Journal of Computing and Security

July 2016, Volume 3, Number 3 (pp. 175–182)

http://www.jcomsec.org

A New Hybrid Method for VoIP Stream Steganography

Hossein Moodi [a,*] Ahmad R. Naghsh-Nilchi [b]

[a] *Computer Engineering Department, Birjand University of Technology, Birjand, Iran.*

[b] *Computer Engineering Department, University of Isfahan, Isfahan, Iran.*

ARTICLE INFO.

Article history:

Received: 16 May 2016

Revised: 01 June 2017

Accepted: 15 October 2017

Published Online: 10 February 2018

Keywords:

Steganography, VoIP, LACK, Digital Data Network.

ABSTRACT

In this article, a new stream steganography method for real time digital data network environment with the focus on VoIP is presented. This method consists of a combination of Least Significant Bits (LSB) algorithm and an algorithm called LACK, which is based on the delayed packets in VoIP streams, and forms a new algorithm called LASB (LACK-LSB combination). The combination allows both the reduction of detection probability of stegano data and the use of LSB high capacity as well as being more robust because of diversifying the source of data embedding. That is, by combing these two methods the probability of detection existing steganography data is reduced extensively. Moreover, in the case of detecting stegano data, the potential eavesdropper is not able to easily reconstruct it. To show the performance, both LACK and LSB algorithms are implemented and are compared with the new LASB algorithm in the VoIP environment in terms of capacity, eavesdropping and robustness under several attacks. The experimental results show that LASB is superior to both LACK and LSB in many aspects.

1 Introduction

Along with spreading of the use of Internet throughout the world, the request for VoIP services has increased significantly. The most significant feature of VoIP is that it costs less than PSTN services offered by conventional telecommunication companies. In this context, information security is a very important and a central issue. Open environment property of Internet makes communicating secret data in the form of steganography much more tempting. Other forms of sending secret data include cryptography, however, in a real time digital data communication, such as VoIP, the steganography method works more efficiently. This is because in a real time environment, time is the top priority; and cryptography methods usually need much more time to encode and decode information [1]. In addition, stegano data is less suspicious for the eavesdroppers. There are a number of methods offered by researchers to achieve this goal. Note that the real time steam communication can be classified into two categories: video and voice. Real time voice which is the field under this research mostly focuses on VoIP [2–5]. Note that there is a wider range of researches on video steganography. For example, some researchers offered promising algorithms for data steganography in the output of electronic advertisement billboard [6, 7]. In addition, data steganography of video clip and digital cinemas were discussed in [8]and [9]respectively. Focusing of the real time voice steganography in a network, Mazurczyk etc. offered a comprehensive classification for network steganography up to the publication of their manuscript [3]. Their classification is modified to include our new LASB method and it is

* Corresponding author.

Email addresses: hmoodi@birjandut.ac.ir (H. Moodi), nilchi@eng.ui.ac.ir (A. R. Naghsh-Nilchi)

ISSN: 2322-4460

shown in Figure 1.

Based on this classification, the network steganography methods are divided in three parts, modification of packets, modification of time relation, and the hybrid methods. In modification of packets steganography methods, network protocol headers or payload fields is modified. Modification of free/redundant header's field in IP, User Datagram Protocol (UDP) or Real-Time Transport Protocol (RTP) protocols during discussion stage is one example of these methods [5]. Another one is data hiding audio packets by use of audio watermarking such as Direct Sequence Spread Spectrum (DSSS), Quantization Index Modulation (QIM), and Least Significant Bit (LSB) [10, 11]. These methods usually allow high volume of data to be transferred in a hidden manner. In addition, it is easy to implement them. However, it is easily detectable! Another disadvantage of these methods is that due to the occupation of some of the fields by hidden data, some of the protocol functionality is reduced. The modification of time relation, which is to modify the timing of the relation packets, is done by modifying the sequence of RTP packets, inter-packet delay or introducing packets as damaged or lost ones [12–14]. There also are methods that combine the two ideas, making a hybrid steganography category. In these methods, not only the content of packets is modified but also the inter-packet?s time relations are modified. We can refer to them as Lost Audio Packets Stenography (LACK) [15, 16] and Retransmission Steganography (RSTEG) [17**?** , 18] methods. As mentioned earlier the steganography methods based on modifying the packets are classified into two groups. Each group along with some of its features is discussed as follows: ? Steganography methods that used protocol header?s fields to send hiding information [15, 19]

o Usually high volume of data can be transferred in a hidden manner. o It is easy to implement and detect. o Drawback of these methods is that due to the occupation of some of the fields by hidden data, some of the protocol functionality is reduced.

Steganography methods that modify the payload of the packets [15, 19]

o In these methods, usually transition capacity of hidden data is lower than header?s fields that modify the protocol. o Detection and implementation of these methods are difficult. o A major drawback for these methods is that the quality of transmitted audio decreases significantly, as the content of packets is modified. In addition, some features of steganography methods based on modifying the relations of timing packets are discussed as follows [15, 19]: o These methods need to synchronize the sender and receiver. o Compare with the packet based methods; it is harder to be detected by intruders and eavesdroppers. o Implementing these methods is rather easy. o A significant drawback of these methods is that the voice quality is reduced. In addition, they offer lower capacity of hidden data. The hybrid steganography methods, which take advantage of both packet based and relation based methods, include the following features [15, 19]: o They modify both content and time relation of packets. o They usually are much harder to be detected. o They are capable of transmitting a higher volume of hiding data compare with the relation based methods. o A drawback of these methods is that the quality of communication channel somewhat decreases. There are a number of methods offered by researchers for voice steganography using each of the above categories. They hybrid methods are much more promising. Among the hybrid methods, LACK steganography method in the VoIP environment shows significant results. However, it suffers from capacity limitation. In order to solve this problem without compromising other positive features of LACK, a new approach named LASB method, which, in fact, is a combination of LACK and use of the least significant bits (LSB) of the contents of the packets, applicable in the real time network including VoIP are presented and discussed. To evaluate the new algorithm, both LSB and LACK algorithms along with the new LASB algorithm are implemented and compared.

2 Methodology

A new stream steganography method for real time digital data network environment with the focus on VoIP called LASB is developed. This method consists of a combination of LSB and LACK algorithms, explained earlier. The motivation behind this combination is that it takes advantages of both methods positive features and gets rid of the negative ones. That is, it slows both the reduction of detection probability of stegano data and the use of LSB high capacity as well as being more robust because of diversifying the source of data embedding. In order to introduce the new method, LSB and LACK algorithms are first briefly discussed.

2.1 LSB Steganography Algorithm

This algorithm replaces the least significant bits of the selected bytes in the communication packets with the hidden data bits. It should be noted that in the real time environment this algorithm works properly since it does not take much time for hiding and extracting stegano data. It also is easy to implement LSB algorithm. In addition, LSB method enjoys a very high capacity. However, the major drawback of this algorithm is that it is easily attacked and its detection is

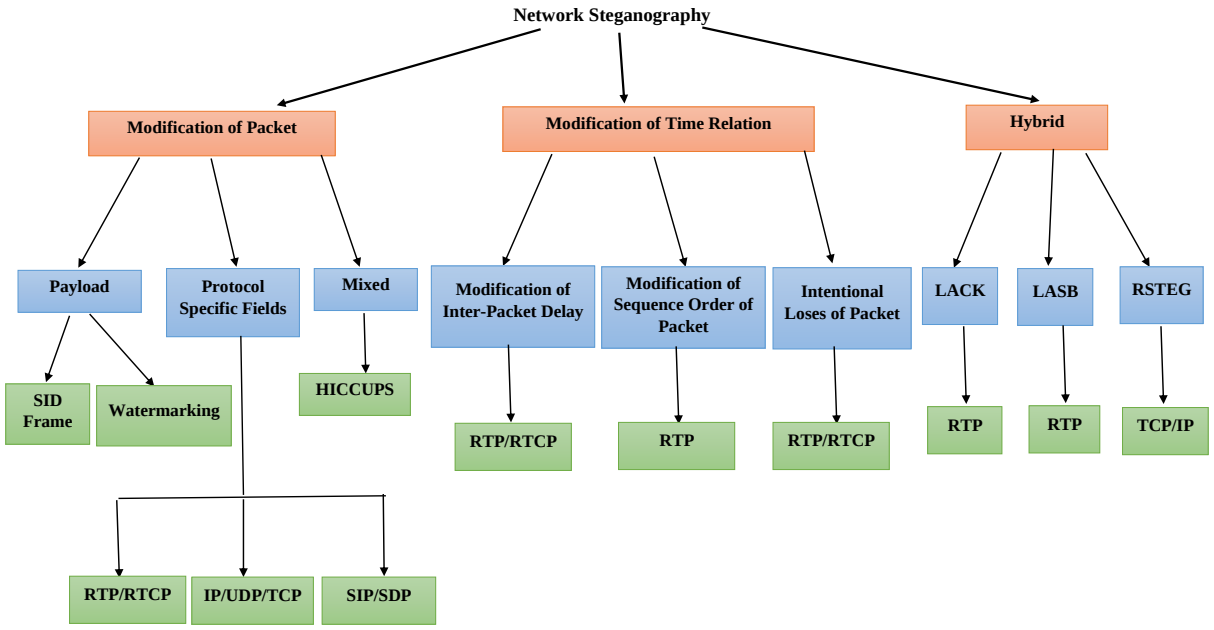

Figure 1. Classification of Network Steganography

easy [20, 21].

2.2 LACK Steganography Algorithm

LACK algorithm was introduced in 2008, and it has been used for steganography in multi-media applications and real time VoIP [15, 16]. This method uses the fact that in communication channels when a packet is excessively delayed (due to RTP [5] protocol use), it is omitted for reconstruction of transmitted voice data in destination. In the LACK method, some packets are deliberately delayed to include the hidden data. When these packets are received at the destination, they are qualified for omission. The LACK algorithm at the destination picks these "delayed" packets to decode and obtain the secret data. The idea behind LACK is illustrated in Figure 2. As shown in Figure 2, in scenario1, one packet, named N4, is chosen from RTP stream. This packet is replaced with an already manufactured packet with the hidden data. Then, the fake N4 packet is sent with a specific time "delay" into the communication channel toward the destination, as shown in scenario 2. In scenario 3, delayed packet would be omitted if it is received by uninformed receiver. The informed recipient, however, instead of removing the packet, picks it and extracts the hidden data, as shown in scenario 4. The performance of LACK depends on several factors, including the detailed communication process (especially the type of codec used, frame sound size and receiver buffer size ...) and network QoS (packets delay and packets loss probability) [15, 16]. In fact, if the communications channel is too noisy and has too much delayed packets,

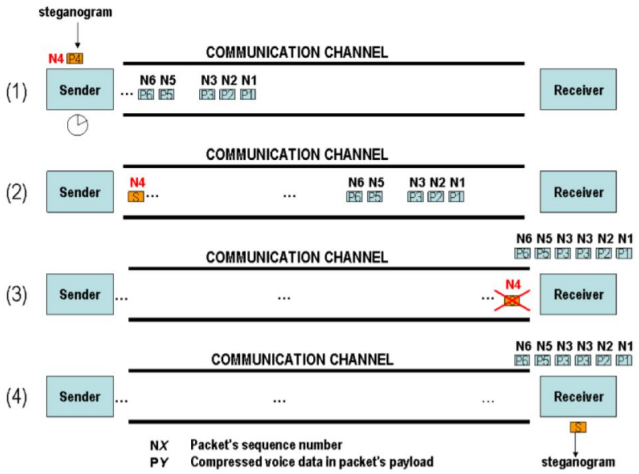

Figure 2. Idea Behind LACK Algorithm [3, 16]

the LACK performance reduces significantly. This is because the informed recipient receives many qualified packets without hidden data, which may confuse the recipient. Besides, the quality of the sound would be reduced since the removal of the chosen packets for data hiding purpose are added to the number of omitted packets at the destination to reduce the audio quality even further. In order to prevent reduction of the receiver's audio quality, the hidden data in VoIP packet loss level using LACK should be controlled. Packet loss level varies across different Codecs. For instance, 1% for G.723.1, 2% for G.729A and 3% for G.711. If additional mechanisms are used to overcome Packet loss, such as PLC (Packet Loss Concealment), then packet loss ratio would increase. (For example, G.711

is about 5-8%) [15] To ensure that RTP packets are recognized as lost on the part of receiver the amount of delay should exceed a certain value. Two significant parameters must be assumed, and assign them right value [15]. o The period of delay with which packet should be sent to be recognized as lost. o Probability of packet lost. (to ensure that voice quality would not decrease by packet lost which is caused by network or LACK algorithm) Like LSB method, LACK algorithm is also almost easy to implement. In addition, the detection of LACK is much harder than LSB. Like LSB, LACK is able to transmit a high volume of hidden data. However, LACK works only in high quality communication channels with very low packet lost. In fact, if there is an excess lose of packets in a communication channel, the performance of LACK system decreases significantly. In addition, statistical lost tracking in LACK is feasible.

2.3 New LASB Steganography Algorithm

A combination of LSB and LACK algorithms leads to a new algorithm called LASB. By combing these two methods, the secret data is partitioned into two parts, one part is embedded in the LACK "delayed" packets and the other part is embedded in the least significant bits. That is, a part of the stegano data would be embedded in the LSB of the normal VoIP packets (for example 40% of the total secret data) and the rest would be embedded using LACK in the "delayed" packets. Therefore, the probability of existence of steganography data in the least significant bits is reduced, extensively. This also is true for the probability of existence of the date in the "delayed" packets in LACK. In addition, the high capacity property of LSB methods is partially used without compromising the secret data, which is the LSB methods' weakness. In addition, part of the secret data which is hidden in the "delayed" packets in LACK, leads to significantly less number of packets (say about 40%) needed when only LACK algorithm is used. Note that, the total delayed packets, both packets that are delayed because of the quality of communication channel and the packets that are deliberately "delayed" for data hiding using LACK algorithm could not exceed 3%. Reducing this percentage by moving part of the secret data into the LSBs, both helps the robustness of the hidden data and increases the quality of the communication channel. It helps the robustness since only part of the data is hidden in the "delayed" packets. It increases the quality of the communication channel since the total delayed packets such that the total delayed packets reduce to 1% to 2%. Therefore, if the network is monitored by an active warden, it would not be able to detect the existence of stegano data in the voice packets as easily as when only LACK is used. In addition, high packet lost (for example, 3% packet lost) would alarm an active warden and may make it suspicious of steganography activities. However, LASB would decrease the packet lost significantly to 1% to 2% and so it may be ignored. Besides, if we decide to use the full load of LASB algorithm for transmitting stegano data, it provides a much higher capacity than each of LACK or LSB algorithms individually. This is because both least significant bits of voice data and the "delayed" packets are used by LASB. In Section 4, the capacity of transmitted stegano data using LASB, LACK and LSB algorithms are compared.

3 Implementation

Visual Studio 2010 implementing environment and C# programming language was used to implement LSB, LACK and LASB algorithms. To create RTP VoIP environment Lumisoft [22] open source class library was utilized. However, in order to support LACK algorithm, the class library was modified, so that the selected packets be transmitted by delay and prevent discarding these received packets. These programs create a VoIP environment for a local network. We had used RTP protocol for creating VoIP environment, and Codec G.711 for coding transferred voice. Voice packets are sent to the destination through UDP protocol. In these programs, each time 400 bytes voice was received from microphone, and it was coded to 200 bytes through G.711 Codec, then was sent to destination. Firstly, the type of stegano data and then stegano data bytes are sent to the destination. These programs support 16 types of files.

3.1 LSB VoIP Steganography Program

This program has been planned to send 1 to 20 bytes of steganography data in each packet. Also the position of hidden bytes in stegano file is sent along with the packet.

3.2 LACK VoIP Steganography Program

In this program, the percentage of the packets which are transferred by LACK method can be determined. (Between 1% to 5%) As the percentage of stegano data increases the quality of voice decreases. A series of packets was chosen randomly and sent to destination by delay. The receiver recognized the packets with out of order sequence number as stegano data and delivered them to the program. The receiver packets were checked for having stegano data.

Table 1. SNR and Call Duration for Sending Attacked Stegano Wav File by LSB Method

Stegano File Type	File Size(KB)	LSB Bytes/Packet	Attack Percentage (%)	SNR(db)	Call Duration(s)	Received Packets
Wav	98.4	10	1	19.3171	252	9991
Wav	98.4	10	2	16.4959	252	9891
Wav	98.4	10	3	15.2050	252	9797
Wav	98.4	20	1	20.3538	126	5004
Wav	98.4	20	2	17.1683	126	4957
Wav	98.4	20	3	15.5382	126	4894

3.3 LASB VoIP Steganography Program

This program is a combination of above programs with little modification. In this program, the capacity of sent stegano data was adjusted by LACK and LSB algorithms. Also, in order not to encounter with a serious problem in data reconstruction in destination, the bytes position of stegano data was sent by each packet.

4 Experimental Results

For recognizing the efficiency of LASB method, we transmitted a wav file (it has 98.4 KB) by using LSB, LACK and LASB to destination. We ran several attacks on both LSB and LASB methods. In this experiment, we assume that if someone eavesdrops during transition, and he intends to interrupt it, he can throw away some of transmitting packets. We experimented several patterns by which the eavesdropper can throw away 1% to 3% of packets. To evaluate steganography data which is received in destination, we calculated Signal to Noise Ratio (SNR). Experimental results are presented bellow in Table 1 and Table 2.

As it is shown in above tables: For sending stegano data by using LSB method, more time is needed in comparison to LASB method. If attacks occur, LASB method is more flexible than LSB method. (By LASB method, SNR in received files shows extra value) If in LASB method 3% of packets are transmitted by LACK method and for other 97%, 20 bytes of stegano data has embedded in each packet, this method (LASB) shows the highest flexibility against attacks. Additionally, less time duration is needed for transmitting stegano data and also the quality of received voice does not decrease. Call duration for transmitting wav file by LACK method is presented in Table 3.

As it is shows in Table 3, call duration for sending stegano wav file depends on the percentage of selected packets. Also much time is needed in order to transfer the file to destination. Finally, we assumed conditions in which an active warden realizes the existence of stegano data in the transmitted voice by LASB algorithm. The findings of this experiment are shown in Table 4. As it noticed in Table 4, if an active warden used either LACK or LSB algorithm for reconstructing stegano wav file, the reconstructed file would be disrupted and unplayable.

5 Conclusion

In this article, a new method, named LASB, based on the combination of LACK and LSB for real time network steganography was introduced. Comparing it with LSB and LACK, this method makes the detection of stegano data more difficult. Moreover, it has higher capacity for transferring hidden data. The new LASB method can be used for stegano data in real time network including VoIP and real-time voice. We specifically implemented LACK, LSB and LASB algorithms by C# program in VoIP environment and compared them with each other. Several experiments for evaluating the performance of our algorithm shows that: (1) Call duration for transmitting stegano data by LASB method was lower than other methods. This implies that the capacity of LASB method for transmitting stegano data is higher than both LACK and LSB methods. (2) If eavesdropper throws away some of packets randomly, or the quality of communication network decreases, it affects LASB transmitted stegano data less than LACK or LSB methods. (3) Detection probability and reconstructing steganography data by eavesdropper decreases if LASB method is used.

Acknowledgements

This work was supported in part by the Iran Telecommunication Research Center (ITRC).

Table 2. SNR and Call Duration for Sending Attacked Stegano Wav File by LASB Method

Stegano File Type	File Size (KB)	Selected Packets Percentage (%)	LSB Bytes/Packet	Attack Percentage (%)	SNR (db)	Call Duration(s)	Received Packets
Wav	98.4	2	10	1	21.5513	188	7478
					16.9006	189	7479
					21.4256	189	7479
Wav	98.4	2	10	2	17.2830	187	7438
					18.2385	187	7407
Wav	98.4	2	10	3	13.1822	187	7358
					15.3781	188	7364
					13.3368	186	7335
Wav	98.4	3	10	1	23.6637	171	6777
					20.5061	165	6647
Wav	98.4	3	10	2	16.4722	152	6063
					17.7745	168	6606
					16.6445	165	6587
					16.7014	165	6585
Wav	98.4	3	10	3	17.6941	168	6544
Wav	98.4	2	20	1	20.8040	109	4347
Wav	98.4	2	20	2	16.2151	109	4304
					17.5220	108	4304
					16.5317	111	4313
Wav	98.4	2	20	3	14.9409	111	4263
					13.9265	109	4282
					15.6919	112	4273
Wav	98.4	3	20	1	21.2562	102	4104
Wav	98.4	3	20	2	19.0259	102	4062
Wav	98.4	3	20	3	15.9195	102	4066
					16.2178	101	4027

Table 3. Call Duration for Sending Stegano Wav File by LACK Method

Stegano File Type	File Size (KB)	Selected Packets Percentage (%)	Call Duration(s)	Packets Received
Wav	98.4	2%	663	26210
Wav	98.4	3%	442	17442

References

[1] SANS white paper. Steganography: Past, Present, Future. `http://www.sans.org/reading_room/whitepapers/stenganography/steganography_past_present_future_552?show=552.php&cat=stenganography`.

[2] Wojciech Mazurczyk and Krzysztof Szczypiorski. *Steganography of VoIP Streams*, pages 1001–1018. Springer Berlin Heidelberg, 2008. ISBN 978-3-540-88873-4. doi:10.1007/978-3-540-88873-4_6.

[3] J. Lubacz W. Mazurczyk and K. Szczypiorski. Hiding Data in VoIP. In *In Proc of: The 26th Army Science Conference (ASC 2008)*, Orlando, Florida, USA, December 1-4 2008.

[4] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. The Secure Real-time Transport

Table 4. Voice Quality of Wav File Detected by an Active Warden

Voice Quality Reconstruction by LACK	Voice Quality Reconstruction by LSB	LSB Bytes/Packet	Selected Packets Percentage (%) by LACK
disrupted and unplayable	disrupted and unplayable	20	3
disrupted and unplayable	disrupted and unplayable	20	2
disrupted and unplayable	disrupted and unplayable	10	3
disrupted and unplayable	disrupted and unplayable	10	2

Protocol (SRTP). RFC 3711, RFC Editor, March 2004. URL `http://www.rfc-editor.org/rfc/rfc3711.txt`.

[5] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. STD 64, RFC Editor, July 2003. URL `http://www.rfc-editor.org/rfc/rfc3550.txt`.

[6] M. Shirali-Shahreza. A New Method for Real-Time Steganography. In *2006 8th international Conference on Signal Processing*, volume 4, 2006. doi:10.1109/ICOSP.2006.345954.

[7] Andreas Westfeld and Gritta Wolf. *Steganography in a Video Conferencing System*, pages 32–47. Springer Berlin Heidelberg, 1998. ISBN 978-3-540-49380-8. doi:10.1007/3-540-49380-8_3.

[8] Chun-Shien Lu, Jan-Ru Chen, and Kuo-Chin Fan. Real-time frame-dependent video watermarking in VLC domain. *Signal Processing: Image Communication*, 20 (7):624 – 642, 2005. ISSN 0923-5965. doi:https://doi.org/10.1016/j.image.2005.03.012.

[9] J. Haitsma and T. Kalker. A watermarking scheme for digital cinema. In *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)*, volume 2, pages 487–489 vol.2, Oct 2001. doi:10.1109/ICIP.2001.958534.

[10] V. Viswanathan. Information hiding in wave files through frequency domain. *Applied Mathematics and Computation*, 201 (1):121 – 127, 2008. ISSN 0096-3003. doi:https://doi.org/10.1016/j.amc.2007.12.003.

[11] Xiaomao Wu, Lizhuang Ma, Zhuoqun Dong, and Lionel Revret. Robust watermarking motion data with DL-STDM. *Computers & Graphics*, 32(3):320 – 329, 2008. ISSN 0097-8493. doi:https://doi.org/10.1016/j.cag.2008.04.002.

[12] D.Kundur and K. Ahsan. Practical Internet Steganography: Data Hiding in IP. In *Proceedings of the Texas Workshop on Security of Information Systems*, April 2 2003.

[13] Vincent Berk, Annarita Giani, and George Cybenko. Detection of Covert Channel Encoding in Network Packet Delays. Technical report, TR2005-536, Department of Computer Science, Dartmouth College, November 2005. URL `http://www.cs.dartmouth.edu/reports/TR2005-536-rev1.pdf`.

[14] S. D. Servetto and M. Vetterli. Communication using phantoms: covert channels in the Internet. In *Proceedings. 2001 IEEE International Symposium on Information Theory (IEEE Cat. No.01CH37252)*, pages 229–, 2001. doi:10.1109/ISIT.2001.936092.

[15] J. Lubacz W.Mazurczyk. A propositional calculus with denumerable matrix. *Telecommunication Systems*, 45:153–163, 2010.

[16] Wojciech Mazurczyk, Jzef Lubacz, and Krzysztof Szczypiorski. On steganography in lost audio packets. *Security and Communication Networks*, 7(12):2602–2615, 2014. ISSN 1939-0122. doi:10.1002/sec.388.

[17] Wojciech Mazurczyk, Miłosz Smolarczyk, and Krzysztof Szczypiorski. Retransmission steganography and its detection. *Soft Computing*, 15(3):505–515, Mar 2011. ISSN 1433-7479. doi:10.1007/s00500-009-0530-1.

[18] Wojciech Mazurczyk, Miłosz Smolarczyk, and Krzysztof Szczypiorski. On information hiding in retransmissions. *Telecommunication Systems*, 52(2):1113–1121, Feb 2013. ISSN 1572-9451. doi:10.1007/s11235-011-9617-y.

[19] Wojciech Mazurczyk and Józef Lubacz. LACK—a VoIP steganographic method. *Telecommunication Systems*, 45(2):153–163, Oct 2010. doi:10.1007/s11235-009-9245-y.

[20] Xiaoyi Yu and N. Babaguchi. Run length based steganalysis for LSB matching steganography. In *2008 IEEE International Conference on Multimedia and Expo*, pages 353–356, June 2008. doi:10.1109/ICME.2008.4607444.

[21] M. Goljan J. Fridrich and R. Du. Reliable detection of LSB steganography in color and grayscale images. volume 8, pages 22–28, Ottawa, Ontario, Canada, October -December 2001.

[22] lumisoft. `http://www.lumisoft.ee/lswww/Download/Downloads/Net/`.

Hossein Moodi was born in Birjand, Iran, in 1984. He received the B.S. degree in Computer engineering (Software) from the Shahid Bahonar University of Kerman, Kerman, Iran, in 2006, and the M.S. degree in Computer engineering from University of Isfahan, Isfahan, Iran, in 2009. In 2014, he joined the Department of Computer Engineering, Birjand University of Technology, as a Faculty Member of Computer engineering. His current research interests include Steganography, Botnet, Botnet Detection, Data Hiding and Malware detection.

Ahmad R. Naghsh-Nilchi is an Associate Professor of Artificial Intelligence and Multimedia Engineering at the University of Isfahan, Iran. He received his B.S., M.S., and Ph.D. degrees from Electrical and Computer Engineering Department in 1988, 1989, and 1996, respectively, all from the University of Utah, Salt Lake City, Utah, USA. He is the Chairman of the Artificial Intelligence and Multimedia Engineering at the University of Isfahan. He has been awarded several research grants from distinguished research institutions and has completed a number of research projects for Iranian industries. He is the author and co-author of several journal articles and conference papers. In addition, he has collaborated with internationally known institutions and peers and was a Research Scholar with the National University of Ireland Maynooth, Ireland, in 2011, and with the University of California, Irvine, in 2012. He also is the chief editor of the Journal of Computing and Security. His research interests include image and signal processing, data hiding, as well as intensive computing.