The Research of Realization of Hidden Channel for Information Transmission with the Use of Steganographic Tools

Georgiy Konakhovich[1[0000-0002-6636-542X]], Yaroslav Symonychenko [1[0000-0002-9404-6610]], Anna Symonychenko[2[0000-0001-5317-3464]] and Yousef Ibrahim Daradkeh [3 [0000-0002-9209-0626]]

[1,2] National Aviation University, Kyiv, Ukraine
[3] Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[3] College of Engineering, Prince Sattam Bin Abdulaziz University, Department of Computer Engineering and Networks,Wadi Addawasir, KSA
yaroslavsim@ukr.net

Abstract. In the work we have conducted the research of realization of hidden channel of information transmission with the use of modern software steganographic tools that can be used for the purpose to gain unauthorized access to confidential information. We have researched software tools for data hiding that are available to any citizen through the Internet. Also we have conducted the research of modern realization of steganographic system and computer steganographic methods with the use of modern software steganographic tools for the purpose of possible preliminary research of organization of hidden channel of data leakage by an attacker. In this research we have found the detection of structural changes in received result computer files with hidden data and also comparing a received result container with an original container. On the basis of the conducted researches we have obtained results concerning the modern realization of methods of data hiding and realization of steganographic system components using steganographic software tools. These results can be used, where appropriate, to further improve efficiency of steganographic analysis. Also the obtained results make possible the modeling the realization of hidden channel of data leakage with the use of steganographic tools that can be used by an attacker and the research using methods of computer steganographic analysis for the purpose of detecting malicious content in result files.

Keywords: steganographic system, software steganographic tools, information protection, hidden channel of data transmission, steganographic analysis.

1 Introduction

The constant use of information technologies (software applications for instant messaging, social network communication, regular bank operations, working with email boxes, etc.) in the life and activities of a modern person led to the urgency of solving the issue of providing the information security and protection of information. Recent-

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

ly, it is constantly mentioned in the media the possibility of use of different technologies of hiding a message in information objects that led to increasing public interest in the technology and the possibility of its use.

One of the modern technologies that can be used not only for the purpose of organization of information protection but also for the purpose of possible organization of hidden channel of data leakage is steganographic information protection. Thus, according to the report of company Accenture Security, using steganographic technologies belongs to one of the five most notable threats faced by company employees in 2017. Also the activity of cyber-espionage group Tick, also known as Bald Knight, Bronze Butler, Nian and RedBaldKnight was associated with the use of steganographic methods of data hiding to gain access to computer network and unauthorized access to confidential information. ESET has reported the detection of network attacks of cyber –espionage group TheDukes (APT29 or CozyBear) on government institutions in Europe that spread necessary URLs of command server and applied steganographic methods to hide data in images to hide malicious content.

2 Task formulation

The use of above-mentioned steganographic methods of data hiding leads to the realization of special steganographic systems. This system embeds the hidden data (message) in information object (a computer file with an image, audio, video, text message, etc.) by using one of computer steganographic method, transmit hidden data by communication channels and decode it from the received information object. The transmission of information object with hidden data can be made by using information and telecommunication systems and the Internet or by a person on information carrier.

Most often, as steganographic means that can be used to hide and decode the hidden data are steganographic software tools. In this way, the purpose of this work is to research and analyze possible hidden channel of information transmission and modern the most widespread realization of steganographic system components using modern steganographic software products that are freely distributed through the Internet and can be used with the purpose to gain unauthorized access to confidential information. In the research we obtain the results concerning modern methods of realization of steganographic system components and computer steganographic methods with the purpose of research possible organization of hidden channel of confidential information leakage. The obtained results allow modeling a hidden channel with the use of modern steganographic software tools that can be used by an attacker and researching the use of computer steganographic analysis methods for the purpose to detect malicious content in result files and for possible increasing its efficiency.

3 Implementation

3.1 The principle of operation of steganographic system

To conduct this research we study more detailed the principle of realization of steganographic system. Under the steganographic system we should understand a combination of methods and tools (steganographic system components) that are used to build a hidden channel of information transmission [2]. A steganographic system embeds a hidden message in a computer file (with graphic data, audio, video, text information, etc.) using a steganocoder, transmits it through a steganographic channel (using telecommunication channels or a person on information carrier) and decodes a hidden message from the received result file using a steganodecoder (see Fig. 1).

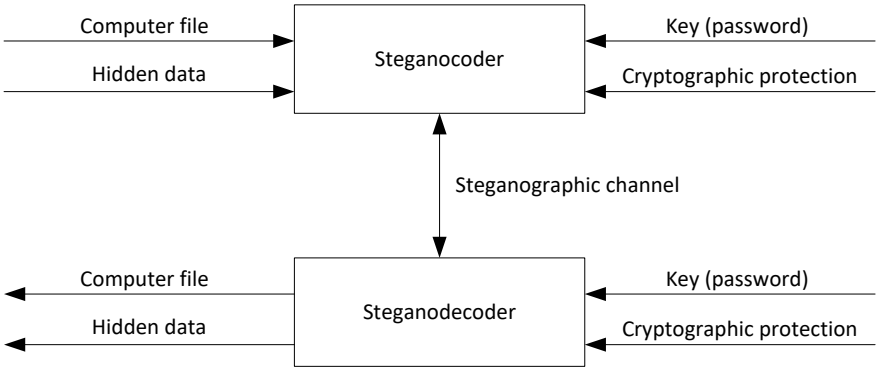

Fig. 1. Generalized model of realization of steganographic system.

Most often, steganographic systems use the key that is used to embed and decode the hidden data. This key defines the algorithm that determines the order of embedding hidden data in a computer file. There are two types of steganographic systems: system with a secret key (use one key to embed and decode data); system with a public key (use different keys to embed and decode hidden data). Steganographic protocols are used in order to coordinate users' actions when using steganographic systems. These protocols can be such types: keyless systems, systems with a public key, systems with a secret key and mixed system.

One of the main features of steganographic system is its bandwidth. Under the bandwidth we understand the maximum data amount that can be embedded in one element of a computer file (for example, pixel image) while using computer steganographic method [3]. By principle of data hiding computer steganographic methods are divided into direct replacement methods that replace least significant parts of a computer file with elements (bits) of hidden data, and spectral methods that use the spectral representation of elements of computer files which is being embedded with hidden data.

The use of a steganographic system leads to the realization of hidden communication channel that can be used by an attacker for the purpose to gain unauthorized access to confidential information [4].

Also the methods of computer steganographic analysis can be used to identify the above mentioned hidden channel of information transmission and the fact of availabil-

ity of hidden data (or malicious content) in a computer file. The main purpose of steganographic analysis is modeling steganographic system for further research to obtain the evaluation of reliability of using computer steganographic conversion and also formation methods of detection of hidden data in a computer file, its modification or destruction [5].

The obtained data can be used for a better understanding of realization and functioning of modern computer steganographic methods of hiding data (or malicious content) to increase the probability to detect hidden channel of information transmission that can be used by an attacker [6-9].

3.2 The research of realization of hidden channel and steganographic system

To research modern realization of possible hidden channel of information transmission we used 22 computer software tools that are available to a citizen through the Internet. The following software products are:

- OpenPuff;
- SilentEye;
- Camouflage;
- FIRA2;
- Hide&Reveal;
- SteganographXPlus;
- Clotho;
- HexaStego-BMP;
- ImageSpyer;
- SteganoG;
- S-Tools;
- XiaoSteganography;
- Hallucinate;
- SteganosSecuritySuite 2007;
- Anubis;
- DeEggerEmbedder;
- OurSecret;
- SteganosPrivacySuite 18;
- ImageSpyer G2;
- Shusssh!;
- JHide;
- QuickStego.

Steganographic coder (steganocoder) and steganographic decoder (steganodecoder) allow us to realize each of the above mentioned software products that provide the opportunity to embed necessary hidden data in a computer file with possible using of additional protection mechanisms (password or cryptographic protection) and decode it. To complete this task, we conduct the analysis of functionalities of software tools and research on the methods of their realization.

When researching the possibility to use the type of a computer file, for the purpose to embed and transmit the hidden data, we obtained the following results:

- support for using an image file was made in 21 software products;
- support for using an audio file was made in 5 software products;
- support for using a video file was made in 4 software products.

In this way, the most common file that can be used by software products is an image file.

When researching the possibility to use the type of hidden data we obtain further results:

- support for possible using a text message can be made in 22 software products;
- support for possible using a graphic message can be made in 15 software products.

As hidden data we use a text message that can be saved in a text file or an image that can be saved in an image file. So, given the functionality of the modern computer steganographic products the most common type of hidden data is a text message.

Additionally, to increase the protection level of accessibility of hidden data, modern software tools provide the opportunity to use a key (password) to protect hidden data from unauthorized cognizance. To increase the protection level of confidentiality of hidden data additionally cryptographic protection can be used. Thus, we obtained the results concerning the possibility of using additional protection mechanisms, namely, keys (supported by 17 software tools) and cryptographic protection mechanisms (supported by 7 software tools).

Taking into consideration the above research, when using the most widespread software tools, we embed a text message or a graphic message in a computer file with graphic information by one of the computer steganographic methods.

For further research we embed data in an image file and receive an image file with hidden data for every software tool. The next step of our research is to analyze the size changes of the received result image files after their modification by computer steganographic software tools compared to the origin image file that doesn't contain hidden data.

When researching this indicator, we obtained the following results: we noted that the size of an image file, after steganoconversion, changes only by using 6 software tools; and in other cases when using other 16 software tools we noted no changes in size, the size remained unchanged. So given the above information, the change of the size of an image file occurred as a result of addition hidden data in the end of a file by using the method "gluing". The size of the other image files, after hiding data, matches the size of the original file. This information can indicate possible use of computer steganographic methods of data hiding which lead to the change in structural content compared to an origin file and allow saving the size of a file after steganographic transformations.

So that the aim of this work is to research computer steganographic methods, we conduct the research of 16 software products that use steganographic methods in its functioning. In order to research possible computer methods of steganographic transformations we conduct more detailed research of 16 images with hidden data that are received by software products using steganographic methods, namely comparison of the pixels of received result images with the pixels of origin image and possible their

modification. When researching this indicator, it was found that the pixel modification of the received result images was detected while using 16 software products. The use of researched computer steganographic methods can lead to possible direct replacement of least significant parts of the image by bits of hidden data.

For more detailed research we research possible modification of color components of received result images. When using 24-bit image it is used a color RGB-model with such components: R- red component of the image, G - green, B – blue. To code the color gradation of each component it is used 8 bit (a total 24 bits to code all color components).

When researching the modification of color component, we obtain the following:

- the modification of all 3 color component was done by 15 software products;
- the modification of the red color component only was done by one software products.

The other 6 software products use the method “gluing”, so the modification of color component and structural content are missing in the received result images. To research the bandwidth of steganographic system that is realized by using 16 above mentioned software products, we conduct the more detailed research of some indicators. We embedded three different text messages of different volume in the image file. The volume of hidden data accounted for 5%, 15% and 25% accordingly of the volume of image file. After receiving three different image files we analyzed the sizes of received result files and found that the size of the files remained unchanged after increasing the volume of hidden data. Also, we researched the visual distortion of received result images when increasing the volume of hidden data and obtained the result that the number of modified pixels of the image increase the volume of hidden data proportionally.

3.3 The analysis of the results of the research

Therefore, during the research we used 22 software tools of data hiding. When conducting the research, we obtained the results concerning the modern methods of realization of steganographic system components and computer steganographic methods [8-12]:

- types of computer files and hidden data that can be used by modern computer steganographic tools (software products) for data hiding;
- research the possibility of using additional mechanisms of hidden data protection by software products;
- research the changes of size of the received result image files compared to the original image file;
- research the visual distortion and the pixel modification of the received result image compared to the original image;
- research the modification of the color components of the received result images when using software products that used by steganographic methods in their functioning.

Taking into consideration the above obtained results of the research, we can make up the conclusions about the realization of components of steganographic system (Table 1).

Table 1. Types of supported computer files and hidden data

Software product	Computer file types (image file / audio file/video file)	Hidden data type (text/graphic)
Camouflage	+ / + / +	+ / +
DeEggerEmbedder	+ / + / +	+ / +
HexaStego-BMP	+ / - / -	+ / +
ImageSpyer	+ / - / -	+ / +
JHide	+ / - / -	+ / +
QuickStego	+ / - / -	+ / -
SilentEye	+ / - / -	+ / +
SteganosSecuritySuite 2007	+ / + / +	+ / +
SteganographXPlus	+ / - / -	+ / -
XiaoSteganography	+ / - / -	+ / -
Hallucinate	+ / - / -	+ / -
Clotho	+ / + / +	+ / +
FIRA2	- / - / -	+ / +
Hide&Reveal	+ / - / -	+ / -
ImageSpyer G2	+ / - / -	+ / +
OurSecret	+ / - / -	+ / +
Shusssh!	+ / - / -	+ / -
SteganosPrivacySuite 18	+ / + / -	+ / +
SteganoG	+ / - / -	+ / +
S-Tools	+ / - / -	+ / +
Anubis	+ / - / -	+ / -
OpenPuff	+ / - / -	+ / +

As a steganocoder and a steganodecoder we can use computer software products that are freely distributed through the Internet and available to every user.

The most common type of supported computer file that can be used to transmit the hidden data (message) is a file with graphic information (an image file of BMP format).

The most common type of hidden data is text information (a message) and graphic information (an image).

Also, the computer steganographic products that we researched in this work let us use additional mechanisms of security protection of hidden data (a message or an image): the use of a password and cryptographic protection of a hidden message that

provides and enhances the level of protection of confidentiality and availability. The use of these mechanisms made impossible the cognizance with hidden data by «third» people. When we researched the indicator of the size of an image file after steganographic transformation, we found that the following software products change the size of an image file, when the volume of hidden data increases:

- Clotho;
- Camouflage;
- DeEggerEmbedder;
- OurSecret, Anubis;
- Shusssh!.

The increasing of the size of a image file was made proportionally to the increasing in volume of hidden data. We can see the change of the size of an image file as a result of the addition hidden data in the end of the file when using the method of "gluing". The size of the image file when using the other 16 steganographic software products remains unchanged, just as to hide the necessary information it is used computer steganographic methods.

To research the realization of the above method we researched visual distortion of the image based on the indicators of pixel modification of the image and its color components (Table 2).

Table 2. Research of the modification of received result images and their color components

Software product	Image pixel modification	Modification of colour components of image (R/G/B)
Camouflage	-	- / - / -
DeEggerEmbedder	-	- / - / -
HexaStego-BMP	+	+ / + / +
ImageSpyer	+	+ / + / +
JHide	+	+ / + / +
QuickStego	+	+ / + / +
SilentEye	+	+ / + / +
SteganosSecuritySuite 2007	+	+ / + / +
SteganographXPlus	+	+ / - / -
XiaoSteganography	+	+ / + / +
Hallucinate	+	+ / + / +
Clotho	-	- / - / -
FIRA2	+	+ / + / +
Hide&Reveal	+	+ / + / +
ImageSpyer G2	+	+ / + / +
OurSecret	-	- / - / -
Shusssh!	-	- / - / -
SteganosPrivacySuite 18	+	+ / + / +
SteganoG	+	+ / + / +
S-Tools	+	+ / + / +
Anubis	-	- / - / -
OpenPuff	+	+ / + / +

It was found that all 16 software products made the pixel modification of the image when embedding a hidden message and the number of modified pixels of the image increases proportionally when the hidden message increases. Only the modification of the red component is made when using software product SteganographXPlus.

Other 15 software products modify all three color components of the image. For a more detailed research on the modification of color components of the image we analyzed the modification of their bit planes. In general, during the research, we made the modification only four bit plains with a bit capacity «0», «1», «2» та «3» (Table 3).

Table 3. The research of modification of bit plains of color component of the image

Software products	Number of the bit plane		
	Red (0/1/2/3)	Green (0/1/2/3)	Blue (0/1/2/3)
FIRA2	+ / + / - / -	+ / + / - / -	+ / + / - / -
HexaStego-BMP	+ / + / - / -	+ / + / - / -	+ / + / - / -
Hide&Reveal	+ / - / - / -	+ / - / - / -	+ / - / - / -
ImageSpyer	+ / + / +/ -	+ / + / +/ -	+ / + / +/ -
ImageSpyer G2	+ / + / +/ -	+ / + / +/ -	+ / + / +/ -
JHide	+ / + / - / -	+ / + / - / -	+ / + / - / -
QuickStego	+ / - / - / -	+ / - / - / -	+ / - / - / -
SilentEye	+ / + / +/ -	+ / + / +/ -	+ / + / +/ -
Steganos Privacy Suite 18	+ / - / - / -	+ / - / - / -	+ / - / - / -
Steganos Security Suite 2007	+ / - / - / -	+ / - / - / -	+ / - / - / -
SteganoG	+ / - / - / -	+ / - / - / -	+ / - / - / -
SteganographX Plus	+ / - / - / -	- / - / - / -	- / - / - / -
S-Tools	+ / - / - / -	+ / - / - / -	+ / - / - / -
Xiao Steganography	+ / - / - / -	+ / - / - / -	+ / - / - / -
Hallucinate	+ / + / +/ +	+ / + / +/ +	+ / + / +/ +
OpenPuff	+ / - / - / -	+ / - / - / -	+ / - / - / -

When we used Hide&Reveal, QuickStego, Steganos Privacy Suite 18, Steganos Security Suite 2007, SteganographX Plus, S-Tools, Xiao Steganography та OpenPuff, we modified one bit plain of the image with a bit capacity «0». The use of FIRA2, HexaStego-BMP, JHide and SteganoG led to modification of two bit plain of the image («0» та «1»). The use of ImageSpyer, ImageSpyer G2 and SilentEye led to modification of three bit plains of the image («0», «1» та «2»). Hallucinate modified four bit plains of the image («0», «1», «2» та «3»). Given the meaning of the indicators of a number of modified pixel values and color components of the received result images, we can make up the conclusions that software products that use computer steganographic methods of data hiding base on the modification of bit plain of color component of the image.

4 Conclusions

We have conducted the research of the realization of hidden channel of information transmission with the use of modern software steganographic tools that can be used for the purpose to gain unauthorized access to confidential information.

The research was based on software tools for hiding data that are available for every person through the Internet. We obtained the results concerning modern realization of components of steganographic system and computer steganographic methods for the purpose of possible preliminary research of the organization a hidden channel of data leakage by an attacker. In this research, we found the structural changes in received result computer files with hidden data compared to the origin file.

Given the results of this research we can make up the following conclusions:

- computer steganographic products can be used as a steganocoder and a steganodecoder;
- the most common type of supported computer file that can be used to transmit the hidden data (a message) is a file with graphic information (an image file of BMP format);
- the most common type of hidden data is text information (a message) and graphic information (an image).

As the method of hiding data in computer file it is used computer steganographic methods that support the direct replacement of least significant parts of the image (extra information) with bits of hidden data. Some software products add the hidden data in the end of a file using the method “gluing”. The results that we obtained help us to model the realization of hidden channel of data leakage with the use computer steganographic tools that can be used by an attacker and research the use of computer steganographic analysis methods for the purpose to detect malicious content in result files.

References

1. Yudin O.F., Veselska O.S.: The spatial pixel method of digital stenography with the use of spatial filtering for decoding a secret message. Science-Based Technologies 1 (37), 67-72 (2018).
2. Buchyk S.F., Shalaev V.S.: The analysis instrumental methods of identification of risks of information security information and telecommunication systems. Science-Based Technologies 3 (35), 215-224 (2017).
3. Buchyk S.F., Grischenko M.S.: The designing and realization of the software of knowledge control subsystem and means of distance learning. Bulletin of Engineering Academy of Ukraine (3), 270-275 (2017).
4. Tolyupa S.F., Parchomenko I.S.: The construction of complex systems of complicated information systems based on the structural approach. Modern information security. (4), 62-70 (2015).
5. Yudin O.F., Boyko Y.S.: The technology of images decompression with the given level of visualization quality. Science-Based Technologies 1 (25), 47-51 (2015).
6. Odarchenko R., Abakumova A., Polihenko O., Gnatyuk S. Traffic offload improved method for 4G/5G mobile network operator, Proceedings of 14th International Conference on

Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2018), pp. 1051-1054, 2018.

7. R. Odarchenko, V. Gnatyuk, S. Gnatyuk, A. Abakumova, Security Key Indicators Assessment for Modern Cellular Networks, Proceedings of the 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC), Kyiv, Ukraine, October 8-12, 2018, pp. 1-7.
8. Z. Hassan, R. Odarchenko, S. Gnatyuk, A. Zaman, M. Shah, Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems, Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, October 16-18, 2018. Kyiv, Ukraine, pp. 283-288.
9. Fedushko S., Syerov Y., Kolos S. Hashtag as a Way of Archiving and Distributing Information on the Internet. CEUR Workshop Proceedings. 2019. Vol. 2386: Workshop Proceedings of the 8th International Conference on “Mathematics. Information Technologies. Education 2019. P. 274–286. http://ceur-ws.org/Vol-2386/paper20.pdf
10. M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Yu. Petrova. A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.
11. Mazin Al Hadidi, Jamil S. Al-Azzeh, R. Odarchenko et al, Adaptive Regulation of Radiated Power Radio Transmitting Devices in Modern Cellular Network Depending on Climatic Conditions, Contemporary Engineering Sciences, Vol. 9, № 10, pp. 473-485, 2016.
12. Al-Azzeh J.S., Al Hadidi M., Odarchenko R. et al, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations, № 10(5), pp. 328-336, 2017.