Journal of Theoretical and Applied Information Technology
15th April 2017. Vol.95. No 7

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING THE HIDING CAPACITY OF AUDIO STEGANOGRAPHY BASED ON BLOCK MAPPING

[1]AHMED HUSSAIN ALI, [2]MOHD ROSMADI MOKHTAR, [3]LOAY EDWAR GEORGE
[1,2] Faculty of Information Science and Technology, UKM, Malaysia
[3]College of Science University of Baghdad, Iraq
E-mail: [1]ahmedhussainali@siswa.ukm.edu.my, [2]mrm@ukm.edu.my, [2]loayedwar57@scbaghdad.edu.iq

ABSTRACT

With the rapid growth in exchanging personal and confidential data through an unsecure channel like the internet and exposing it though disclosing by intruders, the necessity of information security became a great demand. As a result, data hiding or steganography appeared as a vital solution. Audio hiding is a concept of injecting the secret data in an audio carrier. This paper proposes a scheme known as ECA-BM, to improve the performance of the audio steganography. ECA-BM contributes in: (1) increases the hiding capacity, (2) maintains the transparency of carrier and (3) enhance the security of the proposed model. To increase the hiding capacity, fractal coding is adopted to create a mapping between the cover and secret blocks in order to encode the secret data into a set of coefficients with minimum size. To maintain the fidelity of the stego file, only 1-LSB from each cover sample is used for embedding. To increase the security of the ECA-BM, the cover samples for embedding are selected in a chaotic manner. LSB technique is utilized for embedding after converting secret coefficients into a binary sequence. Objective metrics, SNR, HC, and NC is used to evaluate the performance of ECA-BM. The Experimental results show a significant increase in the hiding capacity compared with some related studies. Moreover, the fidelity of the stego and reconstructed secret file are preserved.

Keywords: *Fractal Coding, Iteration Function System (IFS), Least Significant Bit (LSB), Steganography, Chaotic map.*

1. INTRODUCTION

Data hiding is the discipline of concealing confidential information in innocent carriers in an imperceptible way so that no one except the intended receiver knows about it. Cryptography, watermarking, and steganography are the main techniques of the information security that are employed to achieve secure communication, Fig.1. Cryptography is the earlier technique that is adopted for scrambling the data in a vague way. Steganography is utilized to hide the existence of the confidential data and transmit it in a secure way while watermark is employed for copyright protection and authentication. These techniques are categorized under information hiding. [1], [2]. Steganography is a word derived from the ancient Greek words steganos, which means covered and graphia, which in turn means writing [3]. In steganography techniques, the scenario is, the sender hides the secret message into a carrier file. This yielded file is a stego-file that is delivered to the receiver. At the receiver side, the receiver will extract the embedded secret data from the stego file. The secret data and the host can be any of various file types 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 host audio file is more challenging than using images since human auditory system (HAS) is more sensitive in comparison to the human visual system (HVS). The audio files are nominated as a carrier for hiding information is due to its popularity. On the other hand, most steganalysis efforts are targeted to image this makes the audio steganalysis is relatively unexplored [4].

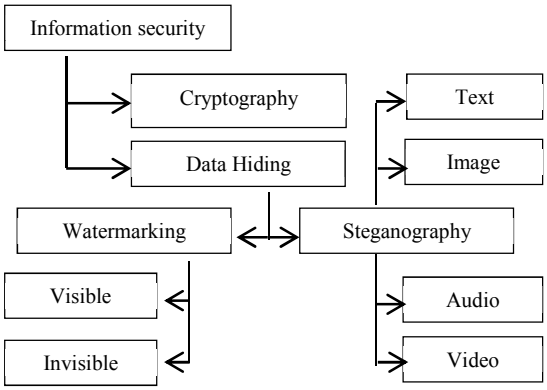

Fig. 1 Information Security System

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Steganography is used in several trends such as covert communication (peoples, defense organization, intelligent agenesis and governments), secure storage (banking transactions, sensitive and patient information) and copy right protection (intellectual property, particularly in industrial societies).

Many audio steganography techniques [5-9] have been introduced in literature to boosting the amount of the confidential data to be embedded (hiding capacity) which is the significant goal in steganography techniques. This is considered as a challenge since hiding capacity is contradictory with the other goals, imperceptibility and robustness. This means that increasing the efficiency of one goal will decrease the others and all the efforts are targeted to make a balance between these goals [10].

The aim of the study is to propose a scheme that adopts fractal coding, LSB and logistic map in embedding and extracting processes. The proposed scheme hides audio message into an audio cover. ECA-BM can successfully embed high capacity of secret message without perceptible degradation to the audio cover. The result shows a large amount of secret audio message up to 80% is successfully embedded in the cover with 69.3 dB and 38.9 dB SNR for stego and reconstructed secret file, respectively.

This paper is organized as follow: section II gives a brief discussion of the methods and the framework of the proposed scheme. Section III presents the experimental results and discussion while the conclusion is provided in section IV.

2. DATA HIDING REQUIREMENTS

Many data hiding schemes were suggested in literature and their performance depends on three main features: transparency, hiding capacity, and robustness, Fig 2. These features are essential and should be achieved in steganography algorithms. 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. For instance, increasing capacity will diminish the transparency and vice versa. A good steganography system has to a trade-off between these requirements and which is hard to achieve in one algorithm [11].

2.1 Imperceptibility

Most of the data hiding techniques have to embed data as much as possible with minimal distortion on the fidelity of the host file. It is one of the most important factors in designing any steganography algorithms. The fidelity of the steganography algorithm is usually known as a perceptual quality between the cover and stego files. 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 [12] and [13] that produce high-quality stego-object.

2.2 Hiding 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.

2.3 Robustness

Robustness is defined as the resistance of the stego file upon attacks and steganalysis techniques. There is two kinds of attacks that may have an effect on the stego-cover: an unintentional attack that tries to modify or destroy the stego-cover (such as compression, rotation, blurring, noising and other filtering techniques) and intentional attack that tries to reveal the stego-cover and extract the hidden information. Usually, there is a trade-off between robustness and capacity that can hardly be achieved in the one steganography system. The robustness is an important factor for copyright protection and watermarking applications, while imperceptibility and high hiding capacity are more significant for steganography applications because the goal is to hide the as large amount of data with preserving the quality of the cover file [14].

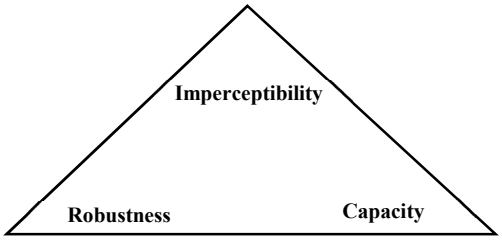

Fig. 2 Data Hiding Requirements

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. DATA HIDING DOMAINS

Data hiding, in general, can be classified into two main domains according to which the steganography technique has been applied: time and transform domain [15] as shown in Fig. 3 and 4.

In the time domain, the secret data is hidden directly into host file and it considered as simple and easy to implement. However, this domain suffers from low robustness and security. The earliest algorithm employed in such domain is LSB which is used in the 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 data hiding methods try to combine time domain 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 the secret data is embedded into the transform coefficients. This enables techniques to embed the data into perceptually significant components and makes it difficult to recover the embedded data. This will offer a 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 data hiding are Wavelet transform (WT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT). Fig. 3 and Fig. 4 show the hiding process of time and transfer domain.

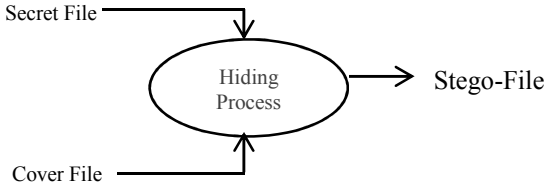

Fig. 3 Time Domain

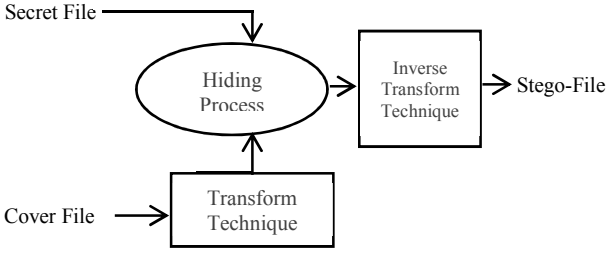

Fig. 4 Transform Domain

4. FRACTAL CODING

The main idea of fractals is based on finding the similarity between objects [16]. Benoit Mandelbrot discovered fractals in 1975. Barnsley is the inventor of the fractal coding for image compression. Barnsley's effort was followed by Jacquin [17] by using the mathematics of IFSs. Jacquin, finally established a practical fractal coding algorithm by using PIFS in the image domain, in which an image is divided into blocks and fractal coding is applied to each block. Fractal coding is one of the approaches that is used for compression. High compression ratio and reconstructed signal fidelity are the main advantages of this technique, moreover, it is a lossy compression [18]. Fractal coding has an asymmetric property which means that the encoding process is time-consuming process while the decoding is simple and fast. The fractal coding consists of encoding and decoding process that is proposed by Al-Hilo [19]:

4.1 Encoding process:

- Partitioning the cover and secret signal into blocks to generate the domain and range pool.
- The range is matched with all the domain blocks to get optimum IFS coefficients for each secret block that has a minimum error using Eq. (1) to (4):

$$Err^2 = \sigma_r^2 + S\left[S\,\sigma_d^2 + 2\bar{d}\bar{r} - \frac{2}{n}\sum_{n=0}^{n-1} d_i r_i\right] \quad (1)$$

$$S = \begin{cases} \frac{\frac{1}{n}\sum_{n=0}^{n-1} d_i r_i - \bar{d}\bar{r}}{\sigma_d^2}, & \text{if} \sigma_d^2 < 0 \\ 0, & \text{if } \sigma_d^2 = 0 \end{cases} \quad (2)$$

$$\bar{r} = \frac{1}{n}\sum_{n=0}^{n-1} r_i \quad , \quad \bar{d} = \frac{1}{n}\sum_{n=0}^{n-1} d_i \quad (3)$$

$$\sigma_d^2 = \frac{1}{n}\sum_{n=0}^{n-1} d_i^2 - \bar{d}^2;\ \sigma_r^2 = \frac{1}{n}\sum_{n=0}^{n-1} r_i^2 - \bar{r}^2 \quad (4)$$

where:
Err^2, the error between the current range and domain block;
d_i, value of the ith sample in the domain block;
r_i, value of the ith sample in the range block;
$\bar{d}, \bar{r}$, the mean value of the domain and range blocks, respectively;
σ_d^2, σ_r^2, the variance of the domain and range blocks, respectively;
S, the scale parameter.

- Saving the optimum IFS coefficients that are used later in the decoding process.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 Decoding process

It is simple and straightforward in which the affine mapping is applied using the retrieved IFS coefficients and stego file samples using Eq. (5):

$$\mathrm{Ret}'_i = S(d_i - \bar{d}) + \bar{r} \quad (5)$$

Where
Ret'_i is the reconstructed range block;
d_i, value of the ith sample of the stego-file block;
$\bar{d}, \bar{r}$, the mean value of the stego and range blocks, respectively;
S, the scale parameter.

5. CHAOTIC MAP

The high sensitivity of the initial parameters is considered the main characteristic of the chaotic map. Logistic map is the simplest chaotic function that is used in the ECA-BM to select the cover samples in a chaotic way for embedding the secret bits and can be represented by Eq. (6):

$$x_{n+1} = t\, x_n\, (1 - x_n) \quad (6)$$
where $0 \leq t \leq 4$, $x_0 \in (0, 1)$

t and x_0 are the parameters of the logistic map [20]. These parameters are considered the secret key that is used in embedding and extraction process.

6. RELATED WORK

Some of the related studies in the literature that contributed in enhancing the hiding capacity are presented in this section using different approaches and domains.

Two approaches are suggested in [5] to audio embedding using the LSB method. They found that the number of LSBs used in embedding could be up to seven, and the number of LSBs depended on the most significant bits of the cover samples. These approaches is considered as multiple and variable LSB's approaches comparing with the standard LSB. For their approach, they used a 16-bit cover sample. The results showed that the gotten hiding capacity is enhanced by 47.4% of the cover size with respect to that when four LSBs were used. The SNR of the stego file is on average 52 dB. These approaches are simple and not easy for steganalysis to detect the hidden data because they used variable LSB.

The author in [6] proposed a method for hiding information in wavelet coefficients using the LSB substitution technique. The carrier is separated into wavelet sub-bands and these sub-bands are compared with a hearing threshold in order to maintain the fidelity of the carrier. Three level DWT is used in this method. The Signal to Noise Ratio (SNR) stego file was 76 dB, and the hiding capacity on average was 34.5% of the cover size.

An algorithm based on wavelet packet transform and bit block matching are adopted by [7]. The message bits block the secret data is hidden in arbitrary position depend on the bit block matching. The cover sample strength and bit block matching are two factors that affect the hiding process. The secret message is recovered without need the original cover file. Embedding capacity is up to 42% of the cover signal with at least 50 dB SNR in the presented results.

Bazyar and Sudirman [8] proposed an embedding technique for increasing carrying capacity. They used an LSB algorithm for embedding and shifting the embedding layer from the fourth LSB layer to the seventh LSB layer. The results showed that the obtained hiding capacity is between 35% and 55%, and the SNR of the stego file is 62 dB on average.

Integer wavelet transform is adopted in the method proposed in [9]. It improves the hiding capacity to 50% of the cover file by transforming the secret data into approximation and detail coefficients and only the approximation is considered. Key generation is embedded into 2-LSB of each detail coefficients of the cover file in order to maintain the fidelity of the cover signal by 39.3 dB.

In short, there are several techniques in the literature were proposed in both domains, time and transform domain to enhance the performance of the audio steganography in terms of hiding capacity and the perceptual quality of the stego file. However, the achieved hiding capacity is up to 55% and 50% in time and transform domain, respectively.

7. THE PROPOSED SCHEME

The detail of ECA-BM is presented in this section. The aim is to improve the performance of the audio hiding. It utilizes fractal coding to map and encode the secret samples and consequently improve the cover capacity. Chaotic LSB using Logistic function is utilized to hide the encoded coefficients in chaotic style. Like other steganography techniques, ECA-BM comprises embedding and extraction processes as shown in Fig. 5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7.1 Embedding Process:

This process is run on the sender side. It begins with the loading of the secret and cover file then, splitting the data from the header. The cover samples are partitioned into overlapped blocks while the secret samples into non-overlapped blocks. Each block has N samples; N depends on the ratio between the size of the cover to the secret file and the number of bits required for each IFS code. Because of its simplicity and requiring less computation time, fixed partitioning is used [21]. Mean and variance for each secret and cover block are calculated using Eq. (3) and (4).

At the end, each secret block is encoded to a set of IFS coefficients by matching it with all cover blocks by obtaining the most similar cover block with minimum error using Eq. (1) and (2). The IFS coefficients for each secret block consist of optimal domain position, scale, symmetry, and range mean [19]. The binary sequence of the IFS is embedded chaotically using the secret key in the cover samples and the 1-LSB in each cover sample is modified for hiding the secret bits.

2) Extraction Process:

The extraction process is quite simple and straightforward. Throughout this process, the particular receiver will collect the IFS coefficients using the secret key. The LSB bits of the selected stego-file samples are gathered to recreate the IFS coefficients in the same order as in embedding process. The retrieved coefficients are used to reconstruct the secret blocks using Eq. (5) then the reconstructed secret file is created.

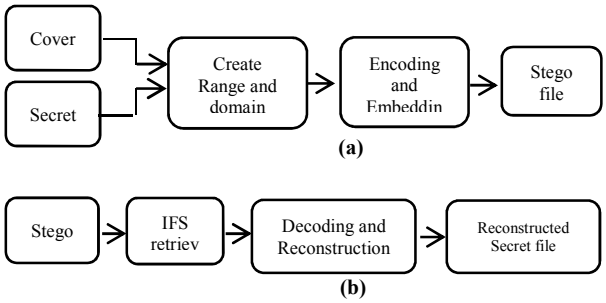

Fig. 5 The framework of ECA-BM
(a) embedding process and (b) extraction process

8. RESULTS AND DISCUSSION

This section is dedicated to evaluating the performance of ECA-BM in terms of hiding capacity and the fidelity of the cover and reconstructed secret files. ECA-BM is implemented using Eclipse Java. The audio files that are used in the experiment are selected from Marsyas dataset [22]. The selected files are with the following specifications: WAVE (.wav) mono format with 16 bits per sample and a sampling rate of 44100 Hz. The selection comprises of three speech files (dialogue, female and voice) and two music files (jazz and vlobos) with different sizes ranging from 1 to 11 seconds. The test is conducted to inspect the impact of the block length on the performance.

Three metrics are utilized to assess the performance of the ECA-BM which is Signal to Noise Ratio (SNR) [23], Normal Correction (NC) [24] and Hiding Capacity (HC) [12] using Eq. (7), (8) and (9) respectively.

SNR represents the ratio of the distortion between two signals input and output. The output signal with higher SNR values is considered as a signal has better fidelity.

$$\mathrm{SNR} = 10\log_{10}\frac{\sum_{i=1}^{N} s1(i)^2}{\sum_{i=1}^{N}(s1(i)-s2(i))^2} \qquad (7)$$

Where, s1(i) and s2(i) are the i^{th} samples of the input signal and output signal respectively and N is the number of samples of each signal.

NC is the most popular metric that measures the similarity between two signals.

$$\mathrm{NC}(S_1, S_2) = \frac{\sum_{i=1}^{L} s_1 s_2}{\sqrt{\sum_{i=1}^{L} s_1^2}\sqrt{\sum_{i=1}^{L} s_2^2}} \qquad (8)$$

where s_1 s_2 are the original secret and reconstructed secret signal, respectively; L indicates the length of samples in each signal. NC near 1 means the two signal are similar almost.

HC means the ratio between the size of the secret and cover data.

$$\mathrm{HC} = \left(\frac{\text{Secret file size}}{\text{Cover file size}} \times 100\right) \qquad (9)$$

When HC increases, means more secret information can transfer with specific cover file size.

The block length effects directly on the fidelity of the stego file and hiding capacity and it is clearly shown in Table 1. In this test, the files used as cover are male, rock and kid with 220500 samples and secret files are pop, kid, and male with a variety of file sizes. Block length with a different number of samples is used. It shows that when the block length increases, the hiding capacity increases while the fidelity of the reconstructed file decreases and vice versa. Regarding the hiding capacity, the results show that ECA-BM achieves hiding capacity of 80 % of the cover size using Eq. (9) with fidelity SNR on average 69.3 dB of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

stego file using Eq. (7) and block length equal to 28 samples.

Table 1. The Effect of Block Length on Hiding Capacity and Fidelity of the Stego File

Cover Sample	Secret Samples		Block length samples	Hiding capacity %	Stego SNR
Male 220500	Pop	44100	8	20	74.5
		88200	14	40	73.9
		176400	28	80	73.9
Rock 220500	Kid	44100	8	20	69.7
		88200	14	40	69.2
		176400	28	80	69.2
Kid 220500	Male	44100	8	20	64.9
		88200	14	40	64.2
		176400	28	80	64.2

In order to assess the similarity between the original and the reconstructed secret file, NC is used in this test. Various audio types (Pop, Rock, Male, Kid) with different secret file sizes are adopted in this experiment. Speech in music, music in speech and speech in speech are used as a cover and secret files. When this value approximates to 1, it means that the two signals are almost similar. Table 2 depicts the contradictory relation between the block length and the fidelity of the reconstructed secret file. When the block length increases the NC decreases and vice versa. On average, the NC is 0.99992 using Eq. (8).

Table 2. The Effect of Block Length on the Fidelity of the Reconstructed Secret File

Cover Sample	Secret Samples		Block length samples	Reconstructed SNR	NC
Male 220500	Pop	44100	8	40.9	0.99996
		88200	14	38.7	0.99993
		176400	28	36.8	0.99989
Rock 220500	Kid	44100	8	41.6	0.99996
		88200	14	39.1	0.99993
		176400	28	39.1	0.99993
Kid 220500	Male	44100	8	39.5	0.99994
		88200	14	37.9	0.99992
		176400	28	36.9	0.99989

On the other hand, ECA-BM is compared with some previous studies that contribute to enhancing the hiding capacity. In this comparison, we select two studies [5, 8] that employed time domain in embedding process using LSB and three studies [6, 7, 9] are selected that adopted transform domain using wavelet transform in their embedding process. The comparison is conducted based on the hiding capacity and SNR of the stego file. As seen in Table 3 and Fig. 6, the proposed outperforms other methods in hiding capacity by increasing rate to 25% comparing with highest hiding capacity achieved by [8]. Moreover, the fidelity of the stego file is maintained 69.3 dB comparing with [5], [7], [8], [9] and slight reduction of 6.7 dB compared by [6].

Table 3. Comparison of the ECA-BM and some other studies

Study	Hiding capacity (%)	Stego Average SNR	Reconstructed Average SNR
Kekre et al. [5]	47	52	NR
Sheikhan et al. [6]	34	76	NR
Shahadi and Jidin [7]	42	50	NR
Bazyar and Sudirman [8]	55	62	NR
Hemalatha et al. [9]	50	39.3	23.4
ECA-BM	80	69.3	38.9

NR: Not reported

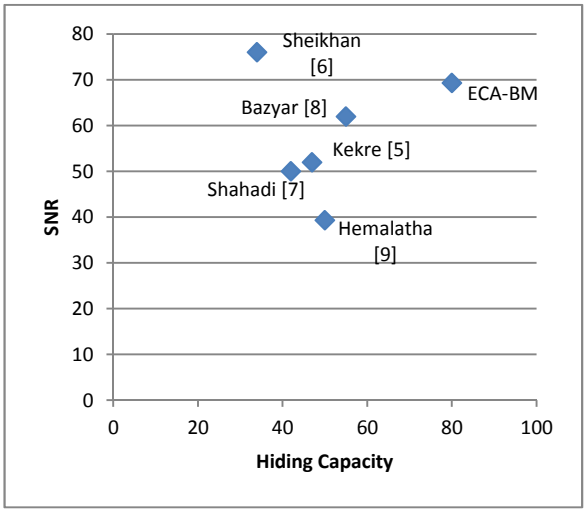

Fig. 6 Comparison of the ECA-BM and some other studies

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

9. CONCLUSIONS

This study proposes an audio hiding scheme using fractal coding and chaotic LSB to improve the efficiency of the audio data hiding. Fractal coding is employed to find a mapping between the secret and cover blocks in order to decrease the amount of the secret data and improve the hiding capacity. Chaotic LSB is adopted as an embedding technique for two reasons, first to enhance the security of ECA-BM and second to maintain the fidelity of the stego. The experimental results exhibit the relation among block length, hiding capacity, the fidelity of stego and retrieved files. The achieved hiding capacity is 80 % of the cover file with maintaining the fidelity of the stego and reconstructed secret file 69.3 and 38.9 dB respectively. Future work of this study is to adopt transfer domain as DCT or DWT in place of LSB embedding technique in order to enhance the robustness of ECA-BM.

10. ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education and Scientific Research, Studies Planning and Follow-up Directorate, Republic of Iraq and Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia for supporting this research.

REFERENCES

[1].Zaidan, B., et al., *On the differences between hiding information and cryptography techniques: An overview.* Journal of Applied Sciences, 2010. **10**: p. 1650-1655.

[2].Ali, A.H., M.R. Mokhtar, and L.E. George, *Recent Approaches for VoIP Steganography.* Indian Journal of Science and Technology, 2016. **9**(38): p. 6.

[3].Nedeljko, C., *Algorithms for audio watermarking and steganography*. 2004: Oulun yliopisto.

[4].El-Khamy, S.E., N.O. Korany, and M.H. El-Sherif, *A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption.* Multimedia Tools and Applications, 2016: p. 1-16.

[5].Kekre, H.B., et al. *Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding*. in *Emerging Trends in Engineering and Technology (ICETET), 2010 3rd International Conference on*. 2010. IEEE.

[6].Sheikhan, M., K. Asadollahi, and R. Shahnazi, *Improvement of Embedding Capacity and Quality of DWT-Based Audio Steganography Systems.* World Applied Sciences Journal, 2011. **13**(3): p. 507-516.

[7].Shahadi, H.I. and R. Jidin. *High capacity and inaudibility audio steganography scheme*. in *7th International Conference on Information Assurance and Security (IAS), 2011* 2011. IEEE.

[8].Bazyar, M. and R. Sudirman, *A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm.* Jurnal Teknologi, 2015. **74**(6): p. 49-53.

[9].Hemalatha, S., U.D. Acharya, and A. Renuka, *Audio data hiding technique using integer wavelet transform.* International Journal of Electronic Security and Digital Forensics, 2016. **8**(2): p. 131-147.

[10]. Parthasarathy, C. and S. Srivatsa, *Increased robustness of LSB audio steganography by reduced distortion LSB coding.* Journal of Theoretical and Applied Information Technology, 2005. **7**(1): p. 080-086.

[11]. Ali, A.H. and L. George, *A Review on Audio Steganography Techniques.* Research Journal of Applied Sciences, Engineering and Technology, 2016. **12**(2): p. 154-162.

[12]. Ballesteros L, D.M. and J.M. Moreno A, *Highly transparent steganography model of speech signals using Efficient Wavelet Masking.* Expert Systems with Applications, 2012. **39**(10): p. 9141-9149.

[13]. George, L.E. and G.A. Mahmood, *Audio Steganography Based on Signal Modulation in Wavelet Domain.* Iraqi Journal of Science, 2010. **9**: p. 10.

[14]. Al-Othmani, A.Z., A.A. Manaf, and A.M. Zeki, *A survey on steganography techniques in real time audio signals and evaluation.* International Journal of Computer Science Issues (IJCSI), 2012. **9**(1).

[15]. Lei, B., et al., *A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition.* Signal Processing, 2012. **92**(9): p. 1985-2001.

[16]. Ibaida, A., D. Al-Shammary, and I. Khalil, *Cloud enabled fractal based ECG compression in wireless body sensor networks.* Future Generation Computer Systems, 2014. **35**: p. 91-101.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[17]. Jacquin, A.E., *Image coding based on a fractal theory of iterated contractive image transformations.* IEEE Transactions on Image Processing, 1992. **1**(1): p. 18-30.
[18]. Sheltami, T., M. Musaddiq, and E. Shakshuki, *Data compression techniques in Wireless Sensor Networks.* Future Generation Computer Systems, 2016.
[19]. Al-Hilo, E. and L.E. George. *Speeding-up Fractal Colored Image Compression using Moments Features*. in *Digital Image Computing: Techniques and Applications (DICTA), 2008*. 2008. IEEE.
[20]. Yu, L., et al., *Improved adaptive LSB steganography based on chaos and genetic algorithm.* EURASIP Journal on Advances in Signal Processing, 2010. **2010**(1): p. 1.
[21]. George, L.E., *IFS coding for zero-mean image blocks.* Iraqi Journal of Science, 2005. **47**(1): p. 190-194.
[22]. Sourceforge, F.i.t. and C.C. Awards. *Marsyas*. 2009 22-11-2015]; Available from: http://marsyasweb.appspot.com/about/.
[23]. Ballesteros L, D.M. and J.M. Moreno A, *Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key.* Computers and Electrical Engineering, 2013. **39**(4): p. 1192-1203.
[24]. Bhat, V., I. Sengupta, and A. Das, *An adaptive audio watermarking based on the singular value decomposition in the wavelet domain.* Digital Signal Processing, 2010. **20**(6): p. 1547-1558.