A Secure Matrix Based Audio Steganography with Dual Encryption

Ratul Chowdhury, Anirban Das, Prof. Samir Kumar Bandyopadhyay

Abstract— **Cryptography and Steganography are the major part of information security. In this paper we combine these two techniques to perform a powerful data encryption. In first level, the concept of sparse matrix has been introduced to encrypt the target string and in second level, by using the standard LSB method, the message is secretly embedded into a cover file in such a way so that its existence is unidentified. A temporary 4*4 matrix is constructed from the target string where most of the elements are zero. Instead of embedding the target string directly, the positional values of the nonzero elements (row and column number) are identified from the temporary matrix. By using the traditional LSB method, the numbers of nonzero elements with their positional value are embedded into the cover file. In the next segment, the performance of the proposed method is calculated in terms of two parameters: the first one is Means square error (MSE) and the second one is Signal to noise ratio (SNR). And finally, a comparison has been carried out with the traditional LSB method. The experimental results and the comparisons demonstrate that our proposed work is highly efficient in terms of encryption and the capacity size of the text. A huge volume of text can be accommodated into the cover file and the difference between the original cover file and the stego file is so minute that it can't be identified by the human auditory system.(HAS).**

Index Terms— **LSB Method; RSA; AES; DES**

I. Introduction

The internet provides a wealth of information and services. Many activities in our daily lives now rely on the internet including various forms of communication, shopping, financial services, entertainment and many other application. As a result securing these information became a critical issue for everyone. Cryptography and steganography are two security methods for provide data confidentiality**.** Cryptography is the art of protecting information by transforming it into an unreadable format called cipher text. Steganography is the hiding of a secret message within a cover media. The cover media can be an image or an audio file. Steganography takes cryptography a step farther by hiding an encrypted message such that no one suspects it exists.

In this proposed method the concept of cryptography and steganography are combined to perform a powerful encryption. In first level the concept of sparse matrix has been introduced. Sparse matrix is a matrix in which most of the elements are zero. In representation of sparse matrix only the value of the nonzero elements are stored in memory to reduce the wastage of memory. In our method a 4*4 temporary matrix has been constructed from the target string where most of elements are zero. We have done the first level encryption by send the location of the nonzero elements i.e their row and column number .And the second advantage is that we don't have to send the value of the nonzero elements because we are using the binary sequence where nonzero means 1. In second level the traditional LSB method has been used. It is the simplest steganography technique embed the bits of the target string into the least significant bits of the cover file. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

In receiving side the reverse algorithm has been used. A temporary 4*4 matrix has been constructed which consists of all zeros. From the least significant bits of stego file the location of the nonzero elements are identified one by one and corresponding row and column number of the temporary array replaced by 1 the rest are zero as usual. Each temporary matrix contains 2 character of the target string after merging two rows two consecutive rows of the temporary array we can get the whole target string.

Finally the quality of the experimental results are analyzed with respect to two parameters one is means square error and the second is signal to noise ratio. The experimental results shows that there is a very negligible change into the stego file which is impossible to identify by the human auditory system.

II. Literature Survey

Cryptography, Steganography, and water marking are the three major part of information hiding. In cryptography sender converts the plain text to cipher text by using an encryption key and in receiving side the receiver decrypt cipher text to plain text. Steganography is used to embed message within another object known as cover file. The cover file can be an audio signal or digital image. Watermarking on the other hand is the process of embedding message on to a host signal. Watermarking, as opposed to steganography has additional requirement of robustness against different types of possible attacks. Water marking can be either visible or invisible.

Cryptographic algorithms are basically divided into two parts, Symmetric key cryptography and asymmetric key cryptography. Symmetric key algorithms use the same cryptographic key for both encryption and decryption purpose or there may be simple transformation to go between the two

Manuscript received March 14, 2016

Ratul Chowdhury, Assistant professor, Future Institute of Engineering and Management Sonarpur Station Road, Kolkata, West Bengal

Anirban Das, UG Student, Jogesh Chandra Chaudhury College

Prof. Samir Kumar Bandyopadhyay, Department of Computer Science and Engineering University of Calcutta

keys. Some popular symmetric key algorithms are AES, DES, Blowfish etc. Asymmetric key cryptography uses a pair of keys to encrypt or decrypt the message so that it arrives securely. The keys are generally called public and private key. RSA, Diffie -Helman key exchange, PGP are the most popular asymmetric key algorithm.

For any audio steganography technique to be implementable it must satisfy three core conditions [1].

1. **Capacity**: Capacity means the amount of secret information that can be embedded within a cover audio file.
2. **Transparency**: Transparency evaluates how well a secret message is embedded into a cover audio so that its existence is undefined.
3. **Robustness:** Robustness measure is the ability of secret message to withstand against attacks.

Audio steganography is the way to store the secret information into a cover file in either frequency domain or time domain. The popular audio steganography techniques are [2, 3].

a. **Low bit encoding:** It is technique to store the data into the least significant bits of the cover file. It is a simple technique and by using this technique and by using this technique a huge volume of text can be embedded into a cover file [7].

b. **Phase coding:** Phase coding works by substituting the phase of an initial audio segment with a reference phase, this phase actually represents the hidden data.

c. **Spread spectrum technique:** It is a technique designed to encode any stream of data via spreading the encoded data across as much of the frequency spectrum as possible [10].

d. **Echo hiding:** Echo technique embeds data into a cover audio signal by introducing an echo; the hidden data can be adjusted by two parameters, the first one is amplitude and the second is offset. These two parameters represent the magnitude and time delay of the embedded echo.

The current trend of audio steganography combines the concept of cryptography and steganography to perform a powerful encryption [14, 15]. Lots of cryptographic algorithms (symmetric and asymmetric key) are used to perform the first level encryption of the message. RSA, AES, DES are the popular algorithm which are used to encrypt the message first after that by using traditional audio steganography method the encrypted version of the message is embedded into a cover audio file. Lots of algorithms from different domain are now use with LSB based audio steganography for security purpose. One approach is modulo operator [12], where the first level encryption is done by using modulo operator and in second level by using standard LSB method the encrypted version of the text is embedded into the cover file Genetic algorithm base approach is another example . Genetic algorithm is a technique for optimization and search. Generating population, creation of fitness function and mutation are the three major parts of genetic algorithm. By using these three parts the message is encrypted in a well manner [6]. An alternative approach is to perform the first level encryption by using XOR operator. Another method is spectrum manipulation where the frequency of the transmitted signal is deliberately varied to perform better encryption. Zigzag LSB method is another approach, where the binary value of the of the secret message is inserted into the last bit of the audio in a zigzag fashion. On the average, only half of the bits are altered in the audio file. So there are no noticeable sound variations of the audio file before and after hiding the data. Multiple least significant bits modification is sometimes used to accommodate large volume of data [4]. This gives an increased robustness against noise addition. The idea of image steganography is used in audio steganography.Spatial-based schemes embed the data into the pixels of the cover image directly, while transform-based schemes embed the data into the cover image by modifying the Coefficients in a transform domain, such as the Discrete- Cosine Transform (DCT).In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information.

In this paper we have used a matrix based technique whose positional values of the nonzero elements are used to encrypt the target string and for transmission purpose the traditional LSB based method has been used.

III. Detailed method for encryption

The detailed encryption process of the proposed method is described in the following subsections.

3.1. Binary equivalent of the cover file and the target string.

The binary equivalent of the cover file and the target string is converted into 8 bits pattern. After digital encoding the cover file has n rows and 8 columns. The conversion of the target string is done according to their ASCII value. Suppose the target string is “abcd”, the character wise blocking and its corresponding binary equivalent is shown in Table 1.

Target string	a	b	C	d
ASCII value	97	98	99	100
Binary equivalent	0110 0001	0110 0010	01100011	01100100

Table 1. Binary equivalence of the target string

3.2. Construction of temporary matrix from the target string

A temporary 4*4 matrix has been constructed form the target string by merging two characters in row major order. Each matrix contains two characters of the target string. The matrix representation is shown in Figure 1.

$$M(1)= \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M(2)= \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Figure 1. Construction of temporary matrix

3.3. Nonzero elements row and column number estimation

A temporary table has been constructed from each 4*4 temporary matrix. This consists of row and column number of each nonzero element. To reduce the number of bits the rows and columns number has started from 0 and ends with 3. The binary equivalent of each rows and column are used further for LSB replacement. The temporary table construction from matrix number 1 and 2 are shown in Table 2 and 3.

No of nonzero elements	Row value	Column value
1	0(00)	1(01)
2	0(00)	2(10)
3	1(01)	3(11)
4	2(10)	1(01)
5	2(10)	2(10)
6	3(11)	3(11)

Table 2. Number of nonzero elements with their location from Figure 1 first matrix.

No of nonzero elements	Row value	Column value
1	0(00)	1(01)
2	0(00)	2(10)
3	1(01)	2(10)
4	1(01)	3(11)
5	2(10)	1(01)
6	2(10)	2(10)
7	3(11)	1(01)

Table 3.Number of nonzero elements with their location from Figure 1 second matrix.

3.4. Size estimation

We are accommodating 2 characters of the target string into the temporary matrix. The number of times the temporary matrix will be constructed are (No of characters in the target string)/2.We have accommodated 10 bits to represent it. So maximum 2^{10}=1024 times we can create the temporary matrix and since each temporary matrix contains 2 characters of the target string so maximum 1024*2=2048 characters we can accommodate into the cover file. This part is used in the receiving end to identify in which part of the cover file the target sting is secretly hidden.

3.5. LSB replacement

The LSB of the first 10 rows of the cover file are replaced by the temporary matrix construction number. From row number 11 onwards select each temporary matrix and replace each LSB of the cover file by the number of nonzero elements contain at that matrix and its location number. After embedding the whole encrypted message into the cover file the required stego file will create.

IV. Detailed Method for Decryption

In receiving side the stego file is the input. The detailed decryption process are described given below.

4.1. Digital encoding of the stego file

It performs bit level manipulation to encode the message. The following steps are

A. Accept the stego file as input.
B. Finds its binary equivalent.
C. Block it into 8-bits pattern.

4.2. Size estimation

The LSB of the first 10 rows of the cover file identifies the number of times the temporary matrix has been constructed.

4.3. Temporary matrix construction

A temporary 4*4 matrix has been constructed into the receiving end where all the elements are initially 0. From row number 11 onwards each 4 consecutive rows first defines the number of nonzero elements of the temporary matrix and the next part defines the row and column number of each nonzero element. After identifying the row and column number of each nonzero element replace the corresponding bits of the temporary matrix by 1. The corresponding matrix construction is shown in Figure 2.

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Figure 2. Temporary matrix in the receiving side

Now let us assume the LSB of the four sequential consecutive blocks are 0111, 0001,0010,0110,0111,1001,1010,1101.The decimal equivalent of the first four LSB is 0111=7 which signifies the number of nonzero elements in the temporary matrix are 7. For the rest of the elements two left most bit signifies the row number and two right most bit signifies the corresponding column number of the nonzero element. The location of the nonzero elements are identified in Table 4.

Two left most bits	Row number	Two right most bits	Column number
00	0	01	1
00	0	10	2
01	1	10	2
01	1	11	3
10	2	01	1
10	2	10	2
11	3	01	1

Table 4: Location identification of the nonzero elements

The row and column number identified from table 4 are the location of the nonzero elements. Since we are using the binary the binary string so here nonzero means 1.After the replacement the temporary matrix of Figure 2 is shown in Figure 3.

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Figure 3.Construction of temporary array with nonzero element

4.4. Construction of the character from the temporary matrix

Two consecutive rows the temporary matrix gives one character of the target string. From Figure 3 after merging two rows we can get two characters of the target string shown in

Table 5. This process will repeat until the whole message is fetched from the cover file.

Bit stream	Decimal equivalent	Character
01100011	99	c
01100100	100	d

Table 5. Retrieval of characters from the bit stream.

V. The algorithm for the encryption and decryption process is given below.

5.1. Algorithm Encryption

Input: A cover audio file and a target string.
Output: A Stego file.

```
1. Start
2. Digitalize the cover file and group it into 8 bits block.
3. Convert the target string into binary form according to their ASCII value.
4. Group it into 8 bits block.
5. Marge two consecutive character of the target string in row major order and form a 4*4 temporary matrix.
6. This temporary matrix construction procedure will continue until the end of the target string.
7. For each 4*4 temporary matrix constructed from the target string find the number of nonzero elements from it.
8. From each 4*4 temporary matrix create a temporary table which consists of each nonzero element's row and column number.
9. Since each 4*4 temporary matrix consists of two character of the target string, so the temporary matrix construction will be performed (number of characters in the target string/2) times. Suppose the number is temp.
10. 10 bits are allotted to represent temp. So the maximum value of temporary matrix construction can be $2^{10}$=1024 and the maximum number of characters we can accommodate is 1024*2=2048.
11. Replace the LSB of row number 1-10 of the cover file with the binary representation of temp.
    For each temp performs the following steps:
    11.1 Replace the next four consecutive LSB of the cover file by the binary equivalent of nonzero elements contains into the temporary matrix constructed from the target string. Suppose the number is num.
    11.2 For each number performs the following steps:
    11.2.1 Replace the next four consecutive LSB of the cover file by the row and column number of each nonzero elements one by one.
12. Convert the Cover file into analog equivalent.
13. Stop .
```

5.2. Algorithm Decryption

Input: The stego file.
Output: The target string.

```
1. Start.
2. Accept the stego file.
3. Finds the digital equivalent of stego file and group it into 8 bits block.
4. From row number 1-10 of the stego file find the number of times the temporary matrix constructed from the target string. Suppose the number is temp.
5. Construct a 4*4 temporary matrix (A) consist of all zeros.
6. For each temp performs the following steps:
7. The decimal equivalent of the next four consecutive rows of the cover file gives the number of nonzero elements into the temporary matrix. Suppose the number is num.
8. For each number performs the following steps:
    8.1 From this point the LSB of each four consecutive rows of the cover file gives the row and column number of each nonzero element into the temporary matrix. The two most significant bits identified row number and the two least significant bits identified the column number.
    8.2 Find the row and column number of each nonzero element.
    8.3 Replace the corresponding row and column of the temporary matrix (A) by 1.
    8.4 After merging the first two consecutive rows of the temporary matrix gives one character and the next two rows gives the second character.
9. The whole target string is constructed form the temporary matrix sequentially.
10. Stop.
```

VI. Result analysis

In result analysis phase, two sets of cover file, Cover file 1 and Cover file 2 has been used as shown in figure 4 and figure 8 respectively. For transmission purpose, 3 sets of data has been used: small, medium and large datasets which contains 112, 256 and 576 characters respectively. After embedding the different length of datasets into the cover file, the corresponding encrypted file are shown in figure 5 to figure 7 and figure 9 to figure 11. Finally a comparison has been made with traditional LSB method by using two parameters: Mean square error and Signal to noise ratio.

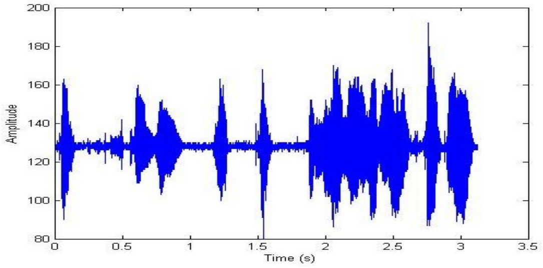

Figure 4. Cover file 1.

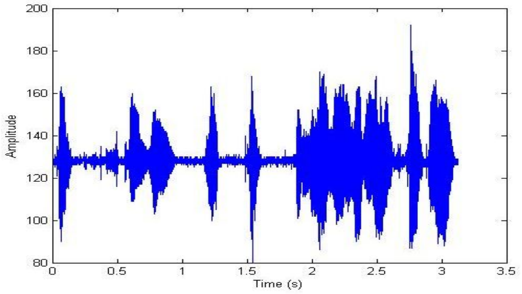

Figure 5.Encrypted file 1
Small Dataset- Number of character 112

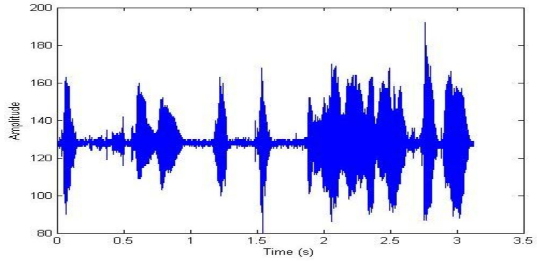

Figure 6.Encrypted file 2.
Medium Dataset-Number of characters 256

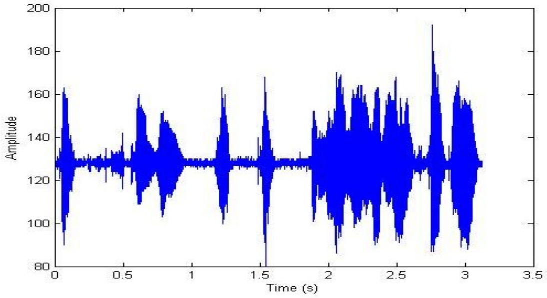

Figure 7.Encrypted file 3.
Large Dataset-Number of characters 576

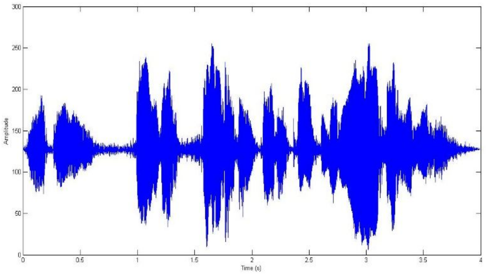

Figure 8.Cover file 2.

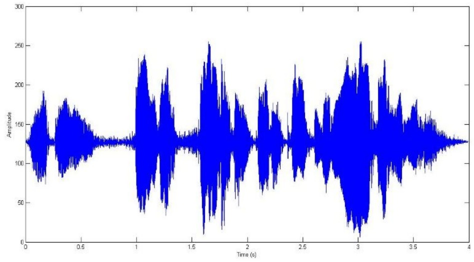

Figure 9.Encrypted file 1.
Small Dataset-Number of characters 112

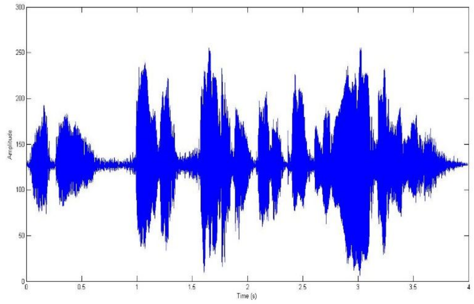

Figure 10.Encrypted file 2.
Medium Dataset-Number of characters 256

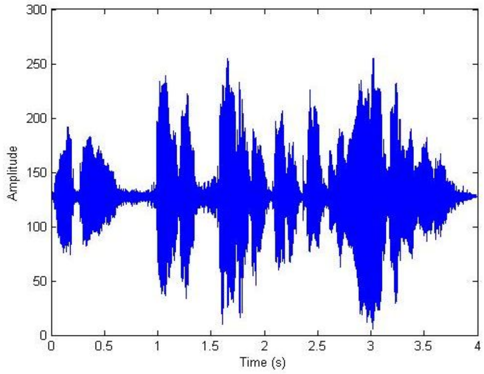

Figure 11.Encrypted file 3.
Large Dataset-Number of characters 576

From the above figure, it is observed that there is hardly any difference between the cover file and its corresponding encrypted file and the sound of both the files are audibly same. In the receiving side, the encrypted file is decoded to retrieve the characters. The characters found in the receiving side is exactly same with the original target string. So we can conclude that the proposed method is completely lossless. In the next section, a comparison has been carried out with respect to two parameters: Mean square error and Signal to noise ratio.

Cover File	Length of Message	Normal LSB Method		Matrix based Method	
		MSER	SN Ratio	MSER	SN Ratio
1	112	0.0063	64.1946	0.0145	60.5451
1	256	0.0145	65.9811	0.0308	57.2779
1	576	0.0333	56.9341	0.0671	53.8965
2	112	0.1102	51.8635	0.1546	50.3955
2	256	0.0230	58.6641	0.0479	55.4751
2	576	0.0517	55.1461	0.1059	52.0302

Table 6.Comparison with standard LSB method.

In the above table it is observed that the mean square error value of the matrix based method is so negligible that it is impossible to identify the existence of a target string into the cover file by human auditory system (HAS).As compared to the normal LSB method, the value of the mean square error is slightly greater and the value of the signal to noise ratio is slightly lesser. But LSB is a well-known technique; there is no security of data. Data in embedded directly into the LSB of the cover file. But the proposed method has used a duel encryption methodology. For encryption purpose the number of bits has slightly increased, so we can conclude that although there is an increase in means square error compared with LSB method, however an improved data security has been obtained by the proposed method and in other word the cost of enhanced data security has been obtained as an increasing Mean square error and decreasing SNR.

CONCLUSION

In this paper a high quality duel encryption technique has been implemented. The matrix based representation has performed the first level encryption and in second level, by using the standard LSB method, the message is secretly hidden into a cover audio file. So the proposed technique is less susceptible to stego attack. At the same time since we are sending only the location of the nonzero elements, so a large volume of data can be transferred. Overall, the proposed technique exceptionally obscures data in such an anonymous way that its existence into the cover file is undetected. The provided result has also confirmed this conclusion.

Further research can improve upon the proposed technique by reducing the number of bits into the target string. Different data compression algorithm can be attached with our algorithm to reduce the number of bits or the encrypted version of the secret message can be embedded into the unused portion of the cover file.

REFERENCES

1. Vimal, Jithu. "Literature Review on Audio Steganographic Techniques."
2. [Kiah, ML Mat, B. B. Zaidan, A. A. Zaidan, A. Mohammed Ahmed, and Sameer Hasan Al-bakri. "A review of audio based steganography and digital watermarking." *Int. J. Phys. Sci* 6, no. 16 (2011): 3837-3850.
3. Zamani M, Manaf A, Ahmad RB, Jaryani F, Taherdoost H, Zeki AM. ”A secure audio steganography approach”. International Conference on Internet Technology and Secured Transactions, (ICITST) (2009 Nov 9) pp. 1-6. IEEE, London, UK.
4. Banerjee, Sean, Sandip Roy, M. S. Chakraborty, and Simpita Das. "A variable higher bit approach to audio steganography." International Conference on In Recent Trends in Information Technology (ICRTIT), pp. 46-49. IEEE, (2013, Jul 25-27), Chennai, India.
5. Roshidi Din, Hanizan Shaker Hussain, and SallehuddinShuib, ―”Hiding secret messages in images: suitability of different image file types”, WSEAS TIONSRANSAC *on* COMPUTERS, vol. 6(1), January 1 2006, pp. 127 -132.
6. Bhowal K, Bhattacharyya D, Pal AJ, Kim TH. “A GA based audio steganography with enhanced security.” Telecommunication Systems. 2013 Apr 1; 52(4):2197-2204.
7. Rahim LB, Bhattacharjee S and Aziz IB. “An Audio Steganography Technique to Maximize Data Hiding Capacity along with Least Modification of Host”. In Proceedings of the First International Conference on Advanced Data and Information Engineering (DaEng-2013) 2014 Jan 1 (pp. 277-289). Springer Singapore.
8. Balgurgi, Pooja P, and Sonal K. Jagtap. "Audio steganography used for secure data transmission." In Proceedings of International Conference on Advances in Computing, pp. 699-706. Springer India, 2012.
9. R. J. Anderson (ed.), “Information hiding”, 1st international workshop, volume 1174 of Lecture Notes in Computer Science, Isaac Newton Institute(Springer-Verlag, Berlin, Germany, 1996).
10. [10]. Nathan, Mark, Nikhil Parab and K. T. Talele. "Audio Steganography Using Spectrum Manipulation." In Technology Systems and Management, pp. 152-159. Springer Berlin Heidelberg, 2011.
11. Malviya S, Saxena M, Khare A. Audio Steganography by Different Methods. International Journal of Emerging Technology and Advanced Engineering [20] (ISSN 2250-2459, Volume 2, Issue 7. 2012.
12. Datta, Biswajita, Souptik Tat, and Samir Kumar Bandyopadhyay. "Robust high capacity audio steganography using modulo operator."International Conference onComputer, Communication, Control and Information Technology (C3IT), IEEE, (2015, December 21-24), Himachal Pradesh, India.
13. Bandyopadhyay S.K, Bhattacharyya D, Ganguly D, Mukherjee S, Das P. “A tutorial review on steganography”. In International conference on contemporary computing 2008 Aug 7 (Vol. 101).
14. Radhakrishnan R, Kharrazi M and Memon N. “Data masking: A new approach for steganography?” Journal of VLSI signal processing systems for signal, image and video technology. 2005 Nov 1; 41(3):293-303.
15. Darsana R, Vijayan A. “Audio steganography using modified LSB and PVD”. In Trends in Network and Communications 2011 Jan 1 (pp. 11-20). Springer Berlin Heidelberg.