I. J. Computer Network and Information Security, **2015, 7, 24-29**
Published Online June 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.07.03

An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys

Ali M. Meligy
Department of mathematics, Faculty of science, Menofia University, Egypt
Email: meligyali@hotmail.com

Mohammed M. Nasef and Fatma T. Eid
Department of mathematics, Faculty of science, Menofia University, Egypt
Email: {mnasef81@yahoo.com or Mohammed_nasef@science.menofia.edu.eg, fatma_taher111@yahoo.com or fatma.taher@fa-hists.edu.eg}

Abstract—Steganography is the art of amalgamating the secret message into another public message which may be text, audio or video file in a way that no one can know or imperceptible the existence of message. So, the secret message can send in a secret and obscure way using steganography techniques. In this paper, we use the audio steganography where the secret message conceal in audio file. We use audio rather than image because the human auditory system (HAS) is more sensitive than human visual system (HVS). We propose an audio steganography algorithm, for embedding text, audio or image based on Lifting Wavelet Transform (LWT) transform with modification of Least Significant Bit (LSB) technique and three random keys where these key is used to increase the robustness of the LSB technique and without it no one can know the sort of secret message type, the length of the secret message and the initial position of the embedded secret message in LSB. The performance of our algorithm is calculated using SNR and we compare the values of our proposed method with some known algorithms.

Index Terms—Steganography, Cryptography, Audio Steganography, and Lifting Wavelet Transform

I. INTRODUCTION

The rapid increase in the use of the Internet and also the increase of digital data transmission over the internet led to the necessity to improve the security of the system. Cryptography provide higher level of security but anyone can know that there is a secret message and this problem can be solved by hiding the existence of message where this schema called steganography but it differ from watermarking, [9].

Cryptography is used for secret information where the secret message is encrypted using an encryption key. The third party can know that there is a secret message but can't read it because it is not understandable, unreadable and opaque to anyone unless the decryption key is available. Cryptography advantages are to protect the content of the message and keep it secure from unintended audiences but it doesn't not hide the message and this make suspicious and also the privacy of the data transmission depends only on the secrecy of a key. Watermarking is used for copyright where some information about cover media is hidden in the message. Watermarking advantage is to prevent the illegal copying or claim of the ownership of digital media but doesn't prevent image copying but we can track down and detect ownership of copied image, vanishes if someone manipulates the file, [3, 12].

Steganography is the method or technique that obscures and hides data within a digital media, so that the communication or the exchange of information is in a secret way and the unauthorized person can't predicate the existence of secret message. It is derived from the Greek word steganos which means, covered or secret and graphy means writing or drawing. Therefore, steganography means, covered writing, [15]. The sender embeds the secret message like text , image , audio, video….etc, in the cover media which called host like image or audio or video, and create a stego file then send it to the receiver who extracts the message from the stego file using the key which known by only two parts, [8,10]. Fig.1. illustrate the general diagram of steganography system.

To access an effective steganographic scheme, you should possess the following desired characteristics, [8]:

a) *Secrecy:* no one can extract the secret message from the stego file without the private key.
b) *Imperceptibility:* the stego file should be same as the original file and there is no noise in the stego.
c) *High capacity:* the cover file should be large as possible so that the secret message can embedded in it.
d) *Resistance:* the secret message should not affect by in manipulation which made in the stego file.
e) *Accurate extraction:* when the receiver extract message, it should be accurate and reliable.

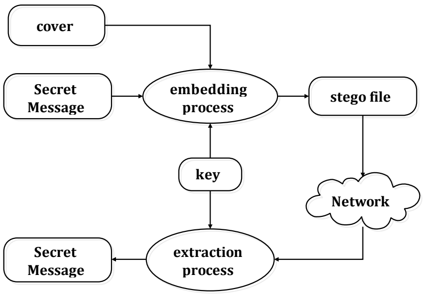


Fig. 1. The general diagram of the steganography system

We use steganography because the secret message is transmitted secretly without discovering the transmission of it where any file(s) over any communication is concealed. Anyone can use steganography for private communications. Audio Steganography techniques can be applied for covert communications using unclassified channels without additional demand for bandwidth or simply for storing data, [2]. Audio steganography is the method of hiding a secret message in digital audio file. We use audio rather than image because the human Auditory system (HAS) is more extensive than human visual system (HVS), [2, 7].

Through this paper, after the introduction in section 2 we view the related work and summarize the idea of each one, in section 3 we explain the proposed method and show the embedding and extraction algorithm, in section 4 we show the results and compare it with some known algorithms, then we summarize the conclusion of this paper and finally the references we depend on our work.

II. Related work

D.M. Ballesteros L, J.M. Moreno A, 2012, [1] proposed method that adapts the Frequency Masking concept using an efficient sorting of the wavelet coefficients of the secret messages and use an indirect LSB substitution for hiding speech signals into speech signals. The proposed method contains four steps: decomposition and pre-scaling by transforming the decimal coefficients of the signals to a binary representation by the Discrete Wavelet Transform (DWT), then using an efficient sorting of the wavelet coefficients of the secret messages, then using an indirect LSB substitution for hiding speech signals into speech signals, and final reconstruct the signals and post-scaling it by applying the inverse wavelet transform.

K.P.Adhiya, S.A. Patil, 2012, [8], proposed method that is converted each audio sample into bits and then the textual information is embedded in it. In embedding process, first the message character is converted into its equivalent binary. The last 4 bits of this binary is taken into consideration and applying redundancy of the binary code the prefix either 0 or 1 is used. To identify the uppercase, lower case, space, and number the control symbols in the form of binary is used. The proposed algorithm gives better result for 16 bit wave audio as compared to 8 bit.

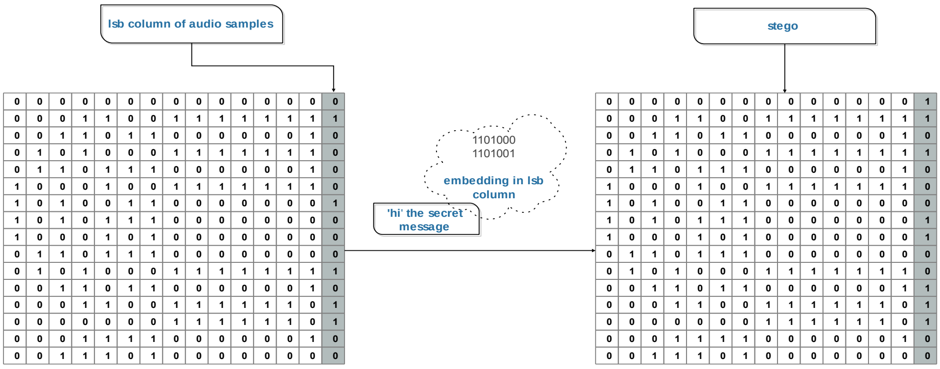
H.I. Shahadi, R. Jidin and W.H. Way, 2014, [5] proposed a new lossless audio steganography approach based on Integer-to-Integer Lifting Wavelet Transform (Int2Int LWT) and Least Significant Bits (LSBs) substitution. The proposed scheme analyze each cover audio frame (4-samples) by using 2-levels of Haar Int2Int LWT ,generate adaptive steganography key (stego-key) that is used for encryption the embedding data and then the first 12-bits from the SM is inserted in the first 6 LSBs after the Starting Depth (SD) from the first and second coefficients of the first detail sub-band, respectively. The reminder 4-bits from the SM are inserted in the first 4 LSBs after the SD from the coefficients of the second detail sub-band then the output stego frame is constructed by performing invers of 2-levels Haar Int2Int LWT after converting all sub-bands to decimal.

R. Tanwar, B. Sharma and S. Malhotra, 2014, [16] proposed a new approach that overcomes the problems of substitution techniques in audio steganography. One problem is that they are less robust against intentional attacks that try to reveal hidden message and second problem is having low robustness against unintentional attacks. The algorithm will hide the message as per the proposed solution (in deeper layers of audio sample and will modify other bits to minimize the error). The method currently uses 2 bits per byte of audio sample. This will progress towards achieving higher capacity and robustness.

N. Gupta and Ms. N. Sharma, 2014, [17] proposed system that aims to provide improved robustness, security by using the concept of DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit) proposed a new method of Audio Steganography. The emphasize will be on the proposed scheme of image hiding in audio and its comparison with simple LSB insertion method for data hiding in audio.

L. Babu, J. John S, B.D, C. Muruganantham and H. S. DivakaraMurthy, August 2013, [18], proposed method that divided sound into samples to be hidden by distributing the bit pattern that corresponds to the secret gray scale image across the LSBs of the preprocessed sound samples. The simplest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information.

M. P. Jain and Prof.V. Trivedi, [19], proposed method that have presented a high capacity and high stego-signal quality audio steganography scheme based on Coefficient comparison in DCT domain where two Coefficients of a segment are compared and based on comparison bits are embedded. The proposed algorithm starts by segmenting the input audio cover signal and then decomposing each segment by using DCT; one represents the DC signal that has the highest power and lowest frequency, while the others are AC signals with decreasing power, starting from the lowest to the highest frequencies details components. Secret message embedding stage is based on comparison of two samples in a segment. All the modified segments, are converted back from frequency domain to time domain. The IDCT is used to reconstruct the segments of stego-signal based on modified AC samples and unmodified DC samples.



0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	0	0	1	1	1	1	1	1	1	1
0	0	1	1	0	1	1	0	0	0	0	0	0	1	0
0	1	0	1	0	0	0	1	1	1	1	1	1	1	0
0	1	1	0	1	1	1	0	0	0	0	0	0	1	0
1	0	0	0	1	0	0	1	1	1	1	1	1	1	0
1	0	1	0	0	1	1	0	0	0	0	0	0	0	1
1	0	1	0	1	1	1	0	0	0	0	0	0	0	0
1	0	0	0	1	0	1	0	0	0	0	0	0	0	0
0	1	1	0	1	1	1	0	0	0	0	0	0	0	0
0	1	0	1	0	0	0	1	1	1	1	1	1	1	1
0	0	1	1	0	1	1	0	0	0	0	0	0	1	0
0	0	0	1	1	0	0	1	1	1	1	1	1	0	1
0	0	0	0	0	0	0	1	1	1	1	1	1	0	1
0	0	0	1	1	1	1	0	0	0	0	0	0	1	0
0	0	1	1	1	0	1	0	0	0	0	0	0	0	0

0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	1	1	0	0	1	1	1	1	1	1	1	1
0	0	1	1	0	1	1	0	0	0	0	0	0	1	0
0	1	0	1	0	0	0	1	1	1	1	1	1	1	1
0	1	1	0	1	1	1	0	0	0	0	0	0	1	0
1	0	0	0	1	0	0	1	1	1	1	1	1	1	0
1	0	1	0	0	1	1	0	0	0	0	0	0	0	0
1	0	1	0	1	1	1	0	0	0	0	0	0	0	1
1	0	0	0	1	0	1	0	0	0	0	0	0	0	1
0	1	1	0	1	1	1	0	0	0	0	0	0	0	0
0	1	0	1	0	0	0	1	1	1	1	1	1	1	0
0	0	1	1	0	1	1	0	0	0	0	0	0	1	1
0	0	0	1	1	0	0	1	1	1	1	1	1	0	1
0	0	0	0	0	0	0	1	1	1	1	1	1	0	1
0	0	0	1	1	1	1	0	0	0	0	0	0	1	0
0	0	1	1	1	0	1	0	0	0	0	0	0	0	0

Fig. 2. LSB method example

III. Proposed Method

Our work is based on LSB technique with some modifications to achieve good method. So, we explain this technique firstly in this section.

A. *LSB CODING (Least Significant Bit)*

It is a very common and one of the earliest methods, which used for hiding information. It is based on embedding the bits of message in the least significant bit of the host which cause less effect in the host signal value and less error compared with the original signal. It allow large amount of data to be concealed within an audio file, [11] and usually not creates audible changes to the host but low robustness against attacks and signal processing modification. Fig 2, illustrates the LSB technique and how you can embed 'hi' message in the audio samples using this technique, [1].

B. *The Embedding And Extraction Process*

In the embedding process, we use three random keys. The first key is used for embedding the type of the secret message "text or audio or image", the second key is used for embedding the length of the secret message and the third is used for skip some of bits randomly to increase the robustness of the LSB. Fig. 3. shows how to apply embedding process.

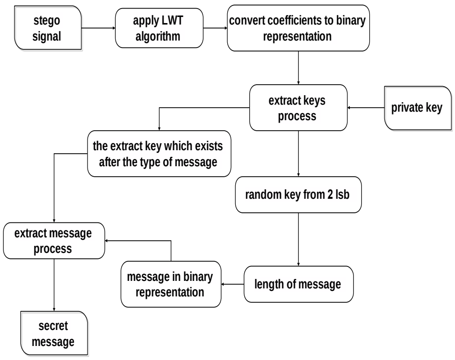


Fig. 3. The general diagram of the embedding process of the proposed method

In the extraction process, the receiver enters the private key which consists of the type of the secret message, skip key and the extract key. The extract key is the number of message characters bit for text message or sample rate for the audio message or the image size for the image message. Fig. 4. shows how to apply extraction process.

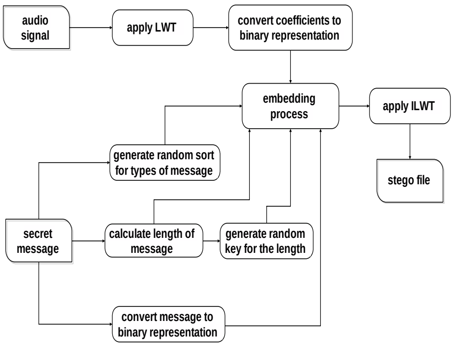

audio signal
apply LWT
convert coefficients to binary representation
embedding process
apply ILWT
stego file
generate random sort for types of message
secret message
calculate length of message
generate random key for the length
convert message to binary representation

Fig. 4. The general diagram of the extraction process of the proposed method

IV. Results

The proposed method was implemented by matlab (2013a) and was tested by several audio signals. The secret message used for embedding is text, audio and image. We calculate the SNR (signal to noise ratio) value and the PSNR (peak signal to ratio) value between cover audio and stego. The Results shown in tables for embedding text, audio, gray image and color image. The SNR is calculated by formula: calculate the SNR (signal to noise ratio) value and the PSNR (peak signal to ratio) value between cover audio and stego. The Results shown in tables [1, 2] for embedding text, audio, gray image and color image. The SNR is calculated by formula:

$$SNR = 10 * log_{10} \frac{\sum_{i=1}^{n} X^{2}(n)}{\sum_{i=1}^{n} [X(n) - Y(n)]^{2}} \qquad (1)$$

The PSNR is calculated by formula:

$$PSNR = 10*\log_{10}\frac{\mathrm{R}^2}{\mathrm{MSE}} \qquad (2)$$

where,

$$MSE = \frac{\sum_1^n [\mathrm{x}-\mathrm{y}]^2}{\mathrm{M*N}} \qquad (3)$$

In the previous equations, x is the original signal, y is the stego signal, M and N are the numbers of rows and columns in the input signals and R is the maximum value of the signal.

We test the proposed method in several steps until achieve the good one. First, we requantize the audio signal to be in 8 bits to use values only between 0 to 255 and to be simple but not give a good SNR. Second, we try to improve the SNR so we don't requantize the audio signals and this get a good SNR. After achieve a good SNR we also need to increase the robustness of the method, so we use the transform domain. We apply the DWT but it gives complex values it makes error when we approximate values and doesn't give the good SNR value, so we use the LWT which are Int2Int values and apply the proposed method in the approximation coefficients (CA) or low frequencies where results shown in Table. 1 and the detail coefficients (CD) or high frequencies where results shown in Table. 2. We find that using CD coefficients give good SNR.

Table 1. SNR and PSNR values for embedding text, audio or image in audio using CA

audio	Capacity (bytes)	payload	Embedded (bytes)	SNR	PSNR
pop	330750	text	36337	83.8934	98.2551
centremic	643462			84.5921	107.1744
vertdisp280cmmic1	659674			76.8611	99.4788
onhold	955821			86.9203	105.7062
narration	555119			83.0921	100.5145
SSeg4	475488			86.1725	108.1330
KSeg3	629760			84.5026	104.5915
guitar	553533			91.3202	104.8788
Average				**84.66929**	**103.5915**
pop	330750	audio	38632	82.4447	102.5082
centremic	643462			77.5557	100.1379
vertdisp280cmmic1	659674			76.5763	99.1939
onhold	955821			87.0809	105.8669
narration	555119			83.2485	100.6709
SSeg4	475488			79.0666	101.0271
KSeg3	629760			84.2404	104.3293
guitar	553533			91.0905	104.6490
Average				**82.66295**	**102.2979**
pop	330750	Gray image	80000	79.3466	99.4101
centremic	643462			74.4834	97.0657
vertdisp280cmmic1	659674			73.5645	96.1821
onhold	955821			83.7669	102.5528
narration	555119			79.9658	97.3882
SSeg4	475488			76.0425	98.0031
KSeg3	629760			81.1910	101.2799
guitar	553533			88.0511	101.6096
Average				**79.55148**	**99.18644**
pop	330750	Color image	227448	74.6022	94.6658
centremic	643462			69.7325	92.3148
vertdisp280cmmic1	659674			68.8417	91.4594
onhold	955821			79.3725	98.1585
narration	555119			75.5676	92.9900
SSeg4	475488			71.3284	93.2889
KSeg3	629760			76.4596	96.5486
guitar	553533			83.3374	96.8959
Average				**74.90524**	**94.54024**

Table 2. SNR and PSNR values for embedding text, audio or image in audio using CD

audio	Capacity (bytes)	payload	Embedded (bytes)	SNR	PSNR
pop	330750	text	36337	87.0258	101.3875
centremic	643462			80.8637	103.4459
vertdisp280cmmic1	659674			80.0185	102.6361
onhold	955821			90.0766	108.8625
narration	555119			86.2406	103.6630
SSeg4	475488			82.4903	104.4508
KSeg3	629760			87.5721	107.6610
guitar	553533			94.4368	107.9953
Average				**86.09055**	**105.0128**
pop	330750	audio	38632	85.4650	105.5286
centremic	643462			80.6182	103.2004
vertdisp280cmmic1	659674			79.7000	102.3176
onhold	955821			90.2191	109.0050
narration	555119			86.3984	103.8208
SSeg4	475488			82.2085	104.1690
KSeg3	629760			87.3555	107.4445
guitar	553533			94.2845	107.8430
Average				**85.78115**	**105.4161**
pop	330750	Gray image	80000	82.3727	102.4363
centremic	643462			77.4890	100.0713
vertdisp280cmmic1	659674			76.5991	99.2168
onhold	955821			86.8618	105.6478
narration	555119			83.0621	100.4845
SSeg4	475488			79.0929	101.0535
KSeg3	629760			84.2401	104.3291
guitar	553533			91.0905	104.6490
Average				**82.60103**	**102.236**
pop	330750	Color image	227448	77.8876	97.9512
centremic	643462			72.9919	95.5741
vertdisp280cmmic1	659674			72.0899	94.7076
onhold	955821			82.4114	101.1973
narration	555119			78.5804	96.0028
SSeg4	475488			74.5938	99.8165
KSeg3	629760			79.7276	99.8165
guitar	553533			86.6108	100.1694
Average				**78.11168**	**98.15443**

Table 3.Comparison of SNR for proposed method with some known algorithms

Researchers/algorithm	SNR
M.P. Jain, P.V. Trivedi,**[9]**	54.69
K.P.Adhiya ,S.A. Patil,**[8]**	68
S.K. Bandyopadhyay, B. Datta, **[13]**	54.7
H.B. kekre, A.Athawale, S.Rao and U.Athawale,**[4]**	68.08
D.Pal, N.Ghashol,**[2]**	64.4402
Proposed algorithm	**83.1461**

V. Conclusion

In this paper, we have presented an audio steganography technique based on LWT and modified LSB technique by using three random keys. We used the three random keys to increase the robustness of the LSB. Also, we used LWT rather than other techniques to avoid the rounded error of the approximate values as LWT is INT2INT transform values. We tested our proposed method by SNR and PSNR. From the result values, we find that using CD coefficients is better than CA coefficients in the embedding process. This because that CD is high frequencies and the change of it is very low and doesn't make a perceptual effect after reconstructed the audio signal. Also, the SNR values of our proposed method are better than other known methods.

References

[1] D. M. Ballesteros L and J. M. Moreno ," Highly transparent steganography model of speech signals using Efficient Wavelet Masking " *Expert Systems with Applications*, vol .39, 2012.

[2] D. Pal and N. Ghashol, "A robust audio steganography scheme in time domain," *International Journal of computer Applications*, vol.80-No.15, October 2013.

[3] F. Djebbar, B. Ayad, K. A Meraim and H. Hamam," Comparative study of digital audio steganography techniques" *EURASIP Journal on Audio, Speech, and Music Processing*, 2012.

[4] H.B. kekre, A.Athawale, S.Rao and U.Athawale, "Information Hiding In Audio Signals," *International Journal of computer Applications*, vol.7-No. 9, October 2010.

[5] H.I. Shahadi, R. Jidin and W.H. Way, "Lossless Audio Steganography based on Lifting Wavelet Transform and Dynamic Stego Key," *Indian Journal of Science and Technology*, Vol 7-No. 3, March 2014.

[6] K. Gandhi and G. Garg," Modified LSB Audio Steganography Approach" *International Journal of Emerging Technology and Advanced Engineering,* Vol 3, Issue 6, June 2013.

[7] K. Gopalan," AUDIO STEGANOGRAPHY USING BIT MODIFICATION" *Multimedia and Expo, 2003. ICME '03.Proceedings*. 2003 International Conference, Vol. 1, July 2003.

[8] K.P.Adhiya and S.A. Patil,"Hiding Text in Audio Using LSB Based Steganography" *Information and Knowledge Management,* Vol 2-No.3, 2012.

[9] M.P. Jain and P.V. Trivedi, "Effective Audio Steganography by using Coefficient Comparison in DCT Domain," International Journal of Engineering Research & Technology (IJERT*)*, Vol. 2, Issue 8, August – 2013.

[10] N.A. Malhotra and N. Tahilramani,"Survey on Speech and Audio Steganography Techniques in Temporal, Transform and Coded Domains", *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 4, Issue 3, March 2014.

[11] N.Cvejic and T. Seppanen," Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding" *Journal of Universal Computer Science*, vol. 11, 2005.

[12] S. Bhattacharyya, A.Kundu and G. Sanyal," A Novel Audio Steganography Technique by M16MA" *International Journal of Computer Applications,* Vol30–No.8, September 2011.

[13] S.K. Bandyopadhyay and B.Datta, "Higher LSB Layer Based Audio Steganography Technique" *The International Journal on Electronics & Communication Technology IJECT,* Vol. 2, Issue 4, 2011.

[14] S.K.Bandyopadhyay1 and B.GBanik2,"Multi-Level Steganography Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique" *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* Vol 1, Issue 2, August 2012.

[15] P. Jayaram, H.R Ranganatha and H.S. Anupama H S," Information Hiding Using Audio Steganography – A Survey" *The International Journal of Multimedia & Its Applications (IJMA),* Vol.3-No.3, August 2011.

[16] R. Tanwar, B. Sharma and S. Malhotra, "A Robust Substitution Technique to implement Audio Steganography" *International Conference on Reliability, Optimization and Information Technology (ICROIT),* Feb 6-8 2014.

[17] N. Gupta and Ms. N. Sharma, "Dwt and Lsb Based Audio Steganography" *International Conference on Reliability, Optimization and Information Technolog (ICROIT),* Feb 6-8 2014.

[18] L. Babu, J. John S, B.D, C. Muruganantham and H. S. DivakaraMurthy, "Steganographic Method for Data Hiding in Audio Signals with LSB & DCT", *International Journal of Computer Science and Mobile Computing,* Vol.2 Issue. 8, August- 2013.

[19] M. P. Jain, Prof.V. Trivedi "Effective Audio Steganography by using Coefficient Comparison in DCT Domain", *International Journal of Engineering Research & Technology (IJERT),* Vol. 2, Issue 8, August – 2013.

Authors' Profiles

Ali M. Meligy is a professor of computer science at the Menofia University in Egypt. Previously, he was the head of computer science and information technology departments at Al-Hussein Bin Talal University in Jordan. His research interests include parallel processing and applications, distributed systems, Petri nets, and reuse-based software engineering.

Mohammed M. Nasef was born in Egypt March 10th 1981. He received the M.Sc and Phd. Degree in computer science at the faculty of science, Menofia University, Egypt in 2007 and 2011, respectively. His research interests include artificial intelligence, audio steganography, audio classification, and audio retrieval. Currently he is a lecturer of computer science in faculty of science, Menofia University, Egypt. Member of the faculty projects for education development as DSAP and CIQAP. He is the manager of It-Unit, Faculty of science, Menofia University since 2013 until now.

Fatma T. Eid is a demonstrator of computer science at Higher Future Institute for Specialized Technological Studies (Future Academy) in Egypt. She was born in Menofia, Egypt, in 1991. She received the BSc degree in pure Mathematics and Computer Sciences in 2012, from the Faculty of Science, Menofia University, Egypt.