Optimization in Audio Steganography

[1]Rohit Tanwar,
[1]Ph.D Scholar, Computer Engg. Deptt.
UIET(Kurukshetra University)

[2]Dr.Sona Malhotra
[2]Asst. Prof. Computer Engg. Deptt.
UIET(Kurukshetra University)

Abstract- As communication is being done by electronic means in open air generally, security of data is highly desirable. One such technique of doing this is steganography. The requirement of a system that ensures high capacity, robustness and security of embedded data there have been so many variants in existing steganography technique. Due to this diversity it needs some technique to optimize the existing traditional substitution technique. The audio file is chosen as cover file due to its practical availability and "Masking Effect".

Keywords: Audio, Optimization, Masking Effect, substitution technique

I. INTRODUCTION

The word steganography comes from the Greek Steganos, which mean covered or secret and –graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening.

The data hiding technique where secret message is hidden using audio as cover file. mp3 and .wav files are being used for this purpose generally. It is so because of their practical availability. Moreover mp3 gives better performance in case of compression.

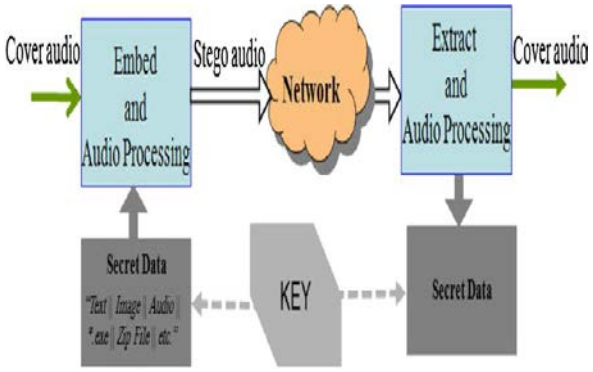


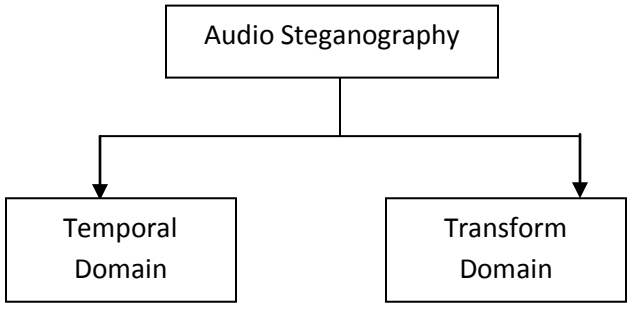
Figure. Audio Steganography

Use of audio file as cover is supported by masking effect of Human Auditory System(HAS) which says that lower frequency voices are suppressed by higher frequency voices. This property makes the stego file to pass hearing test.

II. LITERATURE REVIEWED

Fatiha Djebbar et. al[1] did a comparative study of digital audio steganography techniques. They found in their study that lots of new steganography techniques were invented in last few years that were very effective in protecting digital information. Audio file is being chosen as preferred carrier due to its highly availability and popularity. Audio steganography techniques focus on embedding secret message in digital audio file . In this work, a comparative study of the literature in audio steganography techniques were given. They enlisted the weakness and strengths of each technique so as to describe their application area in a better way. They conclude in their study that frequency domain techniques are better than temporal domain in terms of capacity, imperceptibility and undetectability. According to their point of view the invention of different variants of steganography techniques will provide better choice for applicability. The choice of using one technique over other depends on the application constraints in use and its requirement of three parameters hiding capacity, embedded data security level and robustness to the attacks encountered[1].

Thus, temporal domain techniques targets the data hiding capacity while transform domain methods focus on making the stego file imperceptible by exploiting masking effect of audio files.



Jayaram et al researched the hiding data in audio files. Discusiion of various audio steganographic methods were their main focus. They also stated their advantages and limitaions[2].

Malviya et al. did their implementation using different approach. Data hiding technique was proposed as a new technique to implement security. Steganography was proposed as a new alternative technique to cryptography to enforce data security. A good technique focuses at hiding data in an robust and secure way in imperceptible manner so that it can be extracted by authorized people [3].

Kekre *et al*. used the concept of LSB and proposed two methods. The First method was parity coding. The second method was XORing of LSB. The XORed operation of the LSB and the next bit had to be equivalent to the message bit to be embedded in their second method. If they were equal, then retain LSB, else flip it. They increased the data capacity and the computation load was decresed [4].

Mazdak Zamani *et.al* did work on substitution techniques. The problems and their problem solutions were discussed. The main issue was their less robustness against various attacks. Attacks are mainly of two types: One that tries to reveal the secret message embedded and other that tries to harm the hidden message. In traditional LSB method the least significant bits were targeted for hiding secret message. Some intelligent algorithm was developed to hide message into multiple MSB's to get higher capacity and increased robustness [5].

Gadicha et al. proposed a method for audio steganography. He proposed a new technique that embed message in 4^{th} LSB. The technique also minimized the distortion thus induced. Use of the proposed technique resulted in high robustness against addition of noises. In addition to this, listening tests were performed which showed that the method proven to be better than traditional LSB in case of perceptual quality [6].

Nedeljko and Tapio proposed a method that was able to hide data in 4^{th},5^{th} and 6^{th} LSB with minimal distortion . the case was chosen according to the bit to be embedded.. Experimental results showed that SNR value was around 8QS (Quantization Step) in the standard algorithm (which uses the 4th LSB) but in the proposed algorithm it was from 1-4QS. The average power of the noise introduced was lesser than the traditional method used (9.31)[7].

Samir and Biswajita proposed a method that resulted the stego signal similar to the cover signal. Experiments proved that the loss of information was negligible. They hide message in audio samples using different logic [8].

Ahmad, D. and P. Mohammad worked on different variants of LSB in different domains. They selected temporal domain. As a result of it, computational load get reduced and implementation became faster. Information of cover signal was used to calculate embedding threshold. Samples magnitude was used to assign threshold. Lower magnitudes have less data hiding capacity as compared to higher magnitudes. SNR comparison was done experimentally as well as theoretically for cover and stego signal which was nearly same. BER calculated for pop, classic, country and speech resulted zero, thus efficient. In presence of slight distortions, this method could not achieve full recovery[9].

Kaliappan gopalan proposed a steganalysis in audio file with an encryption key for the embedded secret audio file[10].

N. Cvejic and T. Seppanen to improve security against distortion and noise of LSB method, some of the papers have increased the depth of the embedding layer from 4th to 6th and 8th LSB layer without affecting the perceptual transparency of the stego audio signal. In it only bits at the sixth position of each 16 bits sample of the original host signal were replaced with bits from the image. To minimize the embedding error, the other bits were flipped in order to have a new sample that was closer to the original one[11].

Mohamed A. et al. shifted the LSB embedding to the eighth bit and had avoided hiding in silent periods or near silent points in the host signal. The increased robustness is because of the fact that the embedding occurs in the eighth bit slightly This method compare to the conventional LSB methods. However, since some of the samples were to be left unchanged to preserve the audio perceptual quality of the audio signal[,the hiding capacity decreased 12].

Harish Kumar and Anuradha invented a new strategy in Steganography to get the minimum effect in audio which is used to hide data into it[13] .

Gopalan proved a capacity of 62 bps for embedding. BER(Bit Embedding Rate) was less than 2 to 2.5 for clean cover and noisy speech. As data can be successfully embedded in the spectral points, a technique was used in which first step was done by extending it to the log spectral domain in perceptually masked regions was proposed. In the study, every frame of speech sample was represented as convolution between Excitation Source Signal and Vocal Tract System (VTS)[14].

Ahmad and Mohammad selected Integer Wavelet Transform domain. Among different types of wavelet transform, Haar Discrete Wavelet Transform were used. That resulted in wavelet co-efficient which converted to integer, were used to calculate the embedding threshold. The encrypted data was embedded based on the threshold. Now the signal was converted to wavelet domain and before transmission, an Inverse Wavelet Discrete Transform was applied The reverse process followed by data extraction using the secret key.at the receiver's end The secret key was given as input to the PN (Pseudo Random Number) Generator which arranges the covert data and according to the threshold, the data packet was formed. SNR was one of the important parameters

determining the efficiency of the algorithm. It was also proved that the SNR values for theoretical and experimental results were equal. Hence without any actual embedding effort, SNR was calculated. By this method, SNR value was about 40 dB which was higher than other methods. They also increased payload, full recovery with better robustness[15].

The main idea proposed by **Samir *et al.*** was based on phase shifting and psycho acoustic theory of persistence. Persistence of hearing was based on the fact that two sounds successively with a difference of less than one-tenth of a second hit our ears, then the difference between the sounds is imperceptible. It is called the phase shift, the change of which is same as the shift in time. Consider S1, T1 and S2, T2 as the sampling rate and total duration of the cover and target file. The target file was split after every second, i varying between 0 and 1/10. Hence the total samples was equal to S2 * i in target audio file. In cover audio file, data was embedded at the interval of (T1*i)/T2 seconds. O(max(m, n)) was the computational complexity of time for both sender and receiver where m and n were number of samples in the cover and target audio file respectively. The insertion was quite undetectable and capacity was large were proved as results16].

M Asad,J Gilani & A Khalid used Advanced Encryption Standard(AES) and proposed an audio steganography with an encrypted audio file 17].

Kaliappan gopalan embeded the information of secret message in spectral domain of a cover audio or image files[18].

Sajad Shirali-Shahreza and M. T. Manzuri-Shalmani embedded a secret message into a cover media without attracting attention, which was known as steganography, was desirable in some security applications. One of the media they used was an audio signal. In this paper they introduced an adaptive wavelet domain steganography with high capacity and low error rate[19].

Rizky M. Nugraha discussed the implementation of steganography in audio data using Direct Sequence Spread Spectrum method.

Based on the test results, the author concluded that the implementation of Direct-sequence Spread Spectrum steganography on audio cover object was possible and practical to use at least for the duration of the first 15 seconds of data. Some suggestions given to improve this method are as follows:

1. Using split radix FFT algorithm, which was claimed to be a lot faster than the radix-4 FFT, or another better FFT ALGORITHM?

2. Partitioning the sample transformed. Audio samples were partitioned into 15-second audio pieces (or smaller) and embedding process was performed by splitting the information into each partition. This method will be faster.

3. Using repeated embedding scheme. If the information exceeds the payload, the cover object can be used again to embed the remaining messages by using different PN sequence. This scheme allows different calculation of payload and noise.

4. Using a file buffering to calculate the Fourier Transform on large audio files. The goal was to reduce RAM usage. Computational results were stored directly in the file buffer. Samples were read and stored in memory only to be calculated[20].

S.S. Divya and M. Ram Mohan Reddy used multiple LSB steganography by using a method of hiding text in audio and provide security using cryptography. The proposed two novel approaches of substitution technique improved the capacity of cover audio for embedding additional data. Here message bits were embedded into multiple and variable LSBs. These methods utilized up to 7 LSBs for embedding data. From the results it is clear that the methods improved the capacity of data hiding of cover audio by 35% to 70% as compared to the standard LSB algorithm which uses 4 LSBs for data embedding. RSA algorithm was used for implementing cryptography[21].

Muhammad Asad et al. proposed a three layered model for audio steganography based on least significant bit replacement. The secret message to be transmitted was passed through two layers before it was embedded within the cover message in the third layer. Experimental results have shown that three layer model achieved a signal to noise ratio of 54.78dB in comparison to 51.12 dB of conventional LSB method[22].

Lovey Rana and Saikat Banerjee implemented an audio steganographic system that provides improved security. To achieve this, dual layer randomization approach was used. First layer of randomization was achieved by randomly selecting the byte number or samples. An additional layer of security was provided by randomly selecting the bit position at which embedding was done in the selected samples[23].

Muhammad Asad et al. proposed two ways to improve the conventional LSB modification technique. The first way was to randomize bit number of host message used for embedding secret message while the second way was to randomize sample number containing next secret message bit[24].

Anupam Kumar Bairagi et al. worked on the substitution technique of audio steganography, resolved its remained problem. In the method proposed, the deeper layer was was embedded by the message bits depending on the host audion environment due to which robustness increased especially

against those intentional attacks which try to reveal the hidden messages[25].

Muhammad Asad et al. proposed a three layered model based on least significant bit replacement for audio steganography. Before Embedding within the cover message in the third layer, the secret message to be transmitted was passed through two layers [26].

Pooja P. Balgurgi and Prof. Sonal K. Jagtap combined two areas of network security, cryptography and steganography and implemented a technique of two level encryption of user data. The additional level of security was shown by the combination of LSB technique with XORing method [27].

S. Imaculate Rosalinel and M. Ashok Raj used Adaptive Pixel Pair Matching and proposed a method for hiding secret message in the cover image.

The most famous LSB method faced its own cons of higher distortion and lower embedding efficiency. That later overcame by the Optimum Pixel Adjustment Process (OP AP) method[28].

Gunjan Nehru and Puja Dhar used LSB and genetic algorithm approach and came up with the detailed look of audio steganography techniques. Their research was based on a study of audio steganography techniques using different algorithms such as genetic algorithm approach and LSB approach[29].

P. T. Yu et al. proposed a work of color image's spatial domain in which the binary watermark was embedded where the neural network get trained bye the set of training patterns. The difference between the intensity of the blue component of the central pixel and the others within the window was taken as training pattern. Each training pattern contains 9 input vectors and 1 output vector. Legal image owner extract watermarks by the trained neural network [30].

C.C. Chang and I. C. Lin developed A novel watermarking scheme for the image data using neural networks based on discrete wavelet transform (DWT). A coordinate set *S* was selected from DWT decomposition using a pseudo-random 8 Santi P. Maity, Malay K. Kundu noise generator (PRNG). A training set was constructed to train the network where each training pattern contains eight input vectors and four expected outputs. The trained network was used to embed watermark[31].

H.-C Huang et al. proposed progressive watermarking where GA was used to find the optimal frequency bands for watermark embedding into DCT based watermarking system, which could simultaneously improve security, robustness and visual quality of the watermarked image. GA was used to choose the DCT coefficients under certain attacks in every iteration and cost function was developed from the combined contribution of imperceptibility and robustness measure[32].

F. H. Wang et al. proposed a work where binary watermark was embedded by pixel value difference of mean gray values of a neighborhood using a spatial domain watermarking technique. The results were seen as a secret key and was used in the extraction process of watermark information[33].

Mazdak *et al.* proposed an algorithm of a robust steganography that embedded the data in the multiple, vague and higher LSB layers. Generally there were two types of attacks namely unintentional attacks like re-sampling, re-quantization, lossy compression, etc and intentional attacks like cropping, recycling, re scaling, white colored noise, etc. By Mazdak *et al.* (2009), solutions were suggested for both type of attacks[34].

Krishna Bhowal et al. resolved the remained problems of substitution technique of Audio Steganography for image transmission by using a novel, principled approach. In the first level, they first extract image data from an image file. In the second level, they used a powerful GA (Genetic Algorithm) based LSB (Least Significant Bit) Algorithm to embed the image data into audio data[35].

Ahmed proposed a hybrid genetic algorithm (GA) and provide a hybrid GA by incorporating a new local search algorithm to the simple GA in order to obtain a heuristic solution to the problem[36].

Kumar and Debroy proposed an alogorithm to calculate the weights in the neural network model by using the conjugate gradient method and a hybrid optimization scheme involving conjugate gradient method and genetic algorithm The hybrid optimization scheme helped in finding optimal weights through a global search[37].

Tantar, et al. proposed an algorithm for solving the structure prediction problem. The parallel hybrid genetic algorithm (GA) presented the Conjugated gradient-based Hill Climbing local search that was combined with the GA, in order to efficiently deal with the problem by using the computational grid[38].

Zhou-Shun et al. combined the local searching ability of conjugate gradient method with global search ability of GA organically. This algorithm changed the problem of solving the linear equations into the problem of equivalent differential by searching the most optimization solution[39].

Li, et al. improved the performance of genetic algorithm for cable forces optimization by presenting a hybrid genetic algorithm which combines the conjugate gradient method with genetic algorithm to 40].

Xie and Liu proposed a hybrid genetic algorithm for geo-physical inversion. According to the properties of the genetic algorithm and the conjugate gradient algorithm, the method had the attributes of the global-convergence of the genetic algorithm and the fast convergence of the conjugate gradient[41].

R Balagi & G Naveen embedded the secret information in some particular frames by extending their work towards video steganography [42].

S.Geetha et al. presented a genetic algorithm (GA) based approach to audio steganalysis. The basic idea was that, the various audio quality metrics calculated on cover audio signals and on stego audio signals vis-avis their de-noised versions, were statistically different. GA was employed to derive a set of classification rules from audio data using these audio quality metrics, and the support-confidence framework was utilized as fitness function to judge the quality of each rule[43].

Bo Liu et al. worked in the direction of cloud computing and use of steganography in that area. There was an increase in tending of enterprises and individuals to store their data in the cloud storage systems, yet, the sensitive data will face serious security threats[44].

Saswati Ghosh et al. used Cryptography and Audio Steganography for mobile network by presenting a double layered secure data transfer technique. Firstly, the characters of secret text message were converted to bit values and were encrypted by XOR operation using a Symmetric key. Then using a secret key-box, it was again scrambled and then divided into 2bit blocks. These blocks from MSB were replaced by the Left Significant two bits of each byte of cover audio bit stream[45].

III. PROBLEM STATEMENT:

Steganography is a technique for data hiding such that the existence of the secret message is concealed. No one is aware about the existence of the message except the intended recipients. If the audio file is used as cover to hide secret data then it is called audio steganography.

The most common technique to implement steganography is substitution technique in which certain bits (generally LSB's) of the cover file are substituted with the bits of secret message. However the technique is very famous but it suffers from certain limitations. The limitations are there due to substitution with LSB's. It makes them susceptible to be attacked whether intentional or un-intentional. The proposed solution is to substitute the message bits with the deeper layer bits of cover file. However this would result in greater distortion in stego file. Thus selection of the deeper layer bits for substitution is to be optimized in such a way that the distortion induced should be below than a tolerable limit.

There has been a tradition of using soft-computing techniques in order to achieve this optimization. Genetic algorithm is a component of soft-computing that is generally used to achieve optimization. The dominant use of GA for optimization is due to its basic nature that is inspired from biological evolution. Moreover the algorithm demands so less as initial input. The algorithm start initially with certain random solutions. Each solution is then evaluated and assigned some fitness value. The more fit solutions are selected to act as parents and go for cross over. After the operation, off-springs are produced. These off-springs are again evaluated using the same fitness function. The more fit off-springs replace the less fit parents and form the new population.

The algorithm keep on running and evolving the solutions until a terminating condition is reached.

Objective of the research work is to develop a tool that can be used to securely transmit secret messages as well as data. The tool developed will provide a pathway to ensure security in the digital transmission of data. The data will be transmitted in such a way that its existence will be concealed. The actual message will be accessible to the intended recipient only. However the third person can only see the audio file that will be chosen as carrier by the transmitter.

IV. CONCLUSION OF THE LITERATURE REVIEWED

The most famous technique to implement steganography was substitution technique in which some of the bits of cover file were substituted with the message bits. The LSB's were chosen for substitution as they contribute least in computation of statistical value of the cover file.

In order to increase the data hiding capacity of cover files, multiple LSB's got substituted. However that type of methods resulted in more distortion produced.

Since substitution with LSB's is very susceptible to intentional as well as unintentional attacks thus solution was proposed to hide data in deeper layers. Hiding data in deeper layers of cover led to more distortion in cover file.

Some algorithms were proposed then which not only hide data in deeper layers but also do adjustments by willingly modifying certain other bits of cover file in order to minimize the distortion thus occurred.

Due to large availability in practical and its inherent masking effect, audio started to begin as a choice for cover file. More over Human Auditory System suppressed low frequency audio with higher frequency audio; called masking effect.

Even after the use of audio as cover the inherent problems of substitution technique remained as it is. Thus lots of variants of conventional LSB method came into practice with an attempt to be more robust.

Another layer of security was introduced by combining cryptography with steganography. Thus message to be hidden in cover was encrypted first and then hidden in cover audio.

It was the time then that researchers started combining soft computing techniques with steganography. However the combination of a particular soft computing technique was there to achieve some specific goal.

In order to develop optimized technique, GA became the first choice to be combined with steganography. However the different techniques differ in their choice of fitness function and the logic of applying GA.

Steganography technique to be used for mobile phone were also developed.

V. REFERENCES

[1] Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraim, "A view on latest audio stegnography",International Conference on Innovations in Information Technology, 2011, pages 409-414.

[2] Jayaram P, Ranganatha H R and Anupama H S,"information hiding using audio steganography ",The International Journal of Multimedia & Its Applications (IJMA) Vol.3, pp. 86-96, Aug. 2011.

[3] Swati Malviya, Manish Saxena, "audio steganography by different methods ", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, pp. 371-376 July 2012.

[4]. Kekre, H.B., A. Archana R. Swarnalata and A. Uttara," Information hiding in audio signals". Int. J.Comput. Appl-2010., 7(9).

[5] Mazdak Zamani *et.al* , "A Secure Audio Steganography Approach", International Conference for Internet Technology and Secured Transactions 2009.

[6] Ajay.B.Gadicha, "audio wave steganography ",International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov.2011.

[7].Nedeljko, C. and S.A. Tapio," Increasing robustness of lsb audio steganography by reduced distortion lsb coding", J. Universal Comput. Sci.-2005 11(1): 56-65.

[8].Samir, K.B. and D. Biswajita," Higher LSB layer based audio steganography technique", IJECT-2011, 2(4).

[9].Ahmad, D. and P. Mohammad , "Adaptive and Efficient Audio DataHiding Method in Temporal Domain", International Conference on Information and Communication Systems-2009.

[10]Gopalan., "Audio steganography using bit modification", 2003 IEEE International conference on Acoustic, Speech and Signal Processing page(s): II – 421 -4 vol.2.

[11]N. Cvejic, T. Seppanen, "Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC04), 2004, vol. 2, pp. 533-540

[12]Mohamed A. Ahmed, Miss Laiha Mat Kiah, B.B. Zaidan and A.A. Zaidan, "A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm", Journal of Applied Sciences, 2010, 10(4), pp. 59-64.

[13]Kumar, H.; Anuradha, "Enhanced LSB technique for audio steganography," *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on* , vol., no., pp.1,4, 26-28 July 2012

[14].Gopalan K., "Cepstral Domain Modification of Audio Signals for Data Embedding," Proceeding of 16th Annual Symposium on Electronic Imaging--Security, Steganography and Watermarking of Multimedia Contents VI, San Jose, CA, January-2004.

[15].Ahmad, D. and P. Mohammad, "Adaptive digital audio steganography based on integer wavelet transform", Circ. Syst. Signal Process.-2008, 27: 247-2590.

[16].Samir, K.B. Tuhin, U.P. and Ra., Avishek, "A robust audio steganographic technique based on phase shifting and psycho-acoustic persistence of human hearing ability", Int. J.Comput. Corporate Res.-2011, 1(1)

[17]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 (ICCNIT), pages 143-147

[18]Kaliappan Gopalan, "A Unified Audio and Image Steganography by Spectrum Modification", International Conference on Industrial Technology, 2009, Page(s):1 – 5

[19]Shirali-Shahreza, S.; Manzuri-Shalmani, M.T., "Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate," *Information and Emerging Technologies, 2007. ICIET 2007. International Conference on* , vol., no., pp.1,5, 6-7 July 2007

[20]Rizky M. Nugraha, 'Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data", International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia

[21]S.S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography", International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012.

[22]Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", International Conference on Emerging Technologies (ICET), 2012.

[23]Lovey Rana, Saikat Banerjee, "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding" , International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013

[24]Asad, M.; Gilani, J.; Khalid, A., "An enhanced least significant bit modification technique for audio steganography," *Computer Networks and Information Technology (ICCNIT), 2011 International Conference on* , vol., no., pp.143,147, 11-13 July 2011

[25]Bairagi, A.K.; Mondal, S.; Mondal, A.K., "A dynamic approach in substitution based audio steganography," *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on* , vol., no., pp.501,504, 18-19 May 2012

[26]Muhammad Asad, Junaid Gilani, Adnan Khalid, "Three Layered Model for Audio Steganography", 2012 International Conference on Emerging Technologies (ICET)

[27]Balgurgi, P.P.; Jagtap, S.K., "Intelligent processing: An approach of audio steganography," *Communication, Information & Computing Technology (ICCICT), 2012 International Conference on* , vol., no., pp.1,6, 19-20 Oct. 2012

[28]Imaculate Rosaline, S.; Ashok Raj, M., "Adaptive Pixel Pair Matching based Steganography for audio files," *Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on* , vol., no., pp.1,5, 7-9

Jan. 2013 Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu, "Techniques for Data Hiding", IBM Systems Journal, vol. 35, no. 3 and 4,pp. 313-336, 1996.

[29]Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach", International Journal of Computer Science (IJCSI), Vol. 9,pp. 402-406, Jan. 2012.

[30].P. T. Yu, H. H. Tsai and J.S. Lin, "Digital watermarking based on neural networks for color images, Signal processing", 81,(2001)663-671.

[31].C.C. Chang and I. C. Lin, "Robust image watermarking system using neural network", *Intelligent Watermarking Techniques*(World Scientific, Singapore 2004) 395-427.

[32].H.-C Huang, J. S. Pan, Y. H. Huang, and K.-C. Huang, "Progressive watermarking techniques using Genetic Algorithms", Circuits, Systems, and Signal Processing,**8,**(2007)58-68.

[33].F. H. Wang, L. C. Jain, and J. S. Pan, "Genetic watermarking on spatial domain", *Intelligent Watermarking Techniques*, (World Scientific, Singapore, 2004)377-393.

[34].Mazdak, Z., A.M. Azizah, B.A. Rabiah, M.Z. Akram and A.., Shahidan, " A genetic-algorithm-based approach for audio steganography", World Acad. Sci.Eng.,-2009 Technol., 52: 360-363.

[35]Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar, P.P. Sarkar, "Audio Steganography Using GA", *CICN*, 2010, Computational Intelligence and Communication Networks, International Conference on, Computational Intelligence and Communication Networks, International Conference on 2010, pp. 449-453, doi:10.1109/CICN.2010.91

[36].Ahmed , Z, H, (2013), "An experimental study of a hybrid genetic algorithm for the maximum traveling salesman problem",Mathematical Sciences , 7:10, doi:10.1186/2251-7456-7-10

[37].Kumar, A., and Debroy, T., 2006," Neural Network Model and Fluid Flow in Gas Metal arc Fillet Welding Based on Genetic Algorithm and Conjugate Gradient Optimization", Science and Technology of Welding and Joining, Vol. 11, No.1

[38].Tantar, A., A., Melab, N., Talib, E. G., Parent, b., and Horvath, D., 2007, "A parallel Hybrid Genetic Algorithm for Protein Structure Prediction on the Computational Grid", Future Generation Computer System, 23, 398-409

[39].Zhou-shun, Z., Xiao-hui, Y., and Guanghui, H., 2008, "Genetic Algorithm with Conjugate Gradient Operator", Journal of Shangrao Normal, 03

[40].Li, J., Li, S., and Zhang, B., 2009, "A Hybrid Genetic Algorithm for Cable Forces Optimization of CFST Arch Bridge",Computational Intelligence and Software Engineering, CiSE,1-4.

[41].Xie, W., and Liu, J., 2010, "Integrated Programming and Application of Genetic Algorithm and Conjugate Gradient Method", Progress in Electromagnetic Research Symposium Proceeding, Xian, China, 22-26

[42]Balagi R, Naveen G, "Secure Data Transmission Using Video Steganography", 2011 IEEE International conference on electro/information technology (EIT).

[43]Geetha, S.; Sindhu, S.S.S.; Kannan, A., "An Active Rule Based Approach to Audio Steganalysis with a Genetic Algorithm," *Digital Information Management, 2006 1st International Conference on* , vol., no., pp.131,136, 6-6 Dec. 2006

[44]Bo Liu; Erci Xu; Jin Wang; Ziling Wei; Liyang Xu; Baokang Zhao; Jinshu Su, "Thwarting audio steganography attacks in cloud storage systems," *Cloud and Service Computing (CSC), 2011 International Conference on* , vol., no., pp.259,265, 12-14 Dec. 2011

[45]Saswati Ghosh, Debashis De and Debdatta Kandar," A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network", IEEE 2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. Pp.29-33.