Enhanced Hiding Performance based Optimal Value Transfer Image Encryption-Compression System

[1]K Girivasu Reddy, [2]G.V Satyanarayana
[1,2]Dept. of Computer Science Engineering, Raghu Institute of Technology, Visakhapatnam, AP, India

Abstract
In useful situation encryption ought to be performed before the image compression. On the off chance that encryption is not performed then there may be the possibilities of taking the data. In this way we have proposed framework where encryption is done preceding the image compression. Here we have considered both the sorts of pressure - Lossless and Lossy pressure. Pressure is done in the forecast area where specialists figure out the expectation blunder of every pixel then encryption is connected on them by irregular stage. Forecast area gives the abnormal state of security. A large portion of the current ETC arrangements actuate critical punishment on the pressure productivity. In this paper we are proposing another methodology named as "Extemporizing Image pressure System by Random Permutation." where pressure is connected on the bunches of encoded image. So image got at the beneficiary end has every one of the attributes of unique image. Here, the estimation mistakes are altered by ideal worth exchange principle. Additionally, the host image is partitioned into various pixel subsets and the assistant data of a subset is constantly implanted into the estimation mistakes in the following subset. A Recipient can effectively extricate the inserted mystery information and recoup the first substance in the subsets with an opposite request. Along these lines, a great reversible information concealing execution is accomplished.

Keywords
Compression of Encrypted Image, Encrypted Domain Signal Processing, Random Permutation, Clustering

I. Introduction

With the fast improvement of mixed media and system advances, the security of sight and sound turns out to be more vital, since interactive media information are transmitted over open systems more every now and again. Ordinarily, dependable security is important to substance assurance of computerized images and recordings. Encryption plans for mixed media information should be particularly intended to ensure sight and sound substance and satisfy the security necessities for a specific mixed media application. For instance, continuous encryption of a whole video stream utilizing traditional figures requires substantial calculation because of the a lot of information included, yet numerous mixed media applications require security on a much lower level, this can be accomplished utilizing specific encryption that abandons some perceptual data after encryption. Government, military and private business gather incredible arrangement of classified images about their patient (in Hospitals), land territories (in exploration), adversary positions (in guard) item, budgetary status. A large portion of this data is currently gathered and put away on electronic PCs and transmitted crosswise over system to other PC, if these classified images about foe positions, quiet, and land zones fall into the wrong hands, than such a break of security could prompt heaps of war, wrong treatment and so forth. Ensuring secret images is a moral and lawful necessity. We store data in PC framework as records. Record is considered as a fundamental element for keeping the data. Thusly the issue of securing image information or data on PC framework can be characterized as the issue of securing document information. It is overall acknowledged certainty that securing document information is imperative, in today's registering surroundings. Great encryption makes a source look totally irregular, conventional calculations are not able to pack scrambled information. Therefore, conventional frameworks make a point to pack before they encode. We are utilizing the idea of open key encryption, for the encryption and decoding of image. In this open key's of sender and collector is known not however private key's are kept mystery. Neither the security nor the pressure productivity will be relinquished by performing pressure in the encoded area. This methodology outlines the image encryption and after that pressure (ETC) which is suitable for both lossy and lossless images. Additionally the plan is worked on the forecast blunder area. JPEG is utilized for the pressure of the image in light of the fact that it performs well than any others. In this paper our attention is on the pragmatic configuration of a couple of image encryption and pressure plans such that compacting the encoded images is just as productive as packing their unique, decoded image. Additionally sensibly abnormal state of security should be guaranteed.

II. Related Work

CALIC- A Context Based Adaptive Lossless image Codec [1] describes the lossless compression by using prediction error method. Where prediction is depends on the best of eight predictors followed by Huffman coding of prediction error. The LOCO-I Lossless Image Compression Algorithm: Principles and Standardization into JPEG-LS [2] describes lossless compression for continuous tone images. Fixed prediction algorithm is used. Method is very slower. Lossless Compression of Encrypted Grey-Level and Color Images[3] describes compressing encrypted grey level and color images, by decomposing them into bit-planes. A few approaches to exploit the spatial and cross-plane correlation among pixels are discussed. This system is suitable for lossy compression only. Lossless compression is not possible with this system. Encrypted Domain DCT based on homomorphic Cryptosystem [4] is one such a encrypted image Discrete cosine Transform (DCT) tool is used to process encrypted data. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1) calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. DCT allows a large no of processing tasks to be carried out on encrypted images like extraction of encrypted data from encrypted image, embedding watermarking in encrypted image etc. Different types of DCT method: 1D DCT, 2D DCT CD BDCT (block based DCT). DCT performs the operation on image like The disadvantage of this method is

Most of the computation time required to transform, quantize, dequantize, and reconstruct an image is spent on forward and inverse DCT calculations. Because these transforms are applied to blocks, the time required is proportional to the size of the image these times are much longer than for comparable functions written in a low-level language such as C. Size of the image get increases after decryption. Composite Signal Representation for Fast and Storage- Efficient Processing of Encrypted Signals [5] analyzed the possibility of reducing the expansion factor required in signal processing encrypted domain. Applications based on homomorphic encryption by packing together several signal samples into a unique composite word. Provided a general framework extending an idea put forward and derived precise conditions that permit to process the underlying signal by operating directly on the composite words thus achieving a significant gain from a computational complexity perspective. Problem that is left for future research is the development of an efficient protocol that permits to pass from the composite to the sample-wise representation without that the parties involved in the protocol share any secret information. Existing schemes, in fact, are either computationally inefficient or can only be applied to the particular case. Lossy Compression and Iterative Reconstruction for Encrypted Image [6] describes novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can re- construct the principal content of the original image by iteratively updating the values of coefficients. On the other hand, the security of encryption used here is weaker than that of standard stream cipher. Privacy Preserving ECG Classification with Branching Programs and Neural Networks [7] describes Privacy protection is a crucial problem in many biomedical signal processing applications. For this reason, particular attention has been given to the use of secure multi- party computation techniques for processing biomedical signals, whereby no trusted parties are able to manipulate the signals al- though they are encrypted. This paper focuses on the development of a privacy preserving automatic diagnosis system whereby a remote server classifies a biomedical signal provided by the client without getting any information about the signal itself and the final result of the classification. Systems prove that carrying out complex tasks like ECG classification in the encrypted domain efficiently is indeed possible in the semi honest model, paving the way to interesting future applications wherein privacy of signal owners is protected by applying high security standards. Disadvantages of this paper is complexity is very high. On Compression of Data Encrypted With Block Ciphers[8]based on Slepian-Wolf coding and hinges on the fact that chaining modes, which are widely used in conjunction with block ciphers, introduce a simple symbol-wise correlation between successive blocks of data. The compression was shown to preserve the security of the encryption scheme. The existence of a fundamental limitation to compressibility of data encrypted with block ciphers when no chaining mode is employed. But this method is theoretically well suited but practically implementation not works properly.

III. The ETC System

This system includes, the details of the three key components in proposed ETC system, namely, image encryption conducted by Alice, image compression conducted by Charlie, and the sequential decryption and decompression conducted by Bob. Encryption refers to set of algorithms, which are used to convert the plain text to code or the unreadable form of text, and provides privacy. To decrypt the text the receiver uses the "key" for the encrypted text. [7] It has been the old method of securing the data, which is very important for the military and the government operations. Now it has stepped into the civilian"s day-to-day life too. The online transactions of banks, the data transfer via networks, exchange of vital personal information etc. that requires the application of encryption for security reasons. The feasibility of lossless compression of encrypted images has been recently demonstrated by relying on the analogy with source coding with side information at the decoder. However previous works only addressed the compression of bi-level images, namely sparse black and white images, with asymmetric probabilities of black and white pixels. Upon receiving the compressed and encrypted bit stream B, Bob aims to recover the original image I. a multimedia technology for information hiding which provides the authentication and copyright protection.

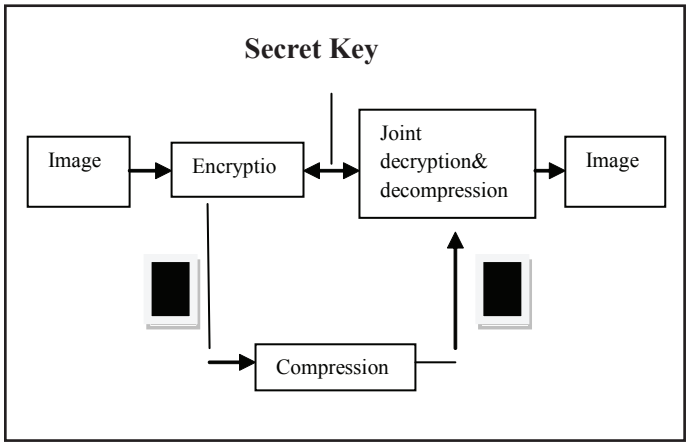

Fig. 1: ETC System

IV. Security Analysis

This section includes, the analysis regarding the security of the proposed permutation-based image encryption method and the efficiency of compressing the encrypted data. The technique involves three different phases in the encryption process.(fig .2) [8]. The first phase is the image encryption where the image is split into blocks and these blocks are permutated. Further permutation is applied based on a random number to strengthen the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key [1]. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The receiver takes the help of the key to construct the secret image in the decryption process. The technique proposed is a unique one from the others in a way that the key is generated with valid information about the values used in the encryption process. Most of the encryption processes first generate the key and then do the encryption process. This technique generates a relation between the encryption process and the key [8].

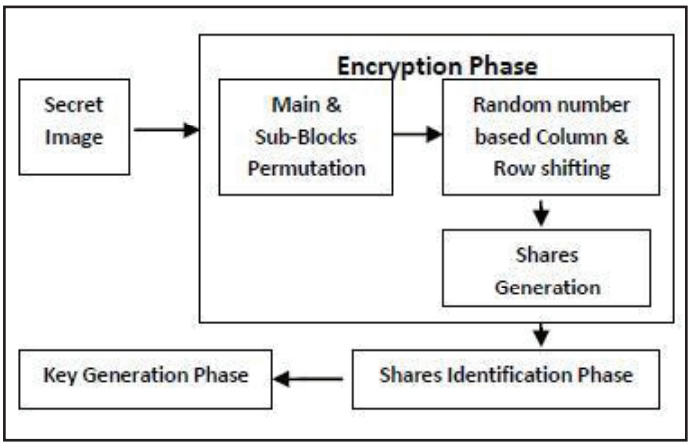

Fig. 2: Image Encryption Process

V. Proposed Technique

This section illustrates the overall technique of our proposed image compression. In this paper we "A Secure Image Encryption-Then Compression System using Prediction Error Clustering and Random Permutation" [9]. In this paper we selects grey scale image to stimulate for encryption and compression. Wavelet transform is the latest method of compression where its ability to describe any type of signals both in time and frequency domain. So researchers take full advantage of the characteristic after wavelet transform and employ proper method to process the image coefficients for achieving effective compression [1,3].

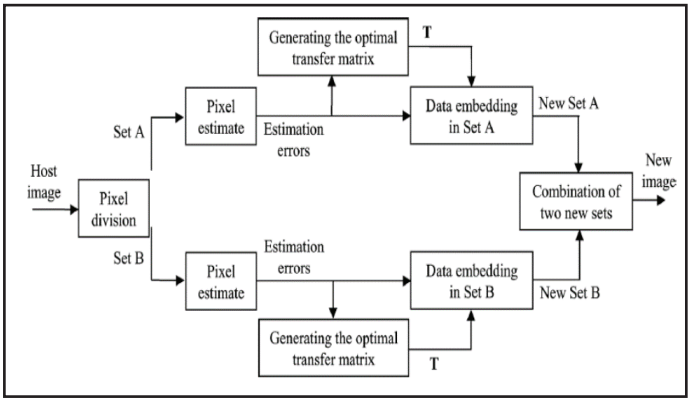

Fig. 3: Proposed System Architecture

A. Why Compression is Needed?

In the last decade, there has been a lot of technological transformation in the way we communicate. This transformation includes the ever present, ever growing internet, the explosive development in mobile communication and ever increasing importance of video communication. Data Compression is one of the technologies for each of the aspect of this multimedia revolution. Cellular phones would not be able to provide communication with increasing clarity without data compression. Data compression is art and science of representing information in compact form. Despite rapid progress in mass-storage density, processor speeds, and digital communication system performance, demand for data storage capacity and data-transmission bandwidth continues to outstrip the capabilities of available technologies. In a distributed environment large image files remain a major bottleneck within systems. Image Compression is an important component of the solutions available for creating image file sizes of manageable and transmittable dimensions. Platform portability and performance are important in the selection of the compression/decompression technique to be employed. [2][3]

B. Why we Need Image Encryption?

If security of the image is paramount, then the usual method is to take the image file and encrypt that like any other data file. This has several drawbacks: first, if you're not well-educated in cryptography and computer programming, you have to run out and buy somebody else's encryption software. Then there's the very likely possibility that the software company or some government agency has a 'backdoor' method of reading files encrypted by the software. Finally, any cryptographic system that isn't based on a random, one-time key is theoretically breakable. Encryption is the technology of keeping information secret. In this context, we define secret as "being protected from unauthorized access and attack." Although you may not think of your graphics files or their contents as ever being under attack, you may want to keep the information contained in these files from being copied or viewed by unauthorized people or computers. If copies of the files are freely available, the only way to keep the files secret is to encrypt them. Cryptography may seem to be a black art requiring extremely complex mathematics and access to supercomputers. This may be the case for professional cryptanalysts (code breakers). But for ordinary people who need to protect data, cryptography can be a strong, often simple to use, and sometimes freely available tool. This section doesn't try to explain cryptography, nor the details of particular cryptosystems [4].

C. Principle behind Image Compression

Images have considerably higher storage requirement than text; Audio and Video Data require more demanding properties for data storage. An image stored in an uncompressed file format, such as the popular BMP format, can be huge. An image with a pixel resolution of 640 by 480 pixels and 24-bit colour resolution will take up 640 * 480 * 24/8 = 921,600 bytes in an uncompressed format. The huge amount of storage space is not only the consideration but also the data transmission rates for communication of continuous media are also significantly large. An image, 1024 pixel x 1024 pixel x 24 bit, without compression, would require 3 MB of storage and 7 minutes for transmission, utilizing a high speed, 64 Kbits /s, ISDN line. Image data compression becomes still more important because of the fact that the transfer of uncompressed graphical data requires far more bandwidth and data transfer rate. For example, throughput in a multimedia system can be as high as 140 Mbits/s, which must be transferred between systems. This kind of data transfer rate is not realizable with today's technology, or in near the future with reasonably priced hardware [5].

D. Discrete Wavelet Transform

The discrete wavelet transform (DWT) refers to wavelet transforms for which the wavelets are discretely sampled. A transform which localizes a function both in space and scaling and has some desirable properties compared to the Fourier transform. The transform is based on a wavelet matrix, which can be computed more quickly than the analogous Fourier matrix. Most notably, the discrete wavelet transform is used for signal coding, where the properties of the transform are exploited to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. The discrete wavelet transform has a huge number of applications in Science, Engineering, Mathematics and Computer Science. [6][10] Wavelet compression is a form of data compression well suited for image compression (sometimes also video compression and audio compression). The goal is to store image data in as little space as possible in a file. A certain loss of quality is accepted (lossy compression). Using a wavelet transform, the wavelet

compression methods are better at representing transients, such as percussion sounds in audio, or high-frequency components in two-dimensional images, for example an image of stars on a night sky. This means that the transient elements of a data [10].

E. Clustering

Clustering can be considered the most important unsupervised learning problem; so, as every other problem of this kind, it deals with finding a structure in a collection of unlabeled data. A loose definition of clustering could be "the process of organizing objects into groups whose members are similar in some way". A cluster is therefore a collection of objects which are "similar" between them and are "dissimilar" to the objects belonging to other clusters [5].

VI. Experimental Results

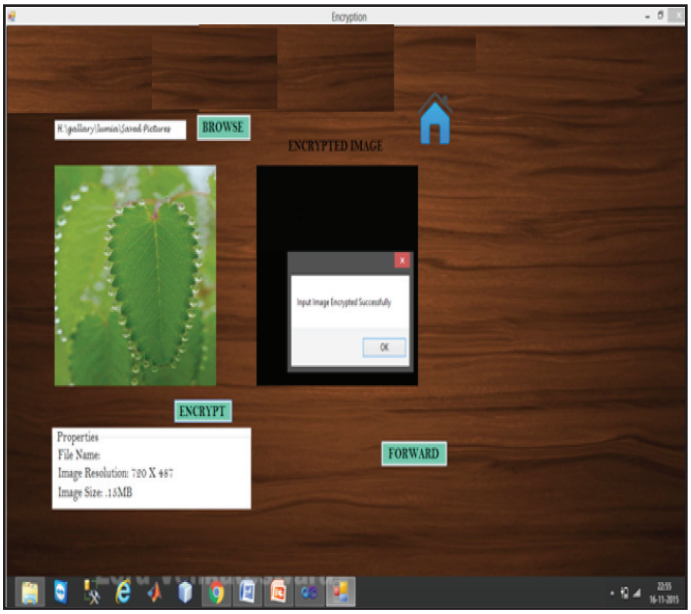

Fig. 4:

The image is been uploaded and preprocessed. After preprocessing we decrypt the image. The decrypted images will be forwarded to mediator.

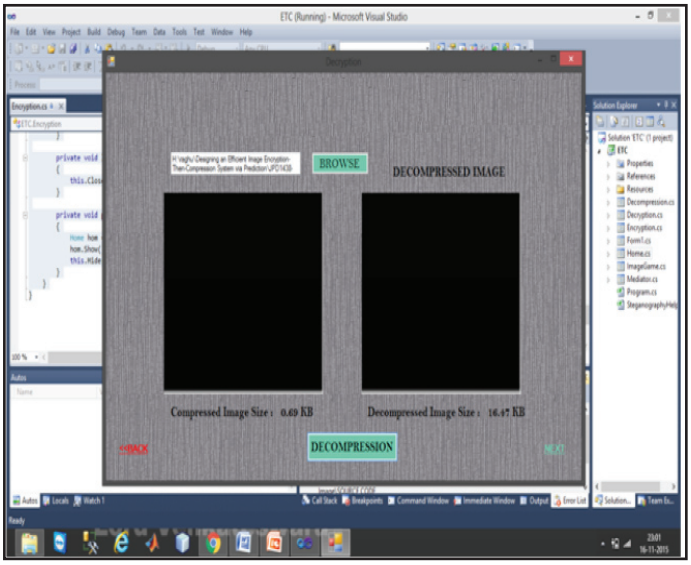

Fig. 5:

The image which is encrypted is now decrypted and forwarded to the destination.

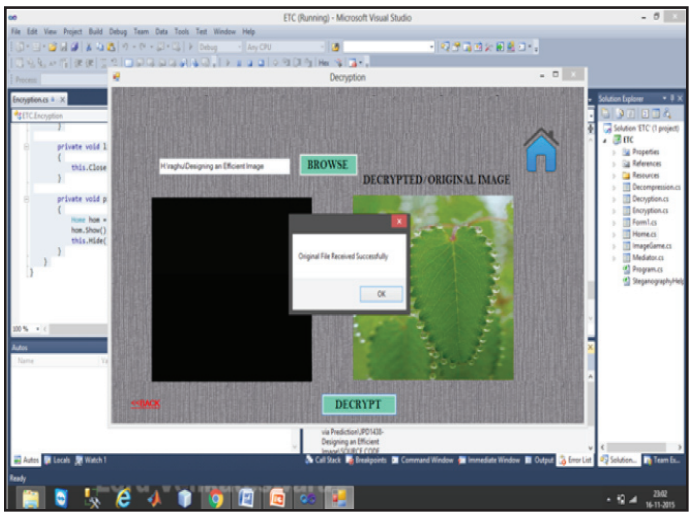

Fig. 6:

The decompressed image now decrypted at the destination and original is obtained.

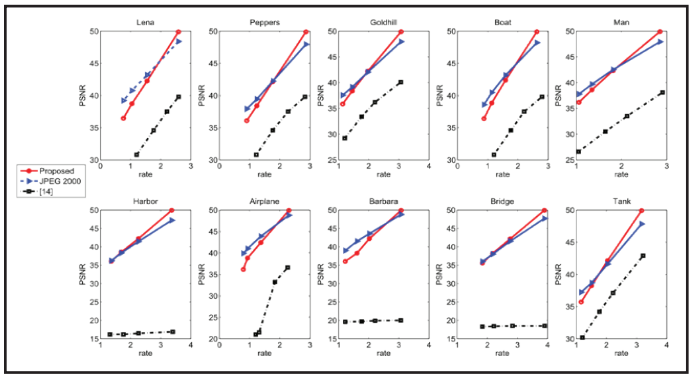

Fig. 6: Comparison of the rate-PSNR Performance

VII. Conclusion

Proposed System is used to design a pair of image encryption and compression technique such that compressing encrypted images. The image encryption has been achieved via random permutation. And compression is achieved by using arithmetic coding where both lossy and lossless compression is considered. The analysis regarding the security of the proposed permutation-based image encryption method and the efficiency of compressing the encrypted data. For lossless compression and data hiding optical value transfer method can also be used. We have designed an efficient image Encryption then Compression (ETC) system. Within the proposed work, the image encryption has been achieved via prediction error clustering and random permutation. Efficient compression of the encrypted data has then been done by arithmetic coding approach. By Arithmetic Coding based, Coding can't be cracked. Both theoretical and experimental results have shown that reasonably high level of security has been retained. The coding efficiency of our proposed compression method on encrypted images is very close to that of the image codec's, which receive original, unencrypted images as inputs. The Compressed image is measured in terms of Quality measures like MSE and PSNR.

References

[1] A. Kumar, A. Makur,"Distributed source coding based encryption and lossless compression of gray scale and color images", In Proc. MMSP, 2008, pp. 760–764.

[2] D. Schonberg, S. C. Draper, K. Ramchandran,"On blind compression of encrypted correlated data approaching the source entropy rate", In Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.
[3] Z. Erkin, T. Veugen, T. Toft, R. L. Lagendijk,"Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, Vol. 7, No. 3, pp. 1053– 1066, Jun. 2012
[4] T. Bianchi, A. Piva, M. Barni,"On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, Vol. 4, No. 1, pp. 86–97, Mar. 2009.
[5] X. Zhang,"Lossy compression and iterative recobstruction for encrypted image," IEEE Trans. Inf. Forensics Security, Vol. 6, No. 1, pp. 53–58 Mar. 2011
[6] X. Zhang, G. Sun, L. Shen, C. Qin,"Compression of encrypted images with multilayer decomposition," Multimed. Tools Appl., Vol. 78, No. 3, pp. 1–13, Feb. 2013.
[7] Jiantao Zhou, Xianming Liu, Oscar C. Au, Yuan Yan Tang, "Designing an Efficient Image Encryption-Then Compression System via Prediction".
[8] "Error Clustering and Random Permutation" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.
[9] SeshaPallaviIndrakanti,"Permutation Based Image Encryption Technique", Associate professor, Department of Computer Applications, GVP Degree College (A),Visakhapatnam. International Journal of Computer Applications, Vol. 28, No. 8, 2011.

K.Girivasu Reddy pursuing hisM. Tech in the department of Computer Science and Engineering, Raghu Institute of Technology,Dakamarri Village, Bhimunipatnam Mandal, Visakhapatnam, A.P., India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI. He obtained his B.Tech(CSE) from Avanthi Institute of Engineering and Technology, Visakhapatnam.

Dr. G.V. Satyanarayana, M.Tech, Ph.D working as Professor in the department of Computer Science and Engineering, Raghu Institute of Technology, Dakamarri Village, Bhimunipatnam Mandal, Visakhapatnam, A.P., India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, NEW DELHI. His research fields are in Embedded Systems, Data Mining and Network Security.