A Novel Technique for Secure Data Transmission using Audio/Video Files

Sanchita Gesu[1], Shivam Vasudeva[2], Snehil Bhatt[3], Santhosh B[4]
Department of Telecommunication Engineering
Dayananda Sagar College of Engineering,
Bangalore, India

***Abstract*--With the advancement of digital technology around the world through the internet data security has become a fundamental need of mankind. In order to fulfil the need, combination of cryptography and steganography is used. In this paper, we propose a highly secure data transmission system which employs these two techniques for audio files. A robust communication system is designed in such a way that it provides confidentiality, integrity, availability of network and security of data from malicious attacks. Cryptography is achieved by DES algorithm which scrambles a message so that it cannot be understood whereas LSB algorithm is employed in steganography which hides the message so that it cannot be seen. The simulation results show that the proposed system displays two level of security**.

Keywords--Cryptography, Steganography, LSB algorithm, DES algorithm

I. INTRODUCTION

Steganography is the process of hiding secret communication between two parties; a stenographic system thus embeds hidden data in a discreet cover file so that no unauthenticated third party could sense its existence. In earlier days, people used hidden tattoos or invisible ink to convey stenographic content. Today, with the advent of technology, steganography becomes easy with the help of advanced communication channel. In steganography, to begin the information hiding process, the redundant bits of the cover medium are calculated (those that can be improvised without disturbing that medium's integrity). A steno environment is created by replacing these redundant bits by the bits of the secret data [4]. The aim of the modern steganographic system is to make the unauthorized party unaware of the presence of any secret data. Cryptography and Steganography are most popular techniques that exploit information in order to cipher or hide their existence respectively. Cryptography makes the message unreadable whereas Steganography hides its mere existence. According to [1], for secure communication, cryptography is not sufficient. Even though both cryptography and steganography provides secured communication individually, a study is being to combine both the systems in one unit so as to come up with the best possible system for providing secured communication [5]. This is indeed the goal of this research. According to [7], the strength of Steganography is in dubiousness of the secret message in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable where the third party knows about its existence. Thus a steganographic system is said to be successful only if an observer is unaware of the existence of the embedded secret message. All efforts must be put to ensure that the message is invisible unless an authenticated user looks for it. The way in which this process takes [lace depends upon the media used for the cover file and the secret message. In each case, the quality of the Steganographic system can be evaluated by measuring how much secrecy can be handled by a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding [7].

Now that we know that cryptography and staganography are the techniques used for information hiding, we might as well want to concentrate on the type of data it can hide. Any data in the form of text, image, audio or video can be hidden. According to [7], the most common techniques of hiding information within a text, image, audio or video is LSB coding, parity coding or by spread spectrum. In this paper, as a demonstration, an audio file was hidden inside another audio file and a more powerful method of employing LSB coding was displayed.

II. COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography and Steganography methods are easily exposed to attacks by Steganalysis, so there is a constant need to develop new method .Steganography hides the existence of secret message. On the other hand, cryptography is the encryption and decryption of data and with a secret key so it cannot be understood. Cryptography creates cipher message which might provoke the attacker. On the other hand an invisible message created with stenographic methods will not. However, steganography can be useful when the use of cryptography is illegal. Where the use of cryptography is barred, steganography can avoid such policies to pass the message secretly. However, steganography and cryptography are looked upon differently.Cryptography fails when the attacker is able to access the content of the cipher message, while steganography fails when the attacker detects that there is a secret message present in the stenographic medium. However, the combination of these two methods will enhance the security of the data embedded. This combined will satisfy the requirements such as authentication, security, and robustness for secure data transmission over an open channel.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

The proposed work combines both cryptography and steganography into a single system to provide strong security because of two levels of data encryption by using LSB steganography the cipher text will hide inside the cover file after the data encryption A pictorial representation of the combined concept of cryptography and steganography is depicted in fig.1

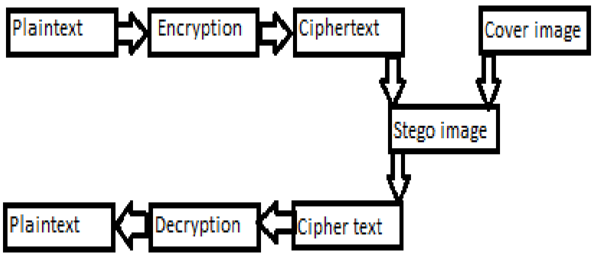
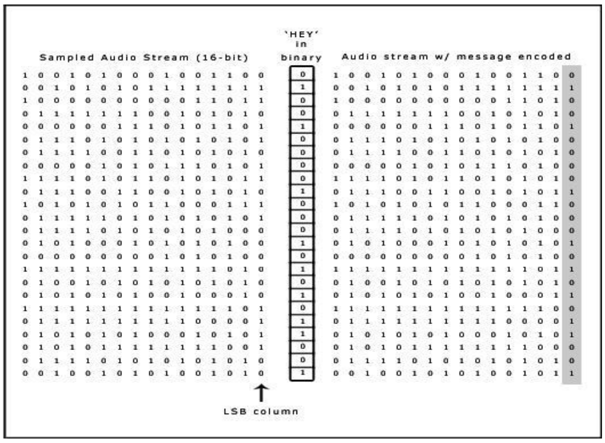


Fig 1: Combination of cryptography and steganography

III. METHODOLOGY

A. Least Significant Bit (LSB)

LSB or least significant bit coding is one the most popular algorithm in which the least significant bits of some of the bytes of the cover file is replaced by some of the sequence of bytes of the secret message [2]. LSB coding is the simplest way in which embedding of secret information takes place by substituting the least significant bit of each sampling points with a binary part of the secret message. Here, the least significant bit (LSB) is that bit of the binary form of the integer that determines whether the number is even or odd. The LSB is also known as the right-most bit, because of theancient rule of positioning the least significant bit to the right most position. It is symmetrical to the least significant digit of a decimal integer, in which the right most decimal digit is the least significant. In a binary number, to refer specific bits, it is mundane to assign each bit a bit number ranging in ascending order from 0 to a number which is one less than the number of bits in that binary number. The least significant is most vulnerable to change rapidly even when there is a slight change in the number. For instance, if 5 (binary 00000101) is added to 4 (binary 00000100), the result will be 9 (binary 00001001) and the least significant bits will change (0100 to 1001). Contradictory to this, the four most significant bits stay as it is (0000 to 0000). Least significant bits are frequently employed in pseudorandom number generators checksums. The figure below illustrates how the message "HEY" is encoded in a 16-bit CD quality sample using the LSB method.In figure 2, the cover medium is the audio file and the secret message is HEY. HEY is to be embedded inside the audio file. First the secret information 'HEY' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information 'HEY'. After embedding the secret message 'HEY', the file is called stego-file. LSB method was employedduring the encoding stage to embed the message inside an audio/video file.



```
                                                 'HEY'
                                                  in
Sampled Audio Stream (16-bit)                   binary    Audio stream w/ message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0                   0       1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1                   1       0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1                   0       1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0                   0       0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1                   1       0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1                   0       0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0                   0       0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1                   0       0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1                   0       1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0                   1       0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1                   0       1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1                   0       0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0                   0       0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 0                   1       0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0                   0       0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0                   1       1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0                   0       0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0                   1       0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1                   0       1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1                   1       0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1                   1       0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1                   0       0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0                   0       0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0                   1       0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1
                              ↑
                          LSB column
```

Fig 2: Illustration of how the message "HEY" is encoded using LSB

.B.Encoding

LSB method's advantage is that it permits a large size of secret information to be embedded in another file. Here we take an audio file which contains set of bytes which can be used for encoding. Bytes in the audio file depend upon the size of the audio file. The steps of encoding are as follows:

- Encryption of message is done with the help of public key.
- The audio file is converted into streams of bits
- Each character in the secret message is then converted into streams of bits
- The LSB of the cover file is then replaced with the LSB of the secret message

C.Decoding

In the decoding stage, the encoded message is decoded to retrieve the hidden message. First decoding of hidden message takes place then decryption is performed with the help of public key which is known only to the authorized receivers or users of the proposed system.

D. Encryption

In the process of encryption, the user is asked to enter a key which has to be chosen carefully preferably a combination of letters, digits and special characters. Now before the encoding takes place, this key is used to encrypt the secret message.

E. *Decryption*

The key which was set by the user is then used to decrypt the message in order to get the original secret message. The processes of encryption and decryption are carried out by DES (Data Encryption Standard) algorithm.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

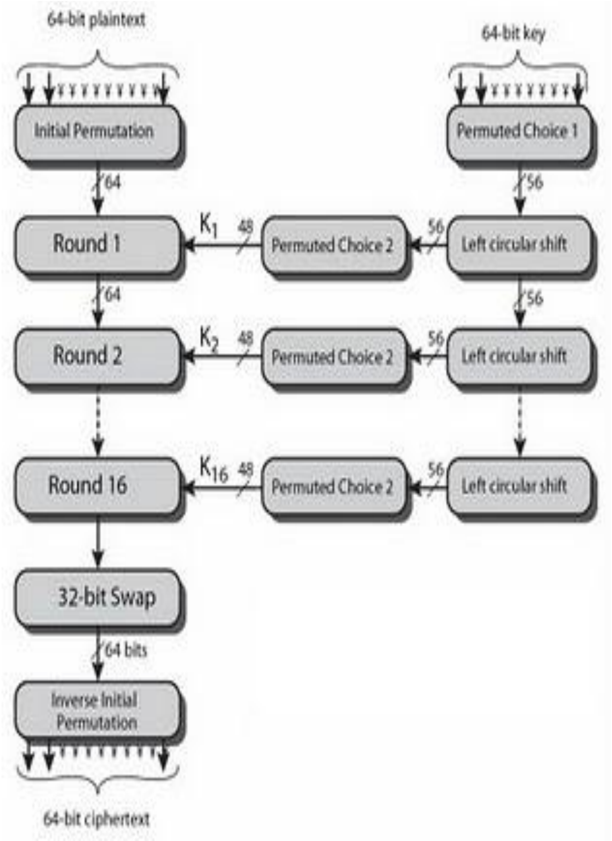


Fig 3: DES Algorithm

IV. RESULTS AND DISCUSSION

A. Main class

The system that is proposed in this paper is implemented using java programming language. As we execute our program, the following GUI is displayed which gives user an option to hide or unhide the file as can be seen on the left hand side of the window file inside the cover file. Moreover, option to transmit the file via client server technique is also provided. The interface also allows the user to exit the application.

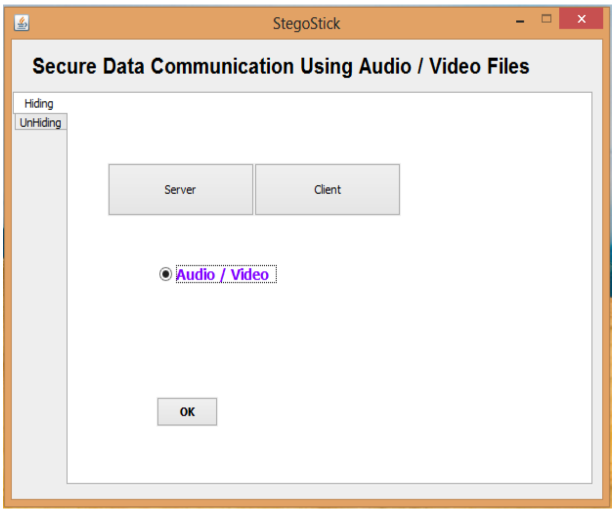
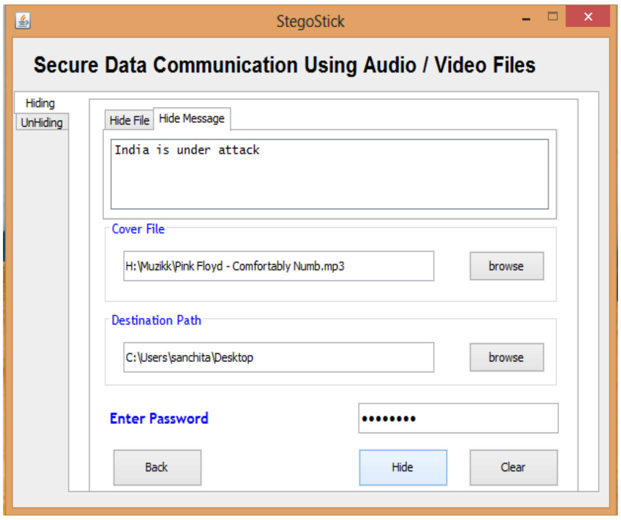


Fig 4: Interface after execution of main class

B. Embedding/Encrypting Process

Figure 5 shows the embedding/encrypting window. This window pops up after we click on the OK button after selecting the Audio/Video radio button. This gives an option to select either a text file or any other file of any format to select as the secret message. Then the option to select the cover file is given through which a file of any format, be it text, image, audio or video can be selected. After that, the destination path is provided where the location for the stego file to be stored is selected by the user. A strong password has to be inputted by the user which works as a key for encryption. After that, hide button is clicked.



India is under attack

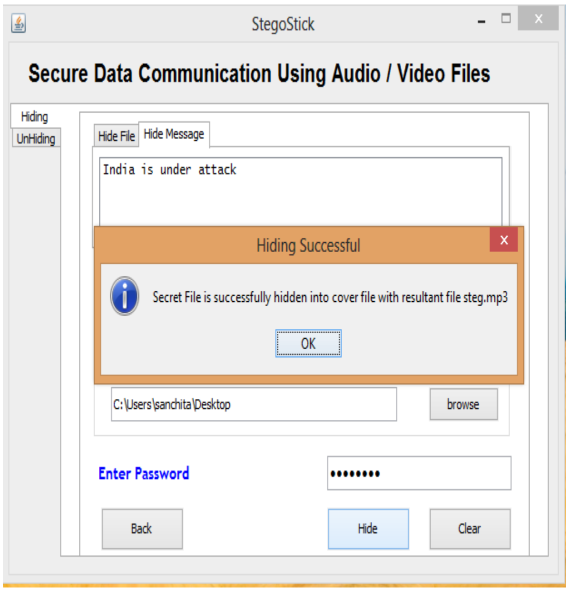
Cover File: H:\Muzikk\Pink Floyd - Comfortably Numb.mp3

Destination Path: C:\Users\sanchita\Desktop

Enter Password: ••••••••

Fig 5: Interface foe selection of secret message and cover file

(This work is licensed under a Creative Commons Attribution 4.0 International License.)



India is under attack

Secret File is successfully hidden into cover file with resultant file steg.mp3

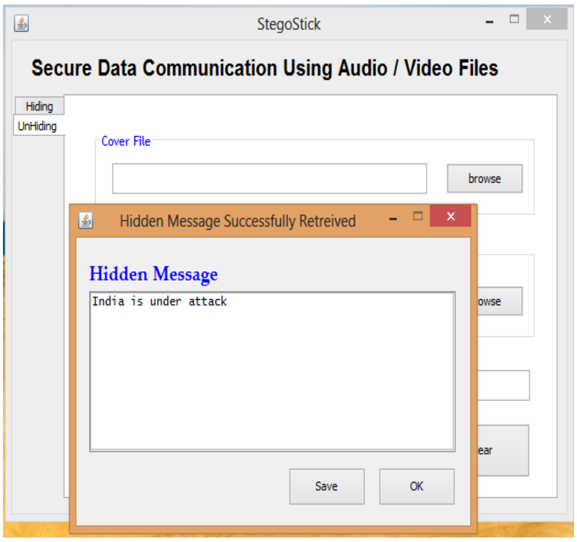
C:\Users\sanchita\Desktop

Enter Password: ••••••••

Fig 6: Interface after the hiding process

After the hide button is clicked, a message is displayed which says that the secret file is successfully hidden into the cover file. The only condition for a success message is that the size of the cover file should be greater than the size of the secret message.

C. Extracting/Decrypting



StegoStick
Secure Data Communication Using Audio / Video Files
Hiding
UnHiding
Cover File
browse
Hidden Message Successfully Retreived
Hidden Message
Save
OK

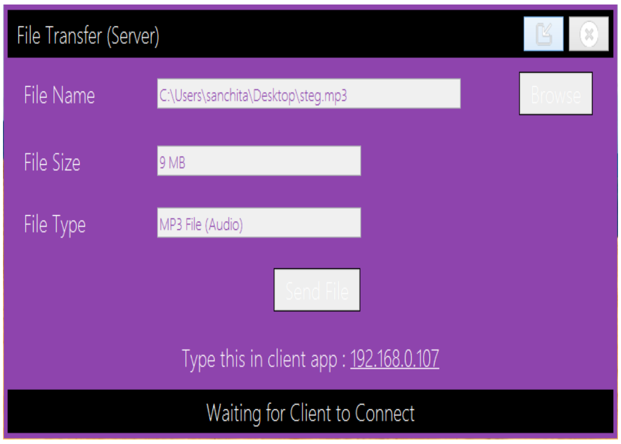
India is under attack

Fig 7: Extracting and decrypting of secret message

The stego file along with the destination path is chosen. After entering the correct password only, the secret message is retrieved successfully. In case of incorrect password, an error message will be displayed

D. Data Transmission

The Graphical user interfaces shown below asks for the encrypted/embedded file after which file can be sent. At the receiver side, the client needs to input the correct IP address of server failing which it won't be able to receive the file.



File Name: C:\Users\sanchita\Desktop\steg.mp3

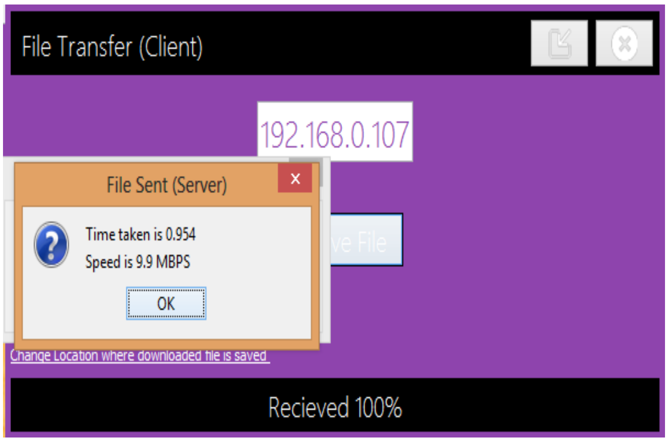
File Size: 9 MB

File Type: MP3 File (Audio)

Type this in client app : 192.168.0.107

Waiting for Client to Connect

Fig 8: Sending of stego file



192.168.0.107

File Sent (Server)

Time taken is 0.954
Speed is 9.9 MBPS

Recieved 100%

Fig 9: Receiving of stego file.

After receiving the stego file, extraction/decryption takes place as mentioned.

V. CONCLUSION

In this paper, we have devised a methodology for embedding data into a cover file which can the either audio or video. The data can be text, image, audio or video. The algorithm will not work properly if the size of cover file is smaller than the size of data to be embedded. Cryptography makes the data unintelligible whereas steganography aims at hiding the data into cover file. Steganography combined with cryptography, creates is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. A highly secured technique of cryptography is used (DES) along with steganography (LSB) which makes the decoding of data much harder for any malicious attacker. The proposed system can be implemented in several field of applications such as military, intelligence, aviation, maritime, national security and business purposes. The encryption and decryption techniques along with

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

steganography creates a two level security which is difficult to intervene. Also, this paper encorporates the system with multi-level security as per required. It means that the user creates a stego file and can use it as cover file to hide another secret data. This would require two different passwords which one has to remember while entering. The process can be repeated over and over again.

VI. REFERENCES

[1] Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. *International Journal of Computer Applications*. 8(9), pp. 7-10.Retrieved 14th August, 2012 from http://www.ijcaonline.org/volume8/number9/pxc3871714. pdf.

[2] Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. *International Journal of Multimedia and ItsApplication*, 3(3), pp. 86-96

[3] Mark D. G. 2003. Chameleon Image Steganography-Technical Paper. Retrieved 14th July, 2012 from http://faculty.ksu.edu.sa/ghazy/Steg/References/ref13.pdf.

[4] Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. *IEEE Computer Society*. IEEE Security and Privacy, pp. 32-44.

[5] Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. *International Journal ofComputer Technology Application*, 2(3), ISSN: 2229-6093, pp. 626-630.

[6] Simon, B., Steve M., and Ray, F. 2005. Object-Oriented Systems Analysis and Design Using UML, (3rd ed.), McGraw Hill.

[7] Sridevi, R., Damodaram, A., and Narasimham, S. 2009. Efficient Method of Audio Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. *Journal of Theoretical and AppliedInformation Technology*, pp. 768-771. Retrieved 21stAugust, 2012 from http://www.jatit.org.

[8] Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and KshitizRastogi 2012. Public-Key Steganography Based on Modified LSB Method. *Journal of Global Researchin Computer Science*, 3(4). ISSN: 2229-371X, pp. 26-29.

[9] Domenico, B. and Luca, L. year. Image Based Steganography and Cryptography.

[10]Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method.
European Journal of Scientific Research, 40(2). ISSN:1450-216X. EuroJournals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.

[11]Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. *Signal & ImageProcessing: An International Journal (SIPIJ)*, 1(2), pp 60-73.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)