ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 8, February 2013

Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding

Lovey Rana[1] Saikat Banerjee[2]
[1] Student, SOIT, Centre for Development of Advanced Computing (CDAC)
[2] Student, SOIT, Centre for Development of Advanced Computing (CDAC)

Abstract - The approach used in this paper is to design a steganography scheme which is used to hide data into an audio file in such a way that the data hiding points or so called the sample point is randomly selected so that with every new embedding process the position of the sample point changes. That signifies that unlike (Least Significant Bit) LSB where the hiding points remains similar for every embedding process the propose algorithm makes sure that the position of sample points changes with every time data is embedded into an audio file along with this the bit position at which the embedding is done is also varied from 1LSB to 7 LSB.

Keywords: **Audio Steganography, Randomization, LSB, Data Hiding.**

I. INTRODUCTION

Steganography is used to communicate secret information between two parties in such a manner that the existence of the secret message is hidden from the third person. The steganography is being used since a long time now and there are many approaches that have been proposed that provides steganographic application for hiding data in cover medium. The cover medium that is used to hide the secret data can be Images, Audio, or Video.

The hiding of the secret data into the cover medium should not make any undesirable changes to the cover medium so that the originality of the medium is affected. The concept of audio steganography is to embed secret data into an audio file in such a manner that human auditory system (HAS) cannot detect the change that has been occurred due to embedding of the data into the audio file. The audio steganography uses approaches such as (**Least Significant Bit**) LSB, Spread spectrum, and Echo hiding along with other recent applications that has been developed in recent years. The properties of audio steganography [5] that is exploited in different steganography applications are

1. Confidentiality.
2. Imperceptibility.
3. Accurateness.
4. High capacity.
5. Resistance.
6. Visibility.
7. Survivability.
8. Difficult detectability.

Audio steganography is found to be a tough approach to deal with then image steganography because human auditory system is much more sensible than human visual system. The idea is to embed the secret data into an audio file such that there is negligible difference between the original audio file and embedded file.

While embedding the secret data the format has to be keep in mind so that that header part of the wave file (first 44 byte) [17] should be untouched because in case the header gets corrupted, the audio file will also corrupt. The second consideration that should be made is not to embed data into the silent zone [6] as that might cause undesirable change to the audio file.

EMBEDDING PROCESS

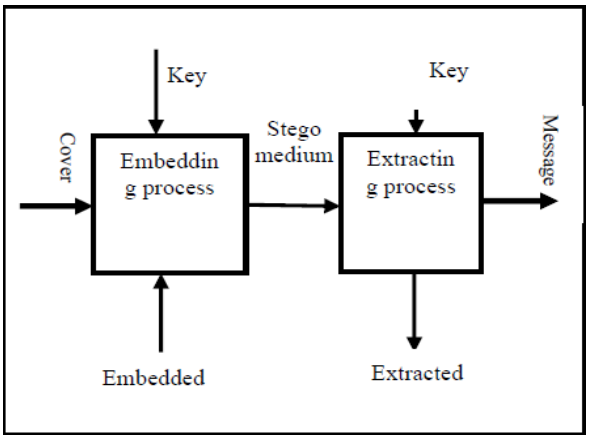


Fig. 1 General Steganography System (Stego-System) [16].

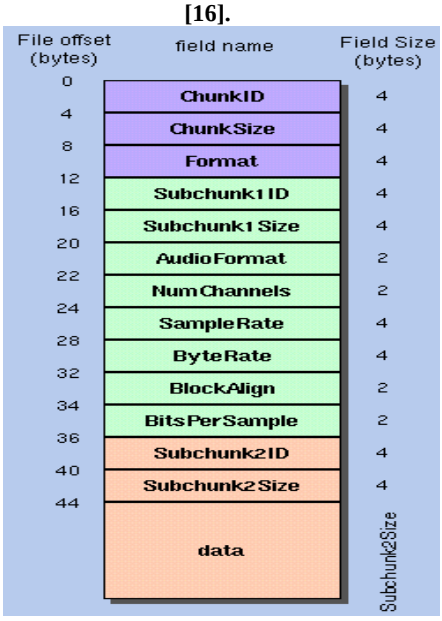


Fig. 2 Wave File Format [17]

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 8, February 2013

II. RELATED WORK

Relevant work has been done on this subject since a long time now. Many have designed system which increase the capacity [4] of the steganography approach and few has increased security by randomizing [5] the position of embedding in the audio file. In recent years, tools for audio steganography such as H4PGP, S-Tools, Steghide[8] has been designed which increases the steganographic features like security and capacity. The most easy and commonly used algorithm for any steganographic application is LSB (least significant bit) it has been used by many designers and in many applications. Concept of Genetic algorithm has also been applied on audio steganography by Mazdak Zamani et al [9]. Here, first problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and Robustness. Creating randomization in the steganographic application can be done using functions like Fibonacci series [5] also a encryption algorithm has been used to encrypt the secret data has to be embedded into the audio file called Kali's technique [10]. Surveys have been done in the field of steganography which shows the strengths and weaknesses of the steganographic approaches against the parameters of capacity, robustness, and security. The steganographic applications are also extended to be used as watermarking schemes to make for the copyright issues and areas where legal issues are concerned [2]. Approaches like spread spectrum of audio data hiding method which hides data throughout an audio file at different frequencies of the file. Work has been done that introduces phase shifting in audio signals to reduce the correlation with PN signal per each sub-band. It allows easy detection of the embedded data signal from audio when de-spreading the compound signal [11]. In [6] a threshold detector is proposed which detects the silent and non-silent places in the cover message. No secret message is embedded in silent places, whereas one or two bits are embedded in LSBs of non-silent places depending upon the intensity of the sound.

In [1], a key management scheme has been used which first decides upon a key that forms the basis of bit index of a byte in the audio cover where the data is to be stored. Polynomial and linear equations are also used in audio steganography to generate the randomization pattern in the steganographic application [14]

There are other methods like echo hiding [15] which is also used in the audio steganography. The basic idea is to provide an idea to store the secret data into random position so that the pattern of hiding the data throughout the audio file changes every time a new embedding process is followed. Moreover, along with finding the secure way to hide the data it should also be taken care of that the file does not get distorted and the extraction of data should be simple if the extraction pattern is known. An audio steganography technique that uses a three-layered architecture for hiding the data has been proposed by Muhammad Asad et al. [13] which gives a secure approach by hiding the secret data first by first mapping the characters of the secret message to bits and than encrypting the secret message and the third layer encodes the message bit throughout the audio file. At the receiver's end the secret message is first extracted and then the extracted message is decrypted and finally character decoding is done. This process enhances robustness and transparency of the process of steganography.

There are ways to make the steganographic application more secure by using the concept of key while extracting the data at the receiver's end. In [10] one such approach has been mentioned which deals with the key exchange between sender and receiver in such a manner that the information about the audio sample points where the data is hidden can be received by the receiver secretly. The other more simple way is to use some pre-defined algorithm at both the sender and receiver's end [12].

III. PROPOSED APPROACH

The approach used in this paper is to randomize the point of embedding of the secret file in the audio file sample points. The size of the secret data file is of a great significance to the randomization algorithm. The randomization pattern used in this design is two fold the first step finds out the byte numbers that will be the sample point for embedding data the second step will be the bit place in that byte where the one bit of the secret data will be embedded. By this way the robustness and transparency of the steganographic technique is increased. The algorithm works as follows.

Some notations used in the proposed scheme are

* Let **K** be the size of secret message file.
* **S_i** is the size of the message file plus 60.
* **T_i** is the additive intermediate result for sum of digits of **S_i**.
* **Q_i**=**T_i**%8.

EMBEDDING PROCESS

1. Read the text message file to be hidden and calculate its size (**S_i**).
2. Read the WAV audio file that will work as cover medium.
3. Convert wav audio file in bit pattern.
4. Read the size of the text file in minimum of three digit e.g. **XYZ** byte.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 8, February 2013

5. Since the header part should be kept untouched so the first 60 byte of the file will be untouched and will not be used for embedding. This is done in case if the message file's length is less than the size of header so that we add 60 byte in order that the embedding starts after the header part.

6. The first bit of the secret data will be embedded into the S_ith byte of the audio data and at Q_ith LSB position of Si

Now for value of j from 1 to (**K**-1)

7. For the next bytes of audio file at which the embedding will be done we add Q_i to S_i that gives S_{i+j} store it to S_i and then again T_{i+j} by adding all digit of S_{i+j} and store it to Ti and similarly we find Q_{i+j} and store it to Q_i

8. For every value of **J** one secret bit of text file is embedded at S_j^{th} byte of audio file and at Q_j^{th} LSB position.

9. In case the value of Q_i comes out to be **0** then it will be automatically changed to 1. Since **0** signifies 8th byte that is the **MSB** where embedding the secret bit can hamper the quality of the data and might change the polarity (sign) of the byte as well.

10. Once all the bit of secret file is embedded the last byte of the audio file will be replaced by the selected value S_i.

11. Apply the symmetric key to the Data and send it across.

EXAMPLE

Let us assume the size of a message file that is to be hidden **K** is 144 byte

S_i= 144+60=204
T_i= **2+0+4** = 6
Q_i= 6%8= 6

The first bit of the message file will be stored into the **204th** position of the audio file and at **6th** LSB position of **204th** byte.

$S_{i+1} = S_i + Q_i$ = 204+6=210
$S_i = S_{i+1}$
T_i= **2+1+0=** 3
Q_{i+1}= **3%8**= 3
$Q_i = Q_{i+1}$

The next bit of the message file will be stored at **3rd** LSB position of the **210th** Byte.

Similarly the **3**rd bit will be embedded at **6th** LSB position of the **213th** Byte.

This will continue till the time all the bit in the secret message gets encoded into the audio file.

Once the embedding is done the data (cover+ message) is encoded using a key this is symmetric key used by both sender and receiver the key could be anything a picture file, message file audio file however, the key should be same at both the end in case the receiver does not have the key he will not be able to extract the message.

EXTRACTION

Extract the data by using the symmetric key.

1. Convert the received audio file into bit pattern.
2. Store the bits into an array.
3. Read the last byte of the audio file to get the position of the first hidden bit (S_i).
4. As done in embedding process, calculate T_i and Q_i for every value of S_i.
5. Divide the entire array into chunks of 8.
6. Set a counter to 1.
7. Get the secret data bit from each S_i^{th} Byte's Q_i^{th} bit position and store it into an array.
8. If value of Q_i is found to be 0 change it to 1.
9. Repeat step 6 to 8 till the counter reaches **K-1. (K= S_i -1)**
10. Read the Decoded array in chunk of 8, and
11. Convert the sequence of bits obtained using 8- bit ASCII code.

EXAMPLE

Let us assume the size of a message file that is to be hidden **K** is 144 byte.

S_i= 144+60=204,
T_i**= 2+0+4 =** 6,
Q_i= 6%8= 6.

The first bit of the message file will be stored into the **204th** position of the audio file and at **6th** LSB position of **204th** byte.

$S_{i+1} = S_i + Q_i$ = 204+6=210
$S_i = S_{i+1}$
T_i= 2+1+0= 3
Q_{i+1}= 3%8= 3
$Q_i = Q_{i+1}$

The next bit of the message file will be stored at **3rd** LSB position of the **210th** Byte.

Similarly the **3**rd bit will be embedded at **6th** LSB position of the **213th** Byte.

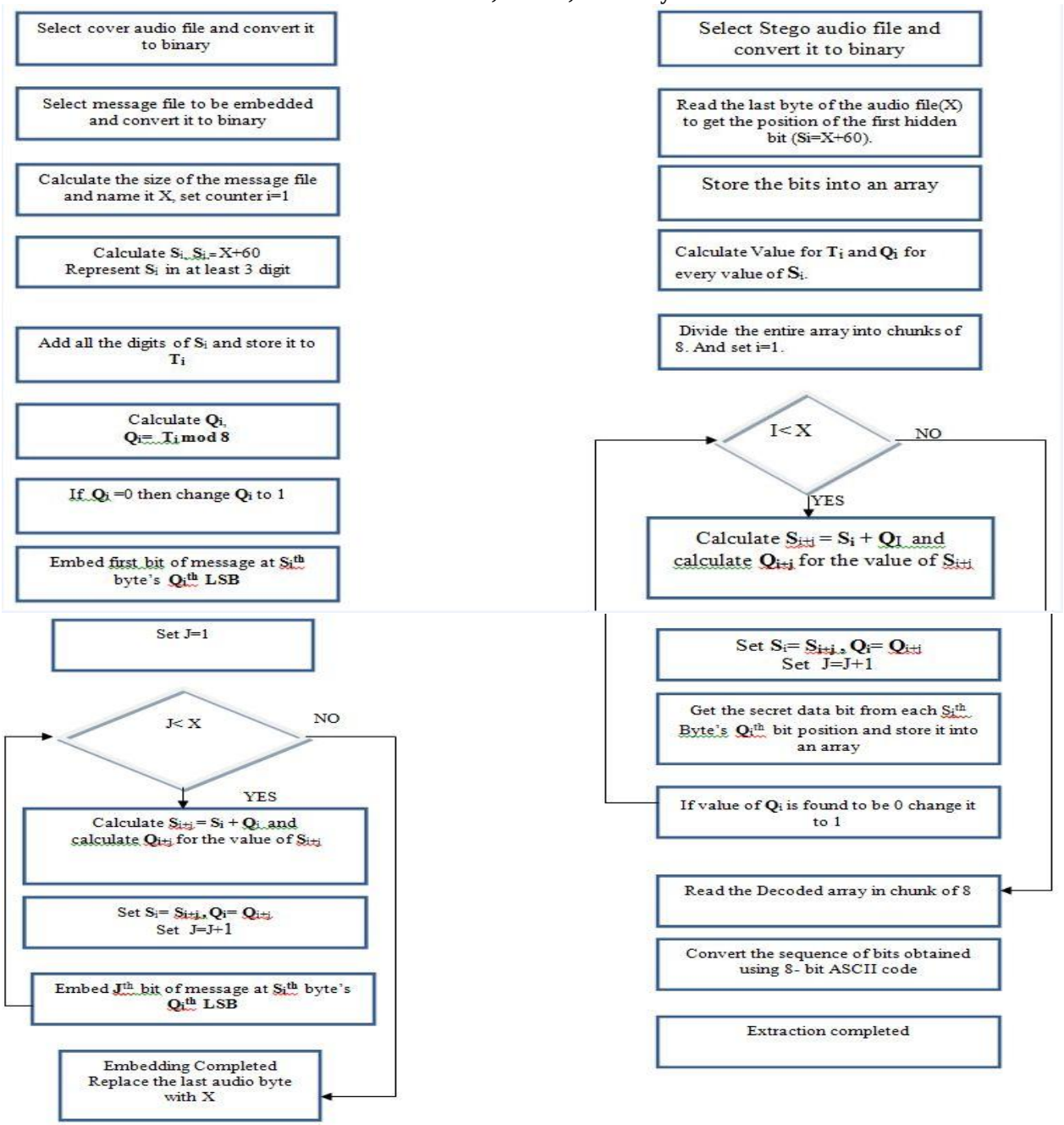
This will continue till the time all the bit in the secret message gets encoded into the audio file.

Once the embedding is done the data (cover+ message) is encoded using a key this is symmetric key used by both sender and receiver the key could be anything a picture file, message file audio file however, the key should be same at both the end in case the receiver does not have the key he will not be able to extract the message.

IV. FLOWCHART

The flowchart of the embedding and the extraction process is as follows. This will give a clear picture about the flow of the process from the beginning till the end of the both the embedding and the extraction process.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 8, February 2013



V. ANALYSIS OF THE PROPOSED SCHEME

The objective of this system is to provide a randomization pattern of the audio steganography system. The Randomization pattern created here is twofold approach first the system randomizes the steganography process by selecting random byte position in the audio file for embedding of the message bit and secondly the system choses random bit from every sample byte for data injection selecting any random bit from 1LSB to 7LSB.

The .WAV audio file in figure 3 of size 330 KB has been embedded with a text of size 200 bytes, and secret key used is a JPEG image of size 23.4 KB which gives the resultant stego audio file in figure 4. The size of the message data is very less in comparison to the audio file hence it does not create any undesirable change to the audio that might cause its sound quality.

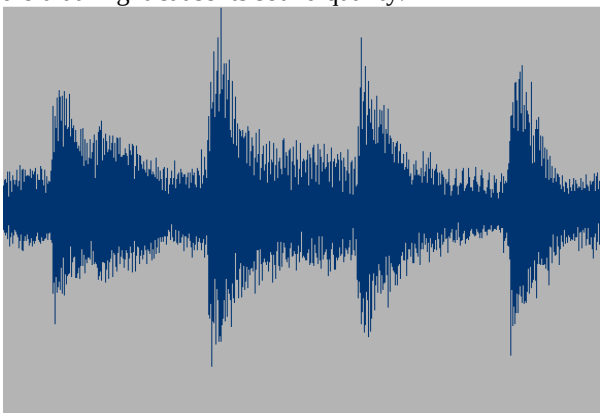


Fig. 3 Audio file before Embedding (cover audio file)

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 8, February 2013

Size of audio file = 330 KB.
Length= 3 Seconds .
Data to be embedded is "This is the first attempt."
Size of message data= 25*8 = 200 Bytes.
Therefore, first audio byte where embedding will be done is 260th byte.

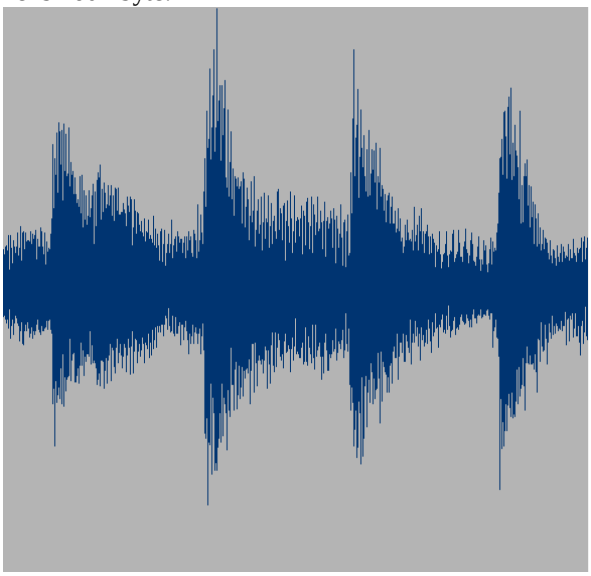


Fig. 4 Audio file after embedding (Stego audio file)

VI. CONCLUSION

Data security has been of a great importance since last few decades. Methods for secure data transmission have been used to transmit digital data in a secure manner which should not be exploited by unintended users. In this paper, data transmission with the use of audio steganography has been used where the secret data is spread throughout the audio file with the concept of randomization. This increases the security of the audio steganography approach and since a key management is also used in this which states that unless and until receiver has the same key as the sender than the receiver cannot extract the data. The randomization technique used in this paper is dual layered as it first randomises the bytes at which the embedding is done and than it randomises the bits at every byte on which a single bit of secret data will be embedded.

REFERENCES

[1] Jassim Mohmmed Ahmed and Zulkarnain Md Ali "Information Hiding using LSB technique" IJCSNS International 18 Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.

[2] F. A. P. Peticolas, et al., "Information hiding–a survey," Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.

[3] S.K.Moon, R.S.Kawitkar "Data Security using Data Hiding" International Conference on intelligence and multimedia Application. IEEE 2007.

[4] Nedeljko Cvejic ,Tapio Seppben " Increasing the capacity of LSB Based audio Steganography", IEEE 2002.

[5] Harish Kumar and Anuradha "Enhanced LSB technique for Audio Steganography" IEEE July 26 2012.

[6] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nozaki, "An audio steganography by a low-bit coding method with wave files", 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 530 - 533.

[7] Kriti Saroha and Pradeep Kumar Singh "A Variant of LSB Steganography for Hiding Images in Audio" International Journal of Computer Applications (0975 – 8887) Volume 11– No.6, December 2010.

[8] Fatiha Djebbar et al., "A view on latest audio steganography techniques" International Conference on Innovations in Information Technology 2011.

[9] Mazdak Zamani et al., "An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography" IEEE 2009.

[10] Kaliappan Gopalan., "Audio steganography using bit modification", 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, Page(s): II - 421-4 vol.2.

[11] H. Matsuoaka "Spread Spectrum Audio Steganography Using Sub-band Phase Shifting" Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP '06. International Conference on **Dec**. 2006 Japan.

[12] Muhammad Asad, Junaid Gilani, Adnan Khalid, "An enhanced least significant bit modification technique for audio steganography", 2011 International Conference on Computer Networks and Information Technology, Pages: 143 - 147.

[13] Muhammad Asad, Junaid Gilani, Adnan Khalid "Three Layered Model for Audio Steganography" IEEE 2012.

[14] Jeddy Nafeesa Begum, Krishnan Kumar, Vembu Sumathy "Design and Implementation of Multilevel Access Control in Synchronized Audio to Audio Steganography Using Symmetric Polynomial Scheme" Journal of Information Security, 2010.

[15] Chunhui Xie, Yimin Cheng and Fubao Wu "A new detection scheme of echo hiding" Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on 17-19 Dec. 2010.

[16] Poluami D., Debnath B., and Tai-hoon K., "Data Hiding in audio signal : A Review", International Journal of Database Theory and Application, vol.2, No.2, June, 2009.

[17]https://ccrma.stanford.edu/courses/422/projects/WaveFormat/ (last accessed on 20th February 2013).

AUTHOR BIOGRAPHY

Lovey Rana, currently pursuing M. Tech in Computer Science and Engineering, at C-DAC Noida prior to this completed her B.Tech in Computer science and engineering from Amity University Noida. Her areas of interest include Cryptography, Steganography currently working on a project in graphical password authentication.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 8, February 2013

Saikat Banerjee, currently pursuing M. Tech in Computer Science and Engineering, at C-DAC Noida. He completed his B.Tech in Computer Science Engineering from Kurukshetra University. Worked with IBM Global Services and Dell International. His areas of interest include Computer security with the essence of Steganography and cryptography. Currently working on a project on Audio Steganography.