

PERFORMANCE ANALYSIS OF CRT FOR IMAGE ENCRYPTION

Dr.O.Srinivasa Rao

Department of Computer Engineering, UCEK, JNTUK ,Kakinada

ABSTRACT

With the fast advancements of information technology, the security of image data transmitted or stored over internet is become very difficult. To hide the details, an effective method is encryption, so that only authorized persons can decrypt the image with the keys available. Since the default features of digital image such as high capacity data, large redundancy and large similarities among pixels, the conventional encryption algorithms such as AES, , DES, 3DES, and Blow Fish, are not applicable for real time image encryption. This paper presents the performance of CRT for image encryption to secure storage and transmission of image over internet.

KEYWORDS

Digital image, Chinese Remainder Theorem, encryption, confidentiality

1. INTRODUCTION

The role of Digital images is important, both in daily life applications as well as in areas of research and technology. An image is a 2-D representation of a three dimensional scene. Due to its large capacity data, huge redundancy and high similarities among pixels, there are several researchers [1-7] done lot of work for image compression for long period except for image encryption, From this, research papers we see that the compression performances are good.

Many number of image encryption schemes combined with compression are proposed. These methods divide the image encryption and image compression into two separate stages [8-13]. These, mainly separate the encryption without considering the compression process. Few propose overcome the drawbacks in Refs. [8-13] by making the image encryption and compression in a single process [14-17]. Refs [18] propose a new image encryption algorithm integrated with compression using 2D hyper-chaos discrete nonlinear dynamic system and Chinese remainder theorem. However these papers do not evaluate the performance of CRT. This paper presents the optimal performance and limitations of CRT for image compression.

2. CHINESE REMAINDER THEOREM

Chinese remainder theorem [19-23] is a theorem about congruence's in number theory. It can be stated as follows:

If m_1, m_2, \dots, m_k are pair-wise relatively prime positive integers , and if a_1, a_2, \dots, a_k are any integers , then the simultaneous congruence's

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ..., $x \equiv a_k \pmod{m_k}$ have a solution, and the solution is unique modulo m, where $m = m_1 m_2 \dots m_k$

From Chinese remainder theorem, using k gray values, a_1, a_2, \dots, a_k , we get a gray value: $x \equiv m_1 m_1^{-1} a_1 + m_2 m_2^{-1} a_2 + \dots + m_k m_k^{-1} a_k \pmod{m}$. Therefore. CRT can encrypt an image, at the same it also compress the image with a given compression ratio k, simultaneously. From the unique solution $x \equiv m_1 m_1^{-1} a_1 + m_2 m_2^{-1} a_2 + \dots + m_k m_k^{-1} a_k \pmod{m}$, we can also get a_i by $a_i \equiv x \pmod{m_i}$, where $i = 1, \dots, k$. The above procedure is used for decryption and to uncompress the image.

The *Chinese Remainder Theorem* can be used for generating Godel numbering for sequences, for Good Thomas Fast Fourier transforms for re-indexing of data, for implementing the RSA encryption and decryption, for distributing the shared key among a group of people, and also used for range ambiguity resolution techniques with medium pulse repetition frequency radar. Some of the important parameters image are PSNR value and Correlations are define as follows

3. PSNR value

Peak signal-to-noise ratio, often abbreviated **PSNR**, is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel scale.

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\ &= 20 \cdot \log_{10} (MAX_I) - 10 \cdot \log_{10} (MSE) \end{aligned}$$

4. CORRELATION

Correlation coefficient is a coefficient that illustrates a quantitative measure of some type of correlation and dependence, meaning statistical relationships between two or more random variables or observed data values.

5. IMAGE ENCRYPTION PROCEDURE USING CRT

Step1: To compress an image with size $H \times W$ in to an image with size $(H \times W)/K$, we , set compression ratio k. This compression ration k is achieved by selecting randomly K integers: $a_1, a_2, \dots, a_k, a_i$, where $a_i > 256$, $\gcd(a_i, a_j) = 1$, $1 \leq i, j \leq k$, where H and W are the height and width of the plain image

Step2: Divide the shuffled gray value sequence S' into

$(H \times W)/k$ blocks: $B_1 = \{S'_1, S'_2, \dots, S'_k\}$, $B_2 = \{S'_{k+1}, S'_{k+2}, \dots, S'_{2k}\}$, ...,

$B_{(H \times W)/k} = \{S'_{H \times W - (k-1)}, S'_{H \times W - (k-2)}, \dots, S'_{H \times W}\}$

Step3: For each block B_i , $i=1, 2, \dots, (H \times W)/k$, by using CRT formula, encrypt each block into a value V_i , and get the encrypted and compressed sequence $V = \{V_1, V_2, \dots, V_{(H \times W)/K}\}$. Note that for each block B_i , x_1, x_2, \dots, x_k can be different, which may enhance the security of the algorithm
Step4: To form the encrypted and compressed image, reshape V back to the 2D value matrix with size $(H \times W)/k$

For experimental purpose, as example, I take $k=4$. This means that the cipher image is compressed into 1/4 of the plain image and further I chosen $m_1 = 311$, $m_2 = 313$, $m_3 = 317$, $m_4 = 293$ randomly for encryption and decryption

The following procedure is used to uncompress and decrypt the image:

Step1: Arrange the encrypted-compressed image into a sequence

$$V = \{V_1, V_2, \dots, V_{(H \times W)/K}\}.$$

Step2: Decrypt each V_i into k integers x_1, x_2, \dots, x_k by $x_j = V_i \pmod{m_j}$, $j = 1, 2, \dots, k$,

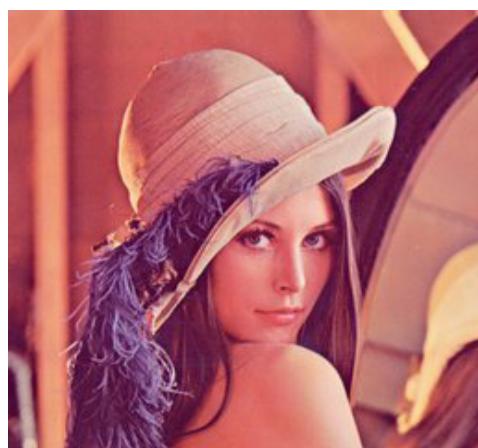
where m_i is defined in the encryption procedure. Then, get a decrypted sequence

$$X = \{x_1, x_2, \dots, x_{(H \times W)}\}.$$

Step3: Reshape $X = \{x_1, x_2, \dots, x_{(H \times W)}\}$ values with H rows and W columns to form the decrypted and decompressed image.

RESULT AND ANALYSIS

The following results shows the histograms of original, encrypted and decrypted image along with the correlation for different key values of the following standard image



Standard.jpg

Key Values used are:

$m = [467]$; m for $a=1$

$m = [971 \ 977]$; for $a=2$

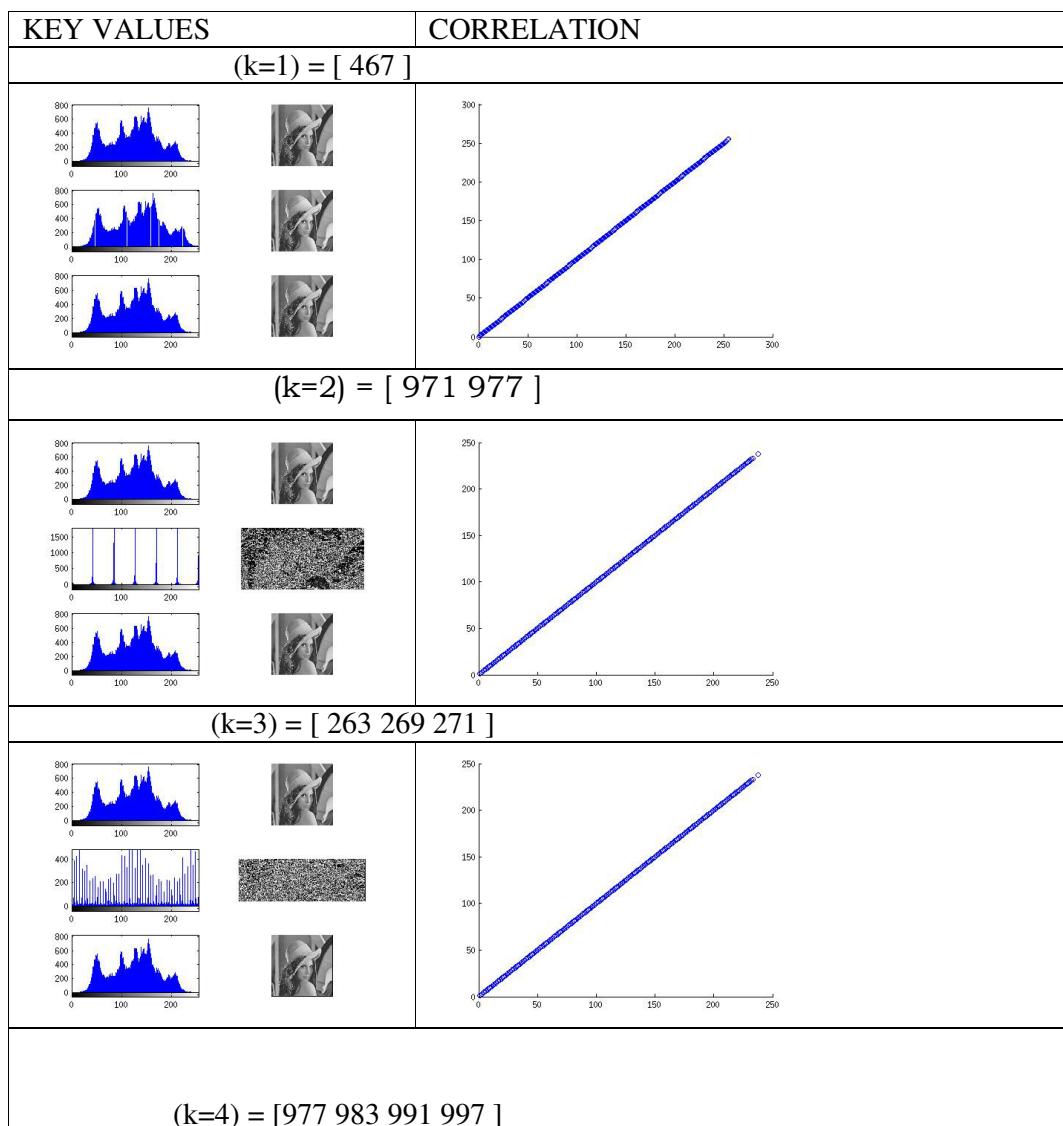
$m = [263 \ 269 \ 271]$; for $a=3$

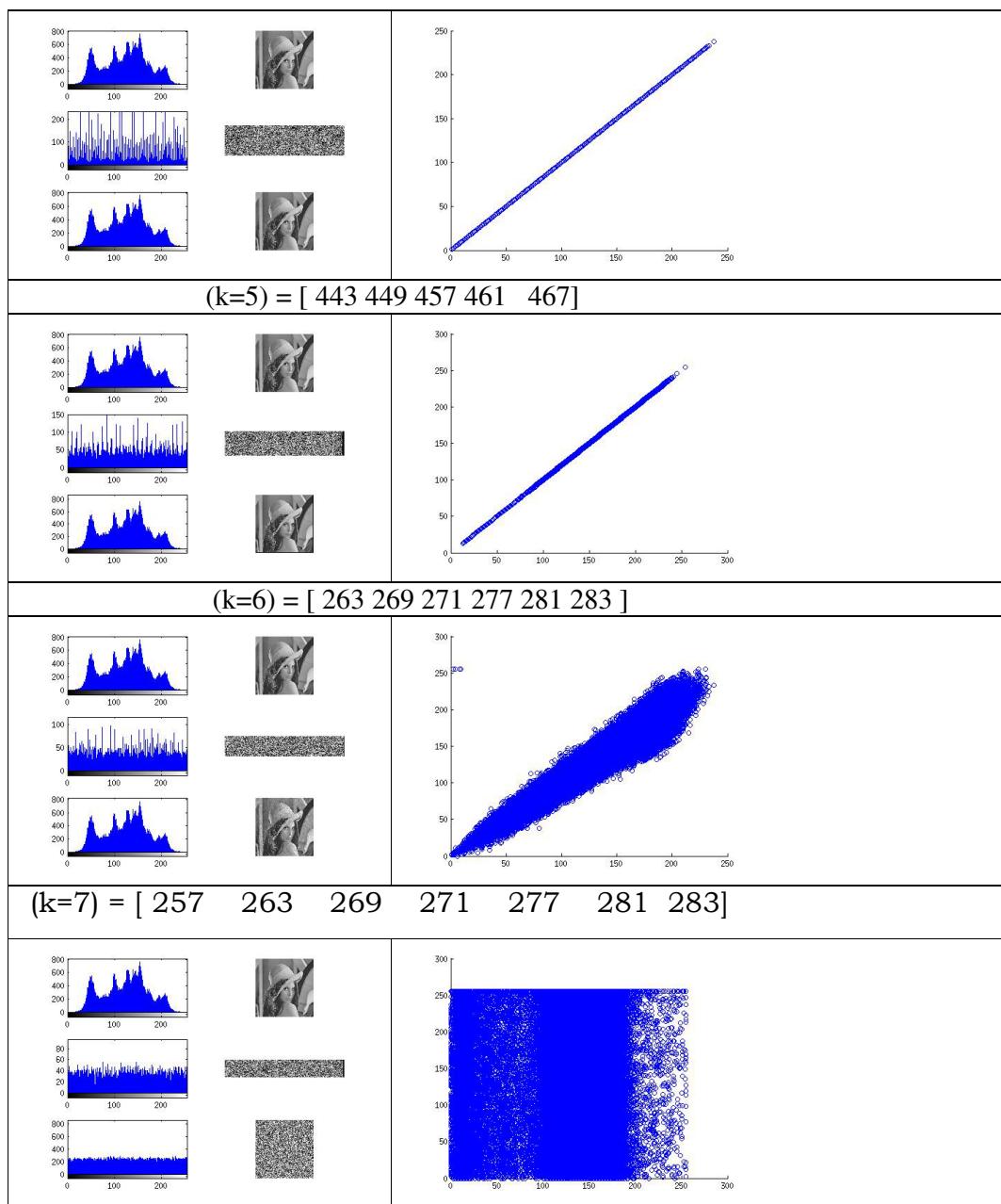
```

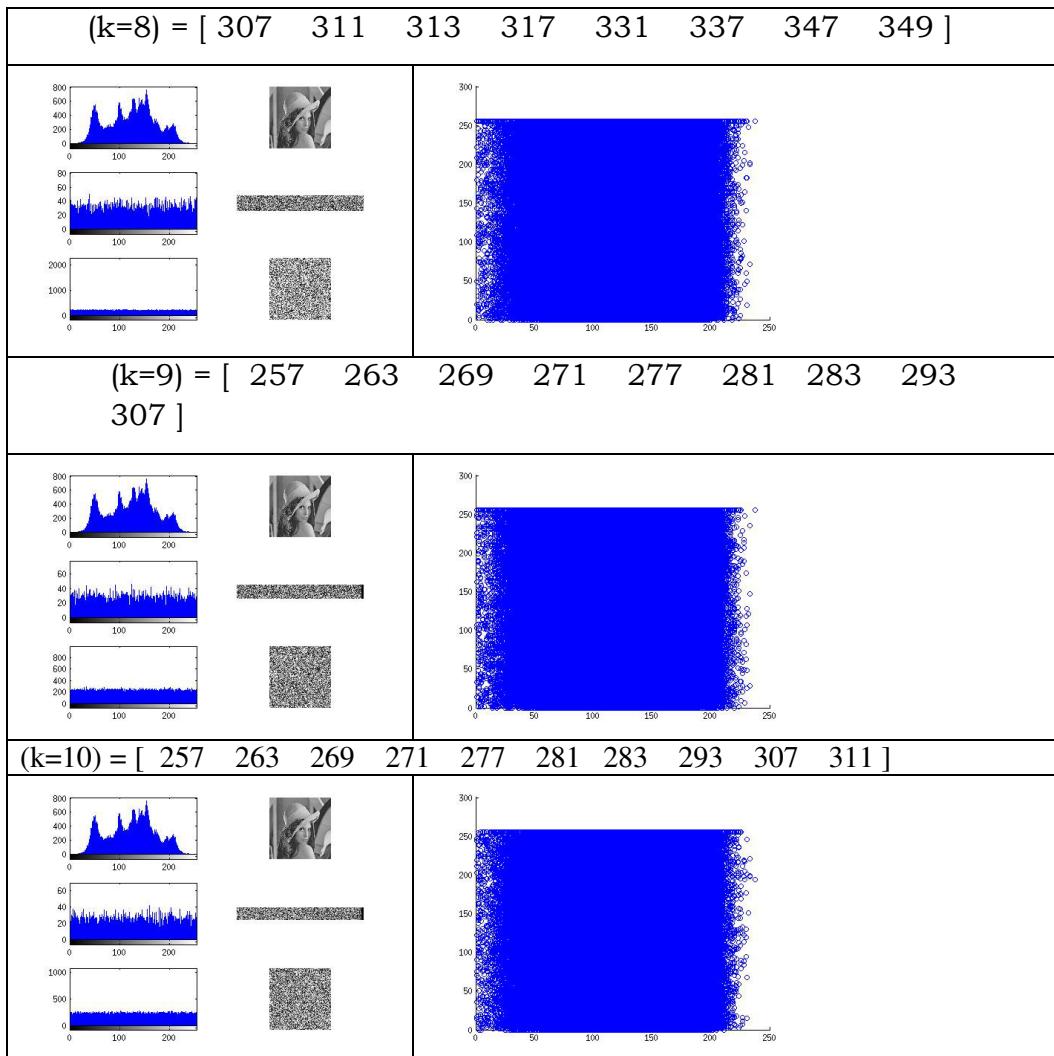
m = [977 983 991 997 ]; for a=4
m = [ 443 449 457 461 467 ]; for a=5
m = [ 263 269 271 277 281 283 ]; for a=6
m = [ 257 263 269 271 277 281 283]; for a=7
m = [ 307 311 313 317 331 337 347 349 ]; for a=8
m = [ 257 263 269 271 277 281 283 293 307 ]; for a=9
m = [ 257 263 269 271 277 281 283 293 307 311 ]; for a=10

```

Standard jpg







ANALYSIS

The following table values of correlation coefficient, PSNR and MSE for the sample image to the number of keys

SAMPLE NAME	Correlation coefficient	PSNR value	MSE value
Number of Keys =1 , m = [467]	1	infinity	0
Number of keys =2 ; m= [971 977]	1	infinity	0
Number of keys= 3, m = [263 269 271]	1	infinity	0
Number of keys= 4, m = [977 983 991 997]	1	infinity	0
Number of keys= 5, m =[443 449 457 461 467]	1	Infinity	0

Number of keys=6, m= [263 269 271 277 281 283]	0.9779	27.9575	104.07
Number of keys=7, m= [257 263 269 271 277 281 283]	-0.0067	8.0042	10296
Number of keys=8, m= [307 311 313 317 331 337 347 349]	-0.00085318	8.0243	10248
Number of keys=9, m= [257 263 269 271 277 281 283 293 307]	0.0013	8.7828	8606
Number of keys=10, m= [257 263 269 271 277 281 283 293 307 311]	0.0024	8.7352	8700.7

6. CONCLUSION

It is concluded from the result analysis of image encryption using CRT, that the encryption and decryption is optimal when the number of keys used are between 2 to 5 and the compression ratio is directly proportional to number keys used for encryption. Further it is observed that, if we increase the keys beyond the 5, the decryption process is unable to produce a valid decrypted image. Hence, this paper concludes, that, the CRT not only be used for image encryption and it also provide compression as well.

REFERENCES

- [1] A. Alfalou, C. Brosseau, Optical image compression and encryption methods, *Advances in Optics and Photonics* 1 (2009) 589–636.
- [2] N. Akrout, R. Prost, R. Goutte, Image compression by vector quantization: a review focused on codebook generation, *Image and Vision Computing* 12 (1994) 627–637.
- [3] A. Alkholidi, A. Alfalou, H. Hamam, A new approach for optical colored image compression using the JPEG standards, *Signal Processing* 87 (2007) 569–583.
- [4] H.S. Soliman, M. Omari, A neural networks approach to image data compression, *Applied Soft Computing* 6 (2006) 258–271.
- [5] A. Alfalou, A. Alkholidi, Implementation of an all-optical image compression architecture based on Fourier transform which will be the core principle in the realisation of DCT, *Proceedings of the SPIE* 5823 (2005) 183–190.
- [6] M. Helsingius, P. Kuosmanen, J. Astola, Image compression using multiple transforms, *Signal Processing: Image Communication* 15 (2000) 513–529.
- [7] M. Krinidis, N. Nikolaidis, I. Pitas, The discrete modal transform and its application to lossy image compression, *Signal Processing: Image Communication* 22 (2007) 480–504.
- [8] X. Li, J. Knipe, H. Cheng, Image compression and encryption using tree structures, *Pattern Recognition Letters* 18 (1997) 1253–1259.
- [9] S.S. Maniccam, N.G. Bourbakis, Lossless image compression and encryption using SCAN, *Pattern Recognition* 34 (2001) 1229–1245.
- [10] O.Y. Lui, K.W. Wong, J. Chen, J. Zhou, Chaos-based joint compression and encryption algorithm for generating variable length ciphertext, *Applied Soft Computing* 12 (2012) 125–132.
- [11] C.H. Yuen, K.W. Wong, A chaos-based joint image compression and encryption scheme using DCT and SHA-1, *Applied Soft Computing* 11 (2011) 5092–5098.
- [12] Y. Zhao, B. Yuan, A hybrid image compression scheme combining block-based fractal coding and DCT, *Signal Processing: Image Communication* 8 (1996) 73–78.
- [13] H.K.C. Chang, J.L. Liu, A linear quadtree compression scheme for image encryption, *Signal Processing: Image Communication* 10 (1997) 279–290.
- [14] A. Alfalou, C. Brosseau, Exploiting root-mean-square time frequency structure for multiple-image optical compression and encryption, *Optics Letters* 35 (2010) 1914–1916.

- [15] H. Hermassi, R. Rhouma, S. Belghith, Joint compression and encryption using chaotically mutated Huffman trees, Communications in Nonlinear 15 (2010) 2987–2999.
- [16] T.H. Chen, C.S. Wu, Compression-unimpaired batch-image encryption combining vector quantization and index compression, Information Sciences 180 (2010) 1690–1701.
- [17] J.L. Liu, Efficient selective encryption for JPEG 2000 images using private initial table, Pattern Recognition 39 (2006) 1509–1517.
- [18] Hegui Zhu , Cheng Zhao , Xiangde Zhang, A novel image encryption–compression scheme using ,hyper-chaos and Chinese remainder theorem, Signal Processing: Image Communication 28 (2013) 670–680
- [19] Ding,D.Pei,A.Salomaa,ChineseRemainderTheorem.ApplicaionsinComputing,Coding,Cryptography,WorldScientificPublishing,1996
- [20] Ding C, Pei D, Salomaa A. Chinese remainder theorem: applications in computing, coding, cryptography. Singapore: World Scientific; 1999
- [21] O.Goldreich,D.Ron,M.Sudan, Chinese remaindering with errors, IEEETrans .Inf.Theory 46(4)(2000)1330-1338.
- [22] Johann GroBschadl: " The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip." Proceedings of IEEE-2008.
- [23] N. Syed Siraj Ahmed, R. Selvakumar, Akshay Taywade ,Public Key Cryptography Algorithm Using Binary Manipulation and Chinese Remainder Theorem, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-5, November 2013

AUTHOR

Dr.O.Srinivasa Rao presently working as Associate professor of CSE, University College of Engineering, JNTUK, KAKINADA. His research field of interest is Computer Networks, Image Processing Network Security and Cryptography,

