International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey on Steganography Techniques

Amruta B. Bhojane[1], Priti A. Kodake[2]

[1]ME (CSE) II Year, Prof. Ram Meghe College of Engineering and Management, Amravati, India

[2]Professor, Department of Computer Science and Engineering. Prof. Ram Meghe College of Engineering and Management, Amravati, India

Abstract: ***User generally need to communicate data in the form of text, image, audio or video. Because of the increase used of internet, information is mostly communicated through the network. But in a network data is not secure, it can get eavesdrop. To protect data from the third person steganography technique can be used. Steganography means hiding secret information inside another data (cover data). Cover data can be text, image, video, audio or network protocol. Different method used for text, image, video and audio steganography are analyze in this paper.***

Keywords: Data hiding, Least Significant Bit method (LSB), image, video, text, audio, encryption

1. Introduction

With the explosive growth of networking, use of internet in every field such as military field, medical field, research filed etc. is become very much important. Every field require a transmission of sensitive data. Sensitive data can be in the form of text, image, audio or video. Data transmission in public communication system is not secure because of eavesdropper. To hide this data in transmission data hiding techniques can be used. This is called steganography. Steganography is an art and science of written hidden message in original message in such a way as, no one other than sender and intended recipient suspect existence of message. Steganography is a Greek origin word and its meaning is "concealed writing" where steganos means "covered or protected" and graphein means "to write" [1]. The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on Steganography and cryptography disguised as a book on magic. Steganography is becoming very popular nowadays because it hide the existence of secret information in a cover data. Sender and receiver only knows about existence of data, hence until third person knows about existence of data, he cannot eavesdrop it. To make data more secure from the eavesdropper, who still knows the existence of sensitive data in addition to data embedding technique, cryptography can be used to encode data. It makes embedded data more secure. Different techniques of data hiding in text, image, video and audio are present but every technique has its pros and cons. Images are most commonly used cover media. Images content more redundant data which can be used to hide secret data. Video steganography provide more embedding capacity than other steganography techniques.

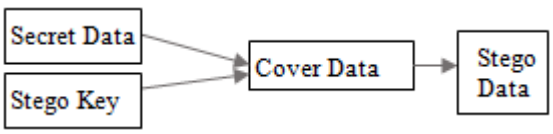

Figure 1: Steganography mechanism

2. Different Method of Data Hiding

A. Data hiding in text

Hiding data in text is most difficult kind of data hiding because there is a lack of redundancy in a text file compare to image or video file.

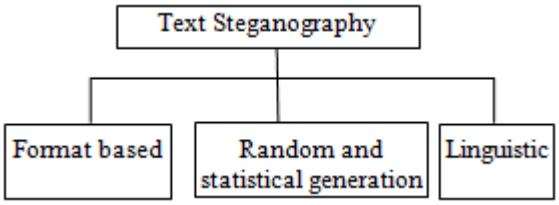

Figure 2: Different methods of text steganography

According to author L.Y. Pore and B. Delina [2] text steganography classified in three types as format based, linguistic method, random and statistical generation. Physical text formatting of text is used as a place in which to hide information in format based method. In this method for hiding steganographic text, existing text has to modify. In random and statistical generation method statistical properties of text are used to generate cover text such a properties are word length, character sequence, word frequency etc. Linguistic properties of modified text are consider in final method i.e. linguistic method.

L.Y. Pore and B. Delina propose a new hybrid approach inter-word spacing and inter-paragraph spacing. In this approach whitespaces between words and paragraph are used for hiding information. This scheme is beneficial because there are more whitespaces in document than appearance of words. It provide more capacity for hiding data. In this method, according to length of secret message cover text is generated dynamically. Proposed method provide more capacity for hiding data

Mohit garg [3] proposed a text steganography technique based on html documents, they use html document as a cover media. Html tags and their attributes are used to hide secret information. Key file is the main component of this technique where key file is the collection of primary and secondary attributes of html tags. Combination of this attributes form a key to hide secret data.

D. Bhattacharyya, A. Haveliya and T. H. Kim [4] proposed a method for secure data hiding in binary text document for authentication. There method is useful for any type of cover file having text information such as .doc file, .ppt file, .txt file, .m file (MATLAB script file) etc. They first convert cover file into single dimension i.e. binary format from matrix form. Also convert secret message file into binary format and perform right shift, XOR operation again right shift, XOR operation and finally 1's complement on this binary format. To embed secret massage into cover file, they replace first bit of every byte in cover file with secret message bit. After complete embedding stego file will generate. Secret message can be extract by reversing this procedure at receiver side.

Youssef Bassil [5] proposed text steganography method using pangram and image mediums. In this paper author used two medium to transfer secret text data between sender and receiver. First medium is pangram English sentence consist of digit, letter and special character of maximum 512 character and second medium is uncompressed image. Data embedding is done using seed index and offset index, where seed index point to random character in pangram sentence. Distance between characters to be encoded which is same as the character in pangram and seed index is the offset index. This seed and offset index are stored into 3 LSB bit of red channel, 3 LSB of green channel and 3 LSB of blue channel per pixel of the image. Sender has to send both pangram and image to the receiver.

P. Singh, R. Chaudhary and A. Agarwal [6] proposed text steganography based on null spaces. In this paper author used white spaces in text document to hide secret data. Generally it is difficult for the people to suspect existence of secret data in white spaces. Author used cover text's one white space to hide bit 0 and two white spaces to hide bit 1 of secret binary data. To encode few bit it require great deal of null spaces. Depending on the length of secret massage extra null spaces can be require, which increases the length of stego cover file.

I. Banerjee, S. Bhattacharyya and G. Sanyal [7] proposed text steganography using article mapping technique (AMT) and SSCE. In this paper, author used secret steganography code for embedding (SSCE) table to encrypt secret message. Then check double letter word in cover text otherwise take first letter and find double word mapped group of letter. Finally based on the mapping information embed particular group of letters for embedding secret message into cover text.

S. Bhattacharyya, P. Indu, S. Dutta, A. Biswas and G. Sanyal [8] proposed text steganography using CALP with high embedding capacity. Where CALP means changing in alphabet letter pattern. Author change pattern/texture of some alphabets in cover text to mapped to each two bits of secret message. This structural modification is not easily distinguishable from original to viewer. In this paper author used this method for English language but it can applied to any other language. Also this method provide high embedding capacity.

Youssef Bassil [9] proposed generation-based text steganography method using SQL queries. In this paper author use SQL queries to hide secret data but there method is limited to only SELECT queries. They use dictionary consist of 65 categories as a hash table, to map characters of secret message. This categories consist of English language letters, decimal digit and special characters. From secret message mapped single character of message with category of dictionary and replace the obtained character with random word in corresponding category. Use this procedure for every character of secret message. Secret message can be embedded in entire query except SELECT, FROM and WHERE keyword. Stego query is difficult to steganalysis by third party because output query will be different for different content of dictionary. This method can be used for other languages also.

B. Data hiding in images ans videos

Image and video has large amount of redundant data to hide secret message. Most commonly used and simple technique for data hiding in images and videos is a least significant bit (LSB) technique. Same techniques can be apply to images and videos because video is made up of images or frames. Other technique use for data hiding are pixel value differencing, reversible data hiding, frequency domain method etc.

S. A. Laskar and K. Hemachandran [10] proposed a LSB based image steganography. They use cryptography along with steganography to provide more security to secret data. They use transposition cipher method to encrypt the secret message. To encrypt the message first write it row wise in matrix form but read out it column wise depending on specific key. For embedding encrypted message into image, convert that message into binary digit and embed it at least significant bit position of each pixel in image. Human visual system cannot detect changes at LSB position of a pixel in image.

H. Noda, T. Furuta, M. Niimi, E. Kuwuguchi [11] proposed application of BPCS steganography to wavelet compressed video. BPCS means bit-plane complexity segmentation. Author proposed two techniques for video compression and apply BPCS steganography technique on that compressed video. First compression technique is 3-D set partitioning in hierarchical trees (SPIHT) algorithm, which encode at a time one bit plane of wavelet coefficient starting with the MSB and generate bit stream. This bit stream is converted into bit plane using SPIHT decoder and used BPCS technique to embed secret data into that bit plane. Again used SPIHT encoder to get bit stream with secret data embedded. Second technique is motion-JPEG2000-BPCS steganography. Intra-frame coding is used in motion-JPEG20000, hence complexity is reduced by this method. JPEG coded each frame of video independently and BPCS steganography can be applied to each frame.

V. Sharma and S. Kumar [12] proposed extension of least significant bit technique. As a pixel consist of red, green and blue component, in this proposed technique data hiding is done by replacing red component in first pixel with a first byte of secret data then replace green component of second pixel with second byte of secret data and so on until the end

of secret message. But the resulting stego image is distorted so they use new cover image to cover this stego image to provide more level of security. Also use compression algorithm to increase storage capacity of cover image.

ShengDun Hu and KinTak U [13] proposed video steganography based on non-uniform rectangular partition. It is a kind of time domain steganography method, which can provide greater embedding capacity without causing more degradation in a host stream. Non-uniform rectangular partition process consist of three main component that is initial partition, control error and Bivariate Polynomial $f(x, y)$. They choose initial partition as an original image area and partitioning process is to stop or not is checked using error control value. Than select bivariate polynomial and put partition grid of stego image onto host image. Read grey values of rectangular sub area and use LSB to hide partition code and gray value differences. Repeat this procedure for R, G and B component. Here different combination of partition code can be used as a security key to enhance steganography security.

C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun [14] propose an adaptive LSB method using pixel value differencing. They use this method for data hiding in edge areas of images instead of smooth area, because more changes can get tolerate in edge area than smooth area. This method provide large embedding capacity. Pixel value differencing used to find difference between values of two neighboring pixel to estimate number of secret bit will be embedded in two pixel. They use k-bit LSB substitution method to embed pixel in edge areas.

W. Luo, F. Huang and J. Huang [15] propose edge adaptive image steganography based on LSB matching revisited (LMBR). There are some modification to LSB replacement method employ LSB matching. Pixel value get deal independently in LSB and LSBM, Whereas LSBMR use pair of pixel for data embedding. One bit of secret message get embedded into LSB of a first pixel, and the another bit of secret message get carried into relationship between two pixel such as odd-even relationship. Advantage of this method is that it require minimum changes in cover image as compared with other method.

A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar [16] author proposed frequency domain steganography technique. This method provide high security and large amount of secret data can be hide. Also there will be no loss of secret message and good invisibility can be provide. This method first convert cover image into 8*8 blocks. Then convert that image representation into frequency representation using two dimensional discrete cosine transformation. Huffman coding is used to encode secret message before embedding it in the cover image to convert it into 1-dimensional bit stream. Decompose that bit stream into 8 bit blocks B. Then replace LSB of DCT coefficients in 8*8 block with a bit taken from 8 bit block B. Finally obtain new image which contain secret image by performing inverse discrete cosine transformation.

X. Zang [17] proposed reversible data hiding in an encrypted image. To hide a host data from a data hider, author encrypt the host image before embedding secret data in it. Encryption is performed using exclusive-or operation on original bits and pseudo random bits. By changing some portion of encrypted image, secret data can embedded. For this data hider has to segment encrypted image into s*s blocks. Where s=8. Then by using data hiding key divide s^2 pixel pseudo randomly into s0 and s1 set for each block. Flip 3 LSBs in set s0 if secret bit to embed is 0 or flip 3 LSBs in set s1 if bit to be embed is 1. This technique is better if it is important to hide original data from data hider.

D. Xu, R. Wang and Y. Q. Shi [18] proposed a scheme of H.264/AVC video encryption, data embedding and data extraction. They use chaotic pseudo random sequence to encrypt the secret information, then obtain codewords of the level by parsing encrypted bit stream. If the codeword belong to C0 or C1codespace then embed secret message bit into host data using codeword substitution. Embed bit 0 if codeword belong to C0 and 1 if codeword belong to the C1. Proposed scheme preserve bit rate after data embedding, also preserve confidentiality of video content.

A. P. Sherly and P. P. Amritha [19] in this paper author proposed a new compressed video steganographic scheme. In this scheme the data is hided in compressed domain. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stego-image for human vision. They separate the cover video in I frame and P& B frame. And use scene change detector to embed secret data in I frame and motion vector to embed data in P&B frame and got stego video by combining this frames. In motion vector they compare the magnitude of motion vector with threshold value and block with the maximum magnitude is use to embed data using PVD method. This algorithm can be applied on compressed videos without degradation in visual quality.

C. Xu, X. Ping and T. Zang [20] proposed steganography in compressed video stream of MPEG. They used P frame and B frame for embedding actual transmitted data and I frame to embed control information which facilitate data extraction. Motion vector of P and B frame are used for data embedding. Each micro block in P frame has one motion vector, while each micro block in B frame has two motion vector. Author does not embed data in all motion vector but only in larger magnitude motion vectors. This technique reduces distortion introduced by data embedding. Control information is usually critical and small and it should get extracted correctly. In I frame control information is embedded in quantized DCT coefficient using least significant bit method, which provide more robustness and imperceptibility.

P. Bhautmage, A. Jeyakumar and A. Dahatonde [21] author proposed advance video steganography algorithm. For the data hiding they convert cover video file into cover frames and embed secret message into one of the frame to get stego frame and combine all the frame to get stego video. But before secret massage embedding they use bit exchange method and XOR method to encrypt secret message. Bit exchange method perform operation in three steps, in first step convert every byte into 8 bit and perform 1 bit right

shift operation to modify each byte. In the second step divide 8 bit in a byte into two 4 bit blocks and perform XOR operation on left side and right side block and in right side substitute new 4 bit. Repeat this second step for each byte. In third step repeat first step with 2 bit right shift and then repeat step 2. Like this author shift 5 bits to right. For embedding data in cover file used alternate byte of cover file, substitute 2 bit of a secret message at LSB and LSB+3 position in cover file and leave next byte intact. Perform this for embedding complete secret message.

C. Data Hiding in Audio

Audio is the most sensitive data, small changes in audio is detectable by human auditory system (HAS). But there are some natural limitation of HAS and audio steganography make use of that limitation. Different technique use for audio steganography are spread spectrum, phase modulation, echo hiding, LSB etc.

X. Zhang and X. Xie [22] proposed data hiding system based on multiple echo hiding method. In the echo hiding method, they add an echo to the original audio to hide data in the original audio. That echo will be inaudible to human ear. To embed stego data in host audio, they divide host audio into non-overlapping frames of same length and transform each frame into 4*4 matrix form of binary data. Then transform each column in matrix to hexadecimal value and use that four hexadecimal values to calculate four delay value. Author use this delay values in standard kernel equation and finally put result of equation in power cepstrum equation to calculate watermark audio signal. In the extraction process they extract frames of equal size from watermark audio signal and use power cepstrum to calculate delay position and use it to extract echo from host audio. This proposed method provide imperceptibility and higher capacity.

G. Nian, S. Wang and Y. Ge [23] proposed audio watermarking based on reverberation. There are some drawback of echo hiding method such as low robustness. Different method can be used to get more robustness such as multiple echo hiding technique. But author proposed reverberation technique to improve the robustness and imperceptibility. Reverb is also a delay in a sound wave but it arrive for a short period of time hence human ear cannot perceive it as a reflection of original audio copy. For example reflections of a sound in a real room produce reverberation. And everybody hear it daily without any specific sense. Author embed the watermark in music. For the embedding they select size, shape and surface material parameters of virtual room to resemble them to the real concert hall. To the watermark audio they ensure the best artistic effect. In the embedding process they first calculate two impulse response from source position of sound and two listener position. Then construct kernel function from two impulse responses and perform linear convolution on kernel function and host audio signal to obtain watermark signal.

H. Matsuoka [24] proposed spread spectrum audio steganography based on sub-band phase shifting. Spread spectrum method spread the data signal across wide frequency. Author use the frequency masking effect to embed that data signal into original audio. M-sequence code is use to spread the data signal, this codes have autocorrelation properties and it is self -clocking. Hence data frame synchronization is easy and embedded data can be retrieve using de-spreading technique. Error probability can be reduce by spread spectrum method but high spread rate increases the time require to send one bit of information. Therefor it is necessary to provide good robustness by low spread rate technique. It is possible to achieve good transmission speed with low error probability when there is a low correlation between spread data signal and host signal and even with a low spreading rate. Author use phase shifting method to decrease the correlation, each sub band signal of host audio undergoes phase shifting to achieve low correlation. This technique make retrieval of data at the receiver easy.

H. Malik and S. S. Kang [25] proposed designing and performance evaluation of spread spectrum technique for audio steganography. Author used watermarking technique which is related to steganography but more secure than it for data embedding. Where watermark is the embedded object. Algorithm use for watermarking should have meet certain requirement such as capacity, perceptibility, speed and reliability. Secret information get spread across the frequency spectrum of original audio signal in spread spectrum method. Author embed watermark image inside the binary form of audio signal. They multiply the total number of element with the spreading factor to get the spreading size and encode watermark using random key sequence and the each element of host matrix undergoes discrete cosine transform. Finally they multiply cosine transform matrix with encoded watermark for embedding watermark.

K. Saroha and P. K. Singh [26] proposed LSB steganography for hiding images in audio. Least Significant Bit technique is the simplest technique for embedding secret information in audio file. Here audio file is use as cover image because size of the audio file is quite large as compared to the image file. For encoding the image bits they use three LSB bits of audio file as a stego key. For the embedding they compare first bit of the image with 1^{st} to 7^{th} MSB of audio sample. If the match is found 3LSB of audio sample replace with binary equivalent of the position of MSB otherwise replace with zero which indicate that audio sample does not contain image bit. Repeat this procedure for all the bits of image. Reverse this whole procedure to extract image from audio file. Large data can be embed using this LSB coding technique.

X. Dong, M. F. Bocko and Z. Ignjatovic [27] proposed data hiding via phase manipulation of audio signals. Audio signal contains frequency and overtone spectrum with relative phases. This harmonics phases can be use as a channel to hide secret data by manipulating it. Author proposed two phase encoding scheme, relative phase encoding and quantization index modulation phase encoding. In the relative phase coding, relative phases of pair or more of spectrum frequency components in each time frame has to reassign. Pseudo-random sequence is use to select phase shift and spectral components. Pseudo-random sequence should be known to sender and receiver only. It is easy to decode after correlating calculated phase spectrum and

pseudo-random sequence. In phase quantization index modulation, segment the audio signal's time representation into series of frames. Compute spectrum of frame and select fundamental tone and overtone series of it. Based on some quantization scale, phase quantized one or more overtone in series. And inverse transform the phase quantize spectrum to convert it into time domain. An artifact of phase modulation technique is that while re-assigning the phase there can be small discontinuity at the boundary of frame, but it can be reduce using some simple technique.

Table 1: Comparision of Different Types of Steganography

Steganography	*Text*	*Image*	*Video*	*Audio*
Capacity	Low	Medium	High	Medium
Embedding difficulty	High	Medium	Low	Medium
Security	Low	Medium	High	Medium
Imperceptibility	Low	Medium	High	Medium
Common Techniques	Semantic method, Word spelling, Line shifting, Abbreviation, Word shifting, Syntactic method.	Least Significant Bit method, Edge adaptive method, Frequency domain method, Reversible data hiding.	Least Significant Bit method, Triway pixel value differencing, Discrete cosine transform.	Least Significant Bit method, Spread spectrum, Phase modulation, Echo hiding.

3. Conclusion

In this paper, different types of steganography techniques are surveyed. And according to survey out of four, videos can be use as a cover media. Videos have more embedding capacity and it is difficult to detect existence of secret data in videos. Least Significant Bit is the most efficient and simple method to embed data in video. Audio is the most sensitive data but it has better embedding capacity. Text has less redundant data hence it has less embedding capacity and it is difficult to embed data in it. Most widely use cover media is image, and image steganography techniques can be apply to video, hence use of video of for data hiding is increasing.

References

[1] A. Swathi and S. A. K. Jilani, "Video steganography by LSB substitution using different polynomial equations", Int. Journal of Computational Eng. Research, ISSN 2250-3005, Vol.2, Issue.5, September 2012.
[2] L. Y. Por and B. Delina, "Information hiding: A new approach in text steganography", 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (Acacos'08), Hangzhou, China, April 6-8, 2008.
[3] M. Garg, "A novel text steganography technique based on html documents", Int. Journal of Advanced Science and Tech., Vol. 35, October 2011.
[4] D. Bhattacharyya, A. Haveliya and T. H. Kim, "Secure data hiding in binary text document for authentication", An Int. Journal Appl. Math. Inf. Sci. 8, No. 1L, 371-378 (2014).
[5] Youssef Bassil, "Text steganography method using pangram and image mediums", Int. Journal of Scientific & Engineering Research, ISSN 2229-5518, Vol. 3, Issue 12, December 2012.
[6] P. Singh, R. Chaudhary and A. Agarwal, "A novel approach of text steganography based on null spaces," IOSR Journal of Computer Eng. ISSN: 2278-0661, Vol. 3, Issue 4 (July-Aug. 2012), PP 11-17.
[7] I. Banerjee, S. Bhattacharyya and G. Sanyal, "Text steganography using article mapping technique (AMT) and SSCE," Journal of Global Research in Computer Science, ISSN 2229-371X, Vol. 2, No. 4, April 2011.
[8] S. Bhattacharyya, P. Indu, S. Dutta, A. Biswas and G. Sanyal, "Text steganography using CALP with high embedding capacity," Journal of Global Research in Computer Science, ISSN 2229-371X, Vol. 2, No. 5, May 2011.
[9] Youssef Bassil, "A generation-based text steganography method using SQL queries", Int. Journal of Computer Applications (0975 – 8887) Vol. 57, No.12, November 2012.
[10] S. A. Laskar and K. Hemachandran, "High capacity data hiding using LSB steganography and encryption", Int. Journal of Database Management Systems (Ijdms) Vol.4, No.6, December 2012.
[11] H. Noda, T. Furuta, M. Niimi and E. Kuwuguchi, "Application of BPCS steganography to wavelet compressed video", International Conference on Image Processing (ICIP), 0-7803-8554-3, April, 2004 IEEE.
[12] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography", Int. Journal of Advanced Research in Computer Science and Software Eng., Vol. 3, Issue 4, April 2013.
[13] ShengDun Hu and KinTak U," Video steganography based on non-uniform rectangular partition", 14th IEEE Int. Conference on Computational Science and Eng., November, 2011.
[14] C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial lsb domain systems", IEEE Trans. On Information Forensics and Security, Vol. 3, No. 3, September 2008.
[15] W. Luo, F. Huang and J. Huang, "Edge adaptive image steganography based on lsb matching revisited", IEEE Trans. On Information Forensics and Security, Vol. 5, No. 2, June 2010.
[16] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, "A novel technique for image steganography based on Block-DCT and Huffman Encoding", Int. Journal of Computer Science and Information Tech., Vol. 2, No. 3, June 2010.
[17] X. Zang, "Reversible Data Hiding in Encrypted Image", IEEE Signal Processing Letters, Vol. 18, No. 4, April 2011.
[18] D. Xu, R. Wang and Y. Q. Shi, "data hiding in encrypted h.264/avc video streams by codeword substitution", IEEE Trans. On Information Forensics and Security, Vol. 9, No. 4, April 2014.
[19] A. P. Sherly and P. P. Amritha, "A Compressed Video Steganography using TPVD", Int. Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010.

[20] C. Xu, X. Ping and T. Zang, "Steganography in compressed video stream", First International Conference on Innovative Computing, Information and Control (ICICIC'06), 0-7695-2616-0, June, 2006, IEEE.
[21] P. Bhautmage, A. Jeyakumar and A. Dahatonde, "Advanced video steganography algorithm", Int. journal of engineering research and applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 1, January -February 2013, pp.1641-1644.
[22] X. Zhang and X. Xie, "Data hiding system based on new multiple echo hiding method", The 21st Int. Congress on Sound and Vibration , 13-17 July, 2014, Beijing/China.
[23] G. Nian, S. Wang and Y. Ge, "Research of improved echo data hiding: audio watermarking based on reverberation", 1424407281, July, 2007, IEEE.
[24] H. Matsuoka, "Spread spectrum audio steganography using sub-band phase shifting", Int. Conf. On Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 0-7695-2745-0, June, 2006, IEEE.
[25] H. Malik and S. S. Kang, "Designing and evaluation of performance of a spread spectrum technique for audio steganography", Int. Journal of Advanced Research in Computer Science and Software Eng., Vol. 3, Issue 8, August 2013.
[26] K. Saroha and P. K. Singh, "Variant of LSB steganography for hiding images in audio", Int. Journal of Computer Applications (0975 – 8887), Vol. 11, No.6, December 2010.
[27] X. Dong, M. F. Bocko and Z. Ignjatovic, "Data hiding via phase manipulation of audio signals", 0-7803-8484-9, April, 2004, IEEE.