Multimed Tools Appl (2017) 76:24091–24106
DOI 10.1007/s11042-016-4113-8

A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption

Said E. El-Khamy[1] **· Noha O. Korany**[1] **· Marwa H. El-Sherif**[1]

Received: 4 April 2016 / Revised: 19 September 2016 / Accepted: 1 November 2016 /
Published online: 28 November 2016

Abstract Steganography is the technique of hiding any secret information like text, image or video behind a cover file. Audio steganography is one of the widespread data hiding techniques that embeds secret data in audio signals. The secret data is hidden in a way that unauthorized people are not aware of the existence of the embedded data and without changing the quality of the audio signal (cover audio). Data hiding in audio signals has various applications such as protection of copyrighted audio signals, secret communication, hiding data that may influence the security and safety of governments and personnel. This paper proposes an efficient steganography scheme based on sample comparison in Discrete Wavelet Transform (DWT) domainwhere the cover audio is decomposed into several multi sub-bands, and then selected coefficients of details are changed by a threshold value depending on the embedding cipher image bit. This approach employs an original image component to perform RSA encryption on it, then cipher bits are embedded in the details components of the audio signal according to a predetermined threshold value. The performance of the algorithm has been estimated extensively against attacks, and simulation results are presented to prove the robustness of the proposed algorithm.

Keywords Cryptography · Discrete wavelet transform · RSA algorithm · Steganography · Human Auditory System (HAS) · Threshold

✉ Marwa H. El-Sherif
marwaelsherif2@gmail.com

Said E. El-Khamy
elkhamy@ieee.org

Noha O. Korany
nokorany@hotmail.com

[1] Department of Electrical Engineering, Alexandria University, Alexandria 21544, Egypt

1 Introduction

Steganography is an important sub-field of information security that focuses on hiding the existence of messages. It's derived from the Greek word Steganos which means (covered) and the word (graphia) which in turn means (writing). For successful hiding and extracting of data, an effective audio steganography should have the following characteristics: perceptual transparency (i.e. the cover and the stego object must be imperceptible), high data rate and robustness of the embedded data. In this paper, the cover medium is defined as the file in which hidden data are embedded and the resultant file is the storage medium. Audio steganography is one of the high challenging steganography methods because the Human Auditory System (HAS) is more sensitive to variations than Human Visual system (HVS). However, there are some holes that one can benefit. While using digital audio one can rely on the different sensitivity of the human ears to sounds of low and high intensity [8]. Recently, there are a lot of common techniques used for audio steganography. They are classified into temporal domain, frequency domain and wavelet domain techniques.

Temporal domain Under temporal domain the techniques include least significant bit (LSB) technique, parity coding and echo hiding techniques. The LSB method [3, 9] changes the lowest bit of the cover media to embed the secret message. It's one of the simplest methods, but it can be easily attacked. In Parity coding technique [5], parity of each group of samples are calculated and if it doesn't match the message bit, then the lowest bit of any of the individual samples in the group is changed to make the parity bit equal to the message bit. This technique is also easily to be extracted. In Echo hiding method [13], short echo is introduced to parts of cover audio with tampering of three parameters: decay rate, offset and amplitude to make the echo inaudible but the embedding capacity here is low.

Frequency domain In frequency domain there are some techniques used in audio steganography like tone insertion, phase coding and spread spectrum techniques. In tone insertion techniques [21] low power tones are masked in the presence of a stronger one. It's a robust method but has low embedding capacity. In phase coding method [2, 13], secret message bits are embedded as phase shift in the phase spectrum of the original cover audio. This method has good robustness, but also has low capacity and doesn't survive low pass filtering. Spread spectrum techniques [11] calculate the frequency masking threshold using psycho-acoustic model, where data signal is spread by an M-sequence code, and the spread signal is embedded in audio below the frequency masking threshold. This method increases transparency but it occupies high bandwidth.

Wavelet domain Wavelet domain techniques use wavelet coefficients. The operation of discrete wavelet transform (DWT) decomposition is to separate high pass and low pass components. There are a lot of techniques that uses wavelet domain to increase the hiding capacity and transparency [6, 7, 9]. In [9] a new algorithm for audio hiding based on (DWT) was proposed. The hidden data are embedded and extracted based on the contextual border upon low-frequency coefficients. This method has good imperceptibility and robustness against attacks, but there's some deficiency in selecting the length of quantization which is based on specific results to determine. In [7] the encrypted data were embedded into the wavelet coefficients after converting them to the integer domain. This method has high embedding capacity and full recovery of data, but the main disadvantage of this technique is

in the robustness against attacks. The technique in [6] used the concept of DWT and LSB for image hiding in audio. It has good robustness and security but with low embedding capacity.

The technique proposed in this paper combines the strategies of audio steganography and cryptography to present more security during transmission and the use of wavelet ensures least audio distortion after embedding process. The security and robustness are achieved using pseudo-number (PN) sequence in selecting coefficients and sample comparison in wavelet domain which is an efficient way for sending image files without revealing its existence. The remainder of this paper is organized as follows: in Section 2 the proposed algorithm is discussed in details, in Section 3 simulation results and related analysis are presented. Section 4 concludes the paper and discusses the future work.

2 Proposed algorithm

This section discusses the algorithm used to hide an encrypted image in a cover audio signal. Algorithm has two phases – embedding and extraction. In embedding phase, encrypted image is hidden inside the cover audio signal. In the extraction phase, the secret image is retrieved from the stego audio.

In this algorithm, audio samples are transformed into wavelet domain. Secret data here is an image, which is encrypted using RSA algorithm. These encrypted values of the image are then hidden in selected details coefficients based on sample comparison in DWT domain [19].

For more security, the used coefficients of audio samples are selected according to PN sequence generator that generates random sequence to specify the order of coefficient used to embed data. Selected coefficients are changed by a threshold value depending upon the embedded cipher image bit.

2.1 Embedding phase

The cover audio signal is read and audio samples are transformed into wavelet domain then the image is encrypted with RSA algorithm and hidden inside chosen cover audio details positions according to random sequence generator and using predetermined threshold value, then the stego audio is changed back to time domain. The following steps were used.

Step 1: Read the cover audio file.
Step 2: Apply DWT
Step 3: Generate a PN sequence N to select the location of detailed coefficients for embedding process.
Step 4: Read secret image and computes its size.
Step 5: Encrypt the image using RSA encryption algorithm and then convert the bits in the cipher image into binary form. This provides more security without reducing the hiding capacity.
Step 6: Embed the encrypted image

The method for embedding the image bits is as follows:

– If the bit in the secret image that is to be embedded is 0 then compare the selected coefficient with threshold value T. If the coefficient is greater than T, then modify the

value of coefficient so that it could become less then T. Otherwise there is no need to change the value of coefficient.

– If the embedded bit in the secret image is1 and if selected coefficient is less than threshold value T, then modify the value of coefficient so that it could become greater than or equal to T, otherwise there is no need to modify the coefficient.

Step 7: Reconstruction of stage-audio signal.

In this stage, stego audio signal coefficients are converted back from frequency domain to time domain using Inverse Discrete Wavelet Transform (IDWT) to get the stego audio output. This stego-audio sounds the same as the cover audio.

2.2 Extraction phase

In extraction phase, the secret image is retrieved from the stego audio by reversing the previous steps then the resulted bits are decrypted to get the original image. The following steps were used:

Step 1: Read the stego audio file
Step 2: Apply DWT to stego audio as in the embedding phase to get detail and approximation coefficients.
Step 3: Generate the same pseudo number sequence as in embedding phase.
Step 4: Retrieve image bits from selected details coefficients using the threshold value, T described in section A. If the coefficient is greater than or equal to the threshold value, it means that Message bit is 1 otherwise the Message bit is 0.
Step 5: Convert image bits to decimal.
Step 6: Decrypt image using an RSA decryption algorithm.

This proposed method to hide an encrypted image in a cover audio signal is shown in Fig. 1.

3 Results and discussions

This section focuses on the experimental results. The program code is generated using MATLAB R2014a, and two different audio samples were considered to embed data one of them is a sound file with audio length of 23 s, sampling frequency of 44,100 Hz and size of 2.02 MB, and the other is a speech sample with duration of 37 s, sampling frequency of 22,050 Hz and size of 6 MB. We selected two images of different sizes; 128*128 and 64*58 to perform our testing. The quality of the stego-audio is analyzed using mean square error (MSE), signal to noise ratio (SNR) and peak signal to noise ratio (PSNR) values.

MSE serves as an important parameter in gauging the performance of the steganographic system.

Suppose that $x = \{x_i \mid i = 1, 2 \ldots N\}$ and $y = \{y_i \mid i = 1, 2 \ldots N\}$ are two finite-length, discrete signals where x is the audio cover data and y is the corresponding audio stego-cover data, then MSE between the signals is given by Eq. (1) [22].

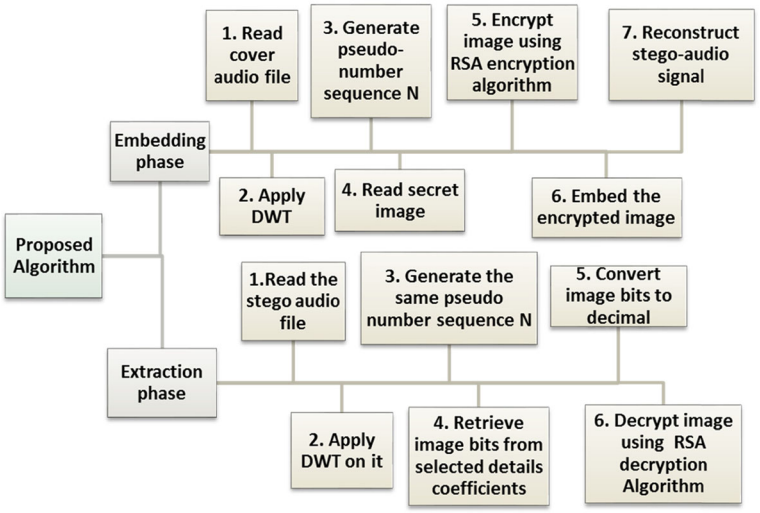


Fig. 1 The proposed method to hide an encrypted image in a cover audio signal

$$MSE(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2, \tag{1}$$

where N is the number of signal samples, x_i is the value of the i^{th} sample in x, and y_i is the value of the i^{th} sample in y.

SNR is a term that refers to the measurement of the level of an audio signal as compared to the level of noise that is present in that signal. It is expressed in decibels (dB). A larger SNR value indicates a better quality [16]. It is given by Eq. (2).

$$SNR(dB) = 10\log_{10}\left(\frac{\frac{1}{N}\sum_{i=0}^{N}x_i^2}{MSE(x,y)}\right), \tag{2}$$

Peak Signal to Noise Ratio is the ratio of the maximum signal to noise in the stego audio signal

$$PSNR(dB) = 10\log_{10}\left(\frac{R^2}{MSE(x,y)}\right), \tag{3}$$

where R is the peak signal value that exists in the original audio signal.

PSNR is measured in dB and it's a good measure for comparing restoration results for the same audio signal. Figures 2 and 3 show the cover audio signals and the frequency response of each of them, which is used to characterize the dynamics of the signal.

3.1 Tests of quality

Haar wavelets are applied on cover audio signals with one decomposition level, although the algorithm is applicable to higher resolution levels of wavelet. Coefficients are selected according to a pseudo-number sequence, then the secret data is hidden using different threshold values. The threshold value has been chosen using two methods. The first one is

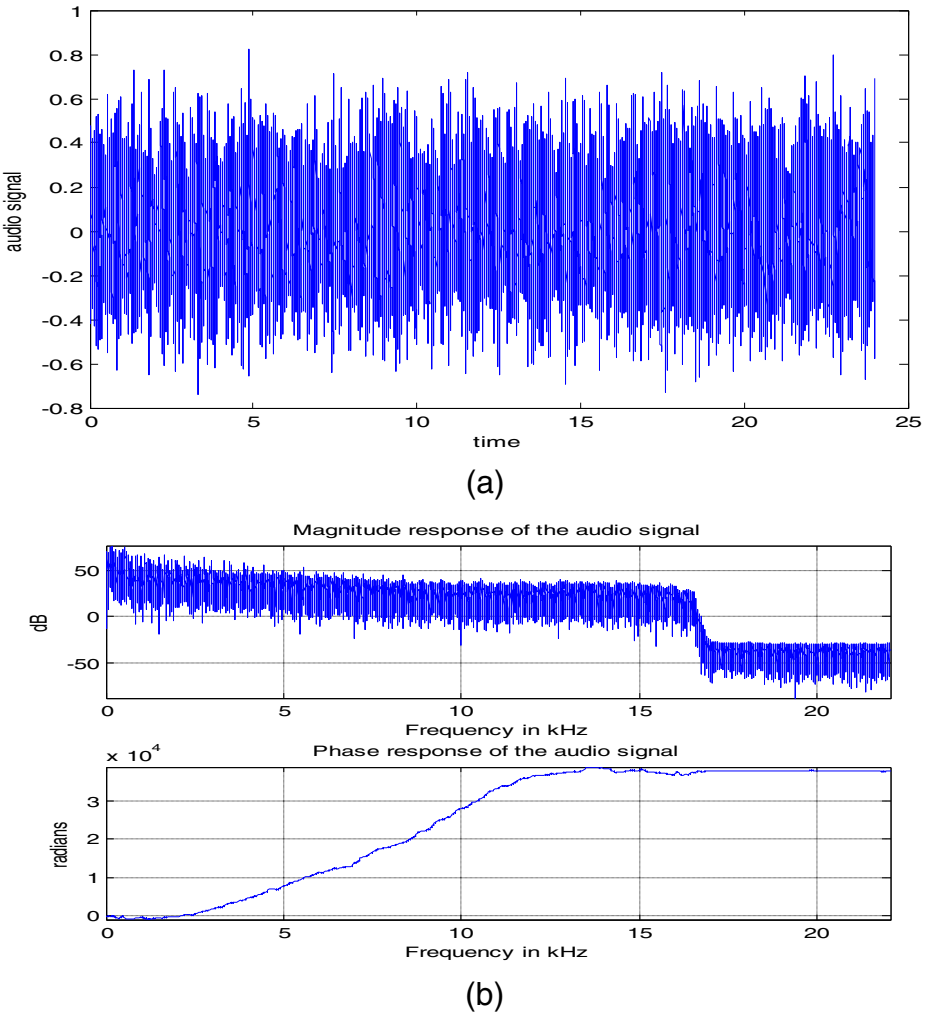


Fig. 2 **(a)** Time domain response of the music audio sample. **(b)** Frequency response of music audio sample

by setting it as a ratio from the maximum of the details values, whereas the other method is by setting the threshold to be the normalized median value which is calculated from the cumulative distribution function (CDF) of the details components. The CDF is the probability that the variable takes a value less than or equal to X for a given x. The CDF F(x) for a discrete vector x is given in Eq. (4), where P(x) is the discrete probability density function (pdf):

$$F(x) = P(X \leq x) = \sum_{X \leq x} P(x). \tag{4}$$

The median value is the value at which 50 % of the data lies beneath it, and 50 % lies above, so a details coefficient is just as likely to be larger than its median as it is to be smaller than it.

The results of the two methods are shown in Table 1. It is clear that when the threshold value is increased, MSE of the audio increases and its quality is degraded. The average SNR is

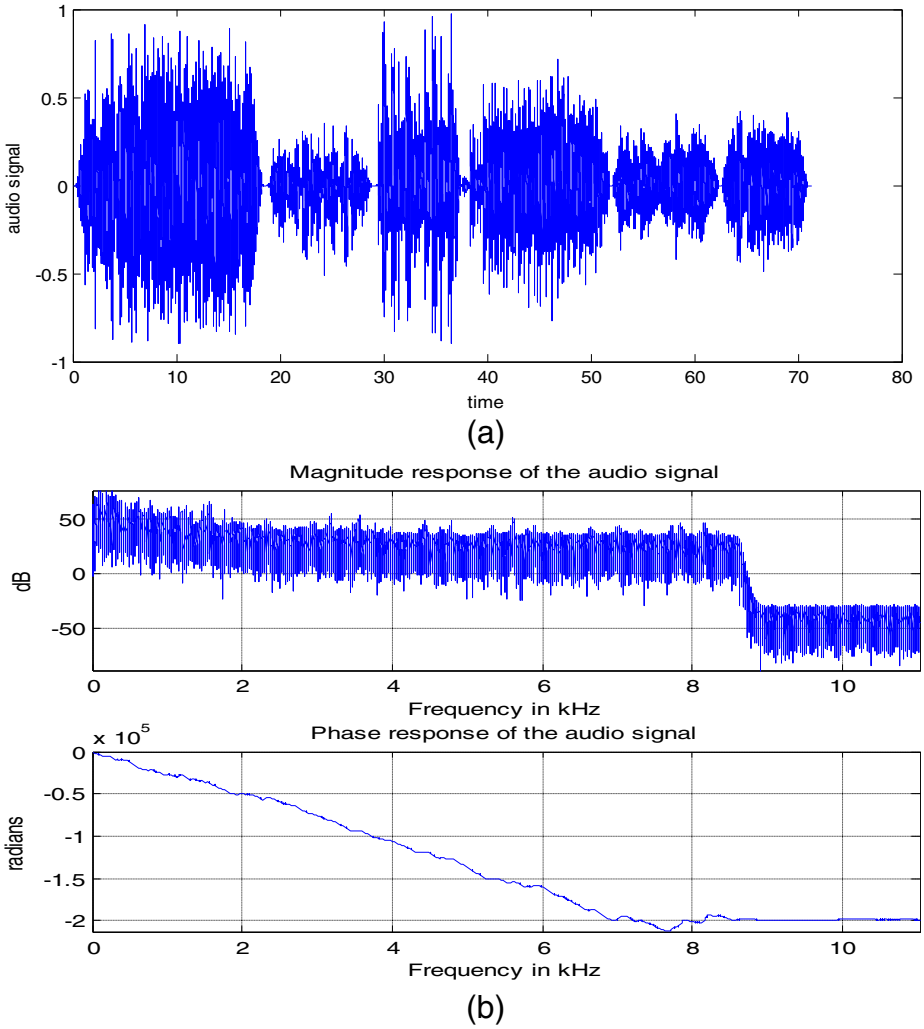


Fig. 3 **(a)** Time domain response of the speech audio sample. **(b)** Frequency response of speech audio sample

above 20 dB in the proposed algorithm which is better than many conventional DWT schemes and with higher embedded capacity. We noticed also that the second method gives better results for audio MSE and SNR than the first one.

Figures 4 and 5 show the original hidden image and the extracted images at different threshold values for two images of size 128*128 and 64 *58. It can be observed that significant changes in images are not perceptible.

The technique was tested also against some attacks like noise, MP3compression and echo addition. The quality difference between the original image and the extracted image is measured through PSNR which represents a measure of the peak error. It is defined as:

$$PSNR(dB) = 10\log_{10}\left(\frac{S^2}{MSE}\right). \tag{5}$$

Table 1 MSE, SNR and PSNR for different threshold values T with hidden image 1of size 128*128 and with hidden image 2 of size 64*58

Audio samples	Threshold value (T)	Image 1			Image 2		
		Cover audio MSE	Cover audio SNR in dB	Cover audio PSNR in dB	Cover audio MSE	Cover audio SNR in dB	Cover audio PSNR in dB
Cover audio1.wav (Music sample)	0.01 × Maximum details value	4.1807e-05	27.5452	42.0806	9.6429e-06	33.9156	48.4510
	0.1 × Maximum details value	1.0973e-04	23.3544	37.8899	2.6507e-05	29.5241	44.0595
	The normalized median value of CDF of details components = 4.3158e-04	3.9812e-05	27.7576	42.2930	9.1116e-06	34.1618	48.6972
Cover audio2.wav (speech sample)	0.01 × Maximum details value	1.6539e-05	30.3896	47.5646	3.8523e-06	36.7174	53.8924
	0.1 × Maximum details value	1.2245e-04	21.6950	38.8701	2.9587e-05	27.8636	45.0387

Fig. 4 Extracted images at different threshold values for image 1 of size 128*128

(a) Original image

(b) Extracted image at threshold value = 0.01* maximum details value

(c) Extracted image at threshold value = 0.1 * maximum details value

(d) Extracted image at threshold value = median of CDF of details components

Fig. 5 Extracted images at different threshold values for image 2 of size 64*58

(a) Original image

(b) Extracted image at threshold value = 0.01* maximum details value

(c) Extracted image at threshold value = 0.1 * maximum details value

(d) Extracted image at threshold value = median of CDF of details components

where MSE represents the cumulative squared error between the original hidden image and the extracted image, and S is the maximum pixel value. PSNR is a good measure for comparing restoration results for the same image, but between different images, comparisons of PSNR are meaningless. One image with 20 dB PSNR may look better than another image with 30 dB PSNR.

3.2 Tests of robustness against addition of Gaussian noise

To study the robustness of data in presence of noise, zero mean Gaussian noise was added to the stego file at different variance values. Data retrieval from the noise added stego signal was done in the same manner as above. Figure 6 shows the extracted images at variance of 0.1, 0.01, 0.001 and 0.0001 for the two different used images. The results of evaluation of the proposed algorithm in the presence of Gaussian noise are presented in Table 2.

From Table 2 and Fig. 6 it's noticed that the worst stego image quality is at variance value of 0.1 which is parallel to a SNR level of 10 dB, but the recovered image is detected and the PSNR values of audio signal still have acceptable ranges.

3.3 Tests of robustness against MP3-compression attack

MP3 is common because it gives a good audio quality with small storage [14]. There are more effective ways to reduce the storage required for digital audio data, while also maintaining a high-quality sound. One idea is rather than cutting out less important frequencies altogether, we could store the corresponding model coefficients with lower precision that is, with fewer bits. This technique is called quantization. The less important frequencies are determined by the magnitude of their Discrete Cosine Transform (DCT) model coefficients. Coefficients of small magnitude correspond to cosine frequencies that do not contribute much to the sound

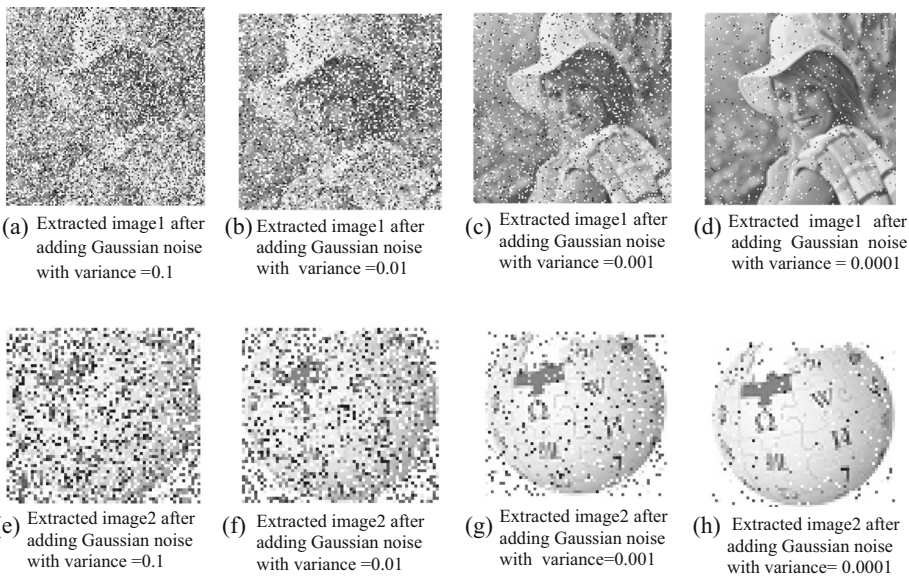


Fig. 6 Extracted images after adding Gaussian noise with different variance values

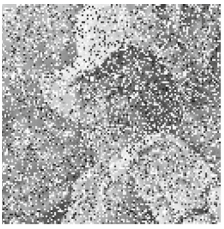
Table 2 MSE, SNR and PSNR for cover audio with noise at different variance values for images 1 and 2

Audio samples	Variance	SNR level	Image 1			Image 2		
			Cover audio MSE	Cover audio PSNR in dB	Hidden image PSNR in dB	Cover audio MSE	Cover audio PSNR in dB	Hidden image PSNR in dB
Cover audio1.-wav	0.1	10	0.0048	22.8950	7.7780	0.0025	25.6919	8.1952
	0.01	20	0.0030	25.0149	8.9132	8.5573e-04	30.4263	9.4026
	0.001	30	0.0028	25.2966	10.9426	6.8766e-04	31.3759	11.4194
	0.0001	40	0.0028	25.3259	13.2041	6.7072e-04	31.4842	13.9377
Cover audio2.-wav	0. 1	10	0.0043	22.0008	7.0781	0.0028	23.7610	7.8832
	0.01	20	0.0020	25.3335	9.4739	6.6264e-04	30.0804	10.2093
	0.001	30	0.0017	25.8686	12.9634	4.4376e-04	31.8217	13.7395
	0.0001	40	0.0017	25.9255	17.3047	4.2204e-04	32.0396	18.5563

samples. A key idea of methods like the mp3 algorithm is to focus the compression on parts of the signal that are perceptually not very important. The proposed algorithm is tested against MP3 compression at bit rates of 64,128 and 320 kbps. Figure 7 and Table 3 show acceptable results.

3.4 Tests of robustness against echo addition

An echo signal is added with a delay of 50 ms and a decay of 1 %, 5 % and 10 % to the stego cover audio signal. The results are listed in Table 4. From the obtained results in Table 4, it's obvious that the proposed algorithm exhibits good robustness against echo addition operation. Figure 8 compares extracted images after echo addition with decay rates of 1 %, 5 % and 10 %.



(a) Extracted image1 after mp3 compression with bit rate = 64 kbps

(b) Extracted image1 after mp3 compression with bit rate =128 kbps

(c) Extracted image1 after mp3 compression with bit rate=320 kbps

(d) Extracted image2 after mp3 compression with bit rate = 64 kbps

(e) Extracted image2 after mp3 compression with bit rate = 128 kbps

(f) Extracted image2 after mp3 compression with bit rate=320 kbps

Fig. 7 Extracted images after mp3 compression attack with different bit rate values

Table 3 MSE, SNR and PSNR for cover audio with mp3 compression at different bit rate values for images 1 and 2

Audio samples	Bit rate	Image 1			Image 2		
		Cover audio MSE	Cover audio PSNR in dB	Hidden image PSNR in dB	Cover audio MSE	Cover audio PSNR in dB	Hidden image PSNR in dB
Cover audio1.-wav	64 kbps	0.0067	20.0053	8.5619	0.0061	20.4148	16.7354
	128 kbps	0.0021	25.1598	10.73349	7.6474e-04	29.4580	19.2186
	320 kbps	0.0017	25.9308	22.7121	4.2018e-04	32.0588	24.0712
Cover audio2.-wav	64 kbps	0.0033	24.5585	9.0204	0.0012	28.8621	9.5769
	128 kbps	0.0028	25.3178	13.0767	6.7664e-04	31.4461	13.5744
	320 kbps	0.0025	25.3291	17.0793	6.6888e-04	31.4962	17.6300

It's obvious that embedded images have been successfully extracted, but with some degradation when the decay rate of the echo signal is increased.

4 Comparison between the proposed approach with some other related works

The proposed technique in this study is compared with some previous methods that utilize DWT like [1, 15, 19], where in [19], redundant bits in the cover file were replaced by the bits of the secret information by sample comparison in DWT domain. In [15] the message is embedded with sequence mapping technique in the bit of a cover audio by applying DWT on audio files for taking the higher frequency. The method in [1] is based on cascading two-well known transforms: discrete wavelet transform and the singular value decomposition.

The comparison is based on hiding capacity and mean of PSNR values. As seen in Table 5, the hiding capacity of the proposed algorithm is more than the other methods, and with a PSNR value of about 42 dB while all other methods have smaller values of PSNR.

Table 4 MSE, SNR and PSNR for cover audio signal after adding an echo at different decay rate percentages for images 1 and 2

Audio samples	Decay rate	Image 1			Image 2		
		Cover audio MSE	Cover audio PSNR in dB	Hidden image PSNR in dB	Cover audio MSE	Cover audio PSNR in dB	Hidden image PSNR in dB
Cover audio1.-wav	1 %	5.8232e-04	30.6415	15.1806	5.0104e-04	31.2944	16.1905
	5 %	6.3855e-04	30.2412	12.9792	5.5676e-04	30.8365	13.9112
	10 %	8.1328e-04	29.1908	11.2499	7.3079e-04	29.6552	12.0963
Cover audio2.-wav	1 %	0.0095	17.4430	15.4011	0.0095	17.4504	16.5353
	5 %	0.0095	17.4430	13.1641	0.0095	17.4403	13.9611
	10 %	0.0096	17.4017	11.6586	0.0096	17.4091	12.1620

(a) Extracted image 1 after adding echo signal with a decay rate of 1%

(b) Extracted image 1 after adding echo signal with a decay rate of 5%

(c) Extracted image 1 after adding echo signal with a decay rate of 10%

(d) Extracted image 2 after adding echo signal with a decay rate of 1%

(e) Extracted image 2 after adding echo signal with a decay rate of 5%

(f) Extracted image 2 after adding echo signal with a decay rate of 10%

Fig. 8 Extracted images after echo addition with different decay rates

5 Proposed technique applications

Information hiding in audio signals has a various range of applications [4, 17, 20]. Audio Steganography techniques can be applied for covert communication using innocent cover signals, like a telephone conversation. Another application, known as (digital) watermarking [18, 10, 12], refers to embedding an inappreciable mark into an object, which can be used for copyright protection of digital media. For example, a digital watermark can be inserted into a piece of music so that it can be monitored automatically for payment purposes.

Audio steganography can be used also in defense organizations and intelligence agencies for the security of private information and secret data storing. It may also be used to embed medical images in audio files that are sent to various recipients such as doctors in-charge of the corresponding patient. Combining cryptography and steganography can help in avoiding suspicion and protect privacy.

The accessibility and popularity of audio files make them desirable to carry hidden information. Furthermore, most steganalysis efforts are more concentrated towards digital images leaving audio steganalysis relatively unexplored.

Table 5 Comparison between the proposed algorithm and some other related works

Method	Hiding Capacity (bps)	Mean PSNR (dB)
Proposed Method	5698	41.73
Reference 1 [15]	890	37.01
Reference 2 [19]	4000	28.1
Reference 3 [1]	1032	38.17

6 Conclusion

In this paper a secure, robust and high capacity audio steganography technique is proposed. It's an efficient way to send image files without revealing its existence. The basic idea of the proposed technique is based on samples comparison in DWT domain where selected coefficients of details are compared with a predetermined threshold value T and bits are embedded according to this comparison which gives an efficient wavelet masking technique. Experimental results give good PSNR and high embedding capacity. The algorithm provides also a robust encryption using RSA technique. Two kind of audio signals were used, speech and music files; and from results we can deduce that SNR was better when using speech sample because most important information were in the low frequencies and so when performing wavelet transform embedding data in details components didn't affect the original audio signal quality by a considerable amount. When the threshold value has been chosen according to the median value of the CDF of the details components it gave better results and improved PSNR for both cover audio and embedded image. The proposed technique also was tested against some of the malicious attacks involving AWGN noise, MP3 compression and echo addition and the experimental results showed good PSNR and high robustness in the noisy environments.

This paper future work can include application of other asymmetric cryptosystems for encryption of embedded data. Additionally, video hiding in audio steganography can be used. Also future research can explore the possibilities of improvements in audio steganography system using different techniques like genetic algorithm, neural networks and chaotic maps to increase the capacity of the audio signal and make it more robust against steganalysis. Besides, this investigation may be further extended to multiple levels of DWT decomposition and different steganography representations to make the system more secure towards detection.

References

1. Al-haj A (2014) An imperceptible and robust audio watermarking algorithm. EURASIP J Audio Speech Music Process. doi:10.1186/s13636-014-0037-2
2. Antony J, Sobin CC, Sherly AP (2012) Audio steganography in wavelet domain a survey. Int J Comput Appl 52(13):33–37
3. Bansal N, Bansal A, Deolia VK, Pathak P (2015) Comparative analysis of LSB, DCT and DWT for digital watermarking. Int Conf Comput Sustain Glob Dev. doi:10.1007/978-981-10-0767-5_13
4. Doshi R, Jain P, Gupta L (2012) Steganography and its applications in security. Int J Mod Eng Res 2(6): 4634–4638
5. Goel S, Rana A, Kaur M (2013) Comparison of Image Steganography Techniques. International Journal of Computers and Distributed Systems 3(1):20–30
6. Gupta N (2013) Hiding image in audio using DWT and LSB. Int J Comput Appl 81:11–14
7. Gupta S, Dhanda N (2015) Audio steganography using discrete wavelet transformation (DWT) & discrete cosine transformation (DCT). IOSR J Comput Eng 17(2):2278–2661
8. Kekre HB, Athawale A, Rao S, Athawale U (2010) Information hiding in audio signals. Int J Comput Appl 7(9):14–19
9. Lihua M, Shuangyuan Y, Qingshan J (2009) A new algorithm for digital audio watermarking based on DWT. In: Global Congress on Intelligent System. 1–5. doi:10.1109/GCIS.2009.452
10. Makarov A, Yakovleva E (2016) Comparative analysis of half toning algorithms for digital watermarking. In: Proceeding of the 18th conference of fruct association. no. 2. doi:10.1109/FRUCT-ISPIT.2016.7561527
11. Marvel LM, Boncelet CG, Retter CT (1999) Spread spectrum image steganography. IEEE Trans Image Process. doi:10.1109/83.777088
12. Neethu V, Kalaivani R (2016) Efficient and Robust Audio Watermarking for Content Authentication and Copyright Protection. Paper presented at 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, 2016, pp. 1–6 doi:10.1109/ICCPCT.2016.7530371

13. Patil BA, Chakkarwar VA (2013) Review of an improved audio steganographic technique over LSB through random based approach. IOSR J Comput Eng 9(1):30–34
14. Qiao M, Sung AH, Liu Q (2016) Revealing real quality of double compressed MP3 audio. ACM Int Conf Multimed. doi:10.1145/1873951.1874137
15. Saroha K, Singh PK (2010) A variant of LSB Steganography for Hiding Images in Audio. International Journal of Computer Applications 11(6)12–16
16. Shikha C, Chaten P (2014) Key based image steganography using Dwt and chaotic map. Int J Eng Manag Res 4(no. 4):94–97
17. Singh PK, Singh H, Saroha K (2009) A survey on Steganography in Audio. Proceedings of the 3rd National Conference; INDIACom 2009, Computing For Nation Development, February 26–27, 2009 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi
18. Subir, Joshi AM (2016) DWT-DCT based blind audio watermarking using arnold scrambling and cyclic codes. In: 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), p 79–84. doi:10.1109/SPIN.2016.7566666
19. Verma SS, R. Gupta, Shrivastava G (2014) A novel technique for data hiding in audio carrier by using sample comparison in DWT domain. 2014 Fourth Int Conf Commun Syst Netw Technol. 639–643. doi:10.1109/CSNT.2014.134
20. Waziri VO, Ochoche A (2012) Steganography and its applications in information dessimilation on the web using images as securityembeddment: a wavelet approach. Int J Comput Inf Technol 01(02):194–202
21. Wenndt SJ (2015) Audio steganography for covert data transmission by imperceptible tone insertion. Int Multi-Conference Wirel Opt Commun
22. Wu Y, Noonan JP (2012) Image steganography scheme using chaos and fractals with the wavelet transform. Int J Innov Manag Technol 3(3):285–289

Said E. El-Khamy received the B.Sc. (Honors) and M.Sc. degrees from Alexandria University, Alexandria, Egypt, in 1965 and 1967 respectively, and the Ph.D. degree from the University of Massachusetts, Amherst, USA, in 1971. He joined the teaching staff of the Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Alexandria, Egypt, since 1972 and was appointed as a Full-time Professor in 1982 and as the Chairman of the Electrical Engineering Department from September 2000 to September 2003. He is currently an Emeritus Professor. Prof. El-Khamy has published more than three hundreds scientific papers in national and international conferences and journals and took part in the organization of many local and international conferences. His Current research areas of interest include Spread-Spectrum Techniques, Mobile and Personal Communications, Wave Propagation in different media, Smart Antenna Arrays, Space–Time Coding, Modern Signal Processing Techniques and their applications in Image Processing, Communication Systems, Antenna design and Wave Propagation problems. Prof. El-Khamy is a Fellow member of the IEEE since 1999. He received many prestigious national and international prizes and awards including the State Appreciation Award (Al-Takderia) of Engineering Sciences for 2004, the most cited paper award from Digital Signal Processing journal for 2008, the IEEE R. W. P. King best paper award of the Antennas and Propagation Society of IEEE, in 1980, the the A. Schuman's-Jordan's award for Engineering Research in 1982. He is also a Fellow of the Electromagnetics Academy and a member of Tau Beta Pi, Eta Kappa Nu and Sigma Xi.

Noha Korany is currently an associate professor at the University of Alexandria, Egypt. She received his B. sc. Eng. From Alexandria university, and her Ph.D. from Alexandria University, Egypt and fellowship Ruhr-University at Bochum, Germany. She was member of the scientific staff of the Institute of Communication-Acoustics, Ruhr-University at Bochum, Germany from 2002 to 2004. Her main research field is acoustics and communications.

Marwa H. El-Sherif is a PhD student at the Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Egypt. She received the B.Sc. and M.Sc. degrees from Alexandria University, Alexandria, Egypt, in 2006 and 2012 respectively. Her research interests include image processing, digital watermarking, cryptography and information security.