LSB,4D-DCT and Huffman Encoding Based Steganography in Safe Message Routing and Delivery for Structured Peer-to-Peer Systems

G.Satyavathy
Research Scholar, Anna University of Technology
Coimbatore – 641 047
sathyasenthil01@gmail.com

M.Punithavalli
SriRamakrishna Engineering College
Coimbatore-641 022
mpunitha_srcw@yahoo.co.in

Abstract- **In structured P2P systems, message deliverance can be done by identifying the peer IDs of the individual systems. The initiator has to decide the destination and can route the message through one or more hops. The message passes from one hop to another correctly by identifying the IP address and finally reaches the destination. In this paper we propose an efficient routing strategy to control the routing path and to identify the malicious nodes. We also eliminate the drawbacks of encryption by introducing steganography in message deliverance. This paper proposes a new steganographic encoding scheme which separates the colour channels of the windows bitmap images and then hides messages randomly in the LSB of one colour component of a chosen pixel where the colour components of the other two are found to be equal to the key selected. In addition to this we apply 4D-DCT based Steganography which embeds the text message in LSB of the Discrete Cosine (DC) coefficient of digital picture. Then Huffman encoding is also performed on the secret messages/images before embedding and each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the LSB of each of the DCT coefficients of cover image blocks. The experimental results shows that the algorithm has a high capacity and a good invisibility. Moreover PSNR of cover image with stego-image shows better results in comparison with other existing steganography approaches. Furthermore, satisfactory security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Huffman table. An implementation of these methods and their performance analysis has been done in this paper.**

Index Terms **-Peer-to-Peer, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Huffman Encoding, Steganography.**

I. INTRODUCTION

Peer-to-Peer [P2P] systems have recently gained a lot of attention from the Internet users and the research community. ”A P2P system is a self organizing system of equal, autonomous entities (peers) which aims for the shared usage of distributed resources in networked environment avoiding central services”. However, they pose new challenge for space. The network becomes more vulnerable to this attack because the attacker can manually influence the ID space where in the new nodes are placed. In this case, the attacker can use a minimal number of nodes and inflict a large amount of damage to the network. Once the attacker has enough nodes in that segment (as compared to the number of legitimate nodes) the attacker can control all messages that pass through the segment.

Castro [2] and Wallach [3] summarize three categories of secure routing required in DHT-based P2P system such as Chord [4], Pastry [5] and Tapstry [6]:
1. Secure assignment node identifiers.
2. Secure routing maintenance.
3. Secure message routing.

Secure assignment node identifiers and secure routing maintenance can be achieved by minimizing the probability that nodes are controlled by attackers. However, an adversary can prevent correct message delivery throughout the overlay. When one or more peers between initiator and target are malicious, a message might be dropped, polluted or forwarded to a wrong place. Satyavathy[1] discusses on the issue of safe and protected message routing combined with steganography in structured P2P systems. Our main idea is to combine steganographic techniques for correct and safe message delivery.

Outline

The remainder of this paper is organized as follows. Section II describes attacks in message routing. In Section III,we propose the tracer routing scheme with acknowledgement and Information Hiding in Bitmap Images Using LSB Based Chromatic Steganography, 3D-DCT Based Steganography and Huffman Encoding[11]. Also an improved version of 3D-DCT Steganography[16]is performed and is given as 4D-DCT Based Steganography. Section IV contains results. Conclusion are given in Section V.

II. ATTACKS IN MESSAGE ROUTING

P2P systems rely on other peers for message routing, thus each message should be properly forwarded to the next hop without any modification. Malicious nodes may attack the message routing in the following ways:

1. simply view the message-passive attack
2. alter the message in transit.
3. disrupt the message routing, or take advantage of locality to control some routes.
4. pretend to be the target

In order to prevent attacks mentioned above, our scheme contains sufficient protection against attacks manipulating the overlay routing. Messages are encrypted and then is transferred to the next hop. Since the probability of modification of messages is larger we go for the special tracer routing[8] combined with Information Hiding in Bitmap Images Using LSB Based and 3D-DCT Chromatic Steganography[9] with Huffman Encoding. Second, the routing path of a message can be controlled by the initiator. On detecting that the message is forwarded to a wrong place, the initiator will search an alternate routing path used to circumvent malicious peers.

III. PROPOSED METHODOLOGY

A. Current Routing Strategies

In this section, we first analyse the performance of current routing strategies and then propose our schemes which combines tracer routing with Information Hiding in Bitmap Images using LSB based Chromatic Steganography, 3D-DCT Steganography with Huffman Encoding.

Current routing strategies of structured P2P systems can be generally categorized into two types: recursive routing and iterative routing. We analyze the characteristics of them as follows. As an example, we deploy them on Chord system.

With recursive routing, the initiator issues a query to the nearest peer to the target according to its routing table. If the intermediate peer, say x, is not the target, x will forward the query to the peer in the next hop, without making any acknowledgement to the initiator. The process repeats until query reaches the target. The target sends the query result back to the initiator directly. Recursive routing enables routing queries as quickly as possible, but the initiator has no control over the routing process.

In iterative routing, the initiator can know the whole routing process. In each step, the initiator asks intermediate peer x to return the IP address of the next hop, instead of letting x forward the query directly. With the returned IP address, the initiator sends the query to each peer of the routing path on its own, repeating until the query reaches the target.

To measure the performance of routing strategies, one metric is adopted: the normal routing latency, which is the latency to complete one query if there is no attacks in the system. Let t be average latency of one hop and h be the average number of hops of each query. The first column of the table I lists the routing latency. The recursive routing is efficient, but is not secure , even combined with the technique of verifying the ID of remote peer such as Peer-ID based signature scheme. The fact that intermediate peers may assist in obfuscating the intermediate peer disrupts the message forwarding. For example, an adversary may do not forward queries that it receives, or forwards them to a wrong place. The initiator has no knowledge about the real cause.

Iterative routing is not efficient, but it gains some benefits due to its manageable behavior. The intermediate peers reply with IP address of the next hops to the initiator, the initiator can send the message to the peer in the next hop directly. We consider three kinds of attacks:

In case 1, the intermediate peer x pollutes or forges the content of the query. The next hop will still receive the original query since initiator sends the query by itself.

In case 2, peer x drops the query. If no relay from the next hop is received in a given time out, initiator will determine that x drops it.

In case 3, peer x returns initiator an incorrect next hop. If the incorrect next hop colludes, the fact that initiator cannot verify the identity of the next hop makes determining which peer sends the incorrect reply impossible. This challenge causes us to believe that the technique of verifying the ID of remote peer is necessary. Combined with Peer-Id based signature scheme, initiator can identify the malicious node x.

B .Tracer routing

To make the routing strategy perform best, we propose an efficient routing strategy, called tracer routing and we include the acknowledgement scheme. Tracer routing enables the initiator to trace the whole routing process. It can reduce normal routing latency from $2h \ast t$ to $(h + 1) \ast t$. The basic principle of the routing strategy is as follows. In each step, the intermediate peer x not only forwards the query to the next hop, but also returns the IP address of the next hop to initiator. With the additional information, the initiator has the knowledge about the whole routing process. Each intermediate peer directly forwards the query to the next hop, thus the query can be routed quickly.

Table 1. Comparison Of Performance Of Three Routing Strategies

Strategy	Normal routing latency	Identify malicious nodes
Recursive	$(h + 1) \ast t$	No
Iterative	$2h \ast t$	Yes
Tracer	$(h + 1) \ast t$	Yes

C. Information Hiding In Bitmap Images Using LSB Based Chromatic Steganography

Redundancy is one of the major aspects of creation. A close inspection reveals that redundancy does exist, and exists in abundance. For e.g. an image on a computer is represented by tons and tons of pixels, which in turn have many redundant information's. The simplest technique here is to fabricate the redundant bits so as to do the covert communication. For e.g. each pixel of an image consists of a variation of all three primary colors, red, green and blue, in a standard 24-bit bitmap, requiring 8 bits each for these three colors. i.e. there are 256 different variations, ranging from 00000000 to 11111111, for each color in a pixel. So, to represent the color white, the code would look like 11111111 11111111 11111111. Keeping in mind that, the human eye cannot distinguish the difference between too many colors, the color 11111110 11111110 11111110 would look exactly the same as white, which means that the last digit in every bit in every pixel could be changed without much visual degradation of quality. This is the basis of the Least Significant Bit(LSB) Insertion technique. We require 8 bits to represent an ASCII text and there are three potential slots extra in every pixel of a picture. Therefore, in a conducive environment, with every three pixels, one ASCII text could be concealed. In order to make this practical to the user, a computer program would be needed. After typing in the secret message and determining a suitable cover message, the program would go through every pixel to find the potential candidate pixels and will change the LSB to represent each bit of the message. The image could then be sent to the recipient who in turn runs his program to take off the LSB to form the secret message. The current study took windows bit map image file format with lossless compression into consideration.

D. DCT Based Steganography

DCT coefficients are used for JPEG compression. The cover image is split into 8*8 blocks and each block is used to encode one message bit. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

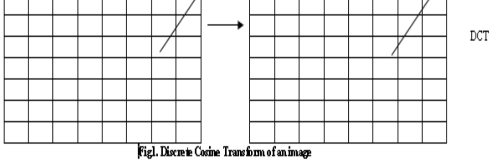


Fig1. Discrete Cosine Transform of an image

The general equation for the 1D (N data items) DCT is defined by the following equation:

$$C(u) = \alpha(u) \sum_{i=0}^{N-1} f(x) \cos\left[\frac{(2x+1)\,u\pi}{2N}\right] \qquad (1)$$

for u=0, 1, 2… N-1.

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u)=\alpha(u)\alpha(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(x,y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] (2)$$

for u, v=0,1,2,…,N-1.

The general equation for a 3D-DCT is defined by the following equation:

$$C(u,v,w)= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} C(i,j,k)\, Xli, Xmj, Xnk \qquad (3)$$

where

$$X_{li} .X_{mj} .X_{nk} = cos\left[\frac{\pi}{N}\left(i+\frac{1}{2}\right)l\right].cos\left[\frac{\pi}{N}\left(j+\frac{1}{2}\right)m\right].cos\left[\frac{\pi}{N}\left(k+\frac{1}{2}\right)n\right]$$

The general equation for a 4D-DCT is defined by the following equation:

$$c(u,v,w,r) = \sum_{i=o}^{N-1} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} c(i,j,k,n) Xli, Xmj, Xnk, Xop$$

(4)

where

$$Xli\ Xmj\ Xnk\ Xop - \cos\left[\frac{\pi}{N}\left(i+\frac{1}{2}\right)l\right] \cos\left[\frac{\pi}{N}\left(j+\frac{1}{2}\right)m\right] \cos\left[\frac{\pi}{N}\left(k+\frac{1}{2}\right)n\right] \cos\left[\frac{\pi}{N}\left(o+\frac{1}{2}\right)p\right]$$

$$PSNR(x,y)=10\log_{10} \frac{\left(\max\left(\max(x),\max(y)\right)\right)}{|x-y|^2} \qquad (5)$$

where PSNR is the Peak Signal to Noise Ratio.

E. Huffman Encoding and Huffman Table

Before embedding the secret image into cover image, it is first encoded using Huffman coding [12,13].Huffman codes are optimal codes that map one symbol to one code word. For an image Huffman coding assigns a binary code to each intensity value of the image and a 2-D M2 × N2 image is converted to a 1-D bits stream with length LH < M2 × N2. Huffman table (HT) contains binary codes to each intensity value. Huffman table must be same for both the encoder and the decoder. Thus the Huffman table must be sent to the decoder along with the compressed image data.

Embedding of Secret Message / Image

We have proposed the secret message/image embedding scheme in the following steps:

Step1:DCT-Divide the carrier image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the cover image to obtain C using equation (1).

Step 2: Huffman encoding

Perform Huffman encoding on the 3-D secret image S of size M2 × N2 to convert it into a 1-D bits stream H.

Step 3: 8-bit block preparation-Huffman code H is decomposed into 8-bit blocks B. Let the length of Huffman encoded bits stream be L_H. If L_H is not divisible by 8, then last block contains r = L_H % 8 number of bits (% is used as modulo operator).

Step 4: Bit replacement-The LSB of all the DCT coefficients inside 8×8 block is changed to a bit taken from each 8 bit block B from left to right. The method is as follows:

For k=1 ; k ≤1; k=k+1

LSB(($C(u,v))_2$) ← B(k) ;where B(k) is the kth bit from left to right of a block B and $(C(u,v)_2$) is the DCT coefficient in binary form.

Step 5: IDCT-Perform the inverse block DCT on C using equation (3) and obtain a new image c1 which contains secret image.

Embedding Algorithm

Input: An M1×N1 carrier image and a secret message/image.

Output: A stego-image.

1. Obtain Huffman table of secret message/image.
2. Find the Huffman encoded binary bit stream of secret-image by applying Huffman encoding technique in Huffman table obtained in step 1.
3. Calculate size of encoded bit stream in bits.
4. Divide the carrier image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the cover image.
5. Repeat for each bit obtained in step 3.
   (a) Insert the bits into LSB position of each DCT coefficient of 1st 8×8 block found in step 4.
6. Decompose the encoded bit stream of secret message/image obtained in step 2 into 1-D blocks of size 8 bits.
7. Repeat for each 8-bit blocks obtained in step 6
   (a)Change the LSB of each DCT coefficient of each 8×8 block(excluding the first) found in step4 to a bit taken from left(LSB) to right(MSB) from each 8 bit block B.
8. Repeat for each bit of the Huffman table
   (a) Insert the bits into LSB position of each DCT coefficient
9. Apply inverse DCT using identical block size.

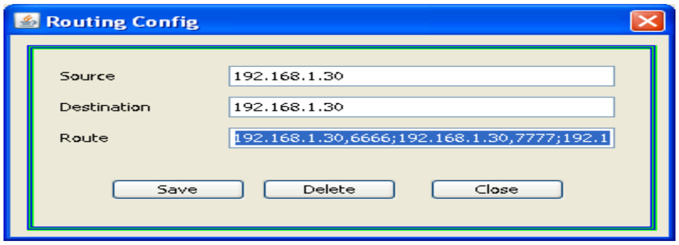
Extraction Algorithm

Input: An M1×N1 Stego-image.

Output: Secret image.

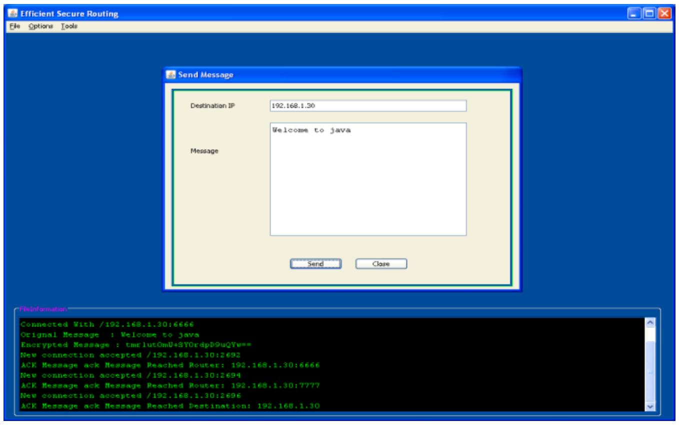
1. Divide the stego-image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the stego-image.
2. The size of encoded bit stream is extracted from 1st 8 × 8 DCT block by collecting the LSB of all the DCT coefficients inside the 1st 8×8 block.
3. The LSB of all the DCT coefficients inside 8×8 block (excluding the first) are collected and added to a 1-D array.
4. Repeat step 3 until the size of the 1-D array becomes equal to the size extracted in step 2.
5. Construct the Huffman table by extracting the LSB of all the DCT coefficients inside 8×8 blocks excluding first block and the block mentioned in step 3.
6. Decode the 1-D array obtained in step 3 using the Huffman table obtained in step 5.

IV. RESULTS



Source: 192.168.1.30
Destination: 192.168.1.30
Route: 192.168.1.30,6666;192.168.1.30,7777;192.1

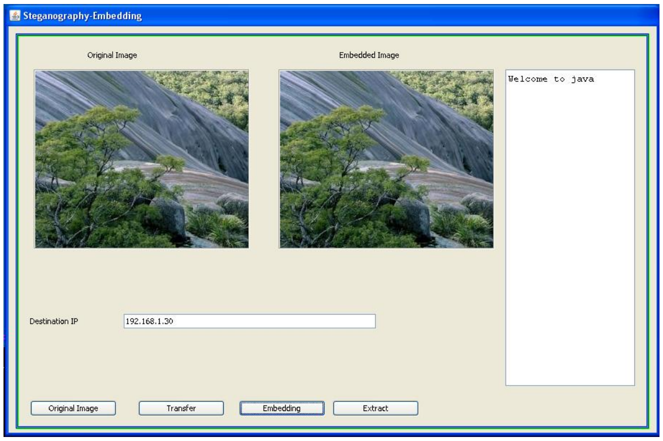
Fig II: The above figure shows the routing configuration.Here we have given the IP address of the source as well as destination and have given the hop routes.



Destination IP: 192.168.1.30
Message: Welcome to java

```
Connected With /192.168.1.30:6666
Orignal Message  : Welcome to java
Encrypted Message : tmrlutOmU+SYOrdpD9uQYw==
New connection accepted /192.168.1.30:2692
ACK Message ack Message Reached Router: 192.168.1.30:6666
New connection accepted /192.168.1.30:2694
ACK Message ack Message Reached Router: 192.168.1.30:7777
New connection accepted /192.168.1.30:2696
ACK Message ack Message Reached Destination: 192.168.1.30
```

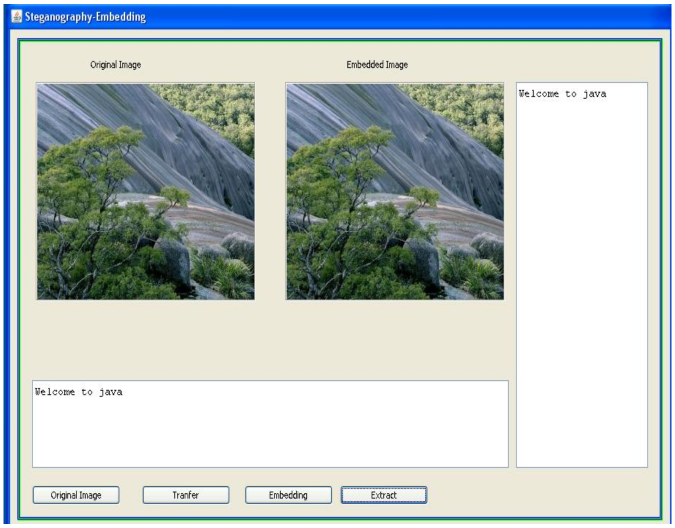
Fig III: Routing path of the message with acknowledgement of each and every hop.



Welcome to java

192.168.1.30

Fig IV: Original image and the message to be embedded with the destination IP.

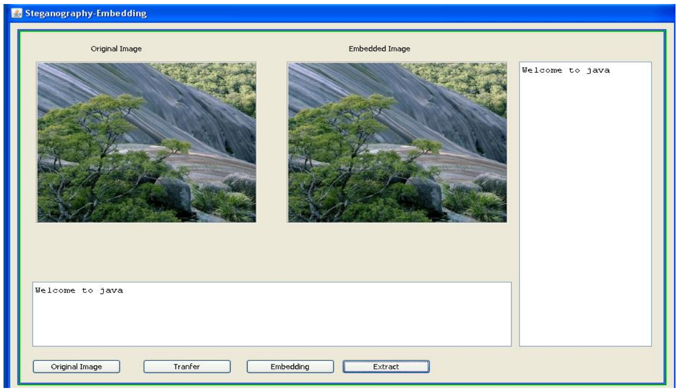


Welcome to java

Welcome to java

Fig V: LSB Based Steganography

Peak Signal Noise Ratio between the Original and Embedded Image = 51.0791 dB

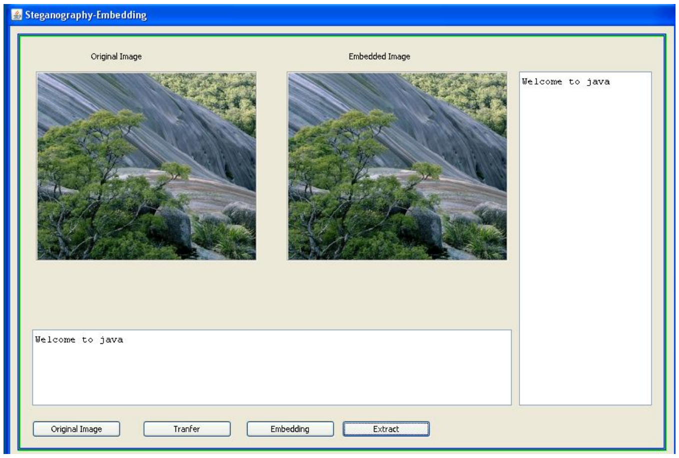


Welcome to java

Welcome to java

Fig VI: 3D-DCT Based Steganography

Peak Signal Noise Ratio between the Original and Embedded Image = 58.0710 dB

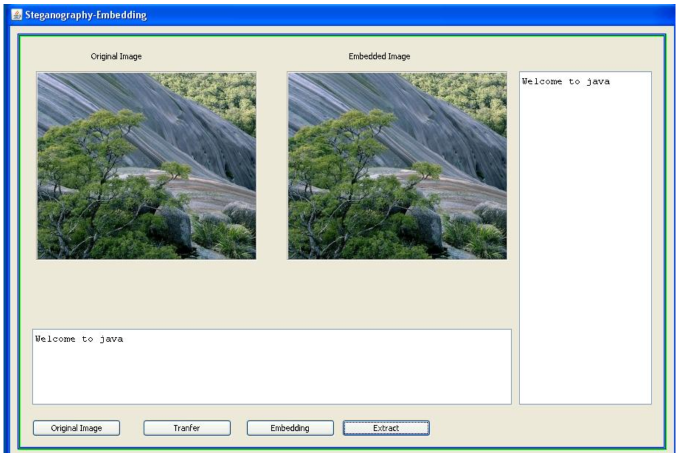


Welcome to java

Welcome to java

Fig VII:3D-DCT Steganography combined with Huffman Encoding.

Peak Signal Noise Ratio between the Original and Embedded Image = 59.0241 dB



Welcome to java

Welcome to java

Fig VIII:4D-DCT Steganography combined with Huffman Encoding

Peak Signal Noise Ratio between the Original and Embedded Image = 59.0352 dB

V. CONCLUSION

In this paper, our objective is to provide directions for designing secure message routing with acknowledgement by using steganography. We consider three aspects: authorization, routing and safe message delivery using steganographic techniques. We have introduced a new steganographic encoding scheme which separates the color channels of the windows bitmap images and then randomly hide messages in the LSB of one component of the chosen pixel where the color coefficients of the other two are found to be equal to the keys selected. In addition to this we have introduced DCT based steganography which embeds the text message in LSB of DC coefficients. This paper implements LSB based steganography, 4D-DCT based steganography combined with Huffman Encoding and computes PSNR ratio. PSNR is the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are of better quality. Comparison of LSB based, 4D-DCT based images and with Huffman Encoding using PSNR ratio shows that PSNR ratio of 4D-DCT based steganography scheme combined with Huffman encoding is high as compared to LSB based and 4D-DCT based steganography scheme for all types of images. 4D-DCT based steganography with Huffman encoding scheme works perfectly with minimal distortion of the image quality as compared to LSB based steganography scheme. Even though the amount of secret data that can be hidden using this technique is very small as compared to LSB based steganography scheme still, 4D-DCT based steganography scheme combined with Huffman encoding is recommended because of the minimum distortion of image quality. Based on this analysis, we propose our scheme keeps the images away from stealing, destroying from unintended users and is more robust against brute force attack. It is also resilient to message routing attack with lower normal routing latency, minimum distortion compared with present routing strategies and steganographic schemes.

VI. REFERENCES

[1]. G.Satyavathy, M. Punithavalli, “Steganography in Safe Message Routing and delivery for Structured Peer-to-Peer Systems”.International Conference on Intelligent Information Systems and Management (IISM’2010), June10-12,2010

[2]. M. Castro, P. Duschel, A. Rowstron, and D. S. Wallach, “Secure routing for structured peer-to-peer overlay network”. In Proceedings of the fifth Symposium on Operating System Design and Implementation, Dec 2002.

[3]. D. Wallach, “A survey of peer-to-peer security issues”. In Proceedings of International Symposium of Software Security - Theories and Systems, Nov 2003.

[4]. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. “Chord: A scalable peer-to-peer lookup service for Internet applications”. In Proceedings of SIGCOMM 2001, pages 149-160, August 2001.

[5]. Rowstron and P. Druschel., “Pastry: scalable, distributed object location and routing for large-scale peer-to-peer systems”. Lecture Notes in Computer Science, 2218:161-172, November 2010 .

[6]. Y. Zhao, J. D. Kubiatowicz, and A. D. Joseph.,”Tapestry: An infrastructure for fault-tolerant wide-area location and routing”. Technical Report UCB/CSD-01-1141, UC Berkeley, Apr, 2001.

[7]. J. R. Douceur, “The Sybil attack”. In Proceedings of the First International Workshop on Peer-to-Peer System, March 2002.

[8]. Xu Xiang,Tan Jin, “Efficient Secure Message Routing for Structured Peer-to-Peer Systems”. 2009 International Conference on Network Security, Wireless Communications and Trusted Computing.

[9]. Jiju A. Mathew, “Steganography and Covert Communications in Open Systems Environment”. 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[10]. Dr.Ekta Walia, Payal Jain, Navdeep, “An Analysis of LSB & DCT Based Steganography”.

[11]. A.Nag,S.Biswas,D.Sarkar,P.PSarkar, ”A novel technique for image steganography based on Block-DCT and Huffman Encoding”-International Journal of Computer Science and Information Technology.

[12]. Gonzalez, R.C. and Woods, R.E., “Digital Image Processing using MATLAB”, Pearson Education, India, 2006.

[13]. Jayaraman, S., Esakkirajan, S. and Veerakumar, T. “Digital Image Processing”, Tata McGraw Hill Education Private Limited, India, 2009.

[14]. Samir kumar Bandyopadhyay, Tuhin Utsab Paul,Avishek Raychoudhary, “A Novel Steganographic Technique Based on 3D-DCT Approach-Computer and Information Science Vol 3, No: 4, November 2010.

[15]. Andrew S.Tanenbaum ,”Computer Networks”,4th edition.

[16].G.Satyavathy, M. Punithavalli, LSB,3-DCT and Huffman Encoding Based Steganography in Safe Message Routing and delivery for Structured Peer-to-Peer Systems. ijcaonline.org/specialissues/ait/number1/2827-208

G.Satyavathy is a research scholar pursuing Ph.D in Anna University, Coimbatore. She has more than 12 years of teaching experience. Her areas of interest include network security, steganography.

Dr.M.Punithavalli is working as a Director in the M.C.A department in SriRamakrishna Engineering College, Coimbatore.She has more than 18 years of teaching experience.Her areas of interest include network security, steganography, datamining and software engineering.