Implementing Covert Channels to Transfer Hidden Information Over Whatsapp on Mobile Phones

Esmira Mustafayeva, Gunay Huseynova, Vagif Gasimov

Abstract— **Covert channels may be used to ensure protection of information during legal transfers, as well as for illegal and secret transfer of official and commercial secrets, confidential and individual data, and state secret with the purpose of sharing necessary information to commit a crime.**

Therefore, the problem of transferring hidden information to create covert channels over WhatsApp has been studied in the article, and the possibilities of using different graphic file formats, as well as using existing stenographic software developed for Windows and Android operating systems have been investigated.

Index Terms— **steganography, secret channel, Whatsapp, steganocontainer, steganographical program**

I. INTRODUCTION

Currently, Internet network and its capabilities are widely used in the world for the purpose of information exchange. Internet network provides equal opportunities for all people and organizations using its services, including criminal and terrorist groups and individuals. Advanced telecommunications systems, computer and information networks, including Internet are used as a tool for information struggle, confrontation and war, as well as cybercrime and cyberterrorism along with being used in service activities by individuals, politicians, businessmen, state, private and religious organizations, criminal and terror groups and special services of rival (enemy) countries [1, 2].

One of the opportunities provided by Internet is creation and use of covert channel. During exchange via such channels, information is not only transferred from one place to another, but the fact of transfer together with sender and receiver can be maintained confidential.

It should be noted that interest in stenographic technology can be related to several factors based on its privacy principles. Some examples of such factors are listed below [3-10]:

- Implementation of hidden information exchange (legal or illegal);
- Spying on political, technical, military and other types of secrets;
- Serving for criminal, terrorist and other unlawful structures;
- Providing group members with instructions, guidance and other information for managing criminal activities;
- Passing the individual, official and commercial secrets to the rivals;
- Creating secret archives;
- Creating secret systems to manage important systems which cannot be monitored by radio and electronic surveillance;
- Protecting copyrights on electronic products;
- Avoiding illegal reproduction and trade of electronic products.

Such stenographic channels can be implemented through service and technologies such as internet e-mail, Web pages, network protocols, social networks, cloud technologies etc. This article studies the methods of creating covert channels for hidden information transfer over WhatsApp.

It is clear that transmitter, receiver and communication channels are required for creation of channel. Such channels may be open or protected. Covert channels are implemented on existing open and protected channels. Covert channels can be created on any open or protected channel. To do this, acontainer capable of carrying hidden information is required along with open or protected channel. Information placed in container and transferred via covert channels is called steganogram [7,8,11,12]. Any file, image, graphic design, audio-video file, electronic mail, message, web-page, user profile, text fragments etc. can act as a container [13].

As a covert channel, protocols such as TCP/IP protocols [14-17], VOIP protocol [18-23], HTTP protocol [24-26], cloud technology [27-31], Skype [32-34] and social networks [35-38] may be used.

Experiments have been carried out on Facebook, Twitter, Google+, Instagram and other social networks in order to create covert channel for hidden information transfer [34-38]. In addition to aforementioned social networks, WhatsApp instant messenger for mobile phones may also be used for creation of covert channel. Despite created relatively later (in 2009), WhatsApp has been able to attract wide range of customers within a short time. Currently, millions of people widely use this service to communicate, transfer image, voice and video or call online.

As mentioned earlier, digital objects (file, image, graphic design, audio, video, Web-page, text etc.) and their transfer via internet may be used to create covert channels for data transfer. That is, any hidden information may be placed (embedded) in an image or graphics and it can be sent using WhatsApp without causing any suspicion.

During this process, file formats of the files transferred via WhatsApp may be subject to change leading to damage or loss of the hidden data embedded in the file. Therefore we have studied format of the files which can be used as a container during transfer of such files via WhatsApp, and investigated whether transferred files have been modified and/or data loss has happened inside the file.

Esmira Mustafayeva, Institute of Control Systems, National Academy of Sciences of Azerbaijan, Baku, Azerbaijan, +994505534346

Gunay Huseynova, Department of Computer Engineering, Faculty of Information Technology and Management, Azerbaijan State University of Oil and Industry, Baku, Azerbaijan, +994517712628

Vagif Gasimov, Department of Computer Systems and Nets, Faculty of Automation and Computer Engineering, Azerbaijan Technical University, Baku, Azerbaijan, +994503172754

II. METHODOLOGY

During experiment, exchange of image files containing information has been carried out via WhatsApp. Toshiba Satellite L655-S5061 model laptop and Samsung Galaxy J1 Ace SM-J110H/DS White 4GB 3G smartphone, as well as Dell Latitude E6420 model laptop and LG-K350Z smartphone have been used as technical platform. Experiments have been carried out in Windows and Android operating systems, and steganographic software developed for these operating systems have been used.

During experiments, performances of S-Tools, Stegan PEG, Open Stego, Quick Stego, JP Hide and Seek, Image Steganography, DeEgger Embedder, Hide N Send, SilentEye and Invisible Secrets 4 steganographic software in Windows operating system and Secret Tigings, Stegais, Secret Image, Steganogropia, Hidden Secrets, Pocket Stego, Photo Hidden, IMessAGE, VIP Secret, Stegos, Monalisa and Steg APP steganographic software in Android operating system have been investigated.

These software are selected among other steganographic software for being free, simple and most commonly used. Along with different format image files (GIF, BMP, PNG, JPEG etc), they also support audio (WAV, MP3) files, even (Invisible Secrets 4 steganographic software) web page (HTML) as container. Moreover, secret data sent may be text, image, video file or simple message. Most of the aforementioned software are also capable of encrypting hidden information.

Steganographic software and password are agreed upon between the parties prior to information exchange process. Sender inserts the secret information to previously selected image by using steganographic software. Once the steganocontainer is ready, it is sent via WhatsApp to recipient. Recipient restores the hidden information through the image she has received via WhatsApp by using the previously agreed upon steganographic software and password.

In this article, we use Stegais software for Android as an example in the experiment to provide a clearerexplanation of information exchange. It should be noted that information hidden in this software can be sent as text or voice. The sender should use the ***Text*** button if the information is sent in the text format or ***Voice*** button if sent in the voice format. Information exchange has been carried out in both format and the result of the experiment was successful.

Text button is selected in the first page of the software. After typing the message "See you tomorrow morning at 9.", previously determined image from the memory of phone is selected as container via ***Choose Image*** button. Then, ***Hidden*** button performs the hiding operation. Once the hiding is completed, it is sent to recipient via ***Send as eMail***. The process of preparation of the steganocontainer is reflected in the Figures 1 and 2.

Steganocontainer received by the recipient in WhatsApp address is opened via Stegais software. Another window is opened by clicking the button ***Reveal the Message*** in the first window**,** and ***Choose Image*** button is selected to download the steganocontainer to the application. Information embedded in steganocontainer, which is the message "See you tomorrow morning at 9", is reflected via ***Reveal*** button. Steganocontainer restoration process is reflected in Figure 3.

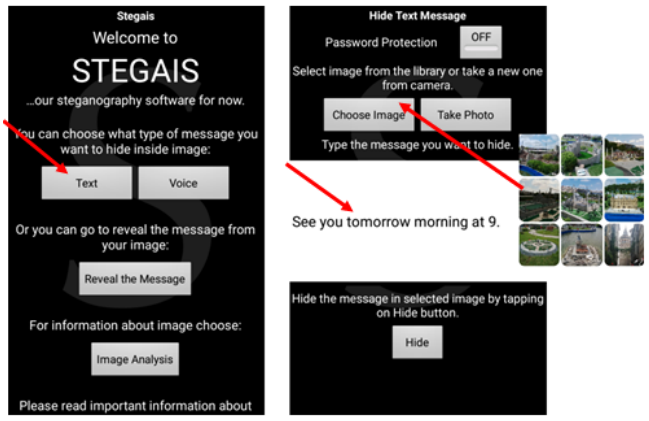

Figure 1

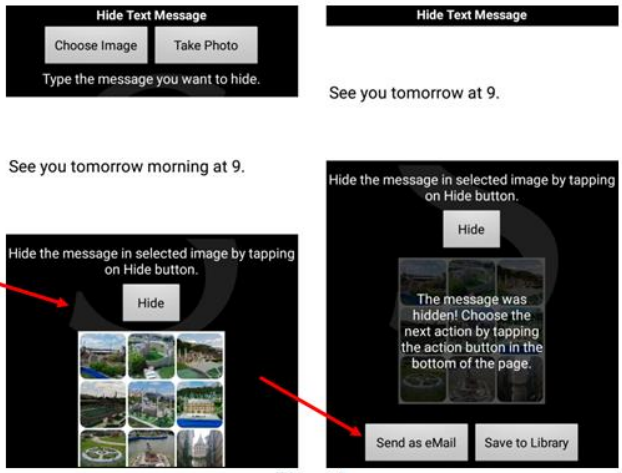

Figure 2

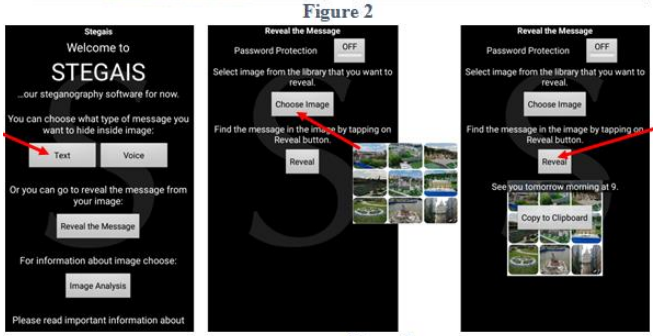

Figure 3

III. RESULTS

Experiment shows that images in gif, bmp, png and other format transferred as container during exchange are received by the recipient in the JPEG format. Therefore, it is reasonable to use JPEG format images. It is revealed that images of other format are altered and the data inside is lost when sent via WhatsApp. Therefore only the images of JPEG format and steganographic software supporting this format have been used during experiment.

As stated above, experiments have been carried out by using several steganographic software such as Stegan PEG, Open Stego, Quick Stego, JP Hide and Seek, Image Steganography, DeEgger Embedder, Hide N Send, SilentEye, Invisible Secrets 4 in Windows and Secret Tigings, Stegais, Secret Image, Steganogropia, Hidden Secrets, Pocket Stego, Photo Hidden, IMessAGE, VIP Secret, Stegos, Monalisa, Steg APP in Android. Several different image files in different formats have been selected as containerin each of the aforementioned software and various data has been embedded in each file. The results throughout all tests have been identical.

Part of the experiment has been carried out in Toshiba

Satellite L655-S5061 model Laptop as some software were developed for Windows operating system, and WhatsApp Web has been used in order to transfer via WhatsApp. To process the steganocontainer, namely, to restore the hidden information, data was sent from LG-K350Z smartphone to Dell Latitude E6420 model laptop.

Experiment has been carried out at two different times. In both experiments, it is observed that the steganocontainer implemented through JPHS and SilentEye software for Windows operating system using WhatsApp Web for Windows 0.2.2732 and WhatsApp Messenger 2.16.371 versions reaches the recipient successfully without any change or loss during information exchange. Another important observation is that the sizes of steganocontainers do not change during transfer.

However, further experiment revealed that data loss occurs in steganocontainer during data exchange via WhatsApp Web for Windows 0.2.4240 and WhatsApp Messenger 2.17.190 version. Both experiment results are reflected in the Table 1.

Table 1. Steganographic techniques supported on WhatsAppforWindows

Steganographic Tools For Windows	Format Used	Successful Extraction Secret Message WhatsApp Web 0.2. 2732 and WhatsApp Messenger 2.16.371	Successful Extraction Secret Message WhatsApp Web 0.2.4240 and WhatsApp Messenger 2.17.190
Stegan PEG	JPEG	No	No
Open Stego	JPEG	No	No
Quick Stego	JPEG	No	No
JP Hide and Seek	JPEG	Yes	No
Image Steganography	JPEG	No	No
DeEgger Embedder	JPEG	No	No
Hide N Send	JPEG	No	No
SilentEye	JPEG	Yes	No
Invisible Secrets 4.	JPEG	No	No

Experiments at both times revealed that no change with respect to size of images has been detected during the information exchange through steganocontainers implemented via WhatsApp by Android's Stegais and Stegos software and data is successfully delivered to the recipient without any change or loss. Results are reflected in the Table 2.

Table 2. Steganographic techniques supported on WhatsApp forAndroid

Steganographic Tools For Android	Format Used	Successful Extraction Secret Message
Secret Tigings	JPEG	No
Stegais	JPEG	Yes
Secret Image	JPEG	No
Steganogropia	JPEG	No
Hidden Secrets	JPEG	No
Pocket Stego	JPEG	No
Photo Hidden	JPEG	No
IMessAGE	JPEG	No
VİP Secret	JPEG	No
Stegos	JPEG	Yes
Monalisa	JPEG	No
Steg APP	JPEG	No

IV. Conclusion

Experiment shows that covert channels can be created by embedding information in image files and using them as container in WhatsApp. Based on the results of the experiment, it becomes clear that covert channels cannot be created in WhatsApp via software running on Windows operating system. Covert channel can only be created through Stegais and Steganos software running on Android operating system. It is also known that image files (containers) should only be JPEG format files.

References

[1] Brunst, Phillip W. ″Terrorism and the internet: New threats posed by cyberterrorism and terrorist use of the internet.″ In A War on Terror?, Springer New York, 2010; 51-78.
[2] Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq. Monoqrafiya. Bakı. Elm. -192 s. 2007.
[3] Bender W, Gruhl D, Morimoto N, Lu A. ″Technique For Data Hiding″ IBm Systems Journal, Vol.35, Issue 3&4, 1996; 316-336.
[4] Husrev T. Sencar, Mahalingam R, Akansu A. Data Hiding Fundamentals and Applications. Content Security in Digital Multimedia. Elsevier Science, Sep 09, 2004; p. 272.
[5] Halder R, Pal SH, Cortesi A. Watermarking Techniques for Relational Databases: Survey, Classification and Comparison. Journal of Universal Computer Science, 16(21): 3164-3190, 2010.
[6] U. Manber. Finding Similar Files in a Large File System. Proceedings of the USENIX Winter Technical Conference; 1994.
[7] Грибунин В, Оков И, Туринцев И. Цифровая стеганография. — М.: Солон-Пресс, -272 с. 2002.
[8] Конахович Г, Пузыренко А. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, -288 с. 2006.
[9] Gasimov V, Mustafayeva E. ″The methods of creation of covert channels on the internet for hidden transfer of information″ National security and military sciences
scientific-practical journal 2016; vol. 2. Number 3, pp. 122-128. (article in Azerbaijani with an abstract in English)
[10] Голубев В. "Компьютерная стеганография – защита информации или инструмент преступления?". http://www.crime-research.ru/library/Steganos.htm
[11] Ahsan K, Kundur D. Practical Data Hiding in TCP/IP // Proc. ACM Wksp. Multimedia Security. — 2002.
[12] Тимонина, Е. Е. Скрытые каналы (обзор) // Jet info. — 2002; — выпуск 11.
[13] Johnson N, Jajodia S. "Steganalysis: The investigation of Hidden Information", IEEE Infonnation Technology Conference, Syracuse, NY, USA, 1-3 September 1998. konfrans
[14] Rowland C. Covert Channels in the TCP/IP Protocol Suite. First Monday, Peer Reviewed Journal on the Internet, 2(5), January 1997.
[15] Ahsan K, Kundur D, ″Practical Data Hiding in TCP/IP″ in Proc. ACM Workshop. Multimedia Security, Dec. 2002.
[16] Giffin J, Greenstadt R, Litwack P, Tibbetts R, "Covert Messaging Through TCP Timestamps" Massachusetts Institute of Technology - MIT, USA, 2002.
[17] Murdoch S, Lewis S. Embedding Covert Channels into TCP/IP. In Information Hiding: 7th International Workshop, volume 3727 of LNCS, pages 247–261. Springer, 2005.
[18] Dittmann J, Hesse D, Hillert R. Steganography and steganalysis in voice-over IP scenarios: operational aspects and first experiences with a new steganalysis tool set, Proc. of SPIE, Vol. 5681, Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, 2005; pp. 607-618.
[19] Wang C, Wu W. Information Hiding in Real-Time VoIP Streams, Ninth IEEE International Symposium on Multimedia (ISM 2007); Taichung, Taiwan, 10-12 Dec. 2007; pp. 255 – 262.
[20] Takahashi T, Lee W. An Assessment of VoIP Covert Channel Threats. In: Proc. of 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007); Nice, France. 2007.
[21] Aoki N. A Technique of Lossless Steganography for G.711 Telephony Speech, International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2008); Harbin, China, 15-17 August 2008; pp. 608-611.
[22] Miao R, Huang Y. An Approach of Covert Communication Based on the Adaptive Steganography Scheme on Voice over IP,

Communications, IEEE International Conference on (ICC 2011); 2011.
[23] Mazurczyk W, Kotulski Z. New security and control protocol for VoIP based on steganography and digital watermarking, In Proc. of 5th International Conference on Computer Science - Research and Applications (IBIZA 2006); Poland, Kazimierz Dolny 9-11 February 2006.
[24] Johnson D, Yuan B, Lutz P, Brown E. Covert channels in the HTTP network protocol:Channel characterization and detecting man-inthe-middle attacks. Rochester Institute of Technology RIT Scholar Works. 2010.
[25] Bowyer L. Firewall Bypass via protocol Steganography. Online posting. 2002; Sep 22.
[26] Bauer M. New Covert Channels in HTTP:Adding Unwitting Web Browsers to Anonymity Sets. In Samarati P, Syverson P, editors. Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society, 2003; Oct 30; Washington, DC. ACM Press. p 72-78.
[27] Ristenpart T, Tromer E, Shacham H, Savage S. ″Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds″. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS‟09), November 2009.
[28] Mazurczyk W, Szczypiorski K. Is Cloud Computing Steganography-proof?. Institute of Telecommunications. Warsaw University of Technology/Warsaw, Poland.
[29] Lipiński B, Mazurczyk W, Szczypiorski K. Improving Hard Disk Contentionbased Covert Channel in Cloud Computing Environment. Warsaw University of Technology, Institute of Telecommunications. Warsaw, Poland.
[30] Волокита А, Бидков А. Защищенная Многоканальная Передача Данных В Cloud Computıng. “АСАУ” – 20(40) 2012. 153-158 с. ISSN 1560-8956. УДК 004.056.
[31] Huseynova G. Realization Of The Covert Channel For Information Transmıssion Via Cloud Technology. Scientific Works of Azerbaijan Technical University, 2017; Number 2, pages 108-113, ISSN 1815-1779. UDC. 004.056:621. (article in Azerbaijani with an abstract in English)
[33] Hartman K. Skype and Data Exfiltration. April18, 2014; Page 2-62.
[34] Varenyuk A, Aleksandrovichivanov M, Makarov V, Shurygin V. By Means of Skype. IJCTA, 9(30), 2016; pp. 241-249. International Science Press.
[35] Galyaev V. About some experiments on the transfer stegomessages through social networks. // MATTEX 2014; pp. 119-122. volume 1. Section of Computing Informatics and Computing Information Technology. (article in Russian with an abstract in English)
[36] Chee A. Steganographic techniques on social media:Investigation guidelines. School of Computing and Mathematical Sciences. Auckland, New Zealand 2013; page 1-255.
[37] Ning J, Singh I, Madhyastha H, Krishnamurthy S, Caox G, Mohapatraz P. Secret Message Sharing Using Online Social Media. 2014; IEEE Conference on Communications and Network Security. Page 319-327.
[38] Szczypiorski K. StegHash: New Method for Information Hiding in Open Social Networks. Intl journal of electronics and telecommunications. VOL. 62, NO. 4, PP. 347-352 Manuscript received October 15, 2016; revised November, 2016.

Esmira Mustafayeva. I received higher education degree in Azerbaijan State Oil Academy, Baku, Azerbaijan. Right now I study PhD in System analysis, control and information processing (in Engineering), in Institute of Control Systems, National Academy of Sciences of Azerbaijan, Baku, Azerbaijan. I work as an assistant of professor on my specialty. The direction of my scientific work is information security. I am the author of 15 articles.

Gunay Huseynova. I had backelor and master degree in Computer Engineering at Azerbaijan State Oil Academy, Baku, Azerbaijan. I study PhD in System analysis, control and information processing (in Engineering), at Baku Engineering University, Baku, Azerbaijan. I work as an assistant of professor in Azerbaijan State University of Oil and Industry, Baku, Azerbaijan. The direction of my scientific work is steganography. I am the author of 14 articles.

Vagif Gasimov was born in Padar Village, Hajigabul of the Republic of Azerbaijan in 1963. He received higher education degree in Applied Mathematics from Moscow Oil and Gas University in 1986, doctor of technical science degree in system analysis and information processing in 2008, professor degree in information security in 2011.

From 1986 to 1990, he was a Research Assistant with the Mathematical Modelling in Biology. From 1990-2000, he has been a head of Computer Networks and Information Systems Laboratory. From 2000-2017, he has been a head of Educational Department and Professor with Information Security Department, Academy of the Ministry National Security. From 2017-2019, he has been a professor of Information Technology Department of National Aviation Academy. At present he is a head of the department of “Computer systems and networks” of Azerbaijan Technical University. He is the author of 20 books, more than 100 articles and 1 invention. His research interests include information security, cryptography, steganography, information retrieval, search methods and systems, computer networks, distributed information systems, information needs.

Prof. Gasimov was awarded by the President of the Republic of Azerbaijan a medal for achievements in the service in 2009, as well as state bodies with medals for excellence in work in 2008, 2009, 2014 and 2015.