Network Steganography System Using Covert Channel For LSBS Stego Data On VOIP Communication

Huzain Azis

ABSTRACT--- Voice over Internet Protocol (VoIP) is a real-time service that enables voice conversations using IP networks, Steganography is the art and science of hiding secret messages in other messages that makes the secret messages are unknowable. VoIP allows as a medium cover carrier on steganography to provide the security of confidential messages. This study built by two-stage of steganography system using Least Significant Bits and Covert Channel that use image and VoIP communication as a medium in the hiding of messages. End of this study, the system will go through the process of performance and functionality testing. The results showed that the method of Covert Channel to the Payload field has the hiding of large capacity that are 56bit per packet, and by using two stages method of steganography can make a Steganogram extraction or analysis more difficult to do..

Kywords: LSBs; Covert Channel; Network Steganography.

I. INTRODUCTION

Telecommunication is a service for exchange of message through electronic media, using electronic media and communication network message can be exchanged quickly and easily. But there is no guarantee of user activities from the risk, Risk of communication technologies such as tapping, alteration, destruction or deletion of messages, especially messages that are confidential. Steganography is the art and science of hiding secret messages in other messages till the secret message can't be discovered [1], [2]. The new concept of the steganography is Network Steganography that using communication control protocol, elements or basic function of telecommunications as a medium or host [3], [4]. IP telephony connections in VoIP consist of two stages, where certain types of traffic are exchanged between the calling parties [5], [6]. The two stages are the Signaling phase and the Conversation phase.

This study will discuss the application of steganography using two methods, namely Least Significant Bits (LSBs) in image data as a medium for text data concealment followed by Covert Channel method that is inserting images into packets set by UDP and RTP protocol in conversation phase using Softphone Ekiga.

II. EXPERIMENTAL DETAILS

This research builds a steganography system that can be an alternative in the delivery of secret messages through Voice over Internet Protocol (VoIP) communication. Processes in the system are described in Figure 1. The developed system has four main processes: Stego I (LSB), Stego II (covert Channel), extract I and extract II processes.

The testing of this study was conducted to ensure the designed system work properly or not. Trying the whole system by various condition those are Message character number, Image size (cover medium I) and communication time using VoIP (cover medium II). Performance testing is divided into two categories, Effectiveness and Efficiency. Effectiveness Testing are noticing at anomaly or unusual events in the image and communication network during the steganography process. Testing will be settled by calculating the Signal to Noise Ratio and Peak Signal to Noise Ratio, Counting Jitter, Counting Package loss and measuring the pattern of time process with linear regression.

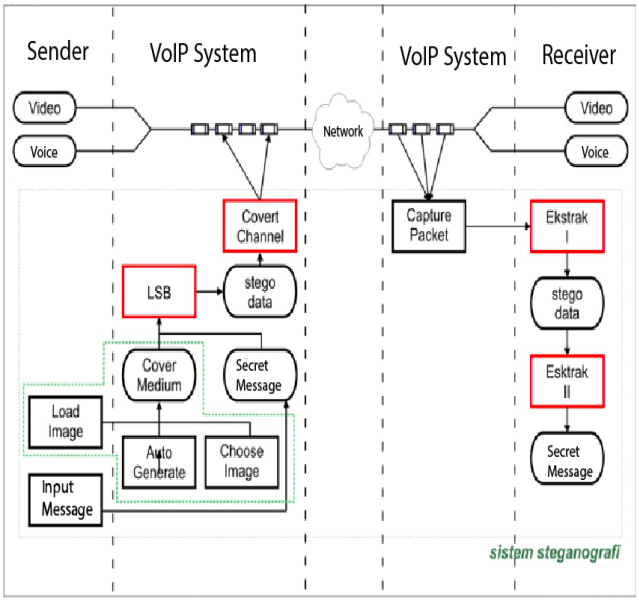

Fig. 1: System architecture

III. RESULT AND DISCUSSION

The previous research about the detection of a network steganography [7], it is possible to trace a steganogram. But the results of this study that analysis based on the package has no effect because the sham packets have same package with VoIP packages.

Based on the results of the implementation, the comparison with the results of previous research on the capacity of delivery [8]. The use of the LACK method has a small delivery capacity of 5 bits per second whereas the

Revised Manuscript Received on April 19, 2019.

Huzain Azis, Faculty of Computer Science, Universitas Muslim Indonesia, Makassar, Indonesia (Email: huzain.azis@umi.ac.id)

applied research has a capacity of 416 bits or 52 bytes per second. The change of bandwidth usage by LACK method is lower than this research. It is 0.3% additional bandwidth for the LACK method while the designed study achieves 2% additional per second bandwidth during the insertion process.

Research on delivery capacity [9], that use of the previous covert channel method in the Identification field of 16 bits per packet whereas the applied research showed in figure 2. has a capacity of 416 bits or 52 bytes per package by use an identification, flags and other field in ipv4 packet.

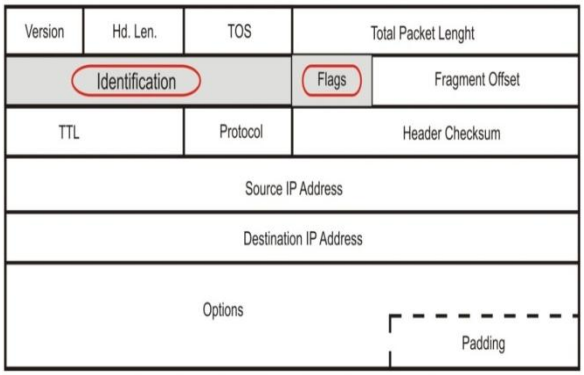

Fig. 2: Field of ipv4

The applied steganogram delivery has a large capacity up to 80 bytes per packet 3 when we compared to the applied research that only had 56 bytes per packet. After going through the compression process of payload content it give a hiding space 3 but the original sound quality decreased. This conducted is absence of a direct process that affects the sound quality

IV. CONCLUSION

Based on the functionality and performance test presented in Table 1, it can be concluded that the maximum number of packets can be read from the Covert Channel method are 256 packets equivalent to 13312 bytes or 75*50 pixels stegodata which can be inserted as many as 2812 characters of messages, due to the development of the system is given only 1 byte as the order of the packets. Testing the SNR and PSNR values of the Cover medium selected by the user have a bad change to content.

Table 2. Shows the average jitter in the presence of secret communication has greater jitter than without secret communications. More details: (1) A large Missing Packets up to 785612 packets was declared lost at the start of the test, because the sequence number ordered in steganography system before sending has set by big value, but after repaired on the system, the lost package can be reduced. (2) Steganography packets also have the risk of packet loss, the risk can be minimized by more than one time because the softphone packet is same with steganography's packet. (3) Sequence Error on existing communication insertion will have more than normal Sequence Error because the system does not insert confidential information into the original packet but creates a similar package and inserts it into other VoIP packets.

The value of jitter, packet lost and sequence error in the test results has not been accurate due to unstable internet connection factor and the duration of testing time is not the same. by using an Auto Generate image alternative then the risk of a bad SNR or PSNR value will decrease while optimizing the Cover Medium size created based on many characters of the message.

REFERENCES

1. C. Cachin, "Digital Steganography," Encycl. Cryptogr. Secur., pp. 159–164, 2005.
2. H. Tian, K. Zhou, H. Jiang, Y. Huang, J. Liu, and D. Feng, "An adaptive steganography scheme for voice over IP," in 2009 IEEE International Symposium on Circuits and Systems, 2009, pp. 2922–2925.
3. M. C. Sekhar, S. K. Chandini, V. S. Rohith, V. J. Lakshmi, and M. P. Kumar, "Data hiding using bit plane complexity segmentation steganography," Int. J. Eng. Technol., vol. 7, no. 2.20, pp. 33–36, 2018.
4. R. Din, M. Mahmuddin, and A. J. Qasim, "Review on Steganography Methods in Multi-Media Domain," Int. J. Eng. Technol., vol. 8, no. 1.7, pp. 288–292, 2019.
5. W. Mazurczyk, P. Szaga, and K. Szczypiorski, "Using transcoding for hidden communication in IP telephony," Multimed. Tools Appl., vol. 70, no. 3, pp. 2139–2165, 2014.
6. W. Mazurczyk and K. Szczypiorski, "Steganography of VoIP streams," in In OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", 2008, pp. 1001–1018.
7. A. S. Nair, A. Sur, and S. Nandi, "Detection of packet length based network steganography," in International Conference on Multimedia Information Networking and Security, 2010, pp. 574–578.
8. W. Frączek, W. Mazurczyk, and K. Szczypiorski, "Multi-level steganography: Improving hidden communication in networks," J. Univers. Comput. Sci., vol. 18, no. 14, pp. 1967–1986, 2012.
9. S. Das, S. Das, B. Bandyopadhyay, and S. Sanyal, "Steganography and Steganalysis: different approaches," arXiv Prepr., vol. 1111, no. 3758, 2011.