Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

A Covert Timing Channel Based on DCT Domain of Inter Packet Delay Sequence

Jiangtao Zhai, Fang Yang, Yuewei Dai

School of Electronics and Information Engineering
Jiangsu University of Science and Technology
No.2 Mengxi Road., Jingkou District, Zhenjiang, Jiangsu, China
jiangtaozhai@gmail.com, yf.1016@163.com, dywjust@163.com

Mingqian Wang

School of Information Engineering
Changzhou Institute of Mechatronic Technology
No.26 Mingxin Middle Road, Wujin District, Changzhou, Jiangsu, China
wmq1989219@126.com

Received July, 2015; revised August, 2016

Abstract. *The existing covert timing channels are always designed in time domain. Although they have high security, they are sensitive to the jitters in the network. In this paper, a new covert timing channel based on frequency domain is proposed to increase its robustness while maintaining the security. The proposed method first transforms the inter packet delay sequence (IPDs) into 1-D DCT domain and embeds secret information into the DCT coefficients. Then the packets are transmitted as the new IPDs after an IDCT transform. When the packets are received, a 1-D DCT transform is performed to the extracted IPDs and the secret information is got according to the relevant decoding method. The experimental results show the proposed method has stronger robustness compared with the existing typical covert timing channels while keeping the same security.*
Keywords: Covert timing channel, Frequency domain, Discrete cosine transform (DCT), Information hiding.

1. **Introduction.** Network covert channel is a hidden communication technique, which utilizes the legitimate traffic as the vehicle to transfer secret information covertly over the network. In recent years, network covert channel has become a hot topic in the field of information security due to the fine properties of network traffic. There are two broad types of network covert channel: covert storage channel and covert timing channel. The former embeds the secret information into the redundancies of network protocols [1, 2]. It's simple to implement, however, it can be detected by the existing methods easily [3]. The latter delivers the secret information by exploiting the time-relevant events of network packets. As its stealthiness is better than the former [4, 5], the research on covert timing channel becomes an increasingly important issue.

In recent years, the research is mainly conducted to improve the stability and robustness of the covert timing channel. However, most of the existing methods would either generate abnormal or reveal distinct properties compared with the normal case. As the embedding of the secret information alters the original carrier-traffic in some way, the covert traffic is deviated from the normal one in some respects. This will make it possible to be detected by the existing methods [6]. Although some model-based covert timing channels

have achieved high security, they are not stable in fact of uncertain disturbances [7]. In addition, most of the research has been conducted in time domain while very few have been done in the frequency domain. The IPDs (Inter Packet Delays) can be regarded as a random signal. For a random signal, there are many processing methods can be used to hide information.

From this point, in this paper, a new covert timing channel based on the frequency domain is proposed. The Discrete Cosine Transform (DCT) is a very popular and typical signal processing method and it is an orthogonal transformation method put forward by Ahmed *et al.* in 1974. In particular, DCT is a Fourier-related transform similar to the Discrete Fourier Transform (DFT), but using only real numbers. As DCT is considered to be one of the most common and effective method of signal transformation, a 1-D DCT-based covert timing channel is proposed in this paper. The DCT-based covert timing channel disperses the embedded information into different parts of the signal, thus it can not only ensure the invisibility of the confidential information, but also improve the robustness of the covert channel. In our method, the regularity and properties of the covert traffic are quite similar to that of the normal one, that's why it is able to resist detection. At the same time, our method has fine robustness, making it superior to other existing methods.

The remainder of this paper is organized as follows. Section 2 reviews some related steganographic methods and gives a brief analysis to DCT. The proposed method is introduced in Section 3. In Section 4, experimental results are presented and analyzed. Finally, the whole paper is concluded.

2. **Related works.**

2.1. **Review of covert timing channels.** Generally, covert timing channel can be divided into three sub-classes: on/off covert channel, delay covert channel, packet sorting and combination based ones. The first covert timing channel is on/off covert timing channel, which transmits one bit secret message by sending packets or not in a fixed time interval. It is easy to implemented, however, the capacity and covertness of this covert channel are a little weak. Cabuk *et al.* proposed an IP covert timing channel called IPCTC [8]. It is a binary on/off channel which transmits a bit '1' or '0' by sending a packet during a certain time interval or not. It has improved considerably on the properties of stability and robustness by overcoming the problem caused by uncertainties in network transmission. Later, many covert timing channels based on modifying the IPDs are proposed. Shah *et al.* designed a keyboard device named Jitterbug, to create a loosely-coupled covert channel capable of leaking information on a keyboard over the network [9]. Jitterbug conveys the information by adding small delays to the original time intervals of key-presses, inevitably altering the properties of the normal traffic.

To imitate the statistical feature of normal traffic, Cabuk developed a more advanced method based on the replay attack, called Time-Replay covert timing channel(TRCTC), in which a sample of legitimate traffic is used as input and is replayed later to transmit information [10]. Gianvecchio proposed a flexible framework of model-based covert timing channel(MBCTC) [11]. MBCTC employs the parametric estimation to construct the statistical model of the normal traffic, which is then utilized to generate inter-packet delays containing the secret information. MBCTC has high security, however, it is very sensitive to the jitters. Based on MBCTC, Liu *et al.* presented a more feasible method to fit the histogram distribution property of the normal traffic, termed as covert timing channel with distribution matching (CTCDM), which improves the accuracy of the transmission [12]. It reduced the encoding complication of MBCTC, however, it is also disturbed by

jitters easily. Rezaei proposed a new covert timing channel called DPOI to improve the performance in terms of covert data rate and latency [13]. The DPOI sends covert "0" bits by doing nothing to the overt traffic while covert "1" bits are delivered by delaying the overt packet for a specific time, thus the bandwidth of the covert network is improved proportionally. These delay-based covert timing channels have better stealthness, however, they are always sensitive to the network jitters. This will constrain their usage.

For overcoming this deficiency, the current research focuses on reduce its capacity to improve robustness. This will make the covert communication process keep longer. From the literatures, it can be seen the existing methods always embed secret information in the time domain of IPDs. As we know, the IPDs can be seen as a random sequence, for a random sequence, there are many signal processing methods can be used. The signal of time to frequency domain transfer is a common method. From this point, a frequency domain covert timing channel is studied in this paper.

2.2. **DCT Analysis.** DCT is considered to be one of the best methods of signal transformation. There are two significant characteristics in DCT [14], which are listed as follows.

1. Energy concentration. The energy of the IPD sequence remain unchanged after DCT transform, but redistributed with a few low frequency coefficients representing most of the energy. If the secret information is embedded into these low frequency coefficients, the covert channel would achieve high robustness, but low invisibility. When the secret information is embedded into those high frequency coefficients, there would be high invisibility and low robustness. In this case, it is compromised to take the intermediate frequency coefficients as the embedding position.

2. Stability. A slight disturbance imposed on the IPD sequence will be dispersed into frequency domain, so there would be no significant impact on DCT coefficients, and vice versa. This keeps the invisibility and robustness of the imposed DCT-based covert timing channel.

Since the 2-D DCT transformation has been used in the area of images generally, and the extracted IPDs are in 1-D form, thus, 1-D DCT is used in this paper. Let $c(x)$ be the IPD sequence and $C(u)$ be the DCT coefficients, the number of IPD is N , then the formula of 1-D DCT will be defined as Eq.1:

$$\begin{aligned} C(0) &= \tfrac{1}{\sqrt{N}} \sum_{x=0}^{N-1} c(x) \\ C(u) &= \sqrt{\tfrac{2}{N}} \sum_{x=0}^{N-1} c(x) \cos \tfrac{(2x+1)u\pi}{2N} \\ c(x) &= \sqrt{\tfrac{1}{N}} C(0) + \sqrt{\tfrac{2}{N}} \sum_{u=0}^{N-1} C(x) \cos \tfrac{(2x+1)u\pi}{2N} \end{aligned} \tag{1}$$

The covert channels have some common features, and the most important points are invisibility, robustness and capacity. It is agreed universally that the contradictory unity among these characteristics makes a system unable to have optimum invisibility, optimum robustness and optimum capacity simultaneously. The much higher capacity will inevitably make the decrease of invisibility and robustness, and vice versa. To achieve a relatively good performance of the whole system, it is decided to embed 60 bits of secret information into every 200 IPDs.

3. **The proposed method.** The process of our method is presented in Fig.1:

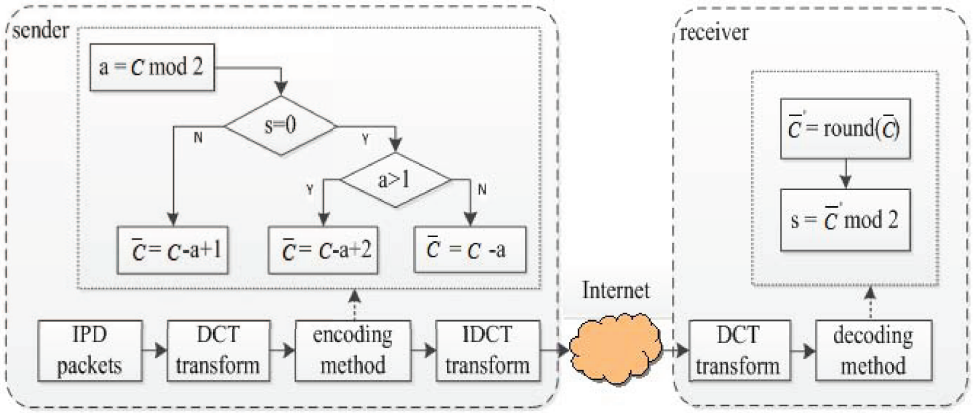


FIGURE 1. The process of the DCT-based covert timing channel

3.1. **Encoding.** The model of our method is demonstrated as follows. Initially, a sample of normal traffic is collected, and the time intervals of the adjacent packets are extracted. A 1-D DCT transform is conducted in time intervals of the normal traffic with the window number is 500, and the size of each window is 200. There are 60 bits of secret information encoded in each window and the promissory frequency coefficients are from No. 81 to No. 140, which are agreed by both the sender and the receiver. Then the covert IPDs are got after the transform of IDCT and the traffic is sent as the covert IPDs.

When the IPDs is transformed into DCT domain, the secret messages can be encoded into the DCT coefficients. If the secret bit is '0', the modified coefficient should be set to the nearest even number to the original coefficient. Otherwise, the modified coefficients are transformed into the nearest odd number to the original coefficient. Let be the primitive coefficient and be the modified coefficient. Let be the remainder of the coefficient divided by 2. The modified coefficient is calculated by , , and the secret information , which is denoted by Eq.2:

$$\overline{C} = \begin{cases} C - a + 2 & s = 0 \; and \; a >= 1 \\ C - a & s = 0 \; and \; a < 1 \\ C - a + 1 & s = 1 \end{cases} \tag{2}$$

3.2. **Decoding.** To get the secret information , a 1-D DCT transform is conducted in the IPDs after the receiver extracts the time intervals of the covert traffic. First, the DCT coefficients are rounded to integers. Then the secret message according to the decoding method can be got. If the integer is an even number, the secret information of binary form is '0', otherwise, it is '1'. Let be the integer of and be the reminder of divided by 2, the secret information is calculated by the parameter , which is denoted by Eq.(3):

$$s = \begin{cases} 0 & a = 0 \\ 1 & a = 1 \end{cases} \tag{3}$$

4. **Experiments and analysis.** The proposed method is protocol-independent, which means that any network application can be used as its carrier. Therefore, it is widely applicable in different scenarios. As it is known to all, an ideal carrier should possess two properties: popularity and complexity. The massive communication traffic and complex transmission pattern of such application can improve the stealthiness of covert channel. YY audio-a very popular network service based on P2P, satisfies the above requirements, thus it is adopted as the normal carrier in the implementation of this paper.

This method can be used in any applications. In this paper, the normal traffic of YY audio is captured from an intermediate router during the communication of the two hosts within the campus networks. In this section, experiments are performed to evaluate the concealment of the proposed method compared with jitterbug and CTCDM and analyzed in some significant properties, such as the statistical feature of histogram, entropy values and robustness. The whole experiments are implemented within the campus network of Jiangsu University of Science and Technology and Changzhou Institute of Mechatronic Technology.

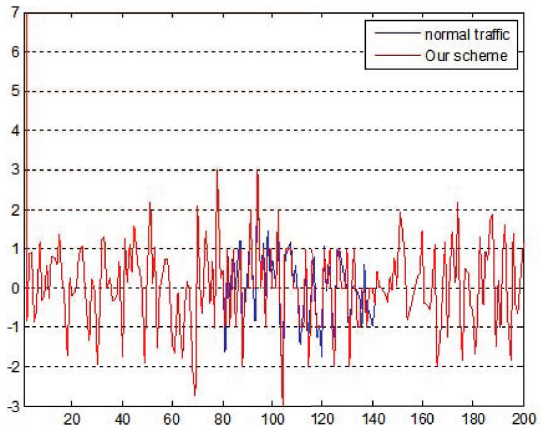
4.1. **The comparison experiments in time domain and frequency domain.** The whole size of the normal traffic is 100,000 IPDs and the normal traffic is departed into 500 windows in the experiments. The secret information is inserted into the DCT coefficients from number 81 to 140 in each window. The performance of the modified time interval is different from the original one after secret message encoding. The comparison between normal and covert traffic is presented in Fig.2. The performance in the DCT domain differs slightly only from 81 to 140 where the secret message is embedded and the original time interval and modified time interval match well in time domain. The results show that the proposed method change the normal time characteristic very slightly, and it has high security.

4.2. **Histogram Analysis.** The histogram distribution property between the normal and covert traffic is demonstrated in Fig.3, where the x-axis shows the time intervals ranging from 6 to 16ms and y-axis shows the data number. For the normal traffic, time intervals between 9 and 13ms occur most while it seldom occurs at other areas. It can also be found intuitively that the distribution of our method only differs slightly from the normal case. The histogram shows that our method keeps the distribution of the time intervals the same as the original one, which means the distribution matching.

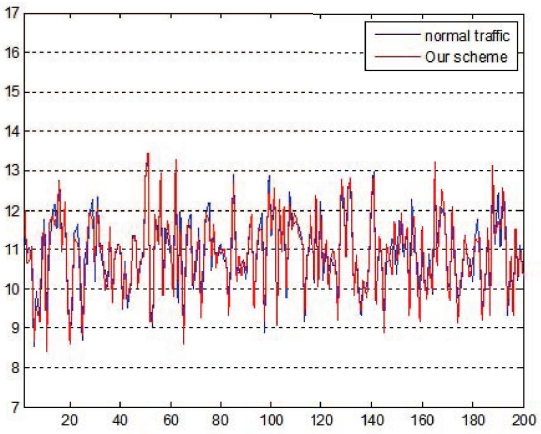
4.3. **Entropy Test.** In entropy test, the whole traffic is divided into 50 windows and each window is divided into L bins to compute the entropy value. The entropy values of 50 windows for normal and covert traffic are compared in Fig.4. From the results, it shows that the difference between methods can hardly be distinguished when L is set to 20, while it becomes obvious with the increase of L, especially when L is 40 or greater. When L is set to 40, most entropy values of the normal traffic appear in the interval of 4.4 to 4.8, so do that of our method, whereas those of the covert traffic generated by CTCDM appear around 4.2 and those by Jitterbug fluctuates around 4. It also shows that the distribution of entropy values of CTCDM and Jitterbug becomes different from that of the normal traffic, while the entropy values of our method coincide with those of the normal traffic, no matter L is 20 or 50. From the above analysis, it can be seen that our method matches the normal traffic better than the existing typical methods.

4.4. **Robustness Test.** Most timing covert channel is easily affected by network jitters. In the experiment, jitters of different powers are injected into the covert traffic of the proposed method. The additive white Gaussian noise is utilized to simulate the channel noise in some aspects. The power of noise is measured by signal-to-noise ratio (SNR) when the power of signal is fixed. In other words, the power of noise increases as SNR decreases. The bit error rate (BER) of our method is shown in Fig. 5, given different SNR ranging from 0 to 70db.

From the results, it can be seen that distortion raised by the noise stays at a high level in Jitterbug till the SNR is 30dB. It can be tolerated with BER of 0.01 when the SNR is about 45dB. And it achieves relatively well accuracy when the SNR is larger than 48dB. In the method of CTCDM, the value of BER decreases smoothly first till SNR is 30dB.



(a)DCT domain



(b) Time domain

FIGURE 2. The comparison between normal and covert traffic of our method in DCT domain and time domain

After that, there is an unstable decline before it reaches the bottom, which means it is robust when SNR is larger than 58dB. While in our method, BER begins to go down when SNR is 20dB and reaches 0.01 when SNR is 35dB. Thus, the proposed method is robust when the power of noise is less than of the signal. It's obviously that our method has better robustness than the other two methods.

From the above results, it is manifest that both of the Jitterbug and CTCDM can be detected by certain methods since the transmission behavior or properties of the original carrier has been significantly altered in their encoding process. However, the performance of our method matches perfectly well with the normal one, thus it performs well in resisting detection. Moreover, our method has better robustness than the other two typical methods. Therefore, it can be concluded that our method possesses better performance than existing one.

5. **Conclusions.** In this paper, a DCT-based covert timing channel is proposed. The secret information is embedded into the agreed 1-D DCT coefficients by making them be odd or even numbers. From the experimental results, it is indicated that the performance of our method is quite close to the normal one, which can successfully evade detection. In addition, our method has better robustness than the other two methods, Jitterbug

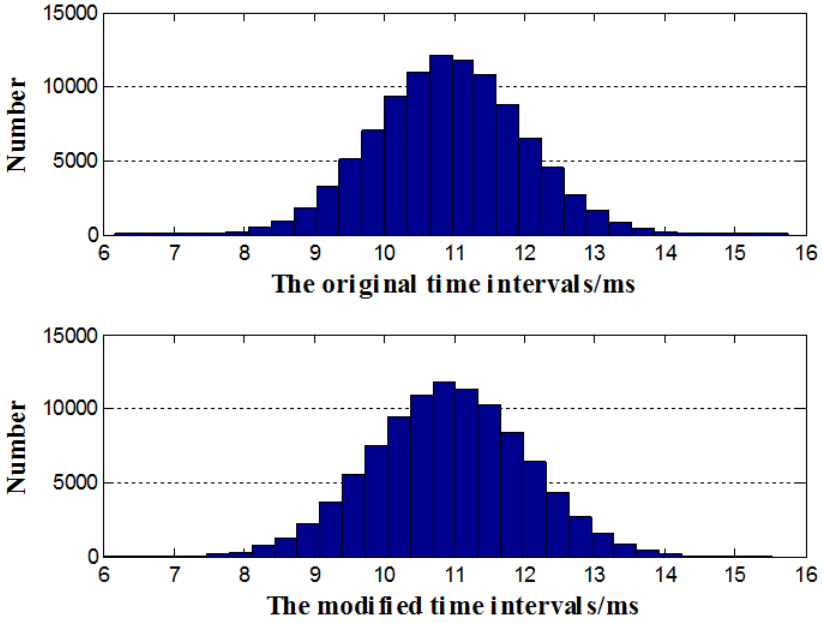


FIGURE 3. The comparison of histogram between normal and covert traffic

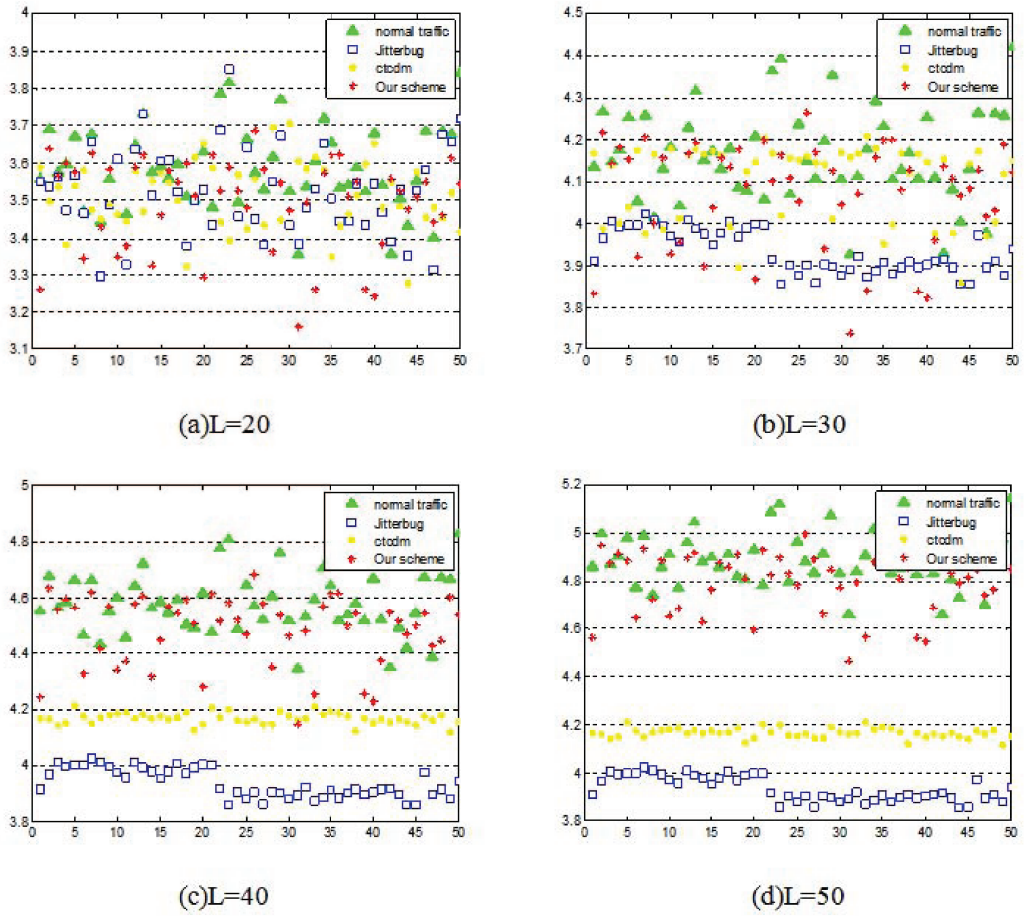


FIGURE 4. The entropy comparison experiments between the normal and covert traffic

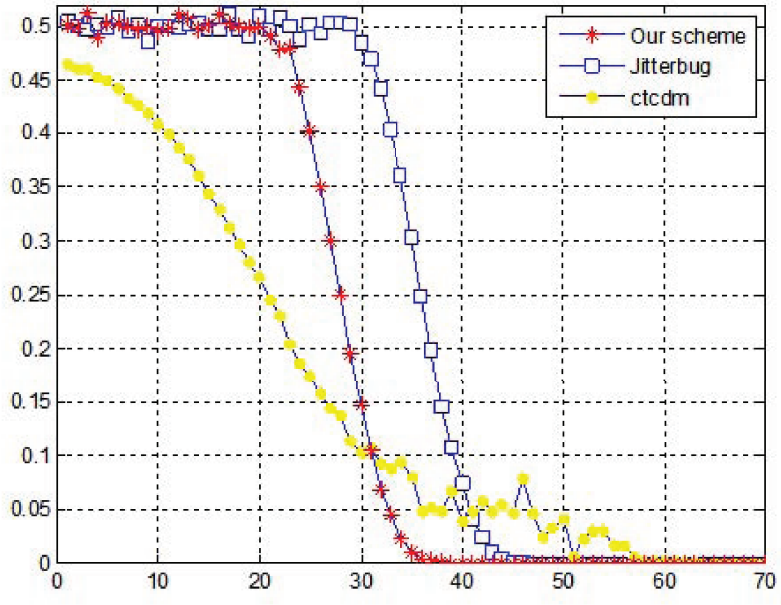


FIGURE 5. The comparison between our method and Jitterbug when SNR ranges from 0 to 70

and CTCDM. Hence, the proposed method outperforms the existing methods in terms of detection resistance and robustness. In the future, the capacity of our method will be further studied. Specifically, the conditions of packet loss and disorder will be considered to evaluate the proposed method.

Acknowledgment. The authors greatly acknowledge the anonymous reviewers for their helpful comments and suggestions during the review process, which contribute to improve the quality of the original manuscript. This work is supported by the NSF of China (Grant No.: 61170250, 61472188) and the NSF of Jiangsu province (Grant No.:BK20150472).

REFERENCES

[1] W. Mazurczyk, M. Karas, K. Szczypiorski. SkyDe: a Skype-based Steganographic Method, *International Journal of Computers, Communications and Control(IJCCC)*. vol.8, no.3, pp.389-400, 2013.

[2] W. Mazurczyk, K. Szczypiorski. Evaluation of steganographic methods for oversized IP packets, *Telecommunications Systems,* vol.49, no.2, pp.207-217, 2012.

[3] S. Grabski, K. Szczypiorski. Network steganalysis: Detection of steganography in IEEE 802.11 wireless networks, *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),* pp.13-19, 2013.

[4] J. Wu, L. Ding, Y. Wang, *et al.*. Identification and Evaluation of Sharing Memory Covert Timing Channel in Xen Virtual Machines, *IEEE International Conference on Cloud Computing (CLOUD),* pp.283-291, 2011

[5] J.F. Lalande, S. Wendzel, Hiding Privacy Leaks in Android Applications Using Low-Attention Raising Covert Channels, *Eighth International Conference on Availability, Reliability and Security (ARES),* pp.701-710, 2013.

[6] H. Zhao, M. Chen. WLAN covert timing channel detection, *Wireless Telecommunications Symposium (WTS),* pp.1-5 2015.

[7] A. Houmansadr, N. Borisov. CoCo: Coding-Based Covert Timing Channels for Network Flows, *Information Hiding, Lecture Notes in Computer Science*, 6958: 314-328, 2011.

[8] S. Cabuk, C.E. Brodley, C. Shields. IP Covert Channel Detection, *ACM Transactions on Information and System Security (TISSEC)*, vol.12, no.4, pp.1-29, 2009.

[9] G. Shah, A. Molina, M. Blaze. Keyboards and covert channels, *15th USENIX Security Symposium*, pp.59-75, 2006.

[10] S. Cabuk. Network Covert Channels: Design, Analysis, *Detection and Elimination. PHD thesis, Purdue university, USA*, 2006.

[11] S. Gianvecchio, H. Wang, D. Wijesekera, et al.. *Model-Based Covert Timing Channels: Automated Modeling and Evasion, Recent Advances in Intrusion Detection, Lecture Notes in Computer Science*, 5230: 211-230, 2008.

[12] G. Liu, J. Zhai, Y. Dai, et al..Network Covert Timing Channel with Distribution Matching, *Telecommunication Systems*, vol.49, no.2, pp.199-205, 2012.

[13] F. Rezaei, M. Hempel, P. L. Shrestha, et al.. Achieving Robustness and Capacity Gains in Covert Timing Channels, *IEEE International Conference on Communications* pp.969-974, 2014.

[14] Y. Yang, M. Lei, X. Niu, et al.. Autio blind watermarking scheme combined DWT-DCT-QR, *Journal of Chongqing University*, vol.35, no.8, pp.62-66, 2012.