ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Reserving Space for Embedding Data in Encrypted Images

P.Manjusha, Dr.R.China Appala Naidu, G. Keerthi, K. Meghana

Assistant Professor, Dept. of I.T., St Martin's Engineering College, Hyderabad, India

Professor, Dept. of CSE, St Martin's Engineering College, Hyderabad, India

Assistant Professor, Dept. of I.T., St Martin's Engineering College, Hyderabad, India

M.Tech Student, VITS, Vishakapatnam, Andhra Pradesh, India.

ABSTRACT: Now a days provide security for images is very difficult for providing security to the images we present a novel approach for steganography images on encryption key. The advantage of steganography technique is, it takes the limited power of human visual system[HVS]. Steganography technique uses image as enclosed medium for embedding covert letter. Reversible data hiding for steganography images is very reliable, because it maintain the superlative property that the original image can be lossless recovered even after the extraction of embedded data while protecting the key content's confidentiality. we propose steganography technique for embedding steganography image. So that, the confidentiality of the original image will improve more and more because the encryption key which is used for encrypting image is secured with steganography technique and RDH technique.

KEYWORDS: RDH(Reversible Data Hiding), Steganography, Data embedding, Image recovery, HVS.

I. INTRODUCTION

RDH in images is a technique, by which reserving the original content without loss after the embed may is extracted [1]. The various applications using RDH techniques are like military imaginary, medical imaginary and law forensics where no loss of original cover is allowed. In Theoretical ,Kalker and Willems[2] established a accuracy and complexity of rate-distortion model for Reversible Data Hiding, proposed a construction for a recursive code and rate-distortion bounds of RDH for memory less covers. To improve Kalker and Willems's method, zhand et al[3] improved conversion techniques for recursive to binary proved to be very useful algorithm for compression which reaches the entropy level.

In practical aspect, there are so many RDH techniques have emerged in recent years. There are two promising strategies for RDH techniques[4], they are one is difference expansion[DE] and histogram shifting[HS]. In histogram shifting [HS] bins of histogram of gray values are shifted for data embedding process. In least significant bit [LSB] zeros are considered for data embedding and expanding each pixel group. In difference expansion[DE], the difference of pixels is extracted and the LSB difference must be equal to zero, which is exhibited in the message embedding.

Steganography is used mainly for cover image and essentially means "to hide in plain sight". As defined by cachin[7] , steganography is the method in which message cannot be detected it is the invention in arts and science communication. From Ages onwards we are using different steganography techniques that made information hiding simpler. Thorough this document we are trying to examine applications on steganography and principles related to it. We focus on discovering why steganography is playing vital role in the current generation. We also consider the issues related to hiding of data that are placed in different files at various locations and attacks that violate the data by the usage of bypass steganography.

In other words, Steganography is define as embed hidden image from sender and receiver suspecting the existence of message. The word steganography means "obscure writing" which was defined from Greek word staganos means obscured or protected and graphy means "to embed". Steganography is also define as technique of hidden message in choose carrier in which intended recipient is aware of its existence one.

Fig1 shows how data hiding is broken into different sections which is an analysis of steganography technique by popa[8] steganography is used to hide a data proposed for later recovery by a specific person (or) group. In this case what we have to do is to take care of data by preventing from the third party.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

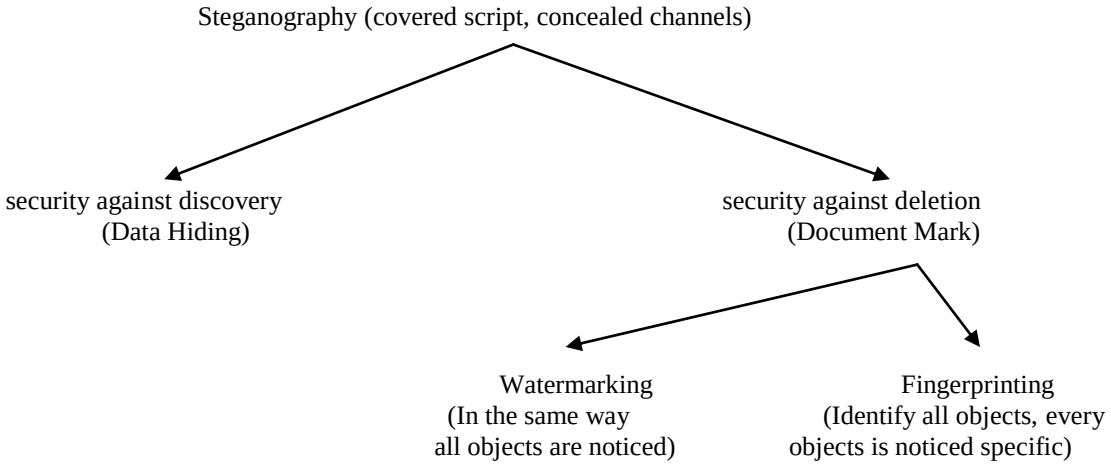


Fig. 1 Types of Steganography

Representation of steganography process by using generic embedding and decoding is shown in Fig 2 In order to produce the stegno image we have to embed a secret image into it then only we can acquire a stegno image. In sequence of steps we start with initial step that is to pass both secret message and cover message into the encoder and which is intern embedded by the information to be hided. Several rules are taken into consideration while performing encoding process in this process we ensure that we insert a secret message and cover message into the encoder. The type of procedure will depend on what data we are going to embed and what we are embedding it in. For an instance information inside the messages will be embedded into image by using set of rules. A Key is often is needed in the embedding procedure. This is in the form of a public or private key so we can encode the secret message with private key and the receiver can decoded using a public key, By this way we can reduce the chance of a attacker getting hold of the stegno object. From the stegno images and decoding it to find out the secret information.

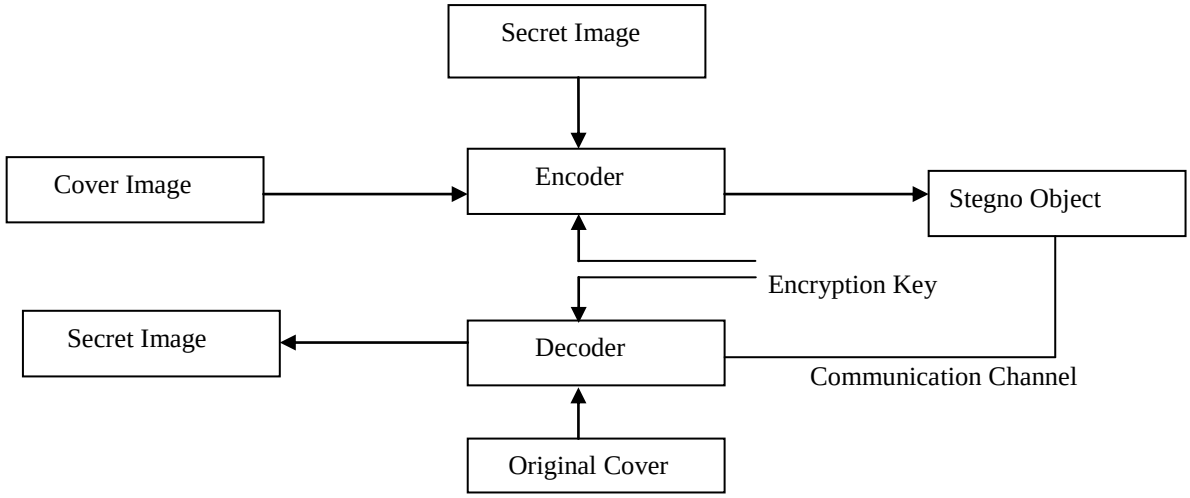


Fig. 2 Generic Process of Encoding and Decoding

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

II. RELATED WORK

In [1] authors said that in now a days public paid more attention for reversible data hiding for encrypting images because this method is very reliable for reserving enough space for data embedding process which is done later. In [2] authors said that information theories in RDH methods reaches bounds for covers and proposed a code for construction recursively but the drawback of this approach is it doesn't reach the bound. In [4] author said that there is a framework in reversible data hiding, in which we first performs extraction operation for compressible features of original image by which we can save the empty space for data embedding. In [7] author said that in steganography method no third party or intruder can find the hidden data. And the techniques in steganography are very reliable for data embedding.

III. PROPOSED SYSTEM

In the this paper we make use of reversible data hiding and apart from that we also make use of steganography techniques , this is the novel approach for images. In the proposed method, we first encrypt the image by using encryption key, Later we reserves space for data embedding by enclosing Least Significant Bits of some pixels into other pixels with traditional RDH method to that original images, so the positions of LSBs in the image can be used to embed data.

The content owner has to reserve the enough space for the original image. Now encrypted image in process is inherited reversibility for the data hider needs to accommodate the data in spare space which is empted out. As, standard RDH algorithm is an ideal operator for reserving the data before encryption and it is easy to apply the framework for RRBE to achieve the better performance compared to previous art.

Fig 3 shows the Architecture for Encrypting and Embedding the image by reserving room to embed the additional data.

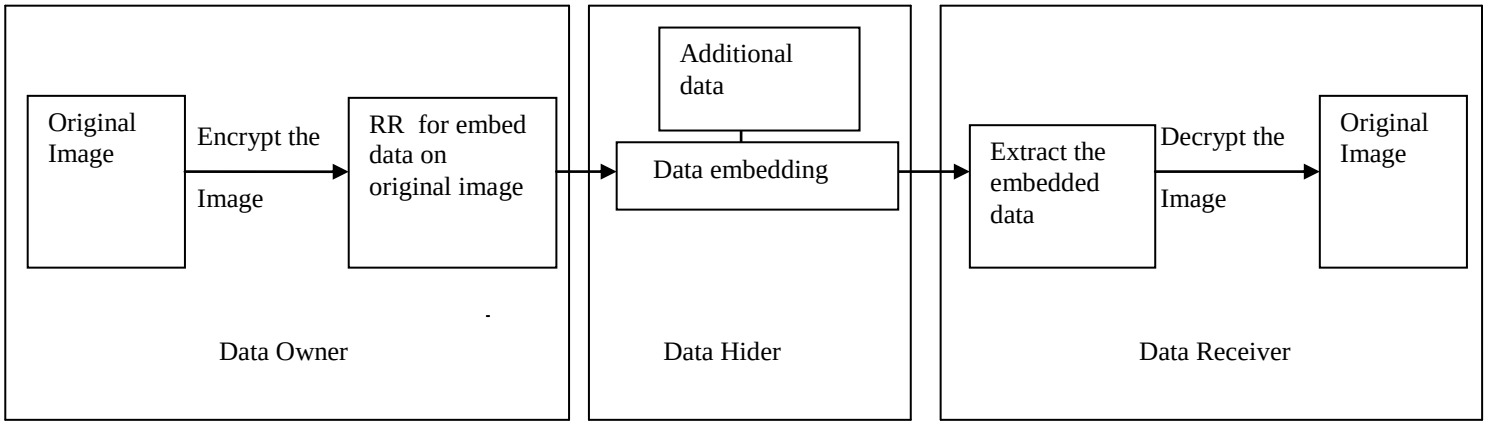


Fig: 3 Architecture for Encrypting and Embedding image

Encrypting the image with respective privacy involves the idea of loosely compression of image (E.g. using RDH technique) and the encrypts with respect to protect the privacy. Next we expand the practical method framework RRBE which consists of four stages,

- Image partition
- Data embedding
- Data extraction
- Image recovery

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

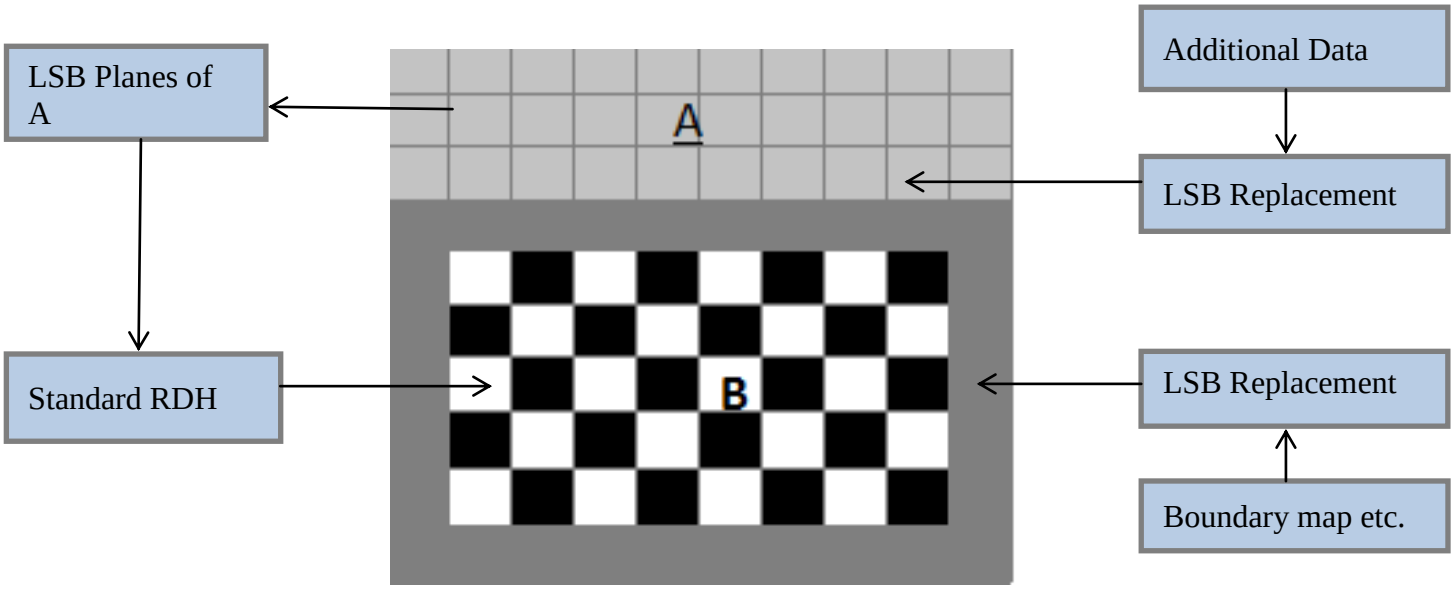
Vol. 3, Issue 11, November 2015

A. Image partition:

We use standard RDH technique for reserving room before encryption. So that the goal at image is to construct a smooth area 'B' on RDH algorithm. To do that assume the image 'C' with 8-bit gray scale at size M X N pixel $C_{i,j}\varepsilon$ [0,255], $1\leq i\leq M$, $1\leq j\leq N$. The content owner first extracts the original image along the rows, several overlapping is determined with the size of embedded message which is denoted by *l*. Second as every block consists of M rows where *m= [l/N]*,and number of blocks *n = M-m+1*.. Each block is overlapped by previous sub sequential blocks along with the rows. Each block defines a function which measures the first order smoothness function.

$$f = \sum_{u=2}^{m}\sum_{v=2}^{N-1}\left|C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4}\right|$$

Higher value of 'f' contains more complex textures that relates to the blocks of owner which selects the particular with highest 'f' to be 'A'. Image concatenation bits the font image by rest of the park 'B' with textured area, as shown in the fig 1.4. The above discussion realizes the fact on single LSB plane of 'A' which is regarded. Two (or) more LSB planes are embedded from a A to B in content owner which leads to half (or) more than half reduction in the size of 'A'. In FSNR the performance of 'A' alter data embedding decreases with the growth of bit planes exploded in second stage. Therefore in this paper we explore the situations of 3 LSB planes of 'A' are employed and determine the number of bit plane with different pay loads in next section.



Self-Reversible Embedding

By employing traditional RDH algorithm LSB planes are embedded to A * B. This is the main aim of self reversible embedding the simple example for the above illustration of self embedding can be as follows,

Consider two sets of image B each image is divided in the form of pixels and for calculating white pixels with the indices INJ we have to calculate (i+j) mod2=0 for calculating black pixels (i+j) mod2=1 and resultant value of i+j indices when modulated by 2 results 0 it leads to white pixels else vice versa if it is , it is black pixel.

$$B'_{i,j} = u_1B_{i-1,j} + w_2B_{i+1,j} + u_3B_{i,j-1} + w_4B_{i,j+1},$$

Weight W should always range as the lesser value of I and it should be less than or equal to '4' and overall range should be between 1 and 4 [1<=i>=4] .Error is calculated as $e_{i,j} = B_{i,j}$-B the error sequence helps in generating messages which can be accommodated further. By calculating error in black pixels errors surrounded i.e., white pixels can be calculated . Multilayer embedding is done only by considering original modified 'B'. For single layer embedding we consider two error sequences.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

B. Data Embedding:

In previous days people use to hidden data in plain sight which was called steganography throughout ages, the recent days in computational powers and technology has improved to the fore part of today's security techniques. In modern days steganography is use to attempt the detectable part only if secret information is known, like secret key this is similar to kerckhoff's principle which holds cryptography system key material. The unmodified cover media should be kept secret for the steganography to remain undetectable because if it expose, a comparison between cover and stegno express the changes immediately. Information theory is more specific on what it means for a system to be perfect security. Information theoretical model for steganography was imposed by Christian cachin, who consider the security for the steganography system against passive eavesdroppers. In this model we assume that the advisory person doesn't know the complete knowledge of secret key in encoding system. So the model is to advice for the probability distribution P_c and P_s for all possible stegno cover media. Now the advisory person can then views the detection theory between hypothesis 'c' and hypothesis 's'.

In this we use JPEG image because,

- Jpeg is most common format for the image.
- Jpeg format is more interesting because system operators in transform space and/or not effected by visual attacks.
- Steganography systems for palette-based images leaving easy detected distortions.

Following , we see some steganography systems how they encode the algorithm in changing an image in detectable way. And also will compare the different systems and construct there relative effectiveness.

1. Discrete cosine Transform:

Discrete cosine Transform (DCT) transform into 8X8 pixel, blocks of image into 64 DCT coefficient in JPEG image format for each colour component. 8X8 block of image pixels f(x,y) for DCT coefficient F(u,v) are given by,

$$F(u,v) = \frac{1}{4}C(u)c(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2x+1)v\pi}{16}\right]$$

Where, c(x)= 1/√2 when x=0,
C(x)=1 when x>0. Next the following operation quantified the coefficient.

$$F^{Q}(u,v) = \left\lfloor\frac{F(u,v)}{Q(u,v)}\right\rfloor$$

Where, Q(u,v) is 64 elements of qunatisize table. We can use the least significant bits of quantified DCT coefficient to embedded the hidden message the modification which have done in single DCT coefficient will effect all the 64 image pixel. Steganography system that modifies LSB of image visual structure are often suspect able to visual attacks, but this is not true for JPEG because the modifications are in frequency domain instead of spectral domain, so there are no visual attacks against JPEG format.

2. Sequential:

Jsteg was the mostly used algorithm for Steganography system for embedding image which is developed by Derek Upham. In this algorithm for embedding data it replaces the least-significant bit of DCT coefficient sequentially with the data which is used. Let us see the algorithm for Jsteg ,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Input: data, original image
Output: stego image
While message left to embed **do**
get next DCT coefficient from original image
if DCT ≠0 and DCT ≠1 then
get next LSB from data
replace DCT LSB with data LSB
end if
insert DCT into stego image
end while

C. Data Extraction and Image Recovery:

After the completion of data embedding process of image, the image which is also known as vessel image is forwarded to receiver. At receiver's side first we have to extract the embedded data and later we have recover the original image by using decryption key. For this process we are using some Traditional RDH methods[10][11].

The following are the steps which are used for data extraction and image recovery:

- Step1: Archive The LSB-planes of A'' for decrypting the data hiding key, and then perform extraction until the end point reached.
- Step2: From LSB marginal area of B'' extract the boundary map along with *LN, RN, LM, RM, LP, RP,* R_b, *X* .
- Step 3: To scan B'' the procedure will be as follows, If $R_b = 0$, then it means, in data embedding process black pixels are not competed. Goto Step 5.
- Step 4: Recover estimating error $e'_{i,j}$ by calculating $e'_{i,j}$ of the black pixels $B''_{i,j}$ when $B''_{i,j} \in [1,254]$ and retrieve the original pixel values. When $e'_{i,j}$ = *LN LM* (or *LP),RM* (or *RP*) and *RN* perform extraction operation on embedded bits. if $B''_{i,j} \in \{0,255\}$ means to the bit b to in boundary map , if b=0, skip this one else perform as $B''_{i,j} \in \{1,254\}$. Reiterate this until the extraction of payload $R_b$is done. If LSBs pixels in marginal area same as extracted bits, restore them instantly.
- Step 5: Recover estimating error $e'_{i,j}$ by calculating $e'_{i,j}$ of the white pixels $B''_{i,j}$ along with extraction of embedded bits. If LSBs pixels in marginal area same as extracted bits, restore them instantly.
- Step 6:repeat the process from step 2 to step 5 x-l whole on B''& perform merging of all extracted bits to obtain LSB-Planes of A.
- Step 7:Supersade LSB-planes of A which are marked with original bits of B which are extracted to acquire original image C.

IV. CONCLUSION

Reversible data hiding is very useful for preserving privacy in cloud, because it benefits the data hider to embed the image on original image effortlessly by using steganography techniques. RDH method is very reliable for reserving empty space in image before encryption by this we can achieve a magnificent performance for plain images without losing secrecy. Steganography is really very interesting topic for embedding data or image in meaningful cover image or original image by which security of the original image is improved because if any intruder hacks encryption key then the original image is secured by embedded image.

REFERENCES

1. Kede Ma, Weiming Zhang, Xianfeng Zhao., "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", in IEEE Transactions On Information Forensics And Security, Vol. 8, No. 3, Marc 2013.
2. T. Kalker and F.M.Willems., "Capacity bounds and code constructions for reversible data-hiding", in Proc. 14th Int. Conf. Digital Signal Processing(DSP2002), 2002, pp. 71–76.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

3. W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding", in Proc 13th Information Hiding (IH'2011),LNCS 6958, 2011, pp. 255–269, Springer-Verlag.
4. J. Fridrich and M. Goljan, "Lossless data embedding for all image formats", in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA, USA, vol. 4675, pp. 572–583, Jan. 2002.
5. J. Tian., "Reversible data embedding using a difference expansion", IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.
6. Z. Ni, Y. Shi, N. Ansari, and S. Wei., "Reversible data hiding", IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
7. Christian Cachin.,"Digital Steganography", IBM Research Zurich Research Laboratory CH-8803 , Ruschlikon, Switzerland, February 17, 2005.
8. Sanjeevkumar , Balasubramanian Raman And Manoj Thakur., "Real Coded Genetic algorithm Based Stereo Image Watermarking", International Journal of Secure Digital Information Age, 1, No.1, June 2009.

BIOGRAPHY

1. **P. Manjusha** completed her M.Tech from JNTU Hyderabad and she has 1 year of teaching experience. She is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. Her area of interest is Network Security, Computer Networks, Mobile Computing and Compiler Design.

2. **Dr.R.Ch.A.Naidu** completed his M.Tech from University of Mysore, Mysore and Ph.D from Andhra University, Vishakhapatnam. He has more than 14 years of teaching experience. He is presently working in CSE Dept as a Professor in St Martin's Engineering College, Hyderabad. He has life membership in professional bodies like ISTE, CSI. His area of interest is Network security, Computer networks, Digital Image processing, Data base management systems, Data Mining, BIG Data.

3. **G. Keerthi** completed her M.Tech from JNTU Hyderabad and she has 3 year of teaching experience. She is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. Her area of interest is operating system, Computer Networks, Information Security and Software Engineering.

4. **K.Meghana** completed her B.Tech from JNTU Kakinada in the year of 2014. Now she is doing her M.Tech in VIT, Vishakapatnam in CSE department. She published 4 papers in international journal. Her interested areas are Network security, Data management systems, Automata and Compiler design.