INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

REVIEW STEGANOGRAPHY METHODS OF AUDIO MP3

Asseel Jabbar Almahdi

Department of Computer Science, Faculty Science Computers and Mathematic, University of Thi-Qar, Iraq

asseelalmahdi@gmail.com

Abstract: - In the last years, with the use of the Internet, electronic communications and the presence of pirates and infiltrators now, one of the concerns that arose is the safe transfer of information. The solution is therefore the Steganography system. Steganography is a science of hiding information, that is, hiding a message in another message so that the enemy cannot know that there is a hidden message in the host's message. Hide can be done in two areas, compressed or uncompressed. Due to the great popularity of MP3 files on the Internet, they do not pay too much attention if they are used as the carrier of the hiding process, so for the sake of the importance of MP3 files, we will study the most important methods of compression related to MP3 audio files and discuss each of these methods separately to know their advantages and disadvantages.

Key words: Steganography, Audio data hiding, Side information, MP3, MDCT, Quantization

1. Introduction

The use of confidential communications by encoded messages was the subject of practical application through ancient and modern history. The hiding is concerned with the confidentiality of the contents of the message as well as the confidentiality of the communication and when the suspect suspects the existence of hidden information, it tries to decrypt or destroy or change the message then. Send them to the recipient who knows how to interpret them. Steganography is a science of hiding information, that is, hiding a message in another object, which increases the security of data transfer and archiving. In the Steganography process, the object in which the data is hidden is called the carrier object and the new object is called stego such as hiding the information in the audio file (Figure 1). The Steganography system contains three basic characteristics, Perceptual Transparency, Robust and Absorption or Hiding Capacity. Perceptual transparency: in this characteristic the carrier file and the hidden file that contains the confidential data do not need to be detectable [1]. Absorption means the amount of data that can be included using a method of masking information. Under this inclusion, the transparency of the audio file is unshakeable, so the listener cannot distinguish confidential information [2]. Hiding Capacity: is the ability of hidden message to remain resistant to damage [3]. These three characteristics are not compatible with each other, increasing each other, reducing the other. Therefore, a compromise should be established between these three features in accordance with the intended application to contribute to the improvement of the required feature. Various methods have been proposed to cover audio files, but due to the high popularity of MP3 files over the Internet, they are important for coverage or concealment. Coverage in MP3 files can be done in side information and in MDCT or time domain transactions. All MP3 files are divided into small parts called frames. Each frame stores 1152 sound samples. In addition, the frame is split into two granules, each containing 576 samples. The Fast Fourier Transform (FFT) and the psycho-auditory

model are then used to determine the threshold for all frequencies. On the one hand, the signal is filtered by a filter bank and turns into 32 sub-band frequencies [4]. According to the output of the psycho-auditory mass, the Modified Discrete Cosine Transform (MDCT) window is selected for long or short, where after placing the sub-sampling window with the specified window, MDCT conversion is taken and transferred to the frequency domain and 175 MDCT coefficients are generated. These coefficients are then quantized. For quantization, two overlapping loops are used in MP3. The internal loop is achieved by encoding 576 samples per granule with the number of bits available.

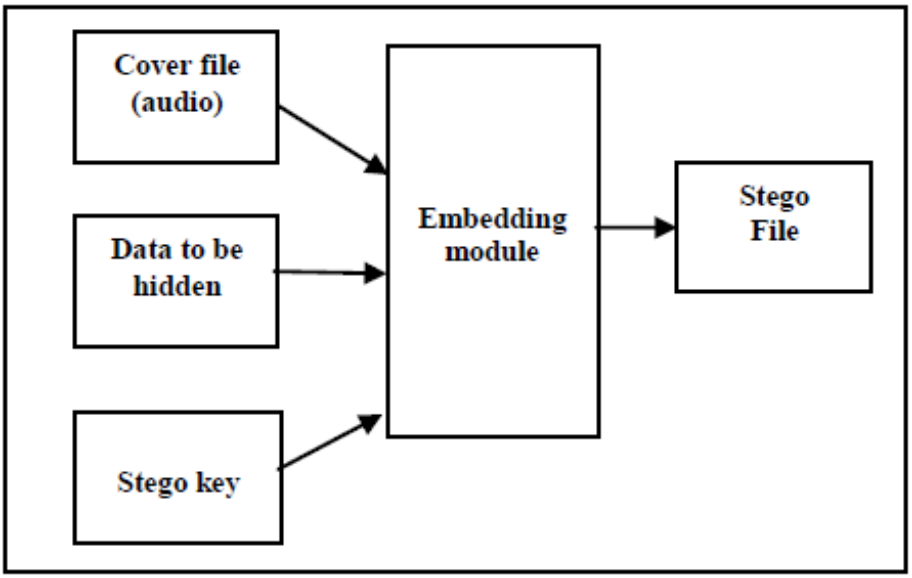

Figure 1: audio Steganography

If the condition does not occur, the quantization step increases and the loop is executed again. After the internal loop is complete, the distortion in the scaling factor ranges is verified by the outer ring so that the permissible distortion is not exceeded and the quantitative samples are introduced into the Huffman coding block where Hoffman scales are used to encode these samples [5]. In the following, we study the proposed methods in this regard, and finally compare the characteristics of these methods.

2. Hide the audio file

The process of hiding data in the audio signal is a major challenge because the human hearing system. It works in a wide range of dynamic frequencies (HAS: Human Auditory System), since the human ear has the ability to recognize the sounds at a high rate of (20Hz - 20000Hz) Which makes it difficult to add data to the original file or delete it which is recognized directly as noise. Therefore, this system is very sensitive to any abnormal changes in the samples, but the existence of some gaps in the human hearing system can be exploited, the concealment and manipulation of the original file data is possible. For example, the human ear does not differentiate between two tons of voice [26] and the high voices conceal the low voices

3. Sample quantization

The quantization process is the number of bytes used to represent the audio sample and is a very important factor in maintaining the accuracy of the sound when converting it to the digital format. The more bytes used in the representation, the sound specification is very close to the real value of the acoustic samples. There are two types of quantization, the first type uses one Byte to represent the audio sample, And the second type uses two Byte to represent the audio sample [27].

4. MP3 files Steganography in the MDCT field

4.1 MP3 audio coverage algorithm in the VLC

In coding theory, a variable-length code is a code which maps source symbols to a variable number of bits [25]. In [21] the watermark hide pattern is provided in Variable Length code (VLC). An experiment was conducted on the abundance of Hoffman tables used in a set of audio files, and the results show that Hoffman's Table 16 is more frequent than the rest. For this purpose, this table is used to embed data. If the length of the code word and the tag bit changes randomly, this change causes a bit of confusion and MP3 audio is not normally encoded. There is no inherent replication in VLC, but confidential information can be embedded by replacing VLC mapping with VLC. Symbols with a variable length of the Hoffman table with a code length and an equal bit tag are divided into two code space with a length equal to V_0 and V_1. V_i or V_i' is one of the code words in two of the code space and N is the sum of the code words in each code space. VLC in V_0 and V_1 are reversed one by one and sequentially define binary information defined as "0" and "1". When the information bit is embedded with "0", V_i for V_0but V_i' for V_1 change to V_i . Conversely, when a bit of "1", V_i is associated with V_1, but V_i for V_0 changes to V_i . The code words that do not belong to V_0 and V_1 are not considered. The information hidden through this processing can be embedded in the VLC and ensures that the structure and length of the MP3 stream is not changed. This algorithm is a Blind watermark. When extracting if VLC belongs to V_0, the information bit is extracted "0". If VLC belongs to V_1, the bit of information will be "1". According to experiments, this algorithm can have a higher ability to hide data with less computational complexity as well as good transparency.

4.2 BvSteg Method

This method has a 4-fold masking capacity in MP3stego and Under MP3Cover, which hides data in the big value area of the long segments [9]. Where embedding is done in (region2) in the 44.1 KHz sampling rate according to the frequency band 5-14 KHz. Because of the density of MDCT [14], most of the spectrum energy is concentrated in region0 and region1. Changes in region2 result in the generation of low noise components in the signal. Thus, the disturbed sound signal as envisioned by the human ear is not very different from the signal without inclusion. In the embedding of each Hoffman table, a matrix is created. If the number of Hoffman bits to denote a pair (x, y) is equal with the number of Hofmann bits needed to encode the pair (x y), then the value of [x] [y] for this matrix will be "1 ". Then, at the end of the inner loop and after the Quantization and coding of Hoffmann, it is first verified that a long segment is used, unless the data is included in the MDCT. Because the number of changes in each granule is determined by 4, it is achieved if the four coefficients have not changed in the current granule. If all conditions are met, the last condition, which is equal to the length of the character encoding, is checked for pairing (x, y) and (y, x). If this condition is met, if we want to embedded the bit "0" and x <y, we encoded the pair (x, y), but if x> y, then (y, x) is encoded. In order to embedded a "1" bit, it works to reflect the "0" bit. In extracting the watermark, the pair of spectral quantities obtained after Hoffman decoding is compared to its range. If we reach (x, y) and all the conditions applied during the embedding process are fulfilled, then if x <y, a bit of 0 is embedded and if x> y, 1 bit will be embedded.

4.3 Replace the LSB that was selected for the transfer of the side information

The purpose of this method is, as in [15] and [16], to embedded 20-50 bits for each granule to mask the loss of the package. This is why the LSB (Least Significant bit) replacement is simple [17] where side information is embedded in the LSB for quantified MDCTs. The side information of each granule contains the information required to encrypt the main data. When a certain amount of side information is filled in an auxiliary data field, the bitrate of the audio stream decreases. If the bitrate is constant, the sound quality will be distorted. In [18] in order to embedded side information, the word encoding G.711 is used. Because G.711 uses non-linearization, as the host signal range is increased, the distortion resulting from the replacement of LSB is exacerbated. The LSB replacement method, therefore, embeds the side information in small-scale models. The embedding at the top

because its coefficients are zero and not encoded, reduces the pressure efficiency and generally damages the sound quality. Because the lower section is further quantized to keep the bitrate constant, so the side information is embedded in the lower part of the MDCT, so be it the range of key transactions is small to replace see figure2.

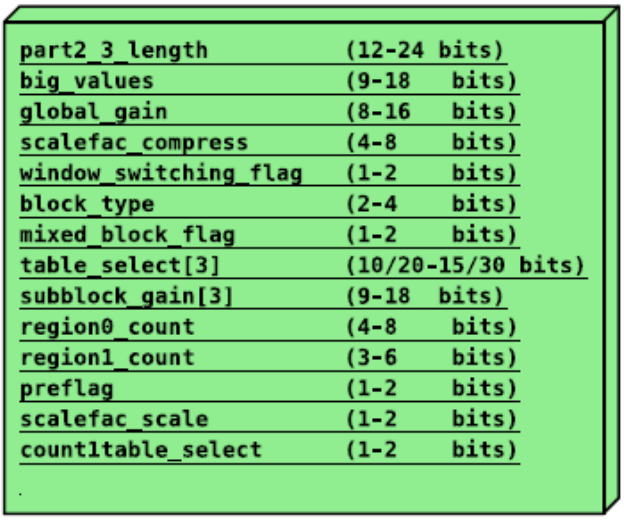

Figure2: side information [28]

In order to connect these two conditions, m is chosen from the granule, and then LSB is removed from them and then arranged vertically. The *n* minimum coefficient of the equivalent is changed with the secret bits ($n \leq m$). During extraction, such as the implementation of the embedding process, at the beginning LSB for *m* is deleted and the incremental order of m is defined. Of which n is chosen as the lowest coefficient. Where the LSB of *n* is the lowest coefficient corresponding to the watermark bits. According to tests, this method provides better sound quality than including side information in the Assistant data field.

4.4 Data Hiding in MP3 Audio by Modifying QMDCT Coefficients

In [20] because of the human auditory system (HAS) model in the quantization stage, noise is controlled by embedding data until the deviation is allowed. This method is simple and has high concealment capability and good transparency as well. Test results indicate that a large amount of data, especially at high compression rates, is inserted into the MP3 audio, so that the audio distortion is retained. After the quantization process, MDCTs are selected to include the hidden message. Then LSB QMDCT coefficients are replaced with password bits. The external ring is used to control noise that is under the threshold of concealment. When each range is skewed, the internal loop is called again. This is why the secret bits are repeated as long as there is no deviation in the bands. To avoid the addition of very large noise, QMDCT is chosen with greater than δ to hide the bit of the secret message, where δ is determined by experiment. For the future, hidden bits can only be extracted by examining LSB for MDCT coefficients.

4.5 Genetic Content-Based MP3 Audio Watermarking in MDCT Domain

The technique of genetic algorithms is characterized by the prevailing traditional techniques that the strength of this technique lies not in its ability to focus on optimal localization solutions, but in the breadth of the area to be represented, and the value of optimal optimization approximation. Academics currently rely on genetic algorithms as a promising technique for optimization in the mid-1970s, beginning with the study of the method of genetic algorithms and then developing into an effective method for determining optimal modeling. The genetic algorithm is used in the watermark system, where multiple keys are generated and the genetic algorithm is obtained. The optimal solution is obtained after the implementation of the genetic algorithm on the primary generation of randomly generated keys. The ideal key used in the process of embedding and retrieving the

watermark is obtained after Select and calculate the fitness function based on correlation coefficient and scale PSNR. In [19] the genetic algorithm was used to select the best L coefficients to include the watermark in granule. This genetic selection is made according to the criteria extracted from the audio content to improve transparency and strength. The security of the watermark increases because of the random nature of genetic selection. Since the selection of transactions depends on the content of the file, the selected MDCT transaction information, which carries the watermark bit, is saved in the database to extract the watermark in the future. In quantization, the values of the MDCT parameters change (the values close to zero are replaced by zero), but the number of points after the decimal point changes infrequently. Thus, hiding the watermark bit can correspond to the even and odd number of zeros after the decimal point on the coefficients. There is an option to add zero to the zeros of a coefficient, a division of 10, but this method is not optimal because of the large variation of the coefficients in the quantization process. Thus, in order to increase the number of zeros of the coefficient X, its value is replaced by $sign(X)\times5\times10^{-Z(x)-2}$ where $Z(x)$ is the number of zeros after the decimal point. In this way, for the new X, the probability of change in the quantization will be very low. Therefore, the chance of losing the watermark is likely to decrease. When $Z(x)$ is increased, $Z(x)$ is more likely to change in the quantization. For this, $Z(x) > 2$ replaces X with zero in the quantization process. As a result, chromosomes like X do not produce high productivity. During extraction, the watermark bit sequence is formed according to the password and the secondary key reaction of the associated watermark from the database. The MDCT coefficients, whose indicators are compatible with the parameters of the bit-bearing coefficients, are then extracted for each factor. If the number of zeros after the even point is double, the inverse bit will be zero and vice versa.

4.6 Steganography for MP3 audio by exploiting the rule of window switching

In MP3 the window is used to obtain high precision in the field of time and frequency. The windows have different types where the normal window is usually used. The standard for selecting the type of windows is the value of cognitive entropy (PE) derived from the audio model. If we are in the normal segment and the entropy value is greater than 1800, the start segment will be selected. Otherwise a normal segment will be selected. If we start and the Entropy value is greater than 1,800, the segment will be short. If in the case of the short segment, and the entropy value is greater than 1800, the short segment is selected again. Otherwise, the stop segment will be selected. In stop mode, if the amount of entropy is greater than 1800, a start segment is selected and in the reverse mode a normal segment is selected. The coverage method in [22] depends on the window change strategy. The main idea to embedded a secret message in MP3 audio is by creating a connection between the window type and the secret bit and changing the window regardless of PE. When bit 1 is hidden, a short window is selected regardless of PE, and the previous granule must also be changed according to the rules. When hiding bit 0, a normal, start or stop window is selected. In this way, there is a flag. Each time after the secret bit is entered, the window becomes stop and becomes flag = 1. When we want to save bits in the next granule, if flag = 1, the previous bit will be reincluded. To extract the watermark, the receiver uses the k key to select the granules in which the data is embedded. The granulomas will be decomposed, the window type selected in each granule and then the watermark bit extracted according to the type of window.

4.7 MP3-ResistantAudio-Adaptive Steganography

The general idea is that the sound signal using conversion Δ transforms into a two-dimensional image [23]. Through a watermark embedding pattern for a reliable image, and the sound quality is maintained by reversing the sound from the watermark image. Audio Steganography with this method turns to easier Steganography of images. In this method, a mathematical transform is designed between the signal-induced coefficients $C = C_A^L$ and the two-dimensional sequence of the coefficients (image). The relationship between the PNSR parameters on the images and two specific audio models under PAQM and NMR are maintained. The low-level coefficients of the wavelet are taken with a distance Δ first, a two-dimensional scan or a scan raster, which are converted into a two-dimensional image. *a* represents the beginning of downsampling and is selected to improve security. Parameters *a* and delta are hidden keys. The size of the image must be raised to force 2 so that the *wxw*

segments can be separated from the image and by a suitable picture embedding method, one bit can be embedded in each segment. The size of the Steganography data depends on the choice of Δ and w. After creating the watermark image, inverse conversion Δ is applied to the watermark image. Where coefficients are re-established less than the first level of wavelets. The conversion IDWT is then applied to C_A^L and C_A^H until we reach the A_w watermark.

4.8 Adaptive Watermarking Algorithm for MP3 Compressed Audio Signals

In [24] Gaussian distribution analysis is used on MP3 frames considering energy to adjust the watermark parameters. This adaptive algorithm is implemented during MP3 encoding. This method is used to keep inaudible incoming noise, where it is placed in high power parts. For embedding, first volunteer the first frame of an appropriate watermark for embedding, for example the first non-zero frame. Two adjacent frameworks will be merged, where macro frame (32 * 36) is created to embed the watermark (each frame containing 32 packages and each packet containing 18 lines). A water pattern matrix is then created (32 * 36) which is equivalent to one macro frame. The content of this template is "+1" or "-1", which displays the watermark bit "1" or "0", respectively. Then, for all MDCT values 32 * 36 in the macrophage, Gauss analysis values are created according to [24]. The energy is calculated to pack the volume factor in MDCT by psycho-auditory model II and then the final watermark is created according to the energy calculation results and the Gauss analysis. In the extraction process, the first frame containing the watermark, which according to the embedding algorithm, ensures the first bit of the watermark in the first non-zero frame. Two adjacent frames are integrated. Gaussian distribution analysis is then applied to all MDCT coefficients in the macro frame to detect the watermark. The watermark w_0' is made based on the Gaussian distribution analysis function on the watermark macro frame. During detection, the sum of w_0' is calculated as Gaussian values in macro frame. If w_0' is greater than +1, the' 1 'bit watermark is embedded in the original macro frame. If w_0' is less than -1, the watermark is embedded with a "0" bit in the original macro frame. If w_0' is between [-1, + 1], there is no watermark embed in the macro frame.

5. Steganography of MP3 files in the field of Side information

5.1 MP3stego Method

MP3stego is considered to be one of the most advanced Steganographic tools [6]. The MP3stego information is embedded when compressing an MP3 file. Embedding principles in MP3stego is to use the parity principle to include the data in the variable block length part2_3_length of the granule in the MP3 file [7]. The variable part2_3_length represents the total number of bits required for encoding part 2 (scale factors) and part 3 (Huffman coded data). Initially, data compression and encoder are selected and a semi-random, SHA-1 random bit generator is selected to embedded data in granule. The normal MP3 encoding for the required granule is performed, and then a parity is compared to the length of the block with the required bit to hide. In case of matching, no changes will be made, and the encrypted section will be placed in the MP3 file. Otherwise, the MP3 encoder step will change and the quantization process will be repeated until the desired parity of the segment on hiding the information in the MP3 file is obtained. If the file cannot include the hidden file in any directory, MP3stego will fail. In order to extract data in the recipient's hand, the granules for which the data is embedded are selected by using the secret key. It is then extracted according to the length of the hidden data segment. If the length of segment parity is equal "1", the embedded bit is "1" and if the length of the segment is "0", the embedded bit is also "0". One of the problems of this method is the possibility of an unfinished loop [8] and low absorption due to the random jumping of granules and the destruction of the watermark by decompressing the file and re-compressing it [9].

5.2 Under MP3Cover Method

Under MP3Cover [10] is a tool for the coverage system where global_gain is used to hide data. Unlike MP3stego, Under MP3Cover hides data previously encoded or encoded in an MP3 file. The modifications are

implemented on LSB for the global_gain variable in the granules that were selected to reflect the embedder bit. This tool uses a spacing parameter to select granulates for embedding. In [11] a method was proposed to detect hidden files via Under MP3Cover. The maximum capacity of the carrier when Under MP3Cover and MP3stego is used is 4 * (number of frames bits). If the stereo signal, both programs can be included in at least 4 bits per frame because the stereo signal contains two channels and, in each channel, there are two granules.

5.3 MP3 audio Steganography based on Quantization Step Parity

In [12] Considering the Quantization Step Parity instead of the size Parity of the segment, it helps to solve the problem of the infinite MP3stego loop, contributes to the improvement of the non-detectable statistical and achieves better transparency and higher security compared to MP3stego. By analyzing the internal loop of the MP3 algorithm, Parity bit of the length of the segment has equal value in many frequencies, but the Quantization step of the adjustment step always changes, because the adjustment step increases one at a time. In the embedding process, the granules required for embedding are selected using a semi-random bit generator. If the bit of the equalization step is similar to the hidden order and the general condition of the loop, the number of bits of Huffman coding is less than the number of bits available, when the inner loop ends. Otherwise, the Quantization step increases and the Quantization is repeated with the new update step until the end-of-loop condition is created. Once the bit number condition is correct, the embedding process can be completed in no more than two duplicates. With these modifications, the infinite loop problem is minimized efficiently. In order to extract the watermark during decoding, if the size of the Quantization step is even, the embedded bit is "1" and if it is an odd, the embedded bit is "0".

5.4 Lossless and Secure Watermarking Scheme in MP3 Audio by Modifying Redundant Bit in the Frames

In [13] a special bit is used to include the data. Because the original data remains unchanged, the watermark does not cause any deviation of the carrier sound. The watermark data is encrypted by Arnold conversion before embedding to improve system security. Because of packet loss during transmission, a synchronized symbol is inserted into the watermark to improve the quality of the watermark update. The n bit of the watermark data is compared with n bits in the original data in the granule (the location of these bits is known to the sender and the receiver), if n bits of the watermark data and n bits of the MP3 file are equal, the special bit is set to "1 ", Otherwise your bit will be" 0 ". Watermark data and MP3 file contain a uniform distribution. If n equals 2, in all four frames 2-bit can be hidden. Therefore, the sampling will be 5.0 bits per frame. Synchronization codes are added to the watermark data to address data loss in real-time applications. To extract the watermark, the special bitrate of the MP3 file frame that is hidden first is checked, and n bit of the MP3 file data is placed in the matrix. also, synchronization codes will be been deleting the from the generated sequence. Arnold's reverse transformation is applied and the original watermark is obtained.

6. Conclusion

In this article, several categories of MP3 audio Steganography methods have been studied. Some methods embed data during the compression process, and some other methods apply the changes to the MP3 file after the encoding process. Others also embed data in the time signal when it is resistant to MP3 compression. The embedding of information in all ways can be divided into two categories: the MDCT field and field of side information.

REFERENCES

[1] Petitcolas. R.J. Anderson, and M.G. Kuhn, “Information Hiding- A Survey,”Proceedings IEEE, vol. 87, pp. 1062-1078, 1999.
[2] CvejicN.andSeppanenT.“Increasingthecapacityof LSB based audio steganography,” Proceedings 5 th IEEE International Workshop Multimedia Signal Processing,” December 2002, pp. 336-338.

[3] Muhammad Asad, Junaid Gilani, Adnan Hkalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography," International Conference on Computer Networks and Information Technology (ICCNIT), 2011, pp. 143-147.
[4] D. Pan, "A Tutorial on MPEG/Audio Compression," IEEE Trans. on Multimedia, Vol.2, No.2, pp.60-74, 1995.
[5] K. Brandenburg, "MP3 and AAC Explained," AES 17th International Conference on Hugh Quality Audio Coding, August 1999.
[6] University of Cambridge,"MP3Stego,"[Online].Available:http://www. petitcolas.net /fabien/steganography /mp3stego/
[7] F. A. P. Ross J. Anderson, "On The Limits Of Steganography," IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, pp. 474-481, May 1998.
[8] K. Brandenburg and H. Popp, "An Introduction to MPEG Layer," Fraunhofer Institut fur Integrierte Schaltungen (IIS), June 2000.
[9] R. J. Menon, "MP3 Steganography and Steganalysis," Master of Science Thesis in Computer Science, university of rhode island, 2009.
[10] Sourceforge,"UnderMP3Cover,"[Online],Available:http://www._leslibrary.com/files/UnderMP3 Cover..html
[11] A. Westfeld, "Steganalysis in the Presence of Weak Cryptography and Encoding," Ecture Notes in Computer Science, vol. 4283, p. 19, 2006.
[12] D. Yan., R. Wang., L. Zhang, "Quantization Step Paritybased Steganography for MP3 Audio," Fundamenta Informaticae - FUIN, vol. 97, no. 1-2, pp. 1-14, 2009.
[13] Y. Bailong., W. Penghui., J. Yaque., M. Jing, "Lossless and Secure Watermarking Scheme in MP3 Audio by Modifying Redundant Bit in the Frames," 6 th International Conference on Information Management, Innovation Management and Industrial Engineering, 2013, pp. 154-157.
[14] Y. Wang, L. Yaroslavsky, M. Vilermo, and M. Vaananen,"Some peculiar properties of the MDCT," in 5 th International Conference on Signal Proceedings, WCCC-ICSP, vol. 1, pp. 61-64, Aug 2000.
[15] M. Suzuki, T. Sakai, A. Ito, and S. Makino, "Reduction method of side information for packet loss concealment based onspectrumstripingcoding,"inProceedings 19th International Congress on Acoustics (ICA), September 2007.
[16] A.Ito,K.Konno,S.Makino,andM.Suzuki,"Packetloss concealment for MDCT-based audio codec using correlationbased side information," in Proceedings IIH-MSP, 2008, pp. 612–615.
[17] F. A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn, "Information hiding — a survey," Proceedings IEEE, vol. 87, no.7, pp. 1062–1078, 1999.
[18] I. Akinori., M. Shozo, "Data Hiding is a BetterWay for Transmitting Side information for MP3 Bitstream," 5 th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009, pp.495-498.
[19] N. Moghadam., H. Sadeghi, "Genetic Content-Based MP3 Audio Watermarking in MDCT Domain," World Academy of Science, Engineering and Technology, vol. 1, pp. 113-116, 2007.
[20] Z. LiGuang., W. RangDing., Y. DiQun, "Data Hiding In MP3 Audio By Modifing QMDCT Coefficients," ISECS International Colloquium on Computing, Communication, Control, and Management, vol. 2, pp. 494-497, Aug 2009.
[21] J.Tan., W. Rangding., Y. Diqun, "An Information Hiding Algorithm for MP3 Audio on VLC Domain," International Conference on Neural Networks and Signal Processing, 2008, pp. 392-395.
[22] D. Yan, R. Wang, X. Yu, J. Zhu, "Steganography for MP3 audio by exploiting the rule of window switching," computer & security, vol. 31, pp. 704-716, July 2012.
[23] P.Bao,M.Xiaohu,"MP3-ResistantAudio-Adaptive Steganography,"NanyangTechnologicalUniversity.
[24] B. Chen., J. Jiying., D. Wang, "An Adaptive Watermarking Algorithm for MP3 Compressed Audio Signals," Proceedings Instrumentation and Measurement Technology Conference (IMTC), May 2008, pp. 1057-1060.
[25] https://en.wikipedia.org/wiki/Variable-length_code
[26] M. Salem, O. Al- Rababah, A. Al-Attili, "New Technique for Hiding Data in Audio File", International Journal of Computer Science and Network Security, April 2011
[27] A.Ozerov, W. Bastiaan "FLEXIBLE QUANTIZATION OF AUDIO AND SPEECH BASED ON THE AUTOREGRESSIVE MODEL", IEEE Xplore,2007.
[28] R.Jayan ,"MP3 Steganography steganalysis', thesis, UNIVERSITY OF RHODE ISLAND,2009