AN IDEAL STEGANOGRAPHIC SCHEME IN NETWORKS USING TWISTED PAYLOAD

Logesh R[1], M Hemalatha[2], A Ramalingam[3], Kanimozhi K[4]

[1]M.Tech Scholar, [2]Assistant Professor, [3]Associate Professor,
[1, 2, 3]Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India
[4]Researcher, Puducherry, India,
logeshr@outlook.com, hemalathamohanraj@gmail.com, a.ramalingam1972@gmail.com, mail4kanimozhi@gmail.com

Abstract

With the rapid development of network technology, information security has become a mounting problem. Steganography involves hiding information in a cover media, in such a way that the cover media is not supposed to have any confidential message for its unintentional addressee In this paper, an ideal steganographic scheme in networks is proposed using twisted payload. The confidential image values are twisted by using scrambling techiques.The Discrete Wavelet Transform (DWT) is applied on cover image and Integer Wavelet Transform (IWT) is applied to the scrambled confidential image. Merge operation is done on both images and Inverse DWT is computed on the same to get the stego image. The information hiding algorithm is the reverse process of the extracting algorithm. After this an ideal steganographic scheme is applied which generates a stego image which is immune against conventional attack and performs good perceptibility compared to other steganographic approaches.

Index Terms: *Network security, Steganography, Discrete Wavelet Transform, Integer Wavelet Transform, Modified Arnold Transform, Merge Operation, Quality Measures*

--***--

1. INTRODUCTION

The continuing improvements in computer technologies and the increase in Internet usage are responsible for the increasing popularity of network-based data transmission. In the field of network security, several techniques are being developed to overcome unauthorized attacks and to protect the secret information during transmission. Network security problems can be categorized roughly into four areas: secrecy, authentication, non-repudiation and integrity control. Secrecy concerns with keeping the information away from the unauthorized users, which means unauthorized users, cannot be able to read and/or understand the information on transit. There are mainly two techniques to achieve secrecy. They are: cryptography and Steganography.

Steganography is used to securely transmit information in open networks. Steganography is an important aspect of security in communications. Digital communication has become an essential part of infrastructure now-a-days, a lot of applications are Internet based and in some cases it is desired that the communication be made secret. Steganography provides to hide the secret information and make communication undetectable. The main goal of Steganography is higher capacity and security of the confidential message.

In Steganography the secret information is hidden inside another file without degrading the quality of that file such that the intruder will not suspect any communication that is happening. Steganography is one such means of achieving security by hiding the data to be communicated within a more innocuous data. The carrier file or cover file can be an image, audio, video or text file. Steganography is used to hide the secret information so that no one can sense the information.

2. LITERATURE STUDY

Review of related work has been conducted on an ideal steganographic scheme in network using twisted payload. Nowadays, Steganography has become the focus of research for copyright protection. Fei Peng et.al., [1] presented a new reversible data hiding algorithm based on integer transform and adaptive embedding. This allows embedding more data bits into smooth blocks while avoiding large distortion generated by noisy ones, and thus enables very high capacity with good image quality. Using combination of IWT and LSB, reversible data hiding provides ideal solution. The technique allows one to embed data in host image, exactly reconstructed from the marked content. Vijay Kumar et al.,[2] proposed a copyright protection scheme that combines the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).

Here first DCT coefficient of secret image and cover image is extracted and then applied DWT coefficients on both separately. Two different secret keys are used for hiding of extracted features of DCT coefficients in the features of cover image. Weiqi Luo et.al.,[3] presented Edge Adaptive Image Steganography Based on LSB Matching Revisited. He used LSB and threshold based algorithm and achieved good visual quality and high security.

Fawzi Al-Naima et al.,[4] proposed a modified high capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion on the cover image with high levels of overall security.

Sumanth Sakkara et al.,[5] has presented proposed method that uses the secret information as a text message which is embedded in a color image. The existing methods hide the information using constant bit length in integer wavelet coefficients. This paper uses variable bit length based on integer wavelet coefficients to hide the data in a particular positions using secret key by LSB substitution method. Hence this algorithm increases the embedding capacity of the text message and obtained stego image is imperceptible for human vision. Gandharba Swain et.al [6] presented a quick review of network security and steganography and also discussed classification of network security techniques. He also emphasized on steganography techniques also.

This paper is prearranged in the subsequent section. Methodology of our proposed technique is explained in section 3. Section 4 begins our proposed model. Testing and quality measures discussed in section 5. Performance analysis is discussed in section 6. Result analysis is illustrated in section 7. Conclusion is discussed in section 8. Finally references are given in the last section.

3. METHODOLOGY

3.1 Preprocessing

The preprocessing performs a variety of basic operations to eliminate known distortion from the image being compared. Pre-processing methods use a small neighborhood of a pixel in an input image to get a new brightness value in the output image. Histograms are functions describing information extracted from the image. The histogram function is defined over all possible intensity levels. For each intensity level, its value is equal to the number of the pixels with that intensity.

3.2 Pixel Value Adjustment

The gray scale cover image and confidential pixel intensity values vary from zero to 255. During the confidential hiding process the intensity values of cover image may exceed lower and higher levels which results in difficulty to retrieve the confidential information at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240 instead of zero and 255.

3.3 Discrete wavelet transform

DWT are applied to discrete data sets and produce discrete outputs. DWT eliminates the ‘blocking’ artifacts that deprive the reconstructed image of the desired smoothness and continuity. Wavelets convert the image into a series of wavelets that can be stored more efficiently than pixel blocks. Discrete wavelet transforms map data from the time domain to the wavelet domain. The result is a vector of the same size.

When applying discrete wavelet transform on an image, four different sub-images are obtained as follows : LL (Approximation Band): A coarser approximation to the original image containing the overall information about the whole image. It is obtained by applying the low-pass filter on both x and y coordinates. HL (Vertical Band) and LH (Horizontal Band) : They are obtained by applying the high pass filter on one coordinate and the low-pass filter on the other coordinate. HH (Diagonal Band) : Shows the high frequency component of the image in the diagonal direction. It is obtained by applying the high-pass filter on both x and y coordinates.

3.4 Integer wavelet transform

In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may make the loss of the hidden information which may lead to the failure of the data hiding system.

Integer Wavelet Transform is a Non linear transform having a structure of lifting scheme and as its rate has less distortion. The performance value is similar to DWT. Wavelet transforms that map integers to integers allow perfect reconstruction of the original image. Integer wavelet transform make an integer data set into another integer data set. The use of such wavelet transform will mainly address the capacity and robustness of the information hiding system features.

3.5 Scrambling based on Modified Arnold Transform

Image scrambling is an important method of image encryption. Its main purpose is to make the target image scrambled so that no one is able to find the true meaning of the image by using human visual system (HVS) or computer system. To transform a meaningful image into a meaningless or disordered image, enhance the security which in turn enhances the power to resist the invalid attack.

The Arnold transform [7] of the matrix and then a new matrix can be obtained in order to achieve image scrambling processing. Set the image pixel coordinates. N is the order of the image matrix, i, j € (0, 1, 2, N−1) and the Arnold transform is defined as equation as

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i' \\ j' \end{bmatrix} (\text{Mod N}) \qquad (1)$$

It can easily be seen that the original Arnold transformations given by equation (1) can be modified to produce a sequence of Arnold transformations as given in equation (2) which representing modified Arnold transform equation.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} i & i+1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{Mod N}) \qquad (2)$$

where $i \in \{1,2,3 \ldots.\}$, The above transform is one-to-one correspondence, the image can do iteration. The Iteration number can be used as a secret key for mining the confidential image. This transformation gives more security and robustness to our algorithm.

3.6 Merge Operation

Add the wavelet co-efficient of both images, due to merge operation Alpha multiplier gives deep depth value to hide the secret image. This approach is capable of achieving more security, imperceptibility, and certain robustness. All the pixels of a image in spatial domain are multiplexed by embedding strength factors alpha or beta. Since alpha and beta are chosen, such that payload is not predominantly seen in the stego image.

Stego image looks very similar to original cover image and produces results in the statistical evaluation. The stego image is obtained using the twofold transform technique and by applying merge operation, such as logical operation, arithmetic operation. The arithmetic operations of multiplication, division, addition and subtraction have been combined in different ways to achieve a better merge effect.

4. PROPOSED WORK

In this section, an ideal steganographic scheme in networks using twisted payload is presented. The proposed method creates high quality stego image thereby increasing security. This proposed method can achieve high embedding capacity and acceptable image quality of stego-image with excellent PSNR value. The capacity of the proposed algorithm is increased as the only approximation band of secret image is considered.

In this scheme, the characteristics of the both integer wavelet transform and discrete wavelet transform is proposed. The diagrammatic representation of information hiding and mining model was shown in Fig-1 and Fig-2. Information hiding process and information mining process will be discussed in section 4.1 and 4.2.

4.1 Information Hiding Process

- Read the cover image and secret image.
- Convert the pixel values of cover image and secret image into a grayscale cover and confidential image.
- Apply PVA on cover image.
- Apply Modified Arnold transform on Confidential image by using secret key to get a scrambled confidential image.
- Apply two fold transforms technique into cover grayscale image and confidential gray scale image.
- By apply merge operation on both images to get stego image.

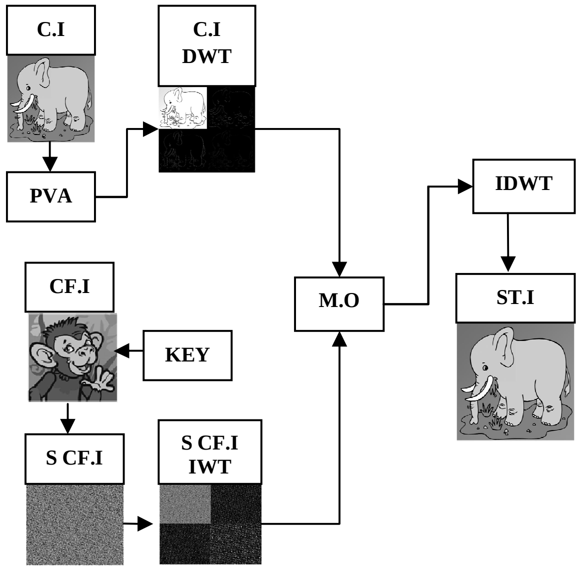


Fig-1: Information Hiding Model [C.I – Cover Image, M.O – Merge Operation , CF.I - Confidential Image, S CF.I – Scrambled Confidential Image, ST.I – Stego Image, IDWT – Inverse Discrete Wavelet Transform]

4.2 Information Mining Process

- Receive the stego image.
- Perform a twofold transform at the level of both stego image and known cover image using merge operation.
- Separate the wavelet coefficients and take inverse transform of the merged image to reconstruct the scrambled confidential image.
- By applying Modified Arnold transform on scrambled confidential image by using secret key to recover the original confidential t image.
- The hidden confidential image will be correctly recovered.

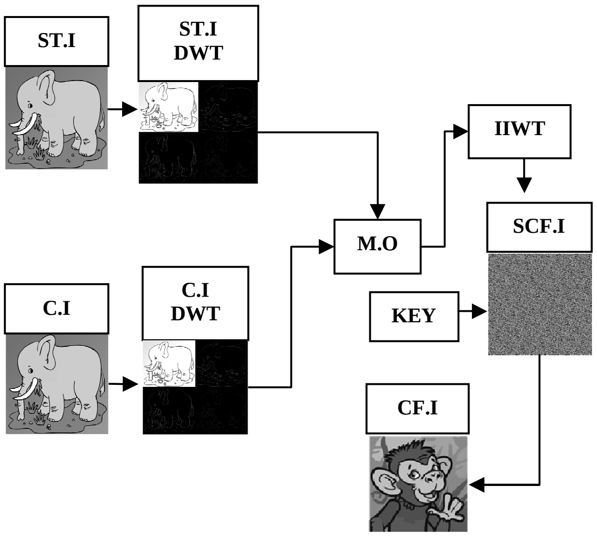


Fig-2: Information Mining Model [CF.I – Confidential Image, M.O – Merge Operation , C.I – Cover Image, SCF.I – Scrambled Confidential Image, ST.I – Stego Image, IIWT – Inverse Integer Wavelet Transform]

5. TESTING AND QUALITY MEASURES

A standard sample images of different sizes of cover image (image without secret image) and confidential image (image to be hidden into cover image) is selected for the analysis of the performance. Here a set of image with different size is hidden into cover image, first set is 512x512 of confidential image into 512x512 of cover image and second set is 256x256 of confidential image into a 512x512 of cover image.

MATLAB is a high performance language for technical computer, integrates computation, visualization and programming in an easy way to use environment. One of the reasons of selecting this is to evaluate the performance of the statistical method. The proposed method is implemented by using Matlab R2010a and 7.10 version.

5.1 Testing

The images from image databases are being tested. Images are collected from database such as SIPI and University of Washington. In order to prove an ideal steganographic scheme in networks using twisted payload is effective, the proposed method is tested and validated over a range of 20 different standard gray scale images of different sizes including Android.jpg, Nest.png, Train.jpg, Blue.jpg, Girl.jpg as the cover image and Eagle.png, Monkey.png, Droplet.png, Blue.jpg, Girl.jpg as the confidential image.

Fig-3 shows their corresponding histogram analyzation of statistical steganography process. It shows that histogram plot of cover image and stego image is same as well as histogram plot of confidential image and recovered confidential image are same. As we seen the stego image given nice invisibility and quality.

5.2 Quality Measures

The measurements of image quality measures not only reduces the image perceptibility but also enhances the robustness to conventional attacks. PSNR and MSE are used to measure the distortion between the original cover image and the stego image.

The other Image quality measures, are Normalized Cross Correlation and Structural Content, are taken for the experiment. The image quality parameters with its corresponding formula are used in this study which is illustrated below.

1).The larger the value of Mean Square Error (MSE) then the image quality is poor. MSE is defined in eqn (3).

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)^2 \qquad (3)$$

2).If Peak Signal to Noise Ratio (PSNR) values is small then the image is in poor quality. PSNR is defined in eqn (4)

$$\mathrm{PSNR} = 10\,\frac{\log_{10}(255)^2}{\mathrm{MSE}}\,\mathrm{dB} \qquad (4)$$

3).The larger the value of Normalized Cross Correlation (NCC) then the image is in poor quality. NCC is defined in eqn (5).

$$\mathrm{NCC} = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)\frac{1}{\sum_{j=1}^{M}\sum_{K=1}^{N}\left(X_{j,k}\right)^2} \qquad (5)$$

4).The larger the value of Structural Content (SC) then the quality of the image is poor. SC is defined in eqn (6).

$$\mathrm{SC} = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k}\right)^2 \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x'_{j,k}\right)^2 \qquad (6)$$

6. PERFORMANCE ANALYSIS

If there are more similarities between the cover image and the stego-image, it will be harder for an attacker to find out that the stego-image has important secret data hidden inside it . This way, the secret data is more likely to travel from the sender to the receiver safe and sound. Fig-4. Shows an ideal steganographic scheme of sample output model

Table-1: The experimental results values of an ideal steganographic scheme with respect to their image quality measures

Table-1: The experimental results values of an ideal steganographic scheme with respect to their image quality measures										
IMAGE SETS	COVER IMAGE (C.I)	CONFIDENTIAL IMAGE (CF.I)	Same size (256 x256) for both C.I and CF.I				C.I (512x512) and CF.I (256x256)			
			PSNR	MSE	NCC	SC	PSNR	MSE	NCC	SC
Image Set 1	Nest.png	Monkey.png	45.9960	1.6349	0.9918	1.0165	51.6756	0.4421	0.9973	1.0055
Image Set 1	Android.jpg	Eagle.jpg	46.1907	1.5632	0.9940	1.0121	52.4941	0.3662	0.9985	1.0029
Image Set 1	Train.jpg	Droplet.png	45.2529	1.9400	0.9928	1.0146	51.0274	0.5133	0.9981	1.0037
Image Set 1	Blue.jpg	Cow.jpg	42.7445	3.4565	0.9937	1.0126	49.4781	0.7333	0.9986	1.0028
Image Set 1	Girl.jpg	Animal.png	42.0377	4.0674	0.9910	1.0182	47.1741	1.2464	0.9976	1.0048
[PSNR – Peak Signal Noise To Ratio, MSE – Mean Square Error, NCC – Normalized Cross Correlation, SC- Structured Content]										

Performance analysis of these two fold transforms is done based on parameters. PSNR is used to measure the quality of the reconstructed image. The PSNR is used to measure the distortion between an original cover image and stego image. MSE is the mean square error representing the difference between the original cover image x sized M x N and the stego image x' sized M x N, and the xj,k and x'j,k are pixel located at the jth row the kth column of images x and x', respectively.

Normalized Correlation coefficient (NCC) between recovered confidential image and original confidential image, is used as a metric for performance evaluation. The value of NCC lies between -1 and +1. If two images are identical, then its value will be +1, if they are completely opposite then its value will be -1 and it will be 0 if images are completely uncorrelated.
Structural Content value ranges between 0 and 1. If value close to one then it shows highest correspondence with the original image The image quality measurement values is compared with the other existing method, and shown in Table-1.

7. RESULT ANALYSIS

This paper deals with secret communication in open environment like internet. Steganographic method has many challenges such as high hiding capacity and imperceptibility. The main goal of steganography is to communicate securely in such a way as to avoid drawing suspicion to the transmission of a hidden data.

It has been observed that when the MSE increases, and this affects the PSNR inversely. So, from trade-off it was found that MSE decrease causes PSNR increase and vice-versa PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e. distortion caused by embedding can be obvious. From Table-1, it is observed that values are acceptable ranges so the confidential image is hidden in the cover image using twisted algorithm securely. PVA is also carried in this technique to improve the PSNR value upto 2dB. However, a high quality stego-image should strive for 40 dB and above. Our results indicate that embedding process introduces less perceptual distortion and higher PSNR.

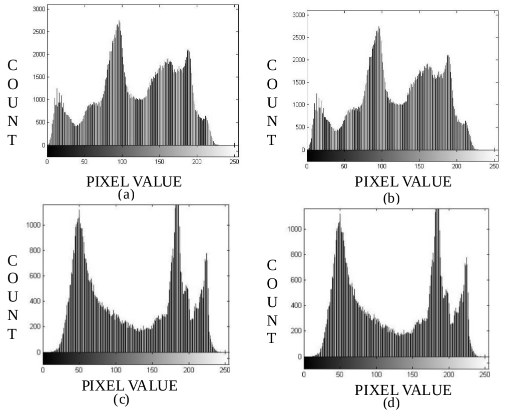
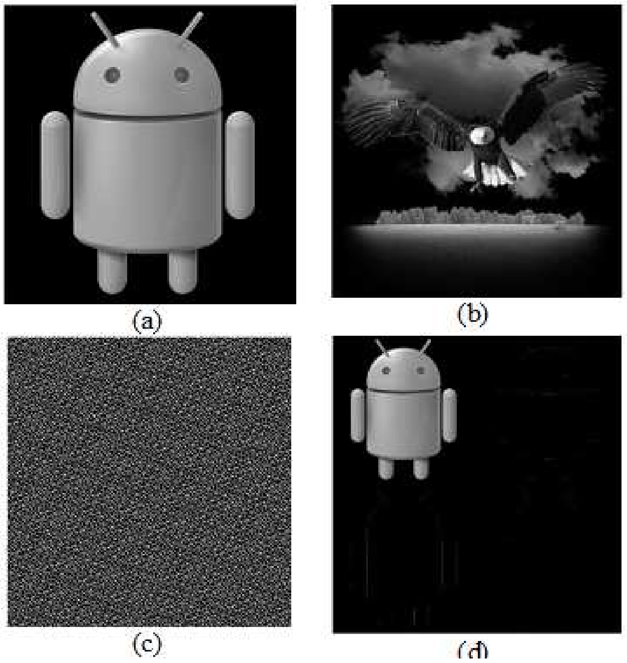


Fig-3: Histogram plot of ideal steganographic scheme (a) cover image, (b) stego image, (c) confidential image (d) recovered confidential image

It is to be noted that PSNR ranging from 42dB to 52 dB means that the quality degradations could hardly be perceived by a human eye. Here the confidential message is hidden in an image file in such a manner that the degradation in quality of the carrier image is not noticeable. Thus the proposed method allows users to send data through the network in a secured fashion and it can be employed for applications that require high-volume embedding with robust against attacks. The steganography method may be further secured if the secret message is compressed first and then encrypted. Finally embed the obtained image inside the cover image. Here confidential image is encrypted before hiding into cover image for security purpose using scrambling algorithm. Modified Arnold Transform used for scrambling the confidential image.

However, steganography can protect data by hiding it in a cover object but using it alone may not guarantee total protection. Thus, the use of encryption in steganography can lead to 'security in depth'. The algorithm pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value. Hence the message will be correctly recovered. Steganography systems do not need to be robust; but they should satisfy high steganography capacity and secret data imperceptibility.



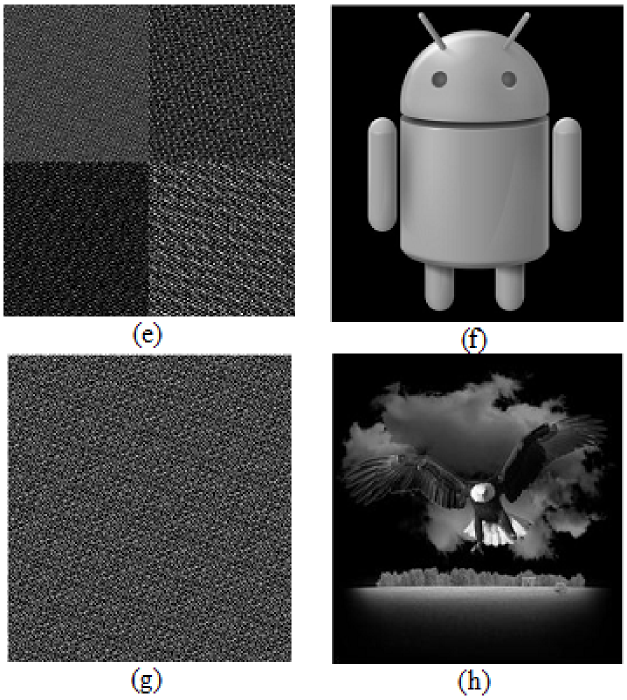


Fig-4: An ideal steganographic scheme of sample output model (a) cover image, (b) confidential image , (c) scrambled confidential image, (d) Cover image DWT , (e) scrambled confidential image IWT, (f) Stego image, (g) Recovered scrambled confidential image, (h) Recovered Confidential image.

8. CONCLUSION AND FUTURE WORK

With the rapid growth of numerous multimedia applications and communications through Internet, secret image sharing has been becoming a key technology for digital images in secured storage and confidential transmission. Though steganography is not implemented in wider ways but it can be the best security tool. Main problem of today's world is to secure their data confidentially, the techniques used currently are not considered the best which can only be replaced by steganography. Although the entire variety of steganography techniques make available high imperceptibility, security and robustness. It is not effortless to develop a method that satisfies all these three needs because for being application dependent may vary from one application to another application.

In future, this technique also compares all possible combination of multiple domains of cover image to increase the security level. This technique will concentrate on perfecting the visual effect of the stego image and the robustness against the various attacks and also compare the twisted techniques by using different wavelet families.

REFERENCES

[1]. Fei Peng, Xiaolong Li, and Bin Yang , "Adaptive reversible data hiding scheme based on integer transform" , Elsevier, Signal Processing ,vol (92), pp: 54–62, 2012.

[2]. V .V. Das, R. Vijaykumar and Dinesh Kumar, " Digital Image Steganography Based on Combination of DCT and DWT " , Springer, ICT,CCIS 101, 00.596-601, pp: 596-601, 2010.

[3]. Weiqi Luo, Fangjun Huang and Jiwu Huang , "Edge Adaptive Image Steganography Based on LSB Matching Revisited" IEEE Transactions On Information Forensics And Security, Vol. 5, No. 2, pp: 201-214, 2010.

[4]. Ali Al-Ataby and Fawzi Al-Naima , "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", International Arab Journal of Information Technology , vol 7 (4) , pp . 1-7 , 2010.

[5]. Sumanth Sakkara. M, Akkamahadevi D.H. , K. Somashekar and Raghu k., "Integer Wavelet based Secret Data Hiding By Selecting Variable Bit Length", International Journal of Computer Applications (0975 – 888) Volume 48– No.19, pp:7-11, 2012.

[6]. Gandharba Swain and Saroj Kumar Lanka, "A quick review of network security and steganography", International Journal of Electronics and Computer Science Engineering , ISSN-2277-1956/V1N2-426-435, pp: 426-435

[7]. Minati Mishra , Ashanta Ranjan Routray and Sunit Kumar, "High Security Image Steganography with Modified Arnold's Cat Map" International Journal of Computer Applications (0975 – 8887) Volume 37– No.9, 2012.

BIOGRAPHIES

Mr. **Logesh R** received B.Tech degree in Computer Science and Engineering from BCET, Karaikal. He is currently pursuing M.Tech degree in Networking at Sri Manakula Vinayagar Engineering College, Puducherry. He has presented papers in national / international conferences. His areas of interest are networking and steganography. Presently working on how to solve network security problems using steganography

Ms. **M Hemalatha** received B.Tech degree in Computer Science and Engineering from BCET, Karaikal. She obtained M.Tech degree in Network and Internet Engineering from Pondicherry University. Presently she holds the position of Assistant Professor of Information Technology at Sri Manakula Vinayagar Engineering College, Puducherry. She has published papers in national / international journals and conferences. Her areas of interest are Ontology, Networking and Image Processing.

Mr. **A Ramalingam** is pursuing his Ph.D at Pondicherry Engineering College. He has 16 years experience. Presently He is working as Associate Professor in Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry. He has published papers in national / international journals and conferences. His areas of interest are Genetic Algorithms, Networking and Image Processing.

Ms. **Kanimozhi K** received B.Tech degree in Information Technology from BCET, Karaikal. She obtained M.E degree in Computer Science Engineering from Annamalai University Chidambaram. Presently doing research on finding new methods to overcome problems for secure communication Her areas of interest are image processing, steganography. She has published papers in national, international conferences and international journals.