 25 (pp. 72-84). Springer, Cham.

[12] Kishore B, Kumar BS, Patil CR. FPGA based simple and fast JPEG encryptor. Journal of Real-Time Image Processing. 2015 Sep;10(3):551-9.

[13] Ramalingam B, Amirtharajan R, Rayappan JB. Stego on FPGA: an IWT approach. The Scientific World Journal. 2014 Jan 1;2014.

[14] Ledesma-Carrillo LM, Lopez-Ramirez M, Cabal-Yepez E, Ojeda-Castaneda J, Rodriguez-Donate C, Lizarraga-Morales RA. FPGA-based reconfigurable unit for image encryption using orthogonal functions. In2016 International Conference on Electronics, Communications and Computers (CONIELECOMP) 2016 Feb 24 (pp. 168-173). IEEE.

[15] Leong MP, Naziri SZ, Perng SY. Image encryption design using FPGA. In2013 International Conference on Electrical, Electronics and System Engineering (ICEESE) 2013 Dec 4 (pp. 27-32). IEEE.
[16] Yan B, Xiang Y, Hua G. Improving the visual quality of size-invariant visual cryptography for grayscale images: an analysis-by-synthesis (AbS) approach. IEEE Transactions on Image Processing. 2018 Oct 8;28(2):896-911.
[17] Gupta P, Sinno Z, Glover JL, Paulter NG, Bovik AC. Predicting detection performance on security X-ray images as a function of image quality. IEEE Transactions on Image Processing. 2019 Jan 31;28(7):3328-42.
[18] Altigani A, Hasan S, Barry B, Naserelden S, Elsadig MA, Elshoush HT. A Polymorphic Advanced Encryption Standard–A Novel Approach. IEEE Access. 2021 Jan 13;9:20191-207.
[19] Altigani A, Barry B. A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and Word Shift Coding Protocol. In2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE) 2013 Aug 26 (pp. 134-139). IEEE.
[20] Suri S, Vijay R. An AES–chaos-based hybrid approach to encrypt multiple images. InRecent Developments in Intelligent Computing, Communication and Devices 2017 (pp. 37-43). Springer, Singapore.
[21] Singhai P, Shrivastava A. An efficient Image Security mechanism based on Advanced Encryption Standard. International Journal of Advanced Technology and Engineering Exploration. 2015 Dec 1;2(13):175.
[22] Nisha N, Singh N. A hybrid approach of AES and file encryption to enhance the cloud security. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY. 2015 Aug;14(11):6250-7.
[23] Krishnamurthy GN, Ramaswamy V. Making AES stronger: AES with key dependent S-box. IJCSNS International Journal of Computer Science and Network Security. 2008 Sep;8(9):388-98.
[24] Hosseinkhani R, Javadi HH. Using cipher key to generate dynamic S-box in AES cipher system. International Journal of Computer Science and Security (IJCSS). 2012;6(1):19-28.
[25] Kazlauskas K, Kazlauskas J. Key-dependent S-box generation in AES block cipher system. Informatica. 2009 Jan 1;20(1):23-34.
[26] Masoumi M, Rezayati MH. Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis. IEEE Transactions on Information Forensics and Security. 2014 Nov 14;10(2):256-65.
[27] Ramírez-Torres MT, Murguia JS, Mejía-Carlos M. Fpga implementation of a reconfigurable image encryption system. In2014 International Conference on ReConFigurable Computing and FPGAs (ReConFig14) 2014 Dec 8 (pp. 1-4). IEEE.
[28] Priyanka MP, Prasad EL, Reddy AR. FPGA implementation of image encryption and decryption using AES 128-bit core. In2016 International Conference on Communication and Electronics Systems (ICCES) 2016 Oct 21 (pp. 1-5). IEEE.[22]
[29] Langenberg B, Pham H, Steinwandt R. Reducing the cost of implementing the advanced encryption standard as a quantum circuit. IEEE Transactions on Quantum Engineering. 2020 Jan 16;1:1-2.
[30] Daemen J, Rijmen V. AES proposal: Rijndael.
[31] Bilgin B, Gierlichs B, Nikova S, Nikov V, Rijmen V. Trade-offs for threshold implementations illustrated on AES. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2015 Apr 3;34(7):1188-200.
[32] Groß H, Mangard S, Korak T. An efficient side-channel protected AES implementation with arbitrary protection order. InCryptographers' Track at the RSA Conference 2017 Feb 14 (pp. 95-112). Springer, Cham.
[33] De Cnudde T, Reparaz O, Bilgin B, Nikova S, Nikov V, Rijmen V. Masking AES with $$ d+ 1$$ shares in hardware. InInternational Conference on Cryptographic Hardware and Embedded Systems 2016 Aug 17 (pp. 194-212). Springer, Berlin, Heidelberg.
[34] De Meyer L, Moradi A, Wegener F. Spin me right round: Rotational symmetry for FPGA-specific AES. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018;2018(3):596-626.
[35] Wegener F, De Meyer L, Moradi A. Spin me right round rotational symmetry for FPGA-specific AES: Extended version. Journal of Cryptology. 2020 Jul;33(3):1114-55.