Research Journal of Applied Sciences, Engineering and Technology 12(2): 154-162, 2016
DOI:10.19026/rjaset.12.2316
ISSN:2040-7459; e-ISSN: 2040-7467

Submitted: May 5, 2015 Accepted: July 14, 2015 Published: January 20, 2016

Research Article

A Review on Audio Steganography Techniques

[1]Ahmed Hussain Ali, [1]Mohd Rosmadi Mokhtar and [2]Loay Edwar George
[1]Research Center for Software Technologi and Management, Faculty of Information Science and Technologi, Universiti Kebangsaan Malaysia, 43600 Bandar BaruBangi, Malaysia
[2]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Abstract: The aim of this study is to present different types of steganography in brief and to give a special attention to audio steganography technique because a huge number of audio files are exchanged through the networks. Nowadays the widening of attacker's abilities to access the private and public information transmitted over public communication system makes way for highlighting a tool that guarantees the secure transmission of hidden information. Information hiding was a common security term that mainly includes three techniques: cryptography, steganography and watermark. Cryptography was an ancient form that is used for confidential data. Steganography is a popular tool that uses digital medium to hide confidential data in innocent carrier such as image, audio, text and video. Steganography is in fact a complement for the earlier data hiding technique cryptography. However watermark is used for copyright protection. Audio steganography is technique that hides any type of secret data in cover audio file. This study also discusses the main requirements of steganography methods and how those methods achieve them. Furthermore it shows steganography domain and, carriers and information hiding techniques used in audio.

Keywords: Carrier, cryptography, fractal coding, LSB, steganography requirements, vector quantization, wavelet transform

INTRODUCTION

Steganography is the schema of concealing confidential data in a cover file like image, audio or text so that no one other than sender and intended receiver is able to notice that secret data is hidden inside (Antony *et al*., 2012). Steganography is a word derived from the ancient Greek words *steganos*, which means covered and *graphia*, which in turn means writing (Cvejic, 2004). The earliest technique used for hiding important data was cryptography which has a similar protocol to steganography in protecting the data but there is a difference between them. The first scrambles the data so that anyone who gets the file can expect that there is something abnormal while the second hides the data in a way that can't be observed or even sense its presence. In steganography techniques, the sender hides the secret message into host file. This produced a stego-file then delivers it to the receiver that will process de-hide the stego file to retrieve the secret message. The secret data and the host can be any of various file type like text, audio, image and video file. If the host file is an audio file then the method is called audio steganography. Embedding secret data in hostaudio file is more challenging than using images since Human Auditory System (HAS) is more sensitive in comparison to Human Visual System (HVS) (Bender *et al*., 1996).

On the other hand, in comparison to other types of files, audio file is larger in size than other carrier’s file, high level of redundancy and high data transmission rate, the facts that make it more suitable as host file (Nosrati *et al*., 2012). Thus, this study focuses on audio Steganography and gives a wide view oftrends in this field.

STEGANOGRAPHY DOMAINS

Hiding data can be classified into three domains according to which the steganography technique has been applied: Temporal, Transform and Compressed domain as shown in Fig. 1.

In temporal domain, the secret data is hidden directly into host file in which the steganography techniques are simple and easy to implement Fig. 2. However this domain suffers from low robustness and

Corresponding Author: Ahmed Hussain Ali, Research Center for Software Technologi and Management, Faculty of Information Science and Technologi, Universiti Kebangsaan Malaysia, 43600 Bandar BaruBangi, Malaysia, Mob.: +601125115284; Fax: +60389216184

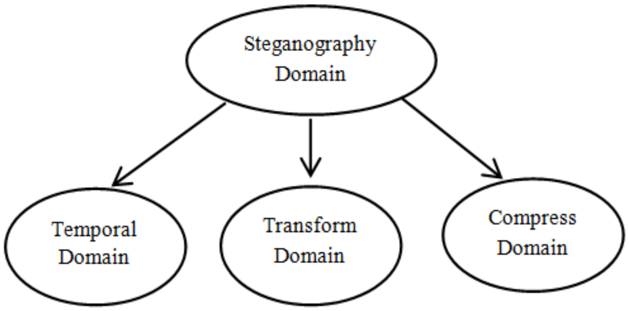

Fig. 1: Steganography domains

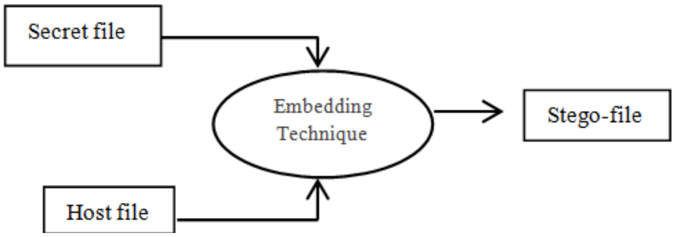

Fig. 2: Temporal domain

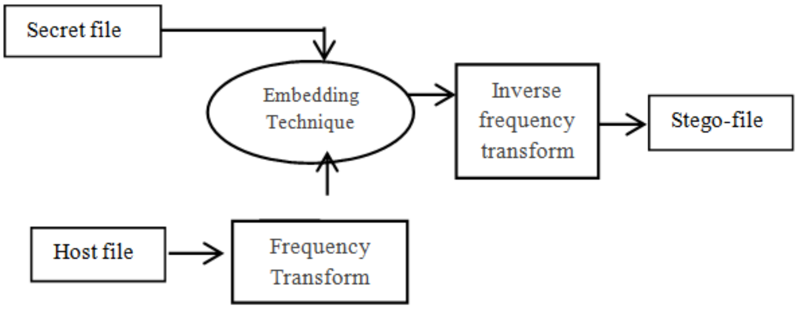

Fig. 3: Transform domain

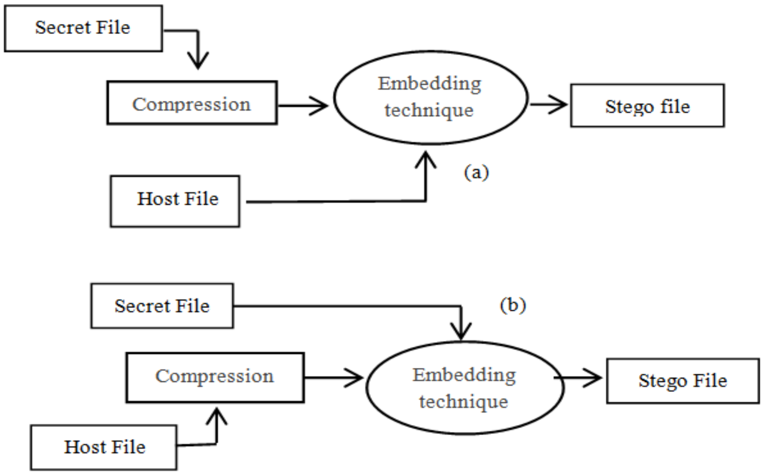

Fig. 4: Compressed domain; (a): Vector quantization; (b): Fractal compression

security (Singh, 2014). The earliest algorithm employed in such domain is LSB which is used in embedding process. This method hides the bits of secret data directly into the least significant bits of the cover file. Although this method has high embedding capacity and easily to implement, it has low robustness and the attacker can easily recover the secret message by collecting the entire LSB bits. Many techniques try to combine temporal steganography with other methods to enhance the robustness. However, they have some drawbacks like less security and sensitivity to compression.

The other domain used in data hiding is transform domain. In this domain, the cover file is transformed first,and then thesecret data is embedded into the transform coefficients Fig. 3. This enables steganography system to embed the data into perceptual significant components and makes it difficult to recover the embedded data. This will offer high level of security and robustness against signal manipulation like amplification and filtering. On the other hand, the hidden data suffer from data compression so the retrieved secret data may not be accurate. The most common transforms used in steganography are Wavelet transform (WT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT).

In compressed domain, varieties of techniques are developed. In this domain cover data or secret data is compressed using different compression techniques to develop steganography techniques and produce high capacity and compression ratio Fig. 4. Vector Quantization (VQ) is one technique that used to hide secret data in compressed cover file. Fractal Compression (FC) is another technique that compresses the secret data before hidden in cover file. Those are the most common compression techniques that are used.

STEGANOGRAPHY CARRIERS

Steganography is used to hide fidelity information in unsecure channels so it has to transmit and receive safely to the authority part using a medium that is called carrier or cover file. In this era, many types of digitalfiles are used to protect the secret data however multimedia files were frequently used because diffusion around the internet and thousands of them is shared daily between users.

In addition, data can also be hidden or embedded using network protocols (Bandyopadhyay *et al*., 2008). This section exhibits a review of the carriers that are used as a cover file for embedding secret data in various steganography techniques which is generally classified into four categories (text, image, video and audio)(Fig. 5).

Text: The process of encoding secret message into text file can be applied in different ways using the properties of the sentences like altering format text or depending on the number of words. It is the earliest method that is used in steganography. This type of steganography is difficult to implement with secret data of huge size due to low redundancy of the information in the text file and thereby low hiding capacity.

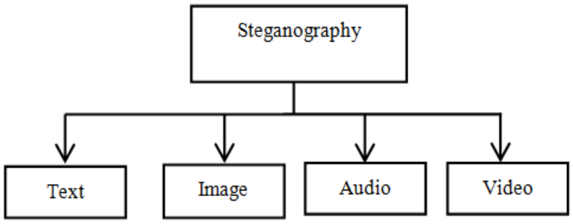

Fig. 5: Steganography carrier

However, recently many researchers published articles dealing with this issue like (Roy and Venkateswaran, 2013;Shu *et al*., 2011).

Image: The most common technique that is used in steganography is image steganography. Image files spread through the Internet between users makes it perfect to use those files for hiding secret information in addition to the low sensitivity toward Human Visibility System (HVS) and the redundancy of information inside the image file. The hidden process is done by slight alteration of the visible properties of the image file in order to reduce the awareness of the presence of the secret data. The earliest methods that were used in embedding involved using the least-significant bit or LSB, echo hiding and spread spectrum. These techniques can be achieved with disparate degrees of success on different kinds of image files (Hemalatha *et al*., 2013; Thenmozhi and Chandrasekaran, 2012).

Video: Video is generally a combination of audios and images. Therefore, most of image steganography techniques can be applied to video files. A large amount of information can be concealed into the video file and changes might not be observed because of continuous flow of information. This is the main advantage of using video steganography (Bhattacharyya and Sanyal, 2012; Satpute *et al*., 2015).

Audio: Audio steganography approach uses the audio file as a host (cover) file in embedding which is not simple and can be considered as a challenge due to the sensitivity of Human Auditory System (HAS). HAS senses the variation of audio file over a range of power greater than one billion to one and range of frequencies greater than one thousand to one. However, it has holes and a large dynamic range can contribute to data hiding (Bender *et al*., 1996). Audio files make convenient host file for hiding because of its high level of redundancy and high data transmission rate in addition to the large size in comparison with other multimedia files. Several techniques are discussed later.

INFORMATION HIDINGREQUIREMENTS

Various information hiding algorithms were proposed for different purposes and it is necessary to measure the efficiency of them. The efficiency depends on several standards which is called requirements. There is a set of certain and essential requirements have to be fulfilled in most of algorithms. These are transparency, capacity, robustness and complexity of algorithm. The hiding capacity is the most significant characteristic in the steganography followed by the transparency and security while robustness has more important role in watermarking. These are related to each other (Rababah and Abdulgader, 2011). For instance, increasing capacity will diminish the transparency and vice versa. A good steganographic system has to trade-off between these requirements and which is hard to achieve in one algorithm.

Transparency: Most of the data hiding techniques have to insert data as much as possible without affecting the perceptual degradation in quality of the host file. It is one of the most important factors in designing algorithms for hiding data. The fidelity of the steganography algorithm is usually known as a perceptual resemblance between the cover file and stego-cover. However, the differences should be with minimal levels. The evaluation of imperceptibility is usually based on an objective measure of quality or subjective test. Some steganography techniques can be categorized as methods that have high transparency such as that proposed by Ballesteros and Moreno (2012), George and Mahmood (2010) and Shah *et al.* (2008) that produce high quality stego-object.

Capacity: The amount of information that information hiding scheme can successfully hide without introducing any perceptual distortion is the capacity. It represents the number of hidden bits according to the size of host cover. The difficulty lies in the way how to embed secret data as much as possible while preserving the quality of the host cover. It is measured in bits per pixel for images steganography and bits per second for audio steganography. Many algorithms were developed to improve the capacity of cover file such as Divya and Reddy (2012) and Sidhik *et al.* (2013).

Robustness and security: Robustness is defined as how hidden message should not be prone to elimination or modification while Security prevents unauthorized person from extracting the hidden data. There are two kind of attacks that may have effect on the stego-cover: unintentional attack that try to modify or destroy the stego-cover (such as compression, rotation, blurring, noising and other filtering techniques) and intentional attack that try to reveal the stego-cover and extract the hidden information (Al-Othmani *et al.*, 2012).

Usually there is a trade-off between robustness and capacity that can hardly be fulfilled togetherin the same steganographic system. The robustness is an important factor for copyright protection and watermarking applications, while imperceptibility and high hiding capacity is more significant for steganography applications because the goal is to hide as large amount of data with preserving the quality of the cover file. Tecniques proposed by Thenmozhi and Chandrasekaran (2012) and Song *et al.* (2011) can be classified as robust systems.

Complexity: Hiding algorithms consumes time in performing hide/de-hide process and this depends on the complexities of the algorithm. Secret data should be rapidly embedded/extracted into/from the host file, so that streaming data hiding real time can be delivered over the network (Delforouzi and Pooyan, 2009).

INFORMATION HIDINGIN AUDIO

As mentioned in the introduction, many steganography techniques that used different digital files were proposed that used different digital file. This part will present several methods that are used in hiding secret data in audio cover file which fall under temporal domain, frequency and compressed domain that can be briefed as follow:

Temporal domain: LSB is the simplest and earliest approach in temporal domain that is used in hiding the secret information into the Least Significant Bit of the audio samples. However, it has demerits like low robustness and easy to recover. Therefore many researches have proposed algorithms to enhance the LSB technique to overcome these demerits (Table 1).

Kekre *et al.* (2010) proposed two methods Parity and XOR for hiding secret data (image, audio, text) in host audio file with encryption to add level of security. The perceptual quality of the stego signal is high while it should increase the security by using multiple LSB's (Kekre *et al.*, 2010).

New schema for audio steganography is presented by Pathak *et al.* (2014) which is based on diffusing the secret message over host audio. Selection position of secret bit from 0^{th} to 7^{th} LSB in host sample depends on the decimal value of 3 MSB's (Pathak *et al.*, 2014).

Rahim *et al.* (2014) also proposed a technique that hides the secret data in dual bits in the $4^{th}$and 1^{st} LSB and makes modification to the other bits on the same sample. Moreover RohitTanwar 2014 presented a technique that used two bits (3th and 4th) for embedding and intelligent algorithm for altering the bits (2^{th} and 5^{th}) to minimize the difference between stego-sample and original audio file (Tanwar *et al.*, 2014).

Encryption also is used with LSB to enhance the security of the stego file, Khan *et al.* (2011) and Asad *et al.* (2011) used AES (Advanced Encryption Standard) approach to encrypt the secret message. However, there is limitation in Khan *et al.* (2011) algorithm in selecting host file because the sample of

Table 1: Audio steganography

Author	Methodology	Carrier file	Domain	Contribution
Kekre *et al*.(2010)	Parity, XOR with LSB and Encryption	Audio	Temporal domain	High quality
Pathak *et al*.(2014)	Modify LSB	Audio		High quality
Rahim *et al*.(2014)	Modify LSB	Audio		Improve hiding quality
Rohit *et al*.(2014)	Modify LSB with algorithm for minimize error	Audio		Improving robustness and capacity
Khan *et al*.(2011)	LSB with AES (Advanced Encryption Standard) and modulation	Audio		Improve the security
Asad *et al*.(2011)	Enhance LSB, AES (Advanced Encryption Standard)	Audio		Increase robustness and security
Bhowal *et al*.(2013)	Random LSB with Genetic method and RSA encryption	Audio		Ensures the secrecy, robustness and reduce distortion
Santhi and Govindaraju(2014)	RSA and Genetic method	audio		Ensures the secrecy, robustness and reduces the noise distortions
Bandyopadhyay and Banik (2012)	Layer approach LSB and parity coding	Audio		Multi-level for security and complexity in decoding process
Kaur and Verma(2014)	Blended approach LSB, Parity coding and Phase coding	Audio		Multi-level for security and complexity
Pooyan and Delforouzi(2007)	LSB with wavelet transform	Audio	Transform domain	Increase the capacity
Delforouzi and Pooyan, 2008)	LSB and wavelet transform	Audio		Increase the capacity
Shirali-Shahreza and Manzuri-Shalmani, 2008)	LSB with Int2int wavelet transform	Audio-speech		High capacity up to 20% from host cover
George and Mahmood (2010)	Amplitude modulation on wavelet transform	Audio		High quality
Shahadi and Jidin(2011)	Adoptive LSB with Discrete Wavelet Transform (DPWT) and secret key	Audio		High capacity up to 42%, quality and security
Verma *et al*.(2014)	Sample comparison in DWT	Audio		High embedding capacity up to 25% from host file
Dieu and Huy (2014)	Modify amplitude using FFT (Fast Fourier Transform)	Audio		Secure and imperceptible
Gomez-Coronel *et al*. (2014)	Hermit transform	Audio		Increase transparency
Shiu *et al*.(2014)	Analog modulation	Audio		High security
Shie and Jiang(2012)	SMVQ	Image	Compressed domain	High payload and preserve bit rate
Lee *et al*.(2013)	VQ with block neighbor correlation	Image		Secret communication and data compression simultaneously
Chang and Nguyen(2014)	adopts VQ and SMVQ	Image		High capacity and speed, small compression rate and high quality of reconstructed image
Pan *et al*.(2015)	Side-match distortion for sorting the VQ codebook and XOR operation for embedding	Image		Preserving the quality of the reconstructed cover image and increasing the capacity
George and Ahmad(2010)	Fractal coding with moment classifier and LSB	Image		Reduce encoding time about 20% and high hiding capacity
George and Ali(2011)	Fractal coding with block index descriptor	Image		Reduce time complexity to 10 times and high hiding capacity with acceptable stego quality
Mehraj(2011)	DCT and fractal compression	Image		Quality and capacity of stego-image in addition to decrease computational time
Ali *et al*. (2013)	Fractal coding with segmentation and stop threshold	Audio compression		Reduce coding time about 70%
Bedan and George(2013)	Fractal coding with block indexing and moment descriptors			Reducing encoding time good quality of the econstructed audio file.

host message should be eight times larger than the number of secret bits to ensure fully embedding and the weakness in Asad's algorithm quality of sound depends on the size of selected audio and length of the message respectively (Asad *et al*., 2011; Khan *et al*., 2011).

Bhowal *et al*. (2013) and Santhi and Govindaraju (2014) presented genetic algorithm by to overcome the substitution problem of LSB techniques. Multi-level steganography system is another technique proposed by Bandyopadhyay and Banik(2012) and Kaur and

Verma(2014)that use two or three steganography techniques that hide more than one secret message to provide multi-level for security and complexity in decoding process.

Transform domain: The following techniques employ frequency domain in embedding process which produce better result than temporal domain in security and capacity although it has high complexity in computation and un-hiding errors. Several systems utilized Wavelet Transform in embedding processas seenin Table 1.

Pooyan and Delforouzi (2007) and Delforouzi and Pooyan (2008) proposed a novel method for hiding the secret data into LSB of wavelet coefficients of the host signal through using hearing threshold to increase the capacity (Delforouzi and Pooyan, 2008; Pooyan and Delforouzi, 2007).

Hiding in LSB detail wavelet coefficients using int2int wavelet and avoiding in silent parts in the host file are methods that are adopted by Shirali-Shahreza and Manzuri-Shalmani (2008) for speech steganography. However it requires using secret key for selecting the coefficients to maximize the security.

George and Mahmood (2010) proposed embedding process based on applying amplitude modulation techniques on the wavelet transform coefficients of the high energy slices of the host file.

Shahadi and Jidin (2011) proposed adoptive LSB that is used in hiding into Discrete Wavelet Transform (DPWT) with secret key to achieve high capacity up to 42% from the size of cover audio signal, quality and security.

A schema was proposed by Verma *et al.* (2014) that hides any data type message into audio cover based on samples comparison in DWT domain. It presented high embedding capacity up to 25% from the input audio file size (Verma *et al*., 2014).

A new method proposed by Dieu and Huy (2014) that modifies the amplitude of the cover file samples after applying FFT (Fast Fourier Transform) for each of them. It embeds the secret message using a key in hiding process to increase the security (Dieu and Huy, 2014).

Hermit transform proposed by Gomez-Coronel *et al.* (2014) is utilized in hiding audio file into another host audio file. The length of secret information that can be hidden is half of the length of the host file. The audio file concealment is imperceptible to human hearing and value of PSNR is above 30db (Gomez-Coronel *et al*., 2014).

Steganographic approach for hiding secret data into acoustic file based on analog modulation was presented by Shiu *et al.* (2014). It is based on translating secret data into digital form, which is transformed into a high frequency signal. This signal is above the threshold of human audibility. After that, it is integrated with public music signal. This approach has accomplishes high security during transmission and it is tested with many attack approaches like high-pass-filter (HPF), direct current (dc), re-quantization (8-16 bits), echo injection and random noise (Shiu *et al*., 2014).

Compressed domain: In the above two domains, embedding secret data requires large size cover file relatively to the size of secret data and high bandwidth to transmit the cover file,therefore many compression techniques for data hiding have been proposed. The main objective for adopting compression algorithms is to increase the amount of the secret information that is transmitted to specific receiver.Generally, the data hiding adopts compression method in two ways: first hiding data in compress-cover file using VQ (Vector Quantization) and second hidden data into cover file after compress it using FC (Fractal Coding) as shown in Table 1.

VQ is one of the popular compressed methods which were widely used with images. It generates a codebook to classify the secret data and use this codebook in reconstruction of the secret data without using cover file in the receiver side. However, shared codebook is needed in both sender and receiver sides (Linde *et al*., 1980).

Hiding secret data in Side Match Vector Quantization SMVQ compressed cover image used by Shie and Jiang (2012) in order to keep a bit rate with a high payload cover image is an example of this domain (Shie and Jiang, 2012).

Lee *et al.* (2013) proposed embedding technique that the secret data is embedded in VQ-compressed image utilizing from high correlation between neighbouring blocks.It is used to achieve secret communication and data compression simultaneously (Lee *et al*., 2013).

Reversible data hiding method in images was presented by Chang and Nguyen (2014). It adopts VQ and SMVQ compression for embedding using more than 50% of indices of transformed index table. Results show that this method achieved high capacity, small compression rate, high speed in the execution time for embedding/reconstruction and high quality of reconstructed image (Chang and Nguyen, 2014).

Pan *et al.* (2015) also proposed a reversible data hiding technique that hides secret bits into image.It uses side-match distortion to sort the VQ codebook to make the index very close to its neighbour and use the residual value between indexes for hiding that it is obtained from XOR operation. It preserves the quality of the reconstructed cover image and increases the hiding capacity (Pan *et al*., 2015).

FC is another method was used to compress multimedia files. The similarity in different parts of audio is exploited so that each block of the audio file can be represented by set of IFS coding and these sets are used to reconstruct the secret data (Xiao, 2005). These sets are the affine transformation coefficients that are produced from mapping function between cover and secret blocks. These will be hidden in cover and used in reconstruction process in the receive side. It is widely used with images steganography. The main weakness of classical fractal coding scheme is the exhaustive mapping search which is time consuming so many developments were found to reduce the fractal time and increase compression.

George and Ahmad, (2010) proposed image steganography in color images using IFS coding for matching process and moment based classifier for cover and secret image blocks to reduce encoding time about 20% and high hiding capacity (George and Ahmad, 2010).

George and Ali (2011) also proposed image steganography using fractal coding with affine mapping and block index descriptor in selecting best match block to reduce time complexity to 10 times compared with the tradition system without descriptor and high hiding capacity with acceptable stego quality (George and Ali, 2011).

Another technique proposed by Mehraj (2011) used watermarking based on DCT and fractal compression on color image to improve the quality and capacity of stego-image in addition to decrease computational time. Earlier there are many attempts to speed up fractal compression during several trends (Mehraj, 2011).

Ali *et al*. (2013) introduced an approach that divide the data into segments then applying fractal coding on each segment separately and using stopping threshold in order to reduce coding time for fractal compression about 70% (Ali *et al*., 2013).

In addition block indexing and moment descriptor in selection strategy instead of tradition search and filtering the cover blocks was another method proposed by Bedan and George (2013) for reduction in the encoding time good quality of the reconstructed audio file.

CONCLUSION

Audio steganography plays a vital role in transmitting secret and important information from the sender to the authorized receiver. The secret information is embedded slightly into host audio through changing the host file directly or transform it into another form in order to achieve optimum capacity and robustness. Several approaches are presented for hiding audio data signals and each of them has achieved a degree of success from a point view of steganography requirements. The techniques that were proposed in temporal domain provide easy and simple way to hide, although they are unable to tolerate the noise, less robust and few techniques have been developed at present. Frequency domain in embedding algorithm has given better result in signal processing, robustness and security. Techniquesthat adopt two different domains to utilize from the poses of these domains are continuously developing andthey accomplish perfect steganography techniques. On the other hand, compressed techniquesare also adopted by several researchers to increase the data to be hidden and develop algorithm that can be utilized in real time data hiding. Finally, steganography requirements are the dependable factors of decision making in selecting technique and the domain.

REFERENCES

Al-Othmani, A.Z., A.A. Manaf and A.M. Zeki, 2012. A survey on steganography techniques in real time audio signals and evaluation. Int. J. Comput. Sci., 9(1).

Ali, S., L.E. George and H.Baker, 2013. Speeding up audio fractal compression. Int. J. Adv. Res. Comput. Sci. Softw. Eng., 3(6): 86-92.

Antony, J., C. Sobin and A. Sherly, 2012. Audio steganography in wavelet domain-a survey. Int. J. Comput. Appl., 52: 33-37.

Asad, M., J. Gilani and A. Khalid, 2011. An enhanced least significant bit modification technique for audio steganography. Proceeding of the 2011 International Conference on Computer Networks and Information Technology (ICCNIT, 2011), pp: 143-147.

Ballesteros, L.D.M. and A.J.M. Moreno, 2012. Highly transparent steganography model of speech signals using efficient wavelet masking. Expert Syst. Appl., 39(10): 9141-9149.

Bandyopadhyay, S.K. and B.G. Banik, 2012. Multi-level steganographic algorithm for audio steganography using LSB modification and parity encoding technique. Int. J.Emerg. Trends Technol. Comput. Sci. (IJETTCS), 1(2).

Bandyopadhyay, S.K., D. Bhattacharyya, D. Ganguly, S. Mukherjee and P. Das, 2008. A tutorial review on steganography. Proceeding of the International Conference on Contemporary Computing.

Bedan, A.K. and L.E. George, 2013. Speeding-up fractal audio compression using moment descriptors. Int. J. Sci. Eng. Res., 4(7).

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35(3.4): 313-336.

Bhattacharyya, S. and G. Sanyal, 2012. A novel approach of video steganography using PMM. In: Venugopal, K.R. and L.M. Patnaik (Eds.), ICIP, 2012. CCIS 292, Springer-Verlag, Berlin, Heidelberg, pp: 644-653.

Bhowal, K., D. Bhattacharyya, A.J. Pal and T.H. Kim, 2013. A GA based audio steganography with enhanced security. Telecommun. Syst., 52(4): 2197-2204.

Chang, C.C. and T.S. Nguyen, 2014. A reversible data hiding scheme for smvq indices. Informatica, 25(4): 523-540.

Cvejic, N., 2004. Algorithms for audio watermarking and steganography. Unpublished Ph.D. Thesis, University of Oulun, Finland.

Delforouzi, A. and M. Pooyan, 2008. Adaptive digital audio steganography based on integer wavelet transform. Circ. Syst. Signal Pr., 27(2): 247-259.

Delforouzi, A. and M. Pooyan, 2009. Adaptive and efficient audio datahiding method in temporal domain. Proceeding of the 7th International Conference on Information, Communications and Signal Processing (ICICS, 2009).

Dieu, H.B. and N.X. Huy, 2014. An improved technique for hiding data in audio. Proceeding of the 4th International Conference on Digital Information and Communication Technology and it's Applications (DICTAP, 2014).

Divya, S. and M.R.M. Reddy, 2012. Hiding text in audio using multiple LSB steganography and provide security using cryptography. Int. J. Sci. Technol. Res., 1(6).

George, L.E. and G.A. Mahmood, 2010. Audio steganography based on signal modulation in wavelet domain. Iraqi J. Sci., 9: 10.

George, L.E. and S.K. Ahmad, 2010. Hiding image in image using Iterated Function System (IFS). Proceeding of the European Conference of Systems, and European Conference of Circuits Technology and Devices, and European Conference of Communications, and European Conference on Computer Science.

George, L.E. and A.H. Ali, 2011. Fast Image Steganography Using Affine Mapping.

Gomez-Coronel, S.L., B. Escalante-Ramırez, M.A. Acevedo-Mosqueda and M.E. Acevedo, 2014. Steganography in audio files by hermite transform. Appl. Math, 8(3): 959-966.

Hemalatha, S., U.D. Acharya, A. Renuka and P.R. Kamath, 2013. A secure and high capacity image steganography technique. Signal Image Process. Int. J. (SIPIJ), 4: 83-89.

Kaur, K. and D. Verma, 2014. Multi-level steganographic algorithm for audio steganography using LSB, parity coding and phase coding technique. Int. J. Adv. Res. Comput. Sci. Software Eng., 4(1).

Kekre, H., A. Athawale, S. Rao and U. Athawale, 2010. Information hiding in audio signals. Int. J. Comput. Appl., 7(9): 14-19.

Khan, M.S., M.V. Bhaskar and M.S. Nagaraju, 2011. An optimized method for concealing data using audio steganography. Int. J. Comput. Appl., 33(4): 25-30, (0975-8887).

Lee, J.D., Y.H. Chiou and J.M. Guo, 2013. Lossless data hiding for VQ indices based on neighboring correlation. Inform. Sciences, 221: 419-438.

Linde, Y., A. Buzo and R.M. Gray, 1980. An algorithm for vector quantizer design. IEEE T. Commun., 28(1): 84-95.

Mehraj, M.M.B., 2011. Watermarking UsingDCT & Fractal Compression. Int. J. Comput. Trend. Technol., 1(2)

Nosrati, M., R. Karimi and M. Hariri, 2012. Audio steganography: A survey on recent approaches. World Appl. Programm., 2(3): 202-205.

Pan, Z., S. Hu, X. Ma and L. Wang, 2015. A new lossless data hiding method based on joint neighboring coding. J. Vis. Commun. Image R., 26: 14-23.

Pathak, P., A.K. Chattopadhyay and A. Nag, 2014. A new audio steganography scheme based on location selection with enhanced security. Proceeding of the 1st International Conference on Automation, Control, Energy and Systems (ACES, 2014).

Pooyan, M. and A. Delforouzi, 2007. LSB-based audio steganography method based on lifting wavelet transform. Proceeding of the IEEE International Symposium on Signal Processing and Information Technology.

Rababah, A. and U. Abdulgader, 2011. New technique for hiding data in audio file. Int. J. Comput. Sci. Network Secur., 11(4).

Rahim, L.B.A., S. Bhattacharjee and I.B. Aziz, 2014. An audio steganography technique to maximize data hiding capacity along with least modification of host. Proceeding of the 1st International Conference on Advanced Data and Information Engineering (DaEng-2013).

Roy, S. and P. Venkateswaran, 2013. A text based steganography technique with Indian root. Proc. Technol., 10: 167-171.

Santhi, V. and L. Govindaraju, 2014. Stego-audio Using Genetic Algorithm Approach. Res. J. Appl. Sci. Eng. Technol., 7(22): 4806-4812.

Satpute, S., S. Shahane, S. Singh and M. Sharma, 2015. An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding).

Shah, P., P. Choudhari and S.Sivaraman, 2008. Adaptive wavelet packet based audio steganography using data history. Proceeding of the IEEE Region 10 and the 3rd International Conference on Industrial and Information Systems (ICIIS, 2008), pp: 1-5.

Shahadi, H.I. and R. Jidin, 2011. High capacity and inaudibility audio steganography scheme. Proceeding of the 7th International Conference on Information Assurance and Security (IAS, 2011).

Shie, S.C. and J.H. Jiang, 2012. Reversible and high-payload image steganographic scheme based on side-match vector quantization. Signal Process., 92(9): 2332-2338.

Shirali-Shahreza, S. and M. Manzuri-Shalmani, 2008. High capacity error free wavelet domain speech steganography. Proceeding of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP, 2008).

Shiu, H., S. Tang, C.H. Huang, R.C. Lee and C. Lei, 2014. A reversible acoustic data hiding method based on analog modulation. Inform. Sciences, 273: 233-246.

Shu, Y., L. Liu, W. Tian and X. Miao, 2011. Algorithm for information hiding in optional multi-text. Proc. Eng., 15: 3936-3941.

Sidhik, S., S. Sudheer and V. Mahadhevan Pillsai, 2013. Modified high capacity steganography for color images using wavelet fusion. Proceeding of the 4th International Workshop on Fiber Optics in Access Network (FOAN, 2013).

Singh, K.U., 2014. A survey on audio steganography approaches. Int. J. Comput. Appl., 95(14): 7-14.

Song, S., J. Zhang, X. Liao, J. Du and Q. Wen, 2011. A novel secure communication protocol combining steganography and cryptography. Proc. Eng., 15: 2767-2772.

Tanwar, R., B. Sharma and S. Malhotra, 2014. A robust substitution technique to implement audio steganography. Proceeding of the International Conference on Optimization, Reliabilty, and Information Technology (ICROIT, 2014), pp: 290-293

Thenmozhi, S. and M. Chandrasekaran, 2012. Novel approach for image stenography based on integer wavelet transform. Proceeding of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC, 2012), pp: 1-5.

Verma, S.S., R. Gupta and G. Shrivastava, 2014. A novel technique for data hiding in audio carrier by using sample comparison in DWT domain. Proceeding of the 4th International Conference on Communication Systems and Network Technologies (CSNT, 2014), pp: 639-643.

Xiao, H., 2005. Fractal audio coding. M.A. Thesis, Queen's University, Canada,7: 20-25.