International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8 Issue-7 May, 2019

FPGA Implementation of AES for Image Encryption and Decryption

Vijayakumar P, Chaitanya Kumar Chittoju, A.V.Bharadwaja, Payal P. Tayade, Tamilselvi M, R.Rajashree, Xiao-Zhi Gao

Abstract**:** ***Information is the key source to mankind and securing it is the biggest task. Unauthorized access of information deals with the security. For securing the data many cryptographic lgorithmshasbeenproposed,fromallofthealgorithms Advanced Encryption Standard (AES) is one of the most widely used algorithm for data encryption and decryption. Many researchers have put their effort to develop a new prototype of cryptographic algorithm and triedtoimplementinFPGAsystem.AESisanetworkof all possible cases of data are scramble, which has mathematical operations performed and itseach output bit depends on every input bit. The encryption process and the decryption process of image isdone with using AES 128 bit encryption algorithm. The m*n image data is turned into a binary or hexadecimal format by using MATLABsyntaxandcreatea textfile.Byusingthis text file as an input and cipher text is fed to the AES for encryption and decryption process. The entire design is functionally simulated using ModelSim-Altera 6.4a. Implementation and other parameters were analyzed using Xilinx ISE synthesis tools. The results were analyzes using device Virtex-6 XC6VLX240T FPGA kit with Xilinx ISE14.7.***

Index Terms**:** ***Advanced Encryption Standard; Field Programmable Gate Array; Cipher; AES Encryption; AES decryption; MATLAB; Image.***

I. INTRODUCTION

In our daily life, information is the main key role for exchange of a large quantity of data in different sectors like banking, medical and financial. So securing these fieldsis essential. For securing these sectorsmostlytheyareusingcryptographyalgorithms sothatdatacan'tbereadbyunauthorizedpersons.The main aim of cryptography is to securing the data and communication in the presence of adversaries. There are many cryptography techniques where proposed such as triple DES, DES, two fish, Blowfish,IDEA,MD5,SHA 1,HMAC, AES, andRSA.In all the techniques available, AES is the standard encryptionalgorithmsofall.AESalgorithmshasfixedblock size and supporting for 128, 192 and 256-bit symmetrickey.Alltheencryptionstandardalgorithms areofpublickeyandprivatekeyencryption,butAES is use private key encryption which isalso known as symmetric key structure. In public key algorithm a very complicated structure has been implemented which takes a very high computation time complicitywhichinvolves twokeyswhichareseparate,oneofis for encryption flow and the other is for decryption flow. Symmetric Key algorithm is one of thesimple form in which encryption and decryption flow, uses samekeyso,thisencryptionhasspeedimplementation flow [3]. The main objective is to encrypt and decrypt the image uses AES-128 bit core implantation on FPGA kit. AES can be implemented in hardware and software but hardware implementation of AES provides the physical security system [5]. In this proposeddesignthemeasuringandcomparisonofthe previous works is done with parameters like power, area, and latency. In this paper, a complex VLSI architecture technique using S-Box which has composite field arithmetic for itsimplementation.

II. RELATED WORK

S.H Kamali [4] here he proposed a (MAES) modified AES algorithm, it has a high security level andthisdesignsystemareoftenusedforagoodimage encryptionsystem.Mainlythemodifieddesignhasthe shifting of the rows and columns in it. If the bit positionsofthe1strowareinevenand1stcolumnsthen the1stand4throwsareunchanged,andeachbyteinthe 2ndand 3rdrows is shifted to the right cyclically. If firstandsecondrowsofthestateareunchanged,then second and fourth rows are shifted to left. Even when entropy is at maximum the security is same. In this design ithasa better standard of encryption than that previous one.Jignesh [3] has proposed mixed hybrid structure which is based on 128 bit key length of AES DES. Here, the input image for encryption is 1stconverted into 128 bit text and then the converted plain text is dividedinto2separatelysetsof64-bitplaintext.DES has this plain text as input data. For more scrambling this 2 encrypted 64-bit messages are converged as 128-bit, which is connected to the AES calculationfor encryptionprocess.Thiskindofmixtureshowgivesa good non-linearity for plain AES when contrasted. Thisplanhasbetterdisseminationbyconvergingwith DEScalculation. .Ju-Young Ho [6] Ju-Young has proposed thatthe concept of Selective Encryption Algorithm with five main criteria such as compression ofplain text, size of the encryption blocks, selectable round, optimized software implementation

Revised Manuscript Received on May 10, 2019

P. Vijayakumar, School of Electronics Engineering, VIT Chennai, Tamilnadu, India.

Chaitanya Kumar Chittoju, Electronics Engineering, Vellore Institute of Technology, Chennai, India.

A.V.Bharadwaja,ECE Dept., GIET Autonomous College of Engineering and Technology, Andhrapradesh, India.

Payal P. Tayade,School of Electronics Engineering, VIT Chennai, Tamilnadu, India.

M. Tamilselvi, Mechatronics Dept.,T.S Srinivasan Centre for Polytechnic and Advanced Training, Chennai, India

R. Rajashree, ECE Dept.,Dr. SJS Paul Engineering (Former), Pondicherry, India.

Xiao-Zhi Gao, University of Eastern Finland, Finland.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

and selective function of the whole routine. The input image file which is compressed gets large security and it reduces up to35% more of an average of its execution time of the originalAES.S. H Kamali [7] here he proposed that themodification of AES algorithm for the image encryption and decryption by adding a simple key to the steam generator which improves the performance by which it reduces the entropy.

III. TRADITIONAL AES 128-BIT ENCRYPTIONALGORITHM

AES can operate with three different bit size, specified by AES – 128 bit, AES – 192 bit, and AES-256bit.Eachbitsizehasdifferentsetofrounds10,12,14 respectively and length of the key is chosen accordingly. Various versions of AES are listed out in Table I. Advanced Encryption Standard is an iterative algorithm flow, every iteration is known as a round. Each and every round comprises of 4 transformations named as Sub Bytes change, Mix Columns change, Shift Rows change and Key Additionchange.SubByteschangeisknownascalled a substitution Byte change. It is non-linear byte substitution and utilized at encryption site. The activity is performed on every byte utilizing the substitutiontableknownasS-boxandfurthermorefor every byte of a state is mapped to alternates. The S- box can be executed utilizing two methodologies, Look-up table approach, and composite field arithmetic approach. ROM based LUT requires a lot ofinformationmemorywhichneedsavastzone.This has a bit of inadequacy at understood anunbreakable suspension with cause's low inertness due to ROM fixed access time. So the S-box is executed utilizing unmistakable procedures, composite field arithmetic bywhichitlessensthezone andifdistrictdiminishes, the power of AES building will additionally diminish. The tally begins with an Add round key stage took after by 9throundsof4th phases and 10thround.

Table I. AES Versions

AES Version	Cipher Text Size	No of Rounds	Secret Key Size	Regular Round
AES-128	128	10	128	9
AES-192	192	12	192	11
AES-256	256	14	256	13

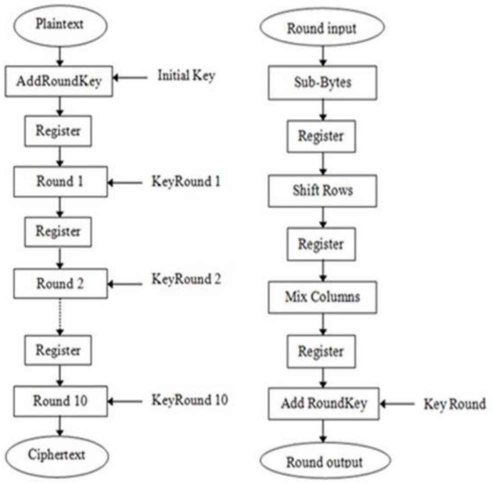


Fig. 1. Encryption and Decryption flow

Amongthe entirealgorithmpresentAESisoneofthe slandered algorithm for encryption and decryption stranded algorithm for any sort of information like image, text, and audio. We have different standard typeofbitlengthsbutweusesamebitlengthwhich is symmetric keys for AES which has 128 bit, 192 bit, 256 bits [4]. Here we use 128-bit AES core algorithm. AES under goes different kinds of stepsin encryption like,addingtext,symmetricKey,shiftrows andmixed columns, S-box contains Sub Bytes and shift rows. Starting with two inputs given to AES such as 128-bit dataand128-bitcipherkey.Theprocessgoeslike128-bitis equallydistributedinto16bytesofthedata,and each byte has of 8 bit length as shown in the fig-1. There are four transformations namely that will take place which are number one SubBytessecond is Shift Rows third is Mix Columns and finally fourth is AddRoundKey. In this 128-bit algorithm we have 10rounds up to nine rounds all transformations are done but at the last round hasonly 3 operation but only except Mix Columns operations. In the last round the bitencryptionhas128-bits.Heretheaimistoconverts the plain text of the image into cipher text. AES operation is done on a 4x4 array block of bytes which is known as a state and undergoes all the four transformations. All operation is listed out as the following.Alltheroundsofthealgorithmarelistedouta s4-stagebelow.

- SubstituteBytes
- ShiftRows
- MixColumns
- Add RoundKey

FinalroundhasMixcolumn operation.Fordecryption algorithm the first 9 rounds are administered by the following the 4stages.

- Inverse SubstituteBytes
- Inverse ShiftRows
- Add RoundKey
- Inverse MixColumns

A. *Add RoundKey*

Here we just add the plane text and the key inthe process of evolving. For addition we use xo r operation. A total of 128-bits of plane text and 128- bits of key are used. From key schedule process each ofthestepisformulated.Togetnext state(k)theinput and key should be samesize.

B. *SubstituteBytes*

InsubstitutebytestheS-boxisusedastheprimary sourceforitsoperation.Thisisperformedforthemost part to change over the framework into nonlinear. A 16 × 16 grid of bytes are as of now characterized by AES. Absolutely there are 256 numbers in that case.

Thecapacityofthissquareis toexchangeorsubstitute the qualities in state exhibit Org with the comparing esteemsintheS-box.Theinversesubstitutebyteplays out the backwards task ofS-box.

C. Shift Rows

This operation is performed in shifting the rows. Here the flow is like 1stof array matrix is not interchangedandtheremamingrows,i.e, 2, 3and4rows are shifted to 1 bit, 2 bits and 3 bits of its left in same pattern.The inverse shift rows operation performs the inverse of shift rows by which it shifts the 2, 3 and 4 rows of matrix to 1, 2 and 3 bytes to theright.

D. MixColumns

Thisoperationismadecolumnbycolumnofeach of the state matrix array. The Galois Field (GF2^8)isconsideredaseachcolumn ofsatematrixarrayandthe polynomials of the Galois Field are multiplied with modulo of |*x*4 + 1|. This result obtained will be the corresponding output ofMixColumns.

IV. PROPOSED S-BOX STRUCTURE FOR AES IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

In the proposed S-Boxarchitecture mainlythree major modifications are madewhencomparedtoother architectures.

- Reduction of critical path and using composite fieldarithmetic.
- Introduction of merging operator ofsome block.
- Implementing multiplicative inverse of GF (2^4).

Design of S-Box using composite field arithmetic

S-Box is the building blocks for an AES engine. The operation performed by the S-Box dependsthe algorithm flow. Generally the S-BOX implemented can be done in two kinds of way, one by using ROM based LUT and the other by using composite field arithmetic. In ROM based LUT the transformation of SubBytesisdonebyusingS-box'smappingtechnique by which is not efficient for large throughput designs inwhichitinvolveseverybytestatemappingforevery clock cycle. For this reason the composite field arithmeticareimplementtheS-boxbyusingthislogic elements.Incompositefieldarithmeticthecomplexityy of the field depends on several factors such as use of irreducible polynomial, field of mapping and isomorphic mapping [10]. In this methodology it employs a multiplicative inverse for s-box implementation with the help of composite field arithmetic. Here we discuss only thesubByte transformation which is implemented using GF (2^8) andthemajortaskhere istofindingmultiplicative.So thedecompositionofGF(2^8) canbedoneintoGF(2^4) and GF (2^4) as it reduces thecomplicity.

- *Isomorphicmapping*

The decomposition of GF (2^8) in to GF of (((2^2)^2)^2) is used for this mapping. GF mean Galois field here, the multiplication operation is the product of polynomials will be modulo of irreducible polynomial so it can be within the finite field. The following Eq. (1)shows the polynomial representation of data bytes in FiniteFields.

a(x) = b7x^7 + b6x ^6 + b5x^5 +b4x^4+ b3x^3 + b2x^2 +b1^x+ b0Eq. (1)

To achieve the transformation of large order fields to lower order fields along with irreducible polynomials in mapping structure is given as:

GF(2^2) $\rightarrow GF(2)$: $x^2 + x + 1$
GF((2^2))^2) $\rightarrow GF(2^2)$: $x^2 + x + \emptyset$
GF(2^2))^2)^2 $\rightarrow GF((2^2))^2)$: $x^2 + x + \lambda$

- *Compositefieldarithmetic*

In Composite field arithmetic all the operation are done in an irreducible polynomial equations. Operations like addition, multiplication and squaring which are operated using GF (2^4) to reduce the complexity [15]. We have several blocks implementation of the S-Box.

- *Addition operation in GF(2^4)*

The addition of elements in Galois field is performed using XOR operation bitwise between two elements.

$$k_3 = q_2 \oplus q_0$$
$$k_2 = q_3 \oplus q_2 \oplus q_1 \oplus q_0$$
$$k_1 = q_3$$
$$k_0 = q_2$$

- *MultiplicationoperationinGF(2^4)*

With composite field arithmetic in GF (2^2) and multiplication constant, multiplication in GF (2^4) is calculated. The decomposition of lower order fields is done by irreducible polynomial. Expressions areshown asfollowing.

$$k_1 = q_1w_1 \oplus q_0w_1 \oplus q_1w_0$$
$$k_0 = q_1w_1 \oplus q_0w_0$$

- *Multiplication with constantφ*

MultiplicationwithconstantGF(2^2),where. It has output k of two bits for input q is of two bits. The output of two bits is represented in following logical expression givenin.

- *Squaring operation in GF(2^4)*

$$k_1 = q_1 \oplus q_0$$
$$k_0 = q_1$$

Inthisoperation(x2)of4bits,theirreducible polynomial of x^2+x+φis being useful. The squaring operation in GF of (2^4) is implemented by decomposing the Galois field max to minfield. The logical expression for four bit output is given as following.

- *Multiplication with constantλ*

$$k_3 = q_3$$
$$k_2 = q_3 \oplus q_2$$
$$k_1 = q_2 \oplus q_1$$
$$k_0 = q_3 \oplus q_1 \oplus q_0$$

After the above operation the polynomial from that is multiplied with a constant (λ) for further calculation, here λ represents {1100}2. An expression of polynomial x2= x+α is used to reduce the product. This logical expression is calculated by using irreducible polynomial with k outputs of 4-bits in the form of q inputs of 4-bits.

V. FPGA IMPLEMENTATION OF S-BOX IN AES IMAGE ENCRYPTION AND DECRYPTION ALGORITHM

S-Box implementation of proposed AES is done in Xilinx FPGA kit. The FPGA device used for implementation is Virtex-6 XC6VLX240T of family Spartan3E.FordifferentblocksofAESandS-Boxare implementedandaresynthesizedbyusingtoolXilinx ISEV14.7. The hardware utilization factor summary of S-Box with number of LUTs and Slices are shown in TABLE II. The TABLE III gives the comparison of number of slices and LUTs of proposed and previous architecture forS-Box.

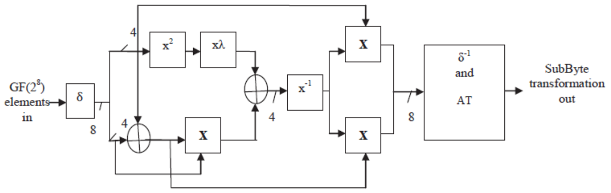


Fig.2. Sub Byte Transformation

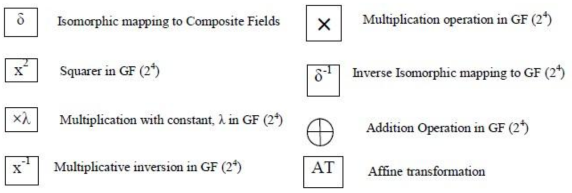

δ
Isomorphic mapping to Composite Fields
x^2
Squarer in GF (2^4)
×λ
Multiplication with constant, λ in GF (2^4)
x^{-1}
Multiplicative inversion in GF (2^4)
×
Multiplication operation in GF (2^4)
δ^{-1}
Inverse Isomorphic mapping to GF (2^4)
⊕
Addition Operation in GF (2^4)
AT
Affine transformation

Fig. 3 Blocks Description

Table Ⅱ: Utilization Summary of S-Box Blocks

S-Box blocks	4-input LUTs (out of61087)	No of Slices (out of30830)
Isomorphic	10	5
Multiplication operation in GF(2^4)	7	4
Multiplicative Inversion	13	7
Inverse Isomorphism	9	5
Affine Transformation	10	5
Multiplication operation GF(2^2)	3	2

The implementation of our proposed design was accomplished on device Virtex-6 XC6VLX 240T using Xilinx ISEV14.7 Design Suite as synthesis and simulation is done with ModelSim-Altera 6.4 a as simulation tools. The entire design was coded using Verilog language. This design occupied 30830slices, no of LUTs used 61087. It takes over 70 to 80 clock cycles latency for the first round. And then after, we get the output at each and every clock cycle. The proposeddesignachievesaleastclockperiodof6.246 ns and a large clock frequency of 276.031MHz, efficiency of 17.36 Mbps/slice and throughput of 69 GbpsEq.(2) and Eq.(3) gives the calculate the throughput and the efficiency η,respectively.

$Th\ rough\ put$ = number $of output bits/$ $Delay of critical path$
Eq. (2)

$Efficiency \eta$ = Throughput / N$oof slice$
Eq. (3)

Table Ⅲ.Comparisonof numberofslices andLook Up Table

Structure	4-input LUTs	No. of slices
Proposed structure	62	31
Conventional	74	42

Over all the main aim of the project is to implement AES algorithm on image. Here the original image is first converted into hexadecimal using the MATLAB code which uses $readmemb– for reading binary file and $readmemh– for reading hexadecimal and the given to the AES algorithm by which it converts into cipher text. The encryption and decryption process follows accordingly with the modifiedS-BOX.ThesamekeyisusedforEncryption andthedecryptionof128bitlength.Thekeyusedfor the process is 0123456789abcdef. The following figure shows the encrypted and the original images and the original image can be reconstructed easily without distortion.

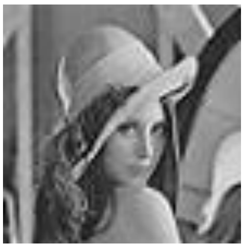


Fig. 4.Originalimage

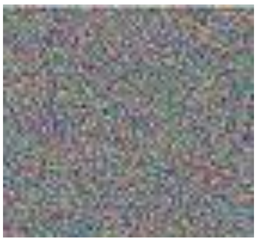


Fig. 5.Encryptedimage

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

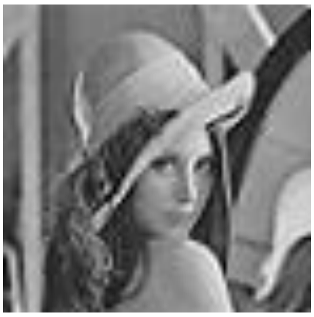
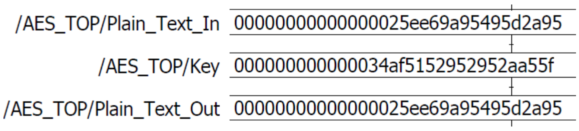


Fig. 6. Decrypted image



```
/AES_TOP/Plain_Text_In    000000000000000025ee69a95495d2a95
/AES_TOP/Key              00000000000034af5152952952aa55f
/AES_TOP/Plain_Text_Out   000000000000000025ee69a95495d2a95
```

Fig.7. Output waveform

VI. CONCLUSION

This paper shows implementation of AESImage file for encryption and decryption for securing the image text from unknown authority. We use symmetric key AES algorithm which is the best of all the encryption standard and decryption standardavailable. By using MATLAB coding the image file can be converted into hex file which can be readable to the process and which is implemented and synthesized. The advantage of using pipelining in S- Box is to avoid delay in LUTs by implementing using combinationallogics. ByusingS-Boxonce,continues thepathwhichincreasesgraduallywiththelogicdelay and this logical delay decreases at maximum clock frequency. To get maximum obtained clock frequency, a pipelining structure with 3-layered was proposed to reduce the logic delay. The composite field arithmetic helps inreducing hardware complexity of AES. AES structure is implemented and runbyVerilogonadeviceVirtex-6XC6VLX240T.This design is implemented in S-Box which has 65 4- input LUTs and 33 slices as compared to other basic structures. The analysis of AES S-Box is improvised by getting highest clock period frequency of 6.246 ns and has a lowest clock period frequency of 276.031MHz. The proposed pipelined structured S- Box has compact and highest speed than other structure.

REFERENCES

1. Rubén Lumbiarres-López, Mariano López-García, Enrique Cantó-Navarro, “Hardware architecture implemented on FPGA for protecting cryptographic keys against side-channel attacks”, 10.1109/TDSC.2016.2610966, IEEE
2. X. Zhang, K. K. Parhi, “High-Speed VLSI Architectures for the AES Algorithm,” *IEEE Transactions on Very Large Scale Integration(VLSI)Systems*, Vol. 12 (9), pp. 957-967, Sep. 2004
3. Transactions on Dependable and Secure Computing. B.A. Forouzan and D. Mukhopadhyay, Cryptography and Network Security, 2nd Ed., Tata McGraw Hill, New Delhi, 2012.
4. JignaeshR.Patel, Rajesh S.Bansode, VikasKaul,”Hybrid security algorithm for data transmission using AES-DES”,.IJAIS-2012.
5. Ai-Wen Luo, Qing-Ming Yi, Min Shi, “Design and Implementation of Area-optimized AES-Based on FPGA”, 978-1-61284-109 0/11/2011 IEEE.
6. Y.Ou ,C.Sur , K. H Rhee”Region based selective Encryption for Medical Imaging”,1st Annual International Workshop-2007
7. S. H Kamali, R.Shakerian, M.Hedayati,”A new modified version of Advanced Encryption Standard based algorithm for image encryption”, International Conference on Electronics and information Engineering, ICEIE-2010.
8. Ju-Young Oh, Dong-II Yang PhD and ki-Hwan Cho,”A selective Encryption Algorithm based on AES for medical Information”,Healthcare informatics research-2010
9. M.Zeghid ,M.Machhout,L.Khriji,A.Baganne and R.Tourki,”A modified AES based algorithm for image encryption”,International journal of computer electrical, Automation, Control and information engineering- 2007.
10. Arundhati Joshi, P. K. Dakhole, Ajay Thatere, “Implementation of S-Box for Advanced Encryption Standard”, 2015 IEEE International Conference on Engineering and Technology (ICETECH), 20th March 2015, Coimbatore, TN, India.
11. Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare” FPGA Implementation of AES Algorithm”, IEEE-2011, Volume : 3,pp 401-405.
12. Monica Lib eratori, Fernando Otero, J. C. Bonadero, Jorge Castifieira”AES-128 cipher.high speed, low cost fpga implementation”, IEEE-2007.
13. Chi-Wu Huang, Chi-Jeng Chang, Mao-Yuan Lin, Hung-Yun Tai, “Compact FPGA Implementationof 32-bits AES Algorithm Using Block RAM”, IEEE-2007.
14. Hazim Kamal Ansari, AsadSuhailFarooqi,”Design Of High Speed Uart For Programming Fpga”,International Journal Of Engineering And Computer ScienceVolume1 Issue 1 Oct 2012 Page No. 28-36.
15. SaurabhKumar,"VLSI Implementation of AES Algorithm", IEEE-2014.

AUTHORS PROFILE

Dr. P. Vijayakumar is currently working as Associate Professor in School of Electronics Engineering at VIT university Chennai campus, India and completed his Ph.D in Wireless Security at Pondicherry University during 2015. He has totally 12 years of teaching and research experience and published more than 40 research papers in SCOPUS /SCI Indexed National / International Journals and Conferences. His area of specialization is Elliptic and Hyperelliptic Curve Cryptography, Blockchain technology, Cryptography and Network Security, Cryptographic Algorithms, DNA Steganography, Embedded System and IoT.

Chaitanya kumar ch received his B.Tech degree in Electronics & Communication Engineering from Lovely Professional University, Jalandhar, Punjab, India in 2016. He has completed M.Tech degree in VLSI Design from Vellore Institute of Technology, Chennai, India. His research interests include low power techniques and VLSI design.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Mr. Bharadwaja A.V working as assistant professor in GIET Autonomous college of Engineering & Technology, Rajahmundry, Andhrapradesh**.** He completed his B.E from Anil Neerukonda Institute of Technology and M.Tech in VIT University, Chennai. He is currently doing research at Sathyabama University, Chennai for past two years. He has total 5 years of teaching and research experience.

Ms. Payal P. Tayade is a Research Scholar from School of Electronics Engineering at VIT University Chennai Campus, India. She completed her BE from Shree SantGajananMaharaj College of Engineering, Shegaon and her ME from Sipna's College of Engineering & management, Amravati. Both colleges are affiliated to SantGadge Baba Amravati University. She has total 7 years of teaching Experience. She is doing PhD in wireless security at VIT Chennai from December 2015.

She is having 10 years of teaching experience in various engineering colleges and handled many electronics oriented subjects. Gold medalist in PG (Mtech VLSI Design) and now pursuing PhD in image processing domain. She published many research papers in reputed national and international journals and conferences and also got best paper award in IEEE digital Xplore Digital Library. She attended 20 hours online course organized by NPTEL and got certification for the same. She motivating the students regularly to participate in various Conferences to present the papers and also guiding them for their projects.

R. Rajashree worked as Assistant professor in Dr. S.J.S Paul Memorial college of Engineering & Technology, Vel's University and GKM College of Engineering & Technology, Chennai, and Tamilnadu, India. She is having total 3 years of teaching experience and published more than 10 SCOPUS indexed Journal and Conference in and around India. Her area of specialization is Elliptic and Hyperelliptic Curve Cryptography, Wireless Network Security, Cryptographic Algorithm, DNA Steganography, Embedded System and IoT.

Xiao-Zhi Gao is now working as a professor in School of Computing. University of Eastern Finland, Finland. He received his D.Sc. (Tech.) degree from the Helsinki University of Technology (now Aalto University), Finland in 1999. His current research interests are nature-inspired computing methods with applications in optimization, machine learning, data mining, signal processing, and control.