International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.405-414
http://dx.doi.org/10.14257/ijsia.2014.8.6.35

A Recent Review of MP3 Based Steganography Methods

Mohsen Bazyar and Rubita Sudirman*

Faculty of Electrical Engineering, University Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia
Mohsenbazyar114@yahoo.com, rubita@fke.utm.my

Abstract

Steganography, the idea of hiding messages and data within other pieces of data, can be useful in many real world applications alongside encryption and other code-writing methods. Data hiding methods are a new kind of technology in secret communication. Multimedia objects like audio are the most used in today's information hiding systems. Audio file due to its high degree of redundancy and high data transmission rate can create a good hiding medium. Several formats such as MP3 have been used in audio data steganography. Varieties of methods have been established for embedding data in digital audio. In this article, in addition to more emphasis on MPEG-1 layer III (MP3) steganography methods with thorough information about weaknesses and strengths of these techniques, we present a complete study of audio file steganography approaches.

Keywords: *MP3, Steganography, LSB method, Audio data hiding*

1. Introduction

The infrastructure of digital media distribution has grown rapidly in the last few years and provides an excellent opportunity for hidden data transmission. Digital steganography has received significant attention recently and it is used to hide data in carriers like digital video, images or audio so that only the intended recipient is capable of retrieving the embedded data. Secret messages are embedded in digital audio in a computer based audio steganography system. The hidden message with a little changing the binary sequence of an audio file is embedded. Existing audio steganography software can embed messages in AU, MP3, and even WAV sound format [1]. With the advent of the Internet, computer users started to distribute, share, and transmit their private data online in a complete overt manner. As a result, securing these data became a critical issue for everyone. Steganography and cryptography are two security methods that provide data confidentiality [2-3]. The purpose of both Cryptography and Steganography methods is information protection in a digital world. The existence of the hidden message is visible to everyone in cryptography, but In Steganography, the receiver and the sender know the existence of the hidden message solely. That is why the majority of experts would propose using both of them to improve the layers of security. Steganographic techniques play an important role at privacy on open system and the future of Internet security. According to this, Steganography methods eliminate the undesirable interest coming to the embedded message. Cryptographic techniques attempt to preserve the message, while steganographic methods try to hide the message along with its content. Actually, when the use of cryptography is forbidden, the steganography can be useful. Steganography can circumvent such policies to pass the message covertly where cryptography and strong encryption are outlawed [4].

Therefore, cryptography and steganography differ in the way they are evaluated: cryptography fails when the enemy detects that there is a hidden message present in the

* Corresponding Author

ISSN: 1738-9976 IJSIA

steganographic medium, but for steganography happens when the enemy can access to the content of the hidden message. Steganography has invited substantial research interests in digital audio and many methods have been proposed based on the feature of the human auditory system (HAS) and digital audio signals [5]. Transparency, capacity and robustness are three most fundamental properties of audio steganographic algorithms.

The remainder of the article is organized as follows: introduce the MP3 file structure and audio steganography, present the existing techniques in MP3 steganography, after that provide conclusion and discussion.

2. Audio Steganography

The Audio file can be used to hide information. Steganography is often used in copyright audio file to protect the rights of music artists. Phase coding, least significant bit insertion, echo hiding and spread spectrum coding are the Techniques which can be used to safeguard the content of the audio file. The biggest challenges face all these methods is the sensitivity of the human auditory system (HAS), it is so sensitive, such that people can often pick up randomly added small noise, and this making hard to successfully hide data within audio data [6-7]. Audio steganography is the practice of hiding the message into another medium such as hiding the information into the audio file. The confidential information is hidden in an audio. Though information is hidden, the perception of an audio does not change. The basic model of audio steganography consists of data which we need to hide, stego key and cover file [8]. Parameter, of the basic model is shown in the Figure 2. The term cover file refers to the medium that require hiding the data into audio [9]. A message that has to be hidden are in various forms like video, audio, images.

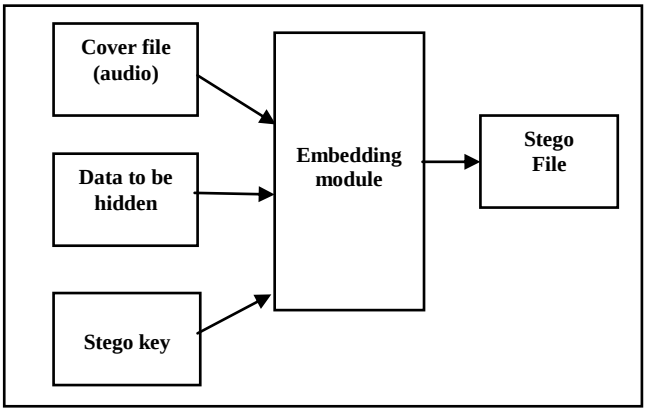

Figure 1. Basic audio Steganography

MPEG1, MPEG2 Layer III (MP3), Waveform audio or other files utilize as a cover of steganography in audio Steganography. Also for embedded messages can use different type of files like speech or text. In digital audio the most common of compression format is MP3 [10].

There are two ways for Mp3 steganography methods: embedding the information when they are compressed or after compression [11].

3. Embedding During Compression

3.1. Least Significant Bit (LSB)

In the scope of steganography, LSB coding is one of the earliest methods that studied in hiding information. In this method least significant of binary sequences of each

digitized audio sample is replaced with the secret message binary equivalent [12-13]. LSB coding permits to a large amount of information to be encoded by replacing a binary message with the least significant bit of each sampling point. 1 kbps per 1 kHz is the ideal data transmission rate in LSB coding. Although, replacing two message bits with two least significant bits of a sample raises the data amount which can be embedded but this lead to raises the noise amount in the original file. Therefore, before choosing the LSB we must consider the used signal content. For instance, an audio file would mask low-bit encoding noise when it was recorded in a bustling subway station. However, the same noise would be heard in an audio file including a piano. The recipient requires access to the sample indices sequence to extract a hidden message inside an LSB encoded audio file which utilize in the embedding step. Typically, the all number of samples in an audio file are more than the length of the encoded secret message. First should decide then on how to select the subset of samples which will contain the hidden message and communicate that decision to the receiver. One simple approach is to start at the beginning of the audio file and perform LSB coding method until the message has been totally embedded, leaving the remaining samples unchanged. It generates a security problem, anyway, statistical feature of the second length of the message. Despite the simplicity of the LSB, the inefficiency of this method raises the signal to noise ratio of the audio file. Furthermore, during the process of utilizing component of the audio file which was not modified is different Compared with the first component of the audio file. Padding the hidden message with random bits is one way to solve this problem that the total number of samples is the same with the both one layer and LSB multilayers the embedded hidden data are most likely to get lost communication. Generally, the LSB robustness can be attained by implantation of a redundancy method along with the encoding of the embedded message. This redundancy approach is a promising method for LSBs to the decrease of transmission rate.

3.2. Echo Hiding

This method adds an echo to the main audio signal to embedding Information within an audio file. Three echo parameters are important to embedding data: decay rate, offset and initial amplitude. Just one bit of information can be encoded, If only one echo is created from the original signal. It becomes more difficult for the human ear to separate among the two signals as the delay decrease between the echo and the original audio [14].

Furthermore, offset to show the binary message is varied. A binary one is shown by the first offset, and binary zero by a second offset value. Just one information bit can be encoded, if just one echo from the original signal is created. Thus, before starting the encoding process the original signal is broken into the blocks. The blocks are combined together when the encoding process is finished to produce the last signal. There is just an original signal among all blocks of signals which are concurrently encoded until the last signal is finished, this is the challenge in echo hiding method. End of the data is deciphered among the signal cluster at the receiver that used to encode them until the original signal is obtained. To decipher the information a robust technique was investigated by [14].

3.3. Phase Coding

Phase coding method depends on this fact that the phase of sound components is not compressible to the human auditory system, unlike the noise and it addresses the disadvantages of the noise based methods of audio Steganography.

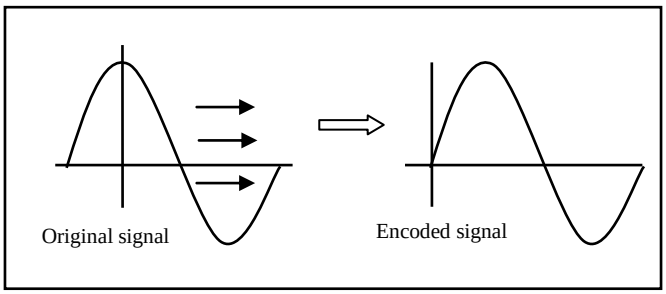

Figure 2. Phase Coding

Table 1. Recent Work in Embedding During Compression Methods

Techniques name	Authors	Abstract	Results
Least significant bit	H. B. Kekre, A. Athawale, B. S. Rao, U. Athawale	Propose 2 new techniques for substitution of audio steganography, which enhances the capacity of cover audio for embedding additional data.	Improve data hiding capacity of cover audio by 35% to 70% as compared to the standard LSB algorithm.
	G.Kaliappan S.Qidong	Presents some results of the tradeoff between the conflicting requirements of payload, data robustness, and imperceptibility.	Experimental results show that noise tolerance increased by using higher bit indices than the traditional LSB and noticeability of embedding is decreased while the payload can be as high as over 3000 bits/s.
	Shirali-Shahreza, S. Manzuri-Shalmani, M.T.	Develop ideal reconstruction filter banks that are Int2Int and hide data in least significant bits (LSB) of details coefficient in an adaptive approach to decrease the error rate.	Having zero error rate for hiding capacity below 100 kilobits-per-second (kbps) and 0.3% error for 200 kbps, in comparison to 0.9% error of the normal wavelet domain LSB.
Phase coding	Matsuoka, H.	Presents an improvement of spread spectrum audio data hiding methods.	The new method creates the quality degradation at the same level of NMR +3dB, but access +6dB noise, and has 3dB benefits.
	Nikhil Parab, Mark Nathan, K. T. Talele	Proposes a new method of camouflaging a block of binary data for secured covert communication in an audio file.	This novel technique provides noise insensitivity robustness, high data capacity, and almost accurate data recovery from the cover signal.
Echo hiding	Hamza Ö zer, İsmail Avcıba, Bülent Sankur, Nasir Memon	Present a statistical method to detect the presence of secret messages in audio signal data.	Experimental results indicate that the new technique can be utilized to detect the presence of secret messages in digital audio signal.
	M.Sameer M.Sathiamoorthy	Proposes a scheme that improves the robustness of echo hiding.	It improved the message recovery rate of echo hiding by encoding the messages with T-codes, a set of self-synchronizing codes.
Spread spectrum	Delforouzi, A. Pooyan, M.	A new approach for digital audio steganography is presented where encrypted covert data is embedded into the coefficients of host audio in integer wavelet domain	The characteristics of this method are high audio quality, large pay load and full recovery.
	Zhang Kexin	Present two algorithms based on machine learning theory and discrete wavelet transform (DWT) for steganalysis SS hiding.	The experimental results of both two proposed algorithms may obtain better detecting performance.
	Xin Li Hong Heather Yu	This paper studies audio data hiding in the subband domain using the spread spectrum (SS) technique.	Experimental results have shown that the data hiding scheme in the subband domain can survive a wide range of attacks while providing transparent audio quality

Phase coding works by replacing a reference phase, which shows the information with the initial audio phase segment. To keep the relative phase among the segments the phase of other segments is adjusted.

Generally, Phase coding replays a reference phase, which shows the hidden data with the phase of an initial audio segment. This can be thought of, as sort of an encryption of the audio signal by using Discrete Fourier Transform (DFT) that is a transformation algorithm for the audio signal. Having low data transmission rate and complexity are disadvantages of this method [15].

A new approach is proposed to cut down the correlation complexities that have a problem in accomplishing quality of signal at the receiving end in [16]. In the other

survey a new method is introduced to develop of stage coding for more robustness and capacity, which inserts bits of information using changed stage modification [17]. By comparing different methods, we can find that to achieve robustness and capacity of the phase coding, the choice of stage in amplitude of the signal increases the noise resistance of the Stage signal. The performance of the steganography method can be tuned to achieve better performance if the degree of difference is calculated beforehand between the end to end frequencies of stage encoding.

3.4. Spread Spectrum

Frequency-hopping schemes and the direct-sequence are two versions of Spread spectrum, which can be used in audio Steganography. This method efforts to spread out the encoded information throughout the existing frequencies as far as it possible. It is like a system that uses the LSB coding implementation which spreads the bits of the message over the audio file randomly. On the other hand, the SS technique, unlike the LSB method, spreads out the hidden message throughout the frequency spectrum of audio file utilizing a code which is independent on actual signal and plays an important role in military, secure communications and commercial [18].

Spread spectrum encodes the audio over almost the entire frequency spectrum. It then transmits the audio over different frequencies which will vary depending on what spread spectrum method is used. Direct Sequence Spread Spectrum (DSSS) is one such method that spreads the signal by multiplying the source signal by some pseudo random sequence known as a (CHIP). The sampling rate is then used as the chip rate for the audio signal communication. Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. The advantage of this method is keeping the robustness simultaneous with moderate data transmission rate. The Spread spectrum technique can provide better data transmission rate and has the capability to protect high level of robustness in Comparison with the phase coding and LSB coding techniques. Creating noise in audio file is disadvantage of this method.

4. Embedding After Compression

Embedding data after compression owing to the difficulty that has because of embedding in a compressed signal has not been widely studied. In steganography process, Signal compressions before use as a material medium for embedding data results in poor spread of hidden messages and also change the quality of signal sound. While another aspect of the inserting message that embedding data during compression doesn't change the quality of signal which means that the SNR (signal to noise ratio) of the technique of hiding the undisclosed message while compression is actually low. A number of examples are described for embedding data after compression for both unused and used audio data [19].

4.1. Embedding in Unused Audio Data

An unused audio data frame consists of padding byte stuffing, unused header bit, between frames and before all frames.

4.1.1. Embedding in Unused Header Bit: The headers of MP3 frame that its utilization are generally disregarded in number of MP3 players are constructed from the original bit, private bit, copyright bit and emphasis bit. They are the one of the essential factors to interpretation of hidden data in an audio signal. This field by replacing the bit stream of hidden massage can embed the secret message through the field. Furthermore, the real

content of hidden message inside the frame may be lost and will make challenge in recovery the signal if the replacing process of the bit in the field and bit stream fails. S. Divya studied on a new approach in audio steganography by using of four bits in each header of frame to obtain better robustness and capacity through the audio signal to hide undisclosed messages [20].

4.1.2. Embedding in Padding Byte Stuffing: One of the methods that recently established for audio steganography is padding byte stuffing. Its technique is relatively direct in terms of execution. Storage capability and having the ability to program 1 byte of data to every frame are the strength points of this approach. The best example of material medium because of allowing for numerous of frames in a hidden message which can use the padding byte stuffing approach is MP3 file [21].

4.1.3. Embedding in Before All Frames: A new approach to developing the before all frames (BAF) is proposed in [22]. This method embeds text message to MP3 audio file. To improve the security of secret message, the text message is hidden by using the RSA approach. With hidden information the first frame will be filled. This process until the frame headers are completed is continued. For MP3 file, about 30 KB capacity is used when encryption algorithm is not used otherwise it needs about 15 KB. Despite the fact that there is the probability to reveal the hidden message for this method, the number of advantages is enough to cover it. For example, the padding method and the unused bit provide more encoding capability even after the frames must have been filled.

4.1.4. Embedding in Between Frames: The author use embedded between frames (BF) approach to developed steganography algorithm in [23-24]. It also hides data within bits format to enhance the security of hidden secret messages by utilizing the RSA technique and same the BAF technique embeds text message to MP3 audio file. The difference between BF and BAF is on the method used in inserting text file within the frames. It selects one frame except the first frame that it sees. However, the BF capacity, which needs 80 MB on original format in comparison with the BAF uses about 40 MB with the encryption algorithm. BF despite having a good capacity for inserting the text is still not resistant against attacks.

Table II. Comparison of Different Methods for Embedding After Compression

Methods	Techniques name	Summary	Strength	Weakness
Embedding after compression	*Unused bit*	In this technique the secret message can embedded in unused bit in header of the frame. In the frame header can find 2 0r 3 unused bit.	Simple	Low robustness and security
	Padding byte stuffing	In the Mp3 frames can find some byte stuffing that use for making the all frame in mp3.	Efficient simple	Not in all Mp3 Low robustness and security
	Between frames	In this approach can embed the secret message after the end of the frame and before the start of the next frame	High capacity simple	Low robustness
	Before all frames	This method can be embedded secret message before all frame start	Low capacity	Low security

This technique provides a platform that is prone to attack because the content of the secret message sent can be easily deciphered by a third party sniffing through the communication link. It also provides only limited capacity for undisclosed message embedding. Therefore, the capacity problem can be solved if the LSB method is utilized to embed speech in MP3 audio file with 8-bit for sample (2, 3 and4 bit exchange) in audio

data to solve the security problem, the use of the key as a lock for hidden secret message is an access method which can obtain maximum security for hidden secret messages.

4.2. Embedding in Used Audio Data:

A new algorithm that uses M16MA and M4M in audio file for embedding the secret message is shown in [25-26]. Due to M16M these algorithms were developed in types of Images. The M4M which is a mathematical function, maps two bits of the hidden message in the required slot utilizing a pseudo random number for embedding the bits of hidden message in a random process in a precise manner. The algorithm which is the best method of insertion worked in an independent manner that the data nature is determined afore hand to be concealed. The M16MA was also improved for deciding on the embedding place. It utilized some statistical function to map each four bit of the hidden message in the pre-determined place. Furthermore, for insert hidden message bits to its location on random basis, it uses a pseudo randomly created number. As a result of its self-determining concept the least possible degradation of concealed audio signal was created through lowest amount degradation.

5. Discussion

The imperceptibility, robustness and capacity are the three main features that show the weaknesses and strength of the MP3 methods in Steganography. Encoding secret messages because of the human auditory system (HAS) that can listen over in audio owing to its dynamic range is the most challenging method to use in Steganography technique. We summarized the weaknesses and strength points of the techniques that used for MP3 Steganography.

6. Conclusion

In this study, we had a survey on audio steganography recent research. Due to that, some basic concepts of audio steganography and HAS including Phase Coding, Least Significant Bit (LSB) Coding, Echo data hiding and Spread Spectrum (SS) were covered. Two common methods of MP3 steganography were presented (embedding during and after compression). Various methods have been discussed for improving imperceptibility, robustness and capacity along with their weaknesses and strength.

For each method based on the Weaknesses, we expressed conclusion and tried by introducing a proposed method can archive to the better result. Nevertheless, in embedding after compression approaches success can be attained if the decoding and encoding process do not perform during the embedding process. Security of hidden information is the best since they travel during communication line using the methods which embed data after compression.

Acknowledgment

The authors would like to thank Universiti Teknologi Malysia for funding the research under vot 05H37. We also would like to thank our research group in supporting and giving positive comment to improve our paper.

Reference

[1] A.B.Gadichal, “Audio Wave Steganography”, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol. 1, No. 5, **(2011)** November, pp.174-176.
[2] P.K. Singh, H. Singh, and K. Saroha, “A Survey on Text Based Steganography", In Proceedings of the 3rd National Conference, **(2009)**, pp. 3-9.
[3] D. Poulami, B.Debnath, K.Tai-hoon “Data Hiding in Audio Signal: A Review”, International Journal of Database Theory and Application, Vol. 2, No. 2, **(2009)** June.

[4] H.B.Kekre, A.Archana, R.Swarnalata, A.Uttara, "Information Hiding in Audio Signals", International Journal of Computer Applications, Vol. 7, No. 9, **(2010)** October.
[5] S. Wang, X. Zhang, and K. Zhang, "Data Hiding in Digital Audio by Frequency Domain Dithering," MMMACNS, Springer-Verlag, Berlin Heidelberg, **(2003)**, pp.383-394.
[6] I. Avcibas. Audio Steganalysis with Content-independent Distortion Measures. IEEE Signal Processing Letters, **(2006)**, 13(2):92-95.
[7] K. Shah, V.R. Lakshmi Gorty, and A. Phirke , "Audio Steganography Using Differential Phase Encoding", ICTSM 2011, CCIS 145, Berlin Heidelberg, **(2011),** pp.146-151.
[8] J.Vivek, K.Lokesh, S.M.Madhur, S.Mohd K.Sadiq, "Public-Key Steganography Based On Modified Lsb Method" Journal of Global Research in Computer Science ,Vol. 3, No. 4, **(2012)** April.
[9] P.Supurovic, "Mpeg Audio Compression Basics", URL: Http://Www.Chested. Chalmers, **(1998)**.
[10] C.Nedeljko, S.Tapio, "Increasing the capacity of LSB-based audio steganography", FIN-90014, Finland, **(2002)**.
[11] K.Arvind, K. Pooja, Steganography "A Data Hiding Technique", Research paper, International Journal of Computer Applications, Vol. 9, No. 7, **(2010)** November.
[12] Sridevi R., Damodaram A., SVL.Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security", Journal of Theoretical and Applied Information Technology, Vol. 5, No. 6 **(2009)** June.
[13] N. Cvejic, T.Seppanen, "Increasing robustness of LSB audio steganography using a novel embedding method," In Proc. IEEE Int. Conf. Info. Tech.: Coding and Computing, Vol. 2, **(2004)** April, pp. 533-537.
[14] F.Djebbar, B. Ayad, K. Abed-Meraim and H. Hamam, "A view on latest audio steganography", 7th IEEE International Conference on Innovations in Information Technology, **(2011)**.
[15] Y.Yardimci, A.E.Cetin and R.Ansari, "Data hiding in speech using phase coding", ESCA. Eurospeech97, Greece, **(1997)** Sept, pp. 1679-1682.
[16] M.Shaveta, S.Arpinder, "A Review of Methods and Approach for Secure Steganography", International Journal of Advanced Research Computer Science and Software Engineering, vol 2, No. 10, **(2012)** October, pp. 67-70.
[17] N. Cvejic, T. Seppanen, "Increasing the capacity of LSB based audio steganography." IEEE Workshop on Multimedia Signal Processing, **(2002)**, pp. 336-338.
[18] M. Nutzinger, Real-time Attacks on Audio Steganograhy. Journal of Information Hiding and Multimedia Signal Processing. Vol. 3, No. 1, **(2012)** January.
[19] B.K.Samir and B.G.Barnali "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique", International of advanced research in computer science, Vol. 1, No. 2, **(2012)** July.
[20] M.Ram Mohan Reddy S.S Divya. "Hiding text in audio using multiple lsb steganography and provide security using cryptography". International Journal of Scientic Technology Research, Vol.1, No. 6, Shobha lokhande. **(2012),** pp.68-70.
[21] Teoh Suk Kuan Rosziati Ibrahim. "Steganography algorithm to hide secret message inside an image", Computer Technology and Application, , **(2011),** pp.102-108.
[22] A.I. Al-Attili, A.A. Osamah, "New technique for hiding data in audio file", IJCSNS International Journal of Computer Science and Network Security, Vol. 10 No .7, **(2010)** July.
[23] B. Chen, "Design and analysis of digital watermarking, information embedding, and data hiding systems," Ph.D. dissertation, MIT, Cambridge, MA, **(2000)** June.
[24] Matsuoka, H., "Spread Spectrum Audio Steganography using Sub – band Phase Shifting", Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP' 06), IEEE, **(2006)**.
[25] Bhattacharyya, S, A Novel Audio Steganography Technique by M16MA. International Journal, Vol. 30, No. 8,.**(2011),** pp**.** 26- 34.
[26] Chen and G.W. Womell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding", IEEE Transactions on Information Theory, Vol. 47, No. 4, , **(2001)** May, pp. 1423-1443.

Authors

Mohsen bazyar, was born in Boshehr, Iran in 1986, and has since lived in Boshehr for the past 27 years. His primary school was Okhovat and secondary was Hedayat, Boshehr. He received his Bachelor and Master's degree from the Islamic Azad niversity of Boshehr in May of 2008 and 2011 respectively, and his Ph.D. in Electrical Engineering has been started from Universiti Teknologi Malaysia in July of 2012.

Rubita, was born in Kampung Parit Puteri Menangis, Pontian, Johor in 1970s, She received her Bachelor and Master degree from the University of Tulsa in May of 1994 and 1996 respectively, and her Ph.D. in Electrical Engineering from Universiti Teknologi Malaysia in July of 2007. In addition to her teaching and research activities, Rubita acts as an advisor for several final year projects and she has been granted with 4 intellectual property rights, 2 copyright software, wrote 18 book chapters, 2 research monographs, and a number of journal and conference proceeding papers. She also published 2 books on electronics.