Secure Opportunistic Notice Passing Using Steganography in Academic Campus

Kavitha.N*, kavithanagaraj710@gmail.com
Kusumanjali.B*, kusumanjalipatel@gmail.com
Shilpa*, shilpasheeth45@gmail.com
Adithya.B*, adithyakoundinya@gmail.com
*Computer Science Department, Jyothy Institute of Technology, Bangalore, India

Abstract - **In the emerging field of distributed mobile computing, plethora of devices are under-utilized in terms of their computing power, memory space and energy. In this paper we have adapted an application for opportunistically passing notices in an academic campus and proposed a way to achieve security and privacy through Steganography resolving the under utilization issue.**

Keywords - Opportunistic networks; Authentication; Interaction; Trust Modeling; Steganography;

I. INTRODUCTION

The cell phones, laptops, tablets, iPods with different access technologies are plenteously loaded in the world; Wi-Fi, Bluetooth, WI-MAX, cellular, RFID and NFC are commonly used access technologies that are available near a device making the way for numerous opportunities for unlimited pair wise device contacts.

When billions of devices share their computing time, memory space and energy in collaborative way, the impact is enormous, this manner that is representative of distributed computing, though in a different paradigm is Opportunistic Computing. Leveraging of opportunities as they exploit the communication between a pair of devices enabling possible sharing of content, resources, and services that are in the vicinity that meet application requirements is called opportunistic computing. Opportunistic Computing exploits humans' mobility and their gregarious natures to enable a transmission only if the users are sufficiently close [1].

In such an entwined network of opportunities, privacy and security is an obvious and major issue. Security is necessary since it helps in securing data from threats such as misuse, enables privacy to the users. In this paper, we have tried to achieve security through Steganography. Steganography is an art that involves communication of secret data in an appropriate carrier such as text, image, audio or video. Steganography's goal is to hide the very existence of embedded data so as not to arouse an eavesdropper's suspicion [2].

A. Application Scenario

This paper deals with the framework of academic campus composed of a wide area, numerous employees and students. Fig.1 shows the hierarchy of academic organization. The Administrator passes the information and notifications to the Principal and Principal to the different levels such as Administrator staff, Examination section, Departments, Placement, System admin and Miscellaneous.

The information can be of three types - Unicast, Multicast and Broadcast. In Unicast, one point sends information to another point (just one sender, and one receiver). In Broadcast, one point to all other points (just one sender sends to all connected receivers). In Multicast, the information is sent from one to a set of other points (one sender and the information is distributed to a set of receivers).

In this existing system, a human transporter transports the information (that is in paper format) to recipient. Either transporter delivers the notices at 11:30 AM or 03:00 PM (pre-defined time intervals). Further, the notice is vulnerable to attack because human user transmits it. A secured opportunistic computing using Steganography technique resolves this issue.

B. Steganography techniques used

The proposed Steganography technique is the idea of combining Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) and exploring the advantages of both algorithms to provide secure opportunistic pair wise contacts between registered and preconfigured nodes, to pass the information from source to various destinations securely.

The academic campus application scenario is composed of huge number of employees and students carrying various cell phones, laptops, tablets, and iPods with different access technologies. These devices can act as transporting media and send information to the destination utilizing devices opportunistically.

C. Organization of the paper

The paper organizes following sections – part II consists of Literature Survey, part III presents the proposed Hybrid Transform Domain Technique, part IV provides the results and part V concludes the paper.

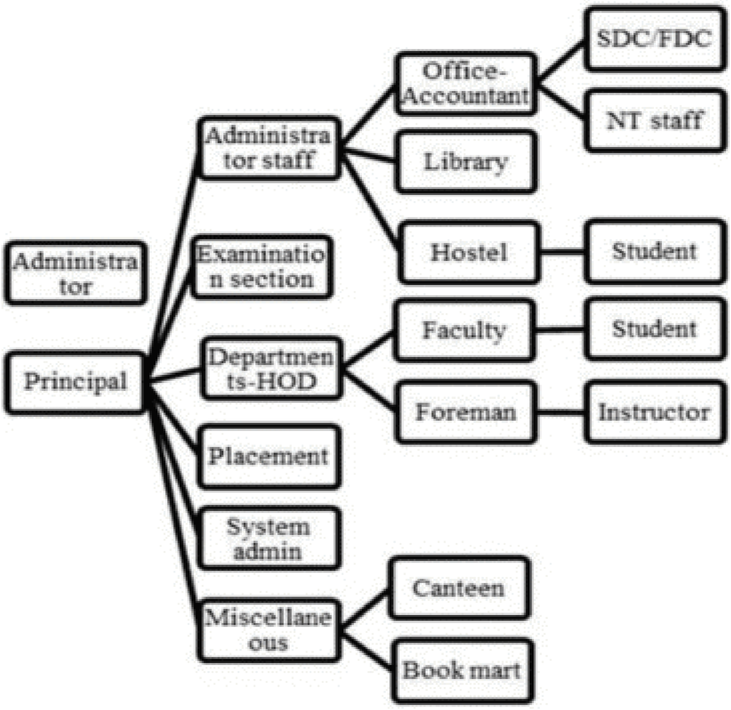

Fig. 1 Hierarchy of Academic Organization

II. LITERATURE SURVEY

The Literature survey has two dimensions.

i) The various Steganography techniques and

ii) The usage of opportunistic networking in various application scenarios

Least Significant Bit (LSB) is one of the easiest technique in which the secrete data is in the binary form has to be hidden into the LSB of the pixels of the cover image. The overall change to the image is so negligible that human eye would not be able to discover this. In 24-bit images, each 8-bit value refers to the red, green and blue color [3]. Compression of image affects embedded data.

DCT method encodes the secret information in the frequency domain by modulating the relative size of two or more DCT coefficients in an image [5]. The DCT has high-energy compaction property and requires less computational resources [6]. The main disadvantages of DCT are introduction of false contouring effects and blocking artifacts at higher compression.

A wavelet is simply a small wave, which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time varying phenomena. Expressing signal as a linear decomposition of sums of products of coefficients and functions is better to analyze. These set of coefficients are Discrete Wavelet Transforms (DWT) of a signal [7]. DWT has spatial frequency locality, which means that if embedded signal will affect the image locally. In addition, they do not take into account the fact that different regions in an image may have different frequency characteristics [5].

Exploring the advantages of the above algorithms generates the combination of the two techniques - hybrid algorithm. Advantage of the hybrid algorithm is that it overcomes the drawbacks in both the algorithms, and provides the advantages of both algorithms i.e. High-energy compaction property and requires less computational Resources provided by DCT and multi-resolution transform technique and variable compression is achieved by DWT [6].

UnaCloud: Opportunistic Cloud Computing Infrastructure as a Service [10]; provides at lower cost than dedicated cloud infrastructures, the basic computing resources (processing, storage and networking) to run arbitrary software, including operating systems and applications. Through the opportunistic use of idle computing resources available in a university, campus provides IaaS model [9]. The model represents an economically attractive solution for constructing and deploying large scale computing infrastructure, avoiding not only, under-utilization of non-dedicated computational resources, but also financial investments in hardware and costs associated with physical space and maintenance process. Several other applications such as the goose [11], condor [12] are also the source of the motivation for the proposed scenario.

III. PROPOSED TECHNIQUE

Proposed technique is Hybrid Domain Transform technique.

A. Discrete Cosine Transformation

DCT is used, but similar transforms are there, for example the Discrete Fourier Transform (DFT) and Discrete Sine Transform. These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image [13]. A signal is transformed from image representation to frequency representation using DCT, by grouping the pixels into 8 x 8 pixel blocks and transforming the pixel blocks into 64 DCT [14].

Use DCT in Steganography as image is broken into 8 x 8 blocks of pixels. Working in horizontal and vertical direction, apply DCT to each block. Compress each block through quantization table to scale the DCT coefficients and embed the message in DCT coefficients [14].

2D images and signals may also use DCT [15]. Two ways of achieving this: by using (1), we can find 1D DCT of the 2D image and then using (2), we can find 1D DCT of each column of the image.

$$s(u,v) = \frac{2}{N} C(u)\, C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} s(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

(1)

$$s(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)s(u,v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right)$$

(2) [5]

Algorithim for DCT

```
1. INPUT: Message and input image
2. OUTPUT: Image containing secret message
3. While data left to hide, do
4.         Get next DCT coefficient from input image
5.                 If (DCT! = 0 && DCT! =1)
6.                 Get next LSB from secrete message
```

```
7.   Replace DCT, LSB with secrete message bit
8.   End if
9.   Insert DCT into output image
10. End while
```

B. Discrete Wavelet Transform

Discretely sampled wavelets are present in DWT. Wavelet transform decomposes a signal into a set of basic functions called wavelets that wave above and below the x-axis, have varying frequency, limited duration, and an average value of zero. A single prototype wavelet Ψ (t) called mother wavelet by dilations and shifting gives wavelet:

$$\Psi(t) = \begin{cases} 1 & 0 \le t < ½, \\ -1 & ½ \le t < 1, \\ 0 & \text{otherwise} \end{cases} \qquad (3)$$

The dwt technique we are using is 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one [16].

Algorithm for 2D - Haar DWT [17]

```
1.  INPUT: cover image ($I_c$) and secret image($I_s$)
2.  OUTPUT: image containing secret image
3.  Evaluate the size of $I_c$
4.  Read the $I_s$
5.  Message vector is prepared by the $I_s$
6.  $I_c$ is decomposed using Haar wavelet transform
7.  Pseudo random number is generated
8.  Details of horizontal and vertical coefficients of wavelet
    decomposition by adding pseudo random number when
    message bit=0
9.  Inverse DWT is applied
10. Stego image is generated
```

C. Opportunistic Notice Passing

Oppnets is new concept of transferring the data from source to destination using mobile devices without properly following a route or path.

This network based on spontaneous connectivity between users with wireless devices. It attempts to overcome the time limits associated with the manual notice passing. Consider a situation where the Principal has to pass a message to all the faculties to meet him within a time interval. In opportunistic networks, route connecting to the devices never exits, devices communicate with each other when they get an opportunity to communicate within the radio range of the source node. The source node, in this case, the principal of institution, passes the message (Stego image in this case) to a nearby node. Among the various potential messenger nodes, their mobility patterns decide the selection of nodes. Nodes move around and while being near to other nodes, they pass the message and at some point, its eventually reaches destination node. Nevertheless, nodes are not supposed to possess or acquire any knowledge about the network topology. Any possible node can opportunistically be used as next hop, provided it is likely to bring message closer to final destination, thus routes are built dynamically as the intermediate nodes keep changing and are not constant.

IV. RESULTS

A. Simulation Procedure

For analysis of the protocol, we are choosing around 450 - 500 devices including cell phones, laptops, and tablets and iPods sending 50 messages in a typical working day.

B. Simulation Environment

This sections models parameters like density of the nodes, success rate, successful transactions, stability and delay in the academic environment.

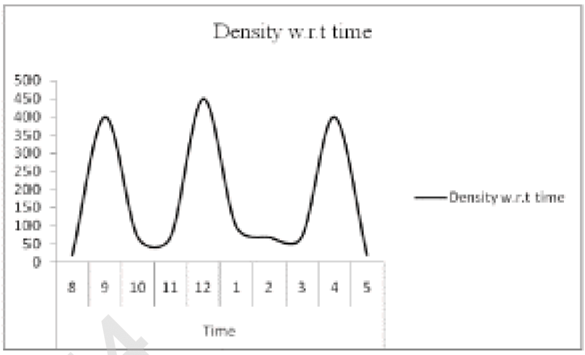

Fig. 2 Density of computing devices v/s Time Slot

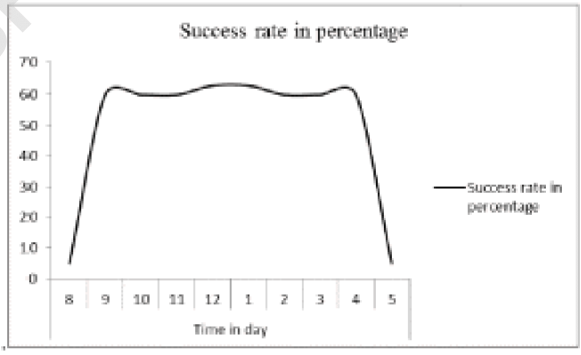

Fig. 3 Delivery success rate v/s Time Slot

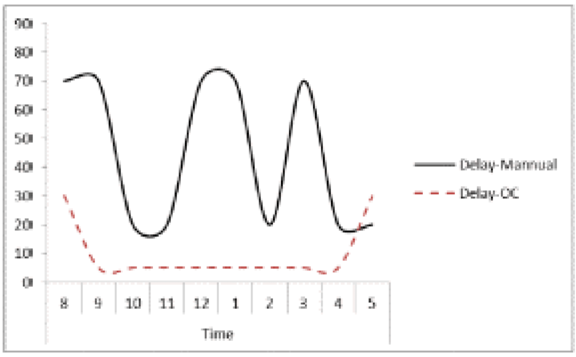

Fig. 4 Comparison of SOC v/s conventional methods with respect to Time Delay

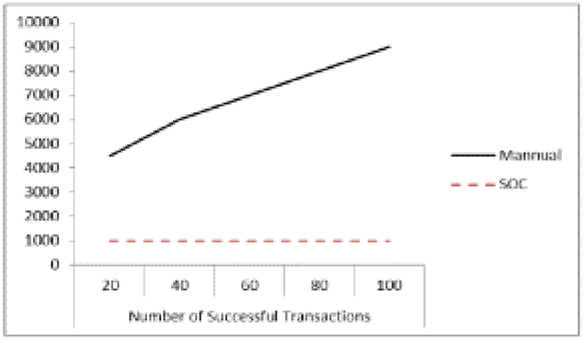

Fig. 5 Comparison of SOC v/s conventional methods with respect to Cost

Fig. 2 gives the plot of the density of the nodes with respect to time. Here for our evaluation, we choose 9 hours slot in a day observing the device density in the academic environment. This plot indicates the probable opportunity for pair wise contacts between the devices, which help in notification passing.

Fig. 4 gives the comparison between Secured Opportunistic Computing (SOC) and manual technique with respect to the time delay in the delivery of the notice. We observed low delay with SOC, due to its nature of forwarding the messages through opportunistic contacts, whereas in the conventional system the delay in the notice delivery is large, due to the fact that the human attainder will collect the notices only twice a day.

Fig. 3 gives the plot of Average Success Rate of message delivery at the given density of nodes. Out of 100 messages at the peak hour, delivery might be more than 50% of messages, and at lean periods, it might be about 12.5% of messages. This is because the density of mobile devices varies over time.

Fig. 5 gives the comparison between SOC and Manual technique with respect to the cost of maintenance. SOC is cost effective because it does not require any salaried attainder. Devices, which come in opportunistic contact with the source node, pass the notices.

V. CONCLUSION

On the Hindsight, in Oppncts all the devices available devices are utilized to provide computing and communication services. In this paper, we have proposed an application where employees pass notices opportunistically in an academic campus utilizing the opportunity provided by human user. The results are intuitive that the application maintains low energy and low cost model in notice passing. The scheme further extends to model its performance, and implement over actual test bed.

REFERENCES

[1] M. Conti, "Opportunities in Opportunistic Computing", Communications Magazine, IEEE, Vol. 43, Issue. 1, pp. 42 - 50, 2010.

[2] Babloo, Saha and Shuchi Sharma,"Steganographic Techniques of Data Hiding using Digital Images", Defense Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18

[3] Ramanpreet Kaur1, Baljit Singh2, Ishpreet Singh, "A Comparative Study of Combination of Different Bit Positions In Image Steganography", IJMER, vol 2, issue, sep-oct.2012 pp-3835-3840

[4] T. Morkel, J. Eloff, and M. Olivier, "An overview of image steganography", In Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), (Sandton, South Africa, Jun/Jul. 2005).

[5] Rohit Goel and Mukta Goel, "Comparative Analysis of Hybrid Transform Domain Image Steganography Embedding Techniques", Vol 2, Issue 2, Feb 2013

[6] Chin-Chen Chang, Chi-Lung Chiang, and Ju-Yuan Hsiao, "A DCT Domain System for Hiding Fractal Compressed Images", Proceedings of IEEE 19th Conference on Advanced Information Networking and Applications, Volume 2, pp. 83-86, march 2005.

[7] Rakesh Dugad, Krishna Ratakonda, and Narendra Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", International Conference on Image Processing, Chicago, USA, pp. 419-423, October 1998.

[8] S.M. Allen, M.J. Chorley, G.B. Colombo, and R.M. Whitaker, "Opportunistic social dissemination of micro-blogs", EPreprint submitted to Elsevier, 2012.

[9] Andrei Goldchleger , Fabio Kon , Alfredo Goldman , Marcelo Finger, Germano Capistrano Bezerra, "InteGrade object-oriented Grid middleware leveraging the idle computing power of desktop machines", Research Articles, Concurrency and Computation: Practice and Experience, Vol. 16 Issue. 5, pp. 449 - 459, 2004.

[10] Eduardo Rosales, Harold Castro, Mario Villamizar, "UnaCloud: Opportunistic Cloud Computing Infrastructure as a Service", The Second International Conference on Cloud Computing, GRIDs, and Virtualization, 2011

[11] Narseo Vallina-Rodriguez, Pan Hui, Jon Crowcroft, "Has anyone seen my Goose?- Social Network Services in Developing Regions", Computational Science and Engineering, Vol. 4, pp. 1048 - 1053, 2009.

[12] M. Litzkow, M. Livny, and M. Mutka, "Condor-a hunter of idle workstations", 8th International Conference on Distributed Computing Systems, pp. 104 - 111, 1988.

[13] Ankur M. Mehta, Steven Lanzisera, and Kristofer S. J. Pister, "Steganography 802.15.4 Wireless Communication".

[14] A Steganography Implementation based on LSB & DCT Gurmeet Kaur and Aarti Kochhar

[15] Adrian G. Bors, Ioannis Pitas, "Image Watermarking Using DCT Domain Constraints", International Conference on Image Processing, Lausanne, Switzerland, pp. 1-4, September 1996.

[16] Stuti Goel, Arun Rana, Manpreet Kaur, " Comparison of Image Steganography Techniques", International Journal of Computers and Distributed Systems www.ijcdsonline.com Vol. No.3, Issue I, April-May 2013.

[17] Barnali Gupta Banik and Prof.Samir K.Bandyodhyay "International journal of advanced research in computer science and software engineering", Vol3, issue 6, June