We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter 5

Multilevel Steganography to Improve Secret Communication

Krishna Bhowal

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.81599

Abstract

This chapter presents multilevel audio steganography, which describes a new model for hidden communication in secret communication technology. At least two embedding methods are used in such a way that the second method will use the first method as a carrier. The proposed method has several potential benefits in hidden communication. This method can be used to increase the level of security while transmitting the confidential information over public channels or internet and also can be used to provide two or more information hiding solutions simultaneously. The performance of the proposed method in terms of imperceptibility, capacity & security is measured through different experiments.

Keywords: audio steganography, multilevel steganography, secret communication, information security, imperceptibility, embedding capacity, discrete wavelet transform

1. Introduction

This chapter depicts multilevel audio steganography, which presents a new model for hidden communication. In multilevel steganography, at least two embedding methods are used in such a way that the second method may use the first method as a carrier. This approach has several potential benefits in hidden communication. It can be used to increase the level of security while transmitting the confidential information over public channels. It can also be used to provide two or more information hiding solutions simultaneously. Another important benefit is that the lower level embedding/extracting method and higher level embedding/extracting method are interrelated in terms of functionality and this makes the hidden communication

harder to detect. If the cover object is interpreted by any adversary, only a decoy message or a partial message will be obtained.

The main aim of steganography is to hide secret information in digital cover. The alteration of the cover caused by embedding secret information remains invisible to the third party opponents. This is possible by designing an appropriate embedding algorithm and choosing a suitable cover. Therefore, there will be no significant dissimilarity between original cover and embedded cover. So, secret information not only is hidden inside the cover, but the fact of the secret information communication is also hidden. Each steganographic method may be characterized by following requirements. First, undetectability which is defined as the inability of detecting secret information inside the embedded cover. Actually, the distortion of the embedded cover convinces the opponent to analyze the statistical properties of the cover and compare them to the distinguishing properties of that cover. Therefore, imperceptibility or inaudibility is directly relational to the undetectability. Second, embedding capacity is defined as an amount of secret information which can be transmitted using a particular algorithm per unit of time. Third, steganographic cost, which defines the amount of alteration of the cover caused due to the secret information embedding method. The steganographic cost depends on the cover used as a carrier and also depends on embedding algorithm used.

For each steganographic method, there is always a trade-off between maximizing hiding capacity and remaining secret information undetected. Therefore, a certain level of tuning between embedding capacity and undetectability is required. If the embedding and extracting algorithm remains secret to the opponent, it can be used to transmit secret information freely. On the other hand, if the both algorithms are known to the opponent, anybody may be able to extract the secret information. This type of problem may be resolved by using the different encryption algorithms appropriate for a particular application. The encryption algorithm AES may be used to encrypt secret information before embedding it to the cover. Therefore, in this case, extracted information will not be readable by the opponent. There is a problem with this method, because the encryption key and the encrypted information are communicated using the same embedding technique. Thus, the encryption key and the secret information both will be revealed on successful detection. Alternatively, embedding capacity may be reduced due to embedding of the encryption key in cover object. The multilevel steganography was originally proposed by Al-Najjar for image steganography in [1]. The main idea in this paper was to hide a decoy image into LSB positions of the cover and the original secret information is embedded into the LSB positions of the decoy image.

Encryption and steganography are two general methods for hiding secret information [2–4]. Information is hidden using an encoding method that only authorized persons with the proper key can decode it in encryption. On the other hand, steganography hides secret information such a way that hidden information is imperceptible to the regular observer. The secret information can be embedded directly or some transformation can be applied to it before the embedding process. Generally, transformations include encryption, compression, transformation or a combination of digital transformation techniques. In [4], Vitaliev proposed two methods of information hiding. In the first method, plain text is hidden into an audio signal and in the second method; an audio file is hidden in an image object. In [5], Petitcolas et al. presented a method where a text object is hidden into another text object. In [6], Al-Najjar et al.

proposed a method where an audio file is embedded in an image after performing encryption and compression. In [7], Marvel proposed a hidden communication method by hiding of an image into another image in his Ph.D. Dissertation. In [8], Solanki presented a multimedia data hiding technique to hide an image into a video file in his Ph.D. Dissertation.

In [9], Lou et al. proposed an information hiding technique to protect a medical information. This paper suggests a multiple-layer data hiding technique in spatial domain. The reduced difference expansion method is utilized to embed the bit stream in the least significant bits (LSBs) of the expanded differences. A large amount of data is embedded in a medical image by using this method where quality of the image is also be maintained. Moreover, the original image can be restored after extracting the hidden data from the stego-image.

Cocktail party effect is used in audio steganography system where blind key concept is applied to resist the attack in the system [10]. Private key on the domain of cosine discrete transform (CDT) is used in steganographic algorithm in [11]. A new quantization technique is used in a steganographic method and the algorithm is designed based on DCT in [12]. A DNA structural concept is utilized in audio steganography in [13]. A novel audio steganography is designed using ZDT in [14]. Here encryption is done using indexed based chaotic sequence.

In this chapter, multilevel audio steganography is discussed to address the above stated problems. The proposed approach extends the concept of steganography to use it in more general purpose.

2. Improved secret communication using multilevel audio steganography

Multilevel steganography can be categorized as per the requirement of its application. Embedding capacity is the basic requirement in some of the applications where imperceptibility may be compromised in a certain level. On the other hand, imperceptibility is the main requirement in some of the applications where embedding capacity may be compromised in a certain level. So, the multilevel steganography may be classified as like below:

(i) Single message multiple covers—multilevel steganography denoted as **TYPE-I**

A message is embedded in multiple covers using several embedding functions to increase the level of security of the system. This approach provides better imperceptibility, but embedding capacity may be compromised in most of the cases.

(ii) Single cover multiple messages—multilevel steganography denoted as **TYPE-II**

Multiple messages are embedded in a single digital cover using several related embedding functions to increase the embedding capacity of the system. This approach provides better embedding capacity, but imperceptibility may be compromised in most of the cases.

2.1. Methodology

In this section, TYPE-I and TYPE-II types of multilevel steganography models are discussed [15].

2.1.1. Single message multiple covers—multilevel steganography model (TYPE-I)

Suppose, the Message is denoted as M, the Covers are denoted as C_i, the Intermediate Covers or stego-covers are denoted as I_i. Here, the value of i depends on the level of steganography, to be performed.

The message M is passed through the transformation T_i. The transformations may include compression, encryption or a transforms like Discrete Cosine Transform (DCT), Fourier Transform (FT) or Discrete Wavelet Transform (DWT), etc. Sometimes a combination of techniques may be used as required by the particular application.

Message embedding and extracting operations are performed by the embedding and extracting function pairs embed() and extract() and denoted by f and f' respectively. The message embedding function may vary to improve the steganography attributes like imperceptibility, capacity, and robustness.

$T_i = I$ means no transformation is applied. In the blind system, hidden information is extracted without using cover C_i at the receiving end.

The TYPE-I multilevel steganography model (for i = 3) is presented in **Figures 1** and **2**.

At the sender end, in phase 1, secret message M is embedded in cover object C_1 using transformation T_1 and embedding function f_1 and stego-object I_1 is generated. In the next phase, stego-object I_1 is hidden in another new cover object C_2 using transformation T_2 and

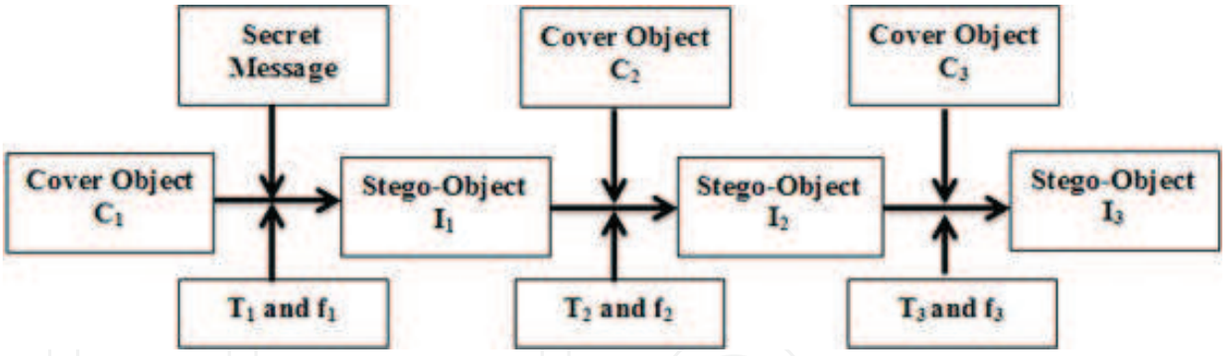

Figure 1. TYPE-I multilevel steganography model at the sender end for level = 3.

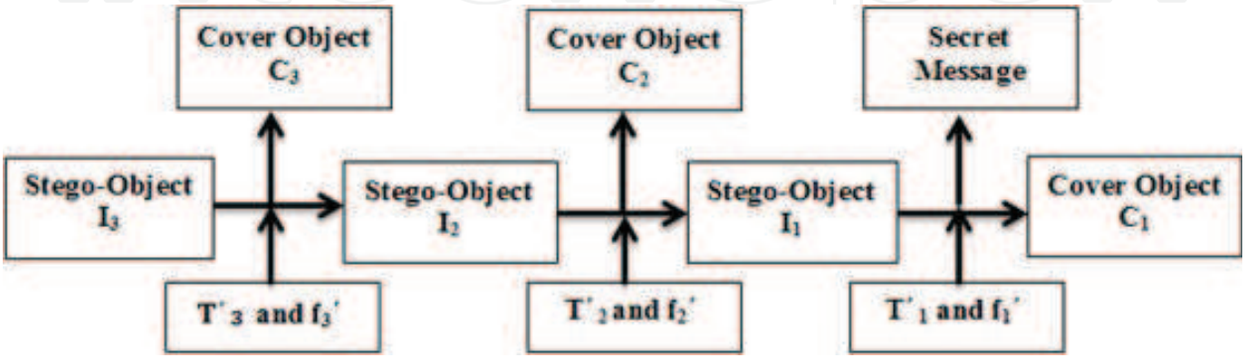

Figure 2. TYPE-I multilevel steganography model at the receiver end for level = 3.

embedding function f_2 and stego-object I_2 is generated. This process is continued as per the requirement of the application. There are three levels of embedding process is shown in **Figure 1**.

At the receiver end, according to the above 2 level embedding process, in phase 1, stego-object I_1 is generated from stego-object I_2 and applying T_2' transformation and f_2' embedding function. In the next phase, secret message M is generated from stego-object I_1 by applying T_1' transformation and f_1' embedding function. There are three level of extraction process shown in **Figure 2**.

Example of TYPE-I: 2 level steganography

Secret message embedding process:

Level-1: for i = 1

The cover is a grayscale image (C_1) and Message is a text message (M). Here, transmission T_1 is an encryption process, i.e., the secret message is encrypted using some standard encryption algorithm. The encrypted secret message bits are embedded at the 2nd LSB position of each pixel value of the cover image. The embedding function f_1 is defined as $f_1(\text{mbit}) = C_1.\text{LSB}(2)$ and f_1 is used to generate Intermediate cover or stego-cover I_1.

Leve-2: for i = 2

In this step, the cover is an audio signal (C_2) and Intermediate Cover or stego-cover is I_1. I_1 is generated in the previous step and it is an embedded image. The image is converted to a bit stream and each bit is embedded at the 1st LSB position of each audio sample of the audio signal. Here, transformation $T_2 = I$ and the embedding function f_2 is defined as $f_2(\text{ibit}) = C_2.\text{LSB}(1)$ and f_2 is used to generate intermediate cover or stego-cover I_2.

Secret message extraction process:

Level-2: for i = 2

The Intermediate Cover (I_2) is an embedded audio signal and the embedded image bits are extracted from the 1st LSB position of each audio sample. Here, transformation $T_2' = I$ and the extracting function f_2' is defined as $f_2'(\text{ibit}) = I_2.\text{LSB}(1)$ and $f_2'$is used to generate intermediate cover or stego-cover I_1.

Level-1: for i = 1

The Intermediate Cover (I_1) is an embedded image and the message bits are extracted from the 2nd LSB position of each pixel value of the embedded image. Here, transmission $T_1'$is a decryption process of the corresponding encryption algorithm used during embedding process. The extraction function $f_1'$is defined as $f_1'(\text{mbit}) = I_1.\text{LSB}(2)$ and $f_1'$is used to generate secret message M.

2.1.2. Single cover multiple messages—multilevel steganography model (TYPE-II)

Suppose, the Cover is denoted as C, the Messages are denoted as M_i, the Intermediate Covers or stego-covers are denoted as I_i. Here, the value of i depends on the level of steganography, to be performed.

The messages M_i are passed through the transformation T_i like previous section. The TYPE-II multilevel steganography model (for i = 3) is presented in **Figures 3** and **4**. At the sender end, in phase 1, secret message M_1 is embedded in a cover object C using transformation T_1 and embedding function f_1 and stego-object I_1 is generated. In the next phase, another message M_2 is hidden in stego-object I_1 using transformation T_2 and embedding function f_2 and stego-object I_2 is generated. This process is continued as per the requirement of the application. There are three level of embedding process as shown in **Figure 3**.

At the receiver end, according to the above 2 level embedding process, in phase 1, message M_2 is generated from stego-object I_2 by applying T'_2transformation and f'_2 embedding function. In the next phase, secret message M_1 is generated from stego-object I_1 by applying T'_1 transformation and f'_1 embedding function. There are three level of extraction process shown in **Figure 4**.

Example of TYPE-II: 2 level steganography

Secret message embedding process:

Level-1: for i = 1

The cover is an audio clip (C) and the two secret messages are M_1 and M_2. Here, transmission T_1 is Discrete Wavelet Transform (DWT) and Inverse DWT (IDWT) of the audio signal. The M_1 message bits are embedded at the 2nd LSB position of each DWT coefficient of the audio signal. The embedding function f_1 is defined as $f_1(\text{mbit}) = \text{C.LSB}(2)$ and f_1 and IDWT are used to generate Intermediate cover or stego-cover I_1.

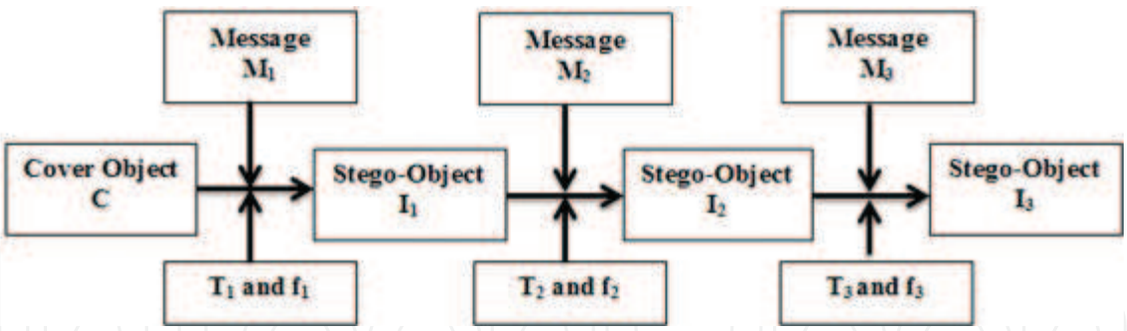

Figure 3. TYPE-II multilevel steganography model at the sender end for level = 3.

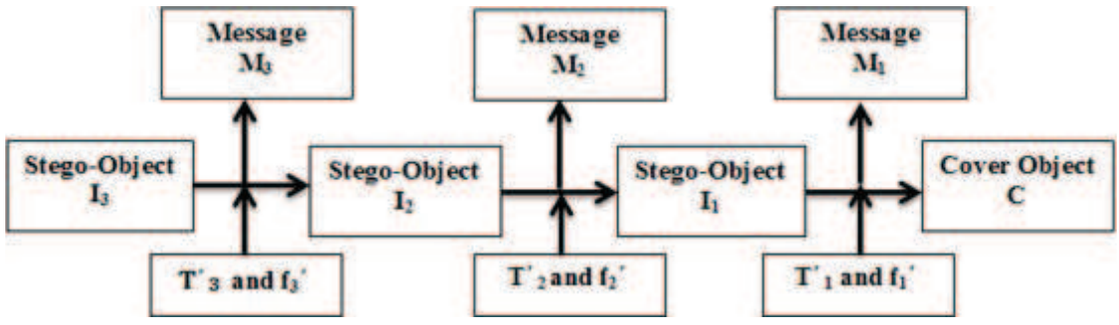

Figure 4. TYPE-II multilevel steganography model at the receiver end for level = 3.

Level-2: for i = 2

In this step, the cover is an Intermediate Cover or stego-cover (I_1). I_1 is generated in the previous step and it is an embedded audio signal. The M_2 message bits are embedded at the 1st LSB position of each audio sample of the audio signal. Here, transformation $T_2 = I$ and the embedding function f_2 is defined as $f_2(\text{mbit}) = C.LSB(1)$ and f_2 is used to generate Intermediate cover or stego-cover I_2.

Secret message extracting process:

Level-2: for i = 2

The Intermediate Cover (I_2) is an embedded audio signal and the M_2 message bits are extracted from the 1st LSB position of each audio sample. Here, transformation $T_2' = I$ and the extracting function f_2' is defined as $f_2'(\text{abit}) = I_2.LSB(1)$ and $f_2'$is used to generate Intermediate cover or stego-cover I_1.

Level-1: for i = 1

The Intermediate Cover (I_1) is an embedded audio and the message bits are extracted from the 2nd LSB position of each DWT coefficient of the embedded audio signal. Here, transmission $T_1'$is DWT and IDWT of the embedded audio signal. The extraction function $f_1'$is defined as $f_1'(\text{abit}) = I_1.LSB(2)$and $f_1'$is used to generate secret message M_1.

3. Experimental result and discussion

Proposed algorithm has been tested on 10 audio sequences from different music styles (classic, jazz, country, pop, rock, etc.). All the Clips are 44.1 kHz sampled mono audio files, represented by 16 bits per sample, and length of the clips ranges from 10 to 20 seconds. An image and the all audio clips are used to test TYPE-I type of algorithm and all the audio clips are used to test TYPE-II algorithm.

3.1. Imperceptibility test

Basic requirement is the imperceptibility in most of the applications, i.e., after hiding secret messages in audio signals; the quality of the embedded audio signals should remain same as original audio signals. Here, Subjective Difference Grade (SDG), Objective Difference Grade (ODG) and Signal-to-Noise Ratio (SNR) is used to measure the imperceptibility of the proposed method. The SDG and ODG listening tests use the 5-grade scale shown in **Table 1**.

3.1.1. Objective quality measurements

The ODG measurements of different audio clips are provided using the advanced ITU-R BS.1387 standard [16] and are calculated using the Opera software [17] which is implemented by maintaining ITU-R BS.1387 standard. ODG values for TYPE-I and TYPE-II approaches are reported in **Tables 2** and **3** and respectively for different types of audio signals. The ODG

Audio standard	Subjective difference grade (SDG)	Objective difference grade (ODG)
Indistinguishable	5	0.0
Distinguishable, but not aggravating	4	−1.0
Slightly aggravating	3	−2.0
Aggravating	2	−3.0
Very aggravating	1	−4.0

Table 1. Subjective and objective grades for audio quality measurement.

Audio types	Objective difference grade (ODG)	Subjective difference grade (SDG)	Signal-to-noise ratio (SNR (dB))
A1	−0.51	5.0	92.25
A2	−0.63	4.9	91.41
A3	−0.61	4.9	91.63
A4	−0.52	5.0	92.43
A5	−0.49	5.0	92.54
A6	−0.50	5.0	92.35
A7	−0.64	4.9	91.55
A8	−0.59	4.9	91.57
A9	−0.49	5.0	92.36
A10	−0.53	4.9	91.78

Table 2. ODG, SDG & SNR values for different audio clips (TYPE-I, level = 2).

Audio types	Objective difference grade (ODG)	Subjective difference grade (SDG)	Signal-to-noise ratio (SNR (dB))
A1	−0.61	4.9	90.15
A2	−0.72	4.8	89.31
A3	−0.70	4.8	88.93
A4	−0.61	4.9	90.41
A5	−0.59	4.9	90.22
A6	−0.60	4.9	90.16
A7	−0.68	4.8	89.25
A8	−0.69	4.8	89.36
A9	−0.58	4.9	90.19
A10	−0.63	4.8	89.14

Table 3. ODG, SDG & SNR values for different audio clips (TYPE-II, level = 2).

values for TYPE-I model are −0.49 to −0.64 and the ODG values for TYPE-II model are −0.58 to −0.72.

3.1.2. Subjective quality evaluation

Subjective quality measurements [18, 19] have been performed to evaluate the imperceptibility of our proposed data hiding scheme. The output of the subjective tests is an average of the quality ratings called a Mean Opinion Score (MOS). SDG values for TYPE-I and TYPE-II approaches are reported in **Tables 2** and **3** respectively for different types of audio signals. The SDG values for TYPE-I model are 4.9–5.0 and the SDG values for TYPE-II model are 4.8–4.9.

3.1.3. Signal-to-noise ratio (SNR) measurement

The signal-to-noise ratio (SNR) value is used to make the difference between the original and embedded audio signal [20]. Normally, if the SNR value is higher than 50 dB, then the secret data which are hidden in the audio signal are imperceptible to the human auditory system. The SNR values for TYPE-I and TYPE-II approaches are measured using equation no. (1) and are reported in **Tables 2** and **3** respectively for different types of audio signals.

$$\text{SNR} = 10\ \log_{10} \frac{\sum_{i=1}^{N} x^2(i)}{\sum_{i=1}^{N} \left(x(i) - y(i)\right)^2} \tag{1}$$

The ODG, SDG, and SNR values are evaluated for different audio signals. Here, 2 level multi-level steganography is performed for TYPE-I and TYPE-II models. The results are presented in **Tables 2** and **3** of TYPE-I and TYPE-II models respectively. For simplicity, 10 audio clips are denoted as A1, A2, A3, A4, A5, A6, A7, A8, A9 and A10.

3.2. Embedding capacity analysis

One of the basic requirements of the secret communication using steganography is increasing the embedding capacity by keeping the imperceptibility in a desired level. In the proposed system, if TYPE-I approach is followed, embedding capacity is not so much desired level, because imperceptibility given higher priority. But, if TYPE-II approach is followed, multiple messages may be embedded in a single cover object by designing appropriate transforms and embedding functions.

The embedding capacity is measured by the number of bits that can be hidden into the audio signal per unit of time. Suppose, D is the duration of the original audio clip in seconds and B is the number of secret information bits. Now, the capacity is measured as:

$$\text{Capacity} = B/D \text{ bps} \tag{2}$$

In this work, the frequency of the carrier signal is fixed, i.e., 44.1 Kz is considered. The sample rate 44.1 kHz means 44,100 samples per second in one channel.

3.3. Security analysis

Security is another very important requirement of hidden communication using steganography. A data hiding method is said to be secured if an adversary would not be able to detect or modify or remove the hidden information in the embedded object. To measure the security of the proposed technique, following scenarios may be considered:

a. The adversary has no information about the hidden information in the host object. So, the proposed method is secure.

b. The adversary has no idea about the embedding or extracting algorithm. Therefore, the proposed method is secure.

c. The adversary has information only about the embedding and extracting algorithm. In this case, the adversary cannot precede the extraction operation without knowing the actual location is used to hide information.

By minimizing the bit flipping during the embedding process is normally guaranteed that the algorithm designed to estimate the hidden data based on statistical analysis may be effectively disabled.

In TYPE-I approach, a message is hidden in a cover object and that stego-cover object is hidden in another cover object, and so on. This approach increases the level of security of the system. Again, the number of levels is used during the embedding process in multilevel steganography is very important information at the receiving end. That means, security may be increased by varying the number of levels during embedding process. Along with this, any of the encryption algorithms may be used at a transformation phase of the system to increase the security of the system.

3.4. Comparative study

In this section, a comparative study is performed with the very recent works on audio steganography as well as audio watermarking proposed by different authors. Actually, impartial comparison is very difficult, because every approach have its own characteristics and also designed to fulfill certain basic requirement. Anyway, most of the algorithm has some common characteristics like embedding capacity, imperceptibility etc. Here, comparisons are performed based on embedding capacity and imperceptibility (SNR & ODG) of the system and reported in **Table 4**.

The method in [21] provides a significant performance in the different properties of the data embedding technique. The method offers moderate data hiding capacity solutions for data hiding in audio file even though the imperceptibility in terms of SNR and ODG is below average in some of the issues. The important achievement of this scheme is robustness against different attacks such as echo, filtering, and noise added. The method in [23] achieves a low embedding capacity for the three audio files considered. The imperceptibility in terms of SNR is below average, but the imperceptibility (ODG) is moderate in this scheme. This scheme has a good performance against compression and the maximum of BER against this is about 1%. The

Algorithm	Capacity (bps)	SNR (dB)	ODG
Xiang et al. [21]	2	42.8–44.4	$-1.66 < ODG < -1.88$
Mansour et al. [22]	4.3	29.5	Not reported
Fallahpour et al. [23]	3 k	30.55	−0.6
Fallahpour et al. [24]	2–6 k	Not reported	$-0.6 < ODG < -1.7$
Fallahpour et al. [25]	11 k	30	−0.7
Kang et al. [26]	64	30–45	$-1 < ODG$
Nishimura et al. [27]	8	Not reported	$-3 < ODG < -1$
Proposed	44,100	92.54	$-0.49 < ODG < -0.64$

Table 4. Comparative studies among different works.

algorithms in [24, 25] offer low embedding capacity, good transparency, and reasonably robustness against selected attacks. The scheme in [24] provides very a low data hiding rate, high distortion, and very robust scheme, while that in [25] provides very low embedding capacity, highly distorted signals (SNR is 30 dB), and moderate robustness against some attacks.

The most important achievement of the proposed method is better imperceptibility in terms of SNR and ODG with higher embedding capacity. The comparison presented in **Table 4** demonstrates the superiority in both capacity and imperceptibility of the proposed method with respect to the schemes discussed in the literature. The proposed method can hide much more information by introducing less distortion in the audio file. In brief, the proposed method achieves higher embedding capacity if we compare it to methods with similar imperceptibility.

The data presented in **Table 4** confirms that the proposed method have better performance in terms of embedding capacity and imperceptibility.

4. Conclusion

In this chapter, two multilevel steganography models are proposed. Normally, the requirement of data hiding application varies from application to application. The proposed models are designed such a way that the customization may be done as per the requirement of a particular application. That means, number of embedding and extracting levels, number of messages to be hidden, and number of cover objects to be used etc. are customizable. The suggested model enhances the security level of the steganography technique in terms of imperceptibility as well as capacity. The stego-object, usually does not seem suspicious, since it looks similar to the original object to the general observer. An adversary may be satisfied with the decoy as the hidden message and may not use additional tools to look further. The authorized receivers have information about the hidden message, as well as the information required to extract the message. Hence, it can be concluded that the proposed models enhanced potentially more security to information hiding.

Acknowledgements

First and most of all, I thank God, the almighty for giving me this opportunity and granting me the ability to carry on the process successfully.

I take this opportunity to show my gratitude to all my teachers, starting from my school days to this day, who have guided me throughout my pursuit for knowledge, who have given me the opportunity to express my thoughts, who gave patient listening to my ideas even though many a time it was unreasonable. This book chapter looks like in its current form due to the guidance and support of several people. I am especially grateful to my supervisor Dr. Debasree Chanda (Sarkar), for her warm encouragement, critical comments, and thoughtful guidance. I also owe thanks to Dr. Partha Pratim Sarkar, Professor, for his insightful discussion, offering valuable advice, encouraging comments, and suggestions throughout this work. Despite his extremely busy schedule, he has gone through the thesis in depth.

Lastly but not the least, I acknowledge the Academy of Technology, Hooghly, Kolkata, India.

Conflict of interest

Replace the entirety of this text with the 'conflict of interest' declaration.

Author details

Krishna Bhowal

Address all correspondence to: ykbhowal@yahoo.co.in

Department of MCA, Academy of Technology, Kolkata, India

References

[1] Al-Najjar J. The decoy: Multi-level digital multimedia steganography model. In: Proc. of 12th WSEAS International Conference on Communications, Heraklion, Greece, July. 2008. pp. 23-25

[2] Anderson RJ, Petitcolas FAP. On the limits of the steganography. IEEE Journal of Selected Areas in Communications. 1998;**16**(4):474-481

[3] Artz D. Digital steganography: Hiding data within data. IEEE Internet Computing Archive. 2001;**5**(3):75-80

[4] Vitaliev D. Digital Security and Privacy for Human Rights Defenders. Dublin: The International Foundation for Human Right Defenders; 2007. pp. 77-81

[5] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding–A survey. Proceedings of the IEEE, Special Issue on Protection of Multimedia Content. 1999;**87**:1062-1078

[6] Al-Najjar AJ, Alvi AK, Idrees SU, Al-Manea AM. Hiding Encrypted Speech Using Steganography. China, Sept. 15–17: WSEAS Beijing; 2007. pp. 275-281

[7] Marvel LM. Image steganography for hidden communication", Ph.D. Dissertation. University of Delaware, spring; 1999

[8] Solanki M. Multimedia Data Hiding: From Fundamental Issues to Practical Techniques", Ph.D. Dissertation. Santa Barbara, US: University of California; 2005

[9] Lou DC, Hu MC, Liu JL. Multiple layer data hiding scheme for medical images. Computer Standards and Interfaces. 2009;**31**(2):329-335

[10] Gupta Banik B, Bandyopadhyay SK. Blind key based attack resistant audio steganography using cocktail party effect. Security and Communication Networks. 2018;**2018**(1781384): 1-21

[11] Lorente AS, Cumbrera R, Fonseca Y. Steganographic algorithm of private key on the domain of the cosine discrete transform. Revista Cubana de Ciencias Informáticas. 2016; **10**(2):116-131

[12] Amin M, Abdullkader HM, Ibrahem HM, Sakr AS. A steganographic method based on DCT and new quantization technique. International Journal of Network Security. 2014; **16**(4):265-270

[13] Tank RM, Vasava HD, Agrawal V. DNA-based audio steganography. Oriental Journal of Computer Science and Technology. 2015;**8**(1):43-48

[14] Sharma S, Yadav VK, Trivedi MC, Gupta A. Audio steganography using ZDT: Encryption using indexed based chaotic sequence. In: ICTCS '16 Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Article No. 66 , Udaipur, India — March 04–05, 2016

[15] Bhowal K, Chanda(Sarkar) D, Biswas S, Sarkar PP. Enhanced secret communication using multilevel audio steganography. International Journal of Computational Engineering Research. 2016;**6**(10):6-12

[16] Thiede T, Treurniet WC, Bitto R, Schmidmer C, Sporer T, Beerens JG, et al. PEAQ–The ITU standard for objective measurement of perceived audio quality. Journal of the Audio Engineering Society. 2000;**48**(1/2):3-29

[17] OPTICOM OPERA software site, [Online]. Available: http://www.opticom.de/products/opera.html

[18] Unoki M, Imabeppu K, Hamada D, Haniu A, Miyauchi R. Embedding limitations with digital-audio watermarking method based on cochlear delay characteristics. Journal of Information Hiding and Multimedia Signal Processing. 2011;**2**(1):1-23

[19] Wang S, Unoki M. Speech watermarking method based on formant tuning. IEICE Transactions on Information and Systems. 2015;**E98-D**(1):29-37

[20] Quackenbush SR, Barnwell IIITP, Clements MA. Objective Measures of Speech Quality. Englewood Cliffs: Prentice Hall; 1988

[21] Xiang S, Kim JH, Huang J. Audio watermarking robust against time-scale modification and MP3 compression. Signal Processing. 2008;**88**(10):2372-2387

[22] Mansour M, Tewfik A. Data embedding in audio using time-scale modification. IEEE Transactions on Speech and Audio Processing. 2005;**13**(3):432-440

[23] Fallahpour M, Megías D. High capacity audio watermarking using fft amplitude interpolation. IEICE Electronics Express. 2009;**6**:1057-1063

[24] Fallahpour M, Megías D. High capacity method for real-time audio data hiding using the fft transform. In: Advances in Information Security and its Application. Berlin, Germany: Springer-Verlag; 2009. pp. 91-97

[25] Fallahpour M, Megías D. High capacity audio watermarking using the high frequency band of the wavelet domain. In: Multimedia Tools and Applications. Vol. 52. New York, NY, USA: Springer; 2011. pp. 485-498

[26] Kang X, Yang R, Huang J. Geometric invariant audio watermarking based on an LCM feature. IEEE Transactions on Multimedia. 2011;**13**:181-190

[27] Nishimura A. Audio data hiding that is robust with respect to aerial transmission and speech codecs. International Journal of Innovative Computing, Information and Control. 2010;**6**:1389-1400