An Image Encryption with improved version of Advanced Encryption Standard Based Algorithm

Maruthi Kumar.D
Assistant Professor/Department of ECE
Srinivasa Ramanujan Institute of Technology,
Anantapur, India
maruthi.srit@gmail.com

Prasanth Babu.P
Assistant Professor/Department of ECE
Srinivasa Ramanujan Institute of Technology,
Anantapur, India
prasanth_440@yahoo.com

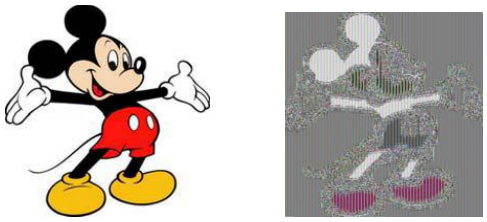
***Abstract*—Security in transmission storage of digital images has its importance in today's image communications and confidential video conferencing. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. Advanced Encryption Standard (AES) is a well known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications. In this paper, we analyze and present a modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption. The modification is done by adjusting the Shift Row Transformation. Detailed results in terms of security analysis and implementation are given. Experimental results verify and prove that the proposed modification to image cryptosystem is highly secure from the cryptographic viewpoint. The results also prove that with a comparison to original AES encryption algorithm the modified algorithm gives better encryption results in terms of security against statistical attacks.**

Index terms -Advanced Encryption Standard (AES), MAES, Image Encryption, Security Analysis, Shift Row Transformation.

I. INTRODUCTION

Encryption is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication,multimedia systems, medical imaging,Tele-medicine and military communication.

With the continuing development of both computer and Internet technology, multimedia data (images, videos, audios, etc.) is being used more and more widely, in applications such as video-on-demand, video conferencing, broadcasting, etc. Now, multimedia data is closely related to many aspects of daily life, including education, commerce, and politics. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA [1, 2], most of which are used in text or binary data. It is difficult to use them directly in multimedia data, for multimedia data [3] are often of high redundancy, of large volumes and require real-time interactions, such as displaying, cutting, copying, bit rate conversion, etc. For example, the image shown in Fig. 1(a) is encrypted into that shown in Fig. 1(b) by AES algorithm directly (ECB mode). As can be seen, Figure 1(b) is still intelligible to some extent.



a) b)

Figure 1. Application of the AES cipher to Mickey plain image/cipher image.

In This paper proposes a new encryption scheme as a modification of AES algorithm. The modification is mainly focused on both ShiftRow Transformations. In the ShiftRow Transformation, if the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. This modification allows for greater security and increased performance.

This paper is organized as follows. Section 2, gives a brief survey of AES techniques. Section 3 announces the proposed encryption algorithm and describes its hardware implementation. Experimental results are shown in section 4, and discuss the efficiency of the proposed algorithm scheme. Section 5 evaluates the performance of AES algorithm with respect to the security in image encryption. The last section concludes the paper.

II. RELATED WORK

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The Advanced Encryption Standard (AES) algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [4].

As the AES algorithm may be used with three different key lengths, these three different ‘‘flavors’’ are generally referred to as ‘‘AES-128’’, ‘‘AES-192’’, and ‘‘AES-256’’. However, The AES algorithm is divided into four different phases, which are executed in a sequential way forming rounds. The encryption is achieved by passing the plaintext through an initial round, 9 equal rounds and a final

round. In all of the phases of each round, the algorithm operates on a 4x4 array of bytes (called the State). In Fig. 2 we can see the structure of this algorithm [5]..

A. KeyExpansion Transformation

The AES algorithm takes the Master Key K, and performs a Key Expansion routine to generate a key schedule. The Key Expansion generates a total of 11 sub-key arrays of 16 words of 8 bits, denoted wi , taking into account that the first sub-key is the initial key. To calculate every wi (except w0) the routine uses the previous wi−1 and two tables, RCon and S-Box. RCon[i] contains the values given by $\{x^{i-1},\{00\},\{00\},\{00\}\}$, with x^{i-1} being powers of x (x is denoted as {02}) in the field GF(28).

B. T SubByte Transformation

The SubByte transformation is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation. The Fig. 2 shows the step of the SubByte transformation.

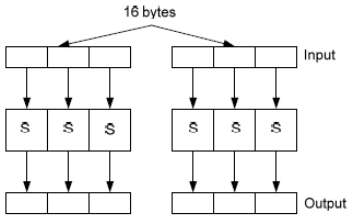


Figure 2. Block diagrams for Substitution

C. Shiftrows Transformation

In the ShiftRow transformation, the bytes in the last three rows of the State are cyclically shifted over 1, 2 and 3 bytes, respectively. The first row is not shifted. The offset of the left shift varies from one to three bytes.

D. Addroundkey Transformation

The AddRoundKey Transformation performs an operation on the State with one of the sub-keys. The operation is a simple XOR between each byte of the State and each byte of the sub key. This transformation is its own inverse.

E. Mixcolumns Transformation

The MixColumns transformation operates on the State column by column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF(28) and multi- plied by a fixed polynomial a(x) modulo x4 □1given by

$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ (1) – (1)

This can be written as a matrix multiplication as follows:

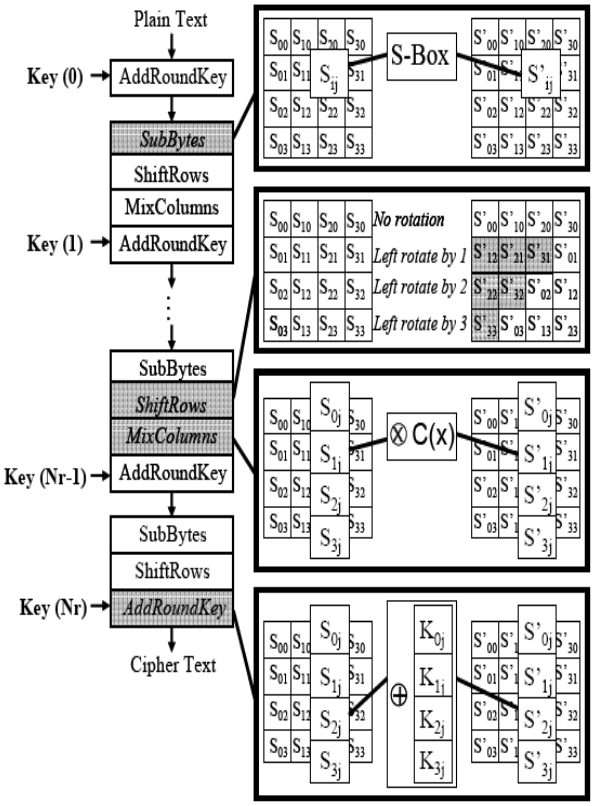
$$S'(x) = A(x) \oplus S(x) \begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} \equiv \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 03 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix} \quad (2)$$

for $0 \le c \le 4$

As a result of this multiplication, the four bytes in a column are replaced as follows:

$$\begin{aligned} s'_{0,c} &= (\{02\}.S_{0,c}) \oplus (\{03\}.S_{1,c}) \oplus S_{2,c} \oplus S_{3,c} \\ s'_{1,c} &= s_{0,c} \oplus (\{02\}.S_{1,c}) \oplus (\{03\}.S_{2,c}) \oplus S_{3,c} \\ s'_{1,c} &= s_{0,c} \oplus s_{1,c} \oplus (\{02\}.S_{2,c}) \oplus (\{03\}.S_{3,c}) \\ s'_{1,c} &= (\{03\}.S_{3,c}) \oplus s_{1,c} \oplus S_{2,c} \oplus (\{02\}.S_{3,c}) \end{aligned} \quad (3)$$

Fig. 3 shows the implementation of the function B =xtime(A) which will be used to make the multiplications of a number by 2 modulo m(x). So, we will only have binary operations as follows:



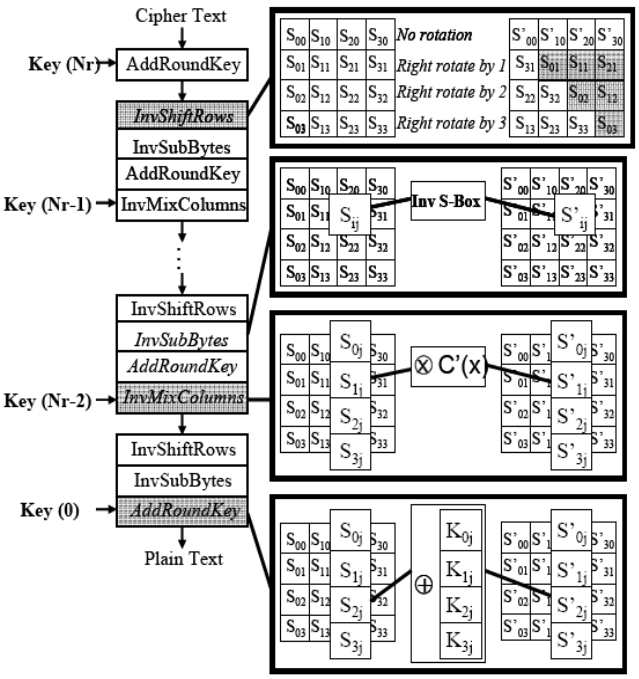


Figure 3. Description of the AES cryptographic algorithm [6].

III. Objectives & Overview Of The Proposed Mechanism

We will modify the AES to be more efficient and secure way by adjusting the ShiftRow Transformation.

A. ShiftRow Transformation

Instead of the original Shiftrow, we modify it as:

a- Examine the value in the first row and first column, (state [0] [0]) is even or odd?

b- If it is odd, The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For MAES, the first and third rows are unchanged and each byte of the second row is shifted one to the left. Similarly, the fourth row is shifted by three to the left respectively (Fig. 4).

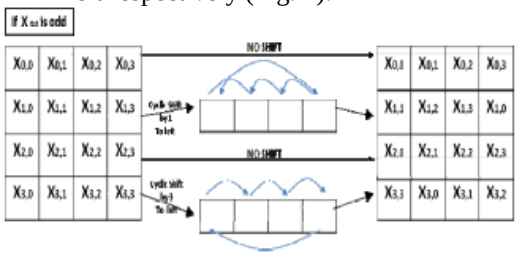


Figure 4. state ([0] [0]) is odd.

If it is even, The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. The first and fourth rows are unchanged and each byte of the second row is shifted three to the right. Similarly, the third row is shifted by tow respectively on to the right (Fig. 5).

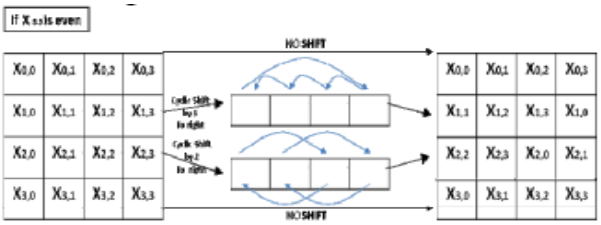
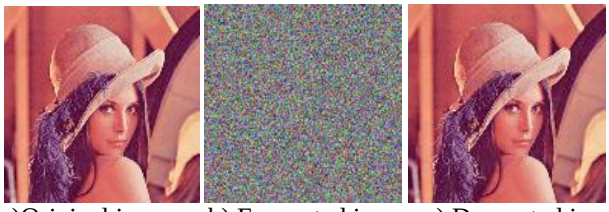


Figure 5. state ([0] [0]) is even.

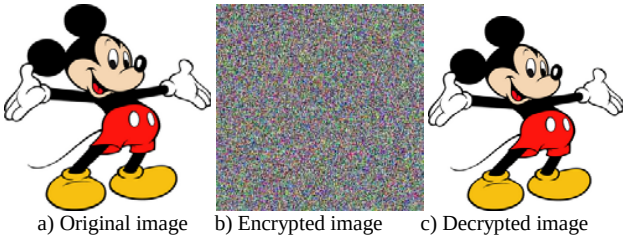
IV. Performance Evaluation

The AES image encryption algorithm is tested and evaluated based on software and hardware imulation. Results of some experiments are given to prove its efficiency of application to digital images. We use several images as the original images (plain images). The encrypted images are depicted in Figs. 6b-8b. As shown, the encrypted images (cipher image) regions are totally invisible. The decrypted images are shown in Figs. 6c-8c. The visual inspection of Figs. 6-8 shows the possibility of applying the proposed MAES successfully in both encryption and decryption. Also, it reveals its effectiveness in hiding the information contained in them.



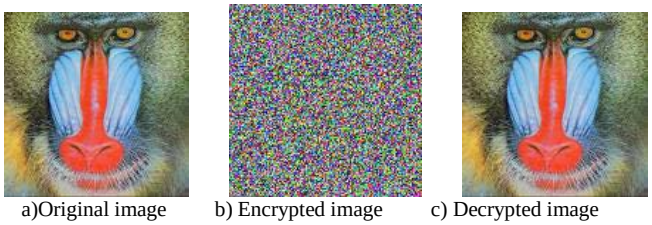
a)Original image b) Encrypted image c) Decrypted image

Figure 6. Application of the modified cipher to Lena plain image/cipher image.



a) Original image b) Encrypted image c) Decrypted image

Figure 7. Application of the modified cipher to Mickey plain image/cipher image.



a)Original image b) Encrypted image c) Decrypted image

Figure 8. Application of the modified cipher to Baboon plain image/cipherimage.

V. SECURITY ANALYSIS BY STATISTICAL APPROACH

A good encryption scheme should resist all kinds of known attacks, such as known-plain-text attack, cipher-text attack, statistical attack, differential attack, and various brute-force attacks. Some security analysis techniques perform on the AES image encryption scheme, including the statistical analysis and key space analysis [7].

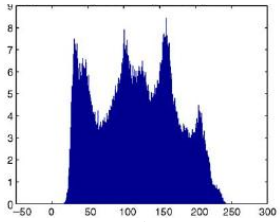
A. Statistical Analysis

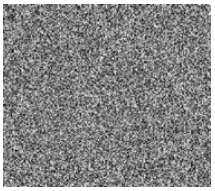
Shannon suggested two methods of diffusion and confusion in order to frustrate the powerful attacks based on statistical analysis. Statistical analysis has been performed on the AES, demonstrating its superior confusion and diffusion properties which strongly defend against statistical attacks. This is shown by a test on the histograms of the enciphered image and on the correlation of adjacent pixels in the ciphered image [8, 11].

1) Histograms of Encrypted Images

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig.9b. The histogram of a plain image (Mickey image (Fig.9a) of size 256x256 pixels) contains large spikes. The histogram of the cipher image as shown in Fig.9d, is uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure. [6-9].


a) Original image


b) Histogram of original image


c)Encrypted image

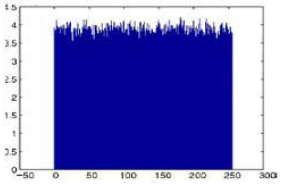

d) Histogram of encrypted image

Figure 9. Histograms of the plain image and ciphered image.

2) Correlation of Two Adjacent Pixels

We test the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in a ciphered image. First, we randomly select n pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient of each pair by using the following formula.

$$r_{xy} = \frac{conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (5)$$

Where x and y are grey-scale values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))2 \qquad (6)$$

$$conv(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

Fig. 10 shows the correlation distribution of two horizontally adjacent pixels in plain image cipher image (Mickey image of size 256x256) for the modified cipher. The correlation coefficients are 0.9452 and -0.0112 respectively for both plain image cipher image, which are far apart. Similar results for diagonal and vertical directions were obtained as shown in Table 1. It is clear that from the Fig. 10 and Table 1 that there is negligible correlation between the two adjacent pixels in the cipher image. However, the two adjacent pixels in the plaintext are highly correlated.

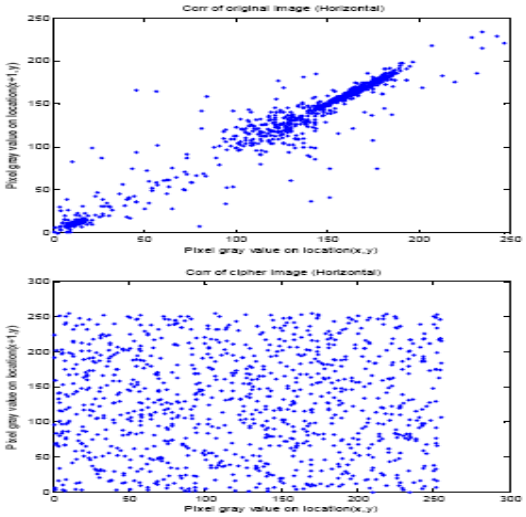


Figure 10. Tow horizontally adjacent pixels Correlation in plain image andcipher image, respectively.

Correlation Coefficient of two adjacent pixels in original and encrypted image is in table 1.

Direction	Plain image	Cipher image
Horizontal	0.945	-0.011
Vertical	0.947	-0.081
Diagonal	0.912	0.009

B. Key Space Analysis

Key space size is the total number of different keys that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [10]. The proposed cipher has 2128 different combinations of the secret key. An image cipher with such a long key space is sufficient for reliable practical use.

C. Information entropy analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [8, 11]. Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy H (m) of a source m, we have

$$H(m) = \sum_{i=0}^{2^N-1} P(m_i)\log_2 \frac{1}{P(m_i)} \; bits \qquad (7)$$

Where P(mi) represents the probability of symbol mi and the entropy is expressed in bits. Let us suppose that the source emits 28 symbols with equal probability, i.e., m = {m1,m2 ,...,m28 }after evaluating Equation (7), we obtain its entropy H(m) =8 , corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. Let us consider the cipher text of image encryption using the proposed block cipher, the number of occurrence of each cipher text block is recorded and the probability of occurrence is computed. We illustrate the entropy analysis of our scheme kept at the same word size w=32, number of rounds r= 10, and secret key length b=16 respectively, and compare it with other schemes. Table 2 indicates the various values of the entropies for encrypted images. It can be noted that the entropy of the encrypted image of MAES are very near to 8 compared to the other schemes.

Entropies of the encrypted images of Mickey image is in table 2.

Encryption Algorithm	Entropy Value
AES	7.9985
MAES	7.992

D. Performance of MAES w/r/b Encryption

Apart from security considerations, some other issues for image cryptosystem algorithm are also important. This includes the running speed, particularly for real time Internet multimedia application. Some experimental tests are given to demonstrate the efficiency of our scheme. An indexed image of a "Mickey" (see Fig. 7a) is used as a plain image and encryption of this image is shown in Fig. 7b. the personal computer used in all programs and test was Intel(R) Core™ 2Duo CPU T5800 2.00GHz with 3.00GB of memory and 230GB hard-disk capacity [12]. Table 3 and Fig.11 shows Performance of AES and MAES w/r/b Encryption on 256 grey-scale image of different sizes, kept at the same word size w=32, number of round r=12 and secret key length b=16 and kept at CBC mode of operation.

Performance of AES and MAES W/R/B encryption is in table 3.

Image size (pixels)	Image size on disk	Encryption time in ms with AES	Encryption time in ms with MAES
256 X 256	192 KB	6.44	6.34
512 X 512	257 KB	8.64	8.56
512 X512	768 KB	25.25	25.07
1024 X 1024	2.25 MB	75.86	75.11

VI. CONCLUSION

In this paper a new modified version of AES, to design a secure symmetric image encryption technique, has been proposed. The modification is done by adjusting ShiftRow Transformation. The proposed cryptosystem does not require any additional operations rather than the original AES. We have shown that MAES gives better encryption results in terms of security against statistical attacks.

REFERENCES

[1]. Kamvar, S., Schlosser, M., and Garcia-Molina, H. (2010), "The Eigen trust Algorithm for Reputation Management in P2P Networks," Proc. Int'l Conf. World Wide Web.
[2]. R. A. Mollin," An introduction to cryptography", CRC Press Boca Raton FL USA. 2008.
[3]. [3] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook, February 2005.
[4]. Federal Information Processing Standards Publication 197(FIPS197), http:// csrc.nist.gov/publications/fips/fips197/fips- 197.pdfS, 2001.
[5]. J. Daemen, V. Rijmen, The block cipher Rijndael, Smart Card Research and Applications (2000) 288–296.
[6]. Zhang, Y. and D. Feng, Equivalent generation of the S-box of Rijndael, Chinese Journal of Computer, vol.27, no.12 pp.1593-1600, 2004.
[7]. Liu, J., B. Wei and X. Wang, An AES S-box to increase complexity and cryptographic analysis, Proc. of the 19th

International Conference on Advances Information Networking and Application, Taiwan, pp.724-728, 2005.

[8]. J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.

[9]. H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. IEEE Trans. Signal Process. 48 (8), 2439–2451, 2000.

[10]. L. Shujun, Z. Xuan, M. Xuanqin, C. Yuanlong, "chaotic encryption scheme for real time digital video", SPIE vol.4666,p.149-160, Real- Time Imaging, March 2002.

Authors Profile

D.Maruthi Kumar received the **M.Tech** degree in Electronics and Communication Engineering (Digital Electronics and Communication Systems) from the Sri Kottam Tulasi Reddy Memorial College of Engineering, Konder, Andhra Pradesh, India, in 2011. His research interest includes image processing, speech processing, and Communication networks.

P.Prasanth Babu received the **M.Tech.** degree in Electronics and communication Engineering from the Rajeev Gandhi Memorial College of Engineering & Technology, Nandyal Kurnool (Dist), JNTUA University, Anantapur, India, in 2009.Currently pursuing **P.hD** in Electronics and Communication Engineering (Image Processing) in JNTUA, Anantapur, India. His research interest includes Image Processing & Signal Processing.