IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006336 |

Performance Analysis of A Number of Software for Steganographic Protection of Information

Asiya Tureniyazova

Nukus Branch of Tashkent University of Information Technologies Nukus, Uzbekistan

ABSTRACT: The article provides an analysis of the efficiencyof work ofa number ofsteganographysoftwarein hiding secret messages.

KEYWORDS: Information security, hiding information, computer steganography, digital steganography, steganography software.

INTRODUCTION

The relevance of ensuring information security against unauthorized access, guaranteeing confidentiality and integrity of transmitted personal, commercial or diplomatic information proceeds from the issues of protecting constitutional human rights, protecting property of business entities, as well as defense ofthe state interests.When choosing amongstthe information protection measures, the decision should be made on the basis of an analysis of the vulnerability of the computer network, the value of information stored and transmittedas well as degree of threat. Applicability of these meansis another subject to be considered.Finally, the choice of information security measures should be justified in terms of economic feasibility and effectiveness of the selected measures and means. This article suggests an analysis of work of steganographysoftware in hiding secret messages.

II.JUSTIFICATION OF USE OF STEGANOGRAPHY TOOLS FOR HIDING THE INFORMATION

The popularity of research in the field of steganography is currently due to two reasons: the restriction on the use of cryptographic tools in several countries of the world and the emergence of the problem of protecting property rights to information presented in digital form.

A common feature of steganographic methods is that the hidden message is embedded in some harmless object that does not attract attention. Then this object is openly transferred to the addressee. With cryptography, the presence of an encrypted message in itself attracts the attention of opponents, with steganography, the transmitted object is not suspicious and the presence of a hidden connection remains invisible [1].

Steganographic methods of hiding information originate from ancient times, starting with a tattoo on a shaved head of a slave, waxing letters on tablets, the method of invisible ink, microdots, as well as methods such as recording on the side of a deck of cards, writinginside a boiled egg, matchboxes, "Slang ciphers" with the conditional meaning of words, stencils for opening only meaningful letters, knots on strings, geometric shape, semagrams and later ones, such as microphotographs, conditional arrangement of characters, secret channelsand communication facilities at floating frequencies, etc.

When protecting the system with steganography methods, the following points should be taken into account[2]:

- the adversary has a complete understanding of the steganographic system and the details of its implementation and does not have information only about the key, with the help of which only its holder can establish the fact of presence and content of the hidden message;
- the potential adversary should be deprived of any technical and other advantages in recognizing or disclosing the content of secret messages, and even information about the existence of a hidden message should not allow him to extract such messages in other data as long as the key is kept secret.

III.ADVANTAGES OF USING THE DIGITAL STEGANOGRAPHY

Steganography tool is used to embed the message in a carrier file by using modulation techniques. In the digital

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006336 |

world, most of the secret messages will be passed from source to destination using media files like videos, images etc.

In computer (digital) steganography, one information is hidden in another, and this concealment must be implemented in such a way that the properties and some value of the hidden information are not lost, as well as the inevitable modification of the information medium not only does not destroy the semantic functions, but also at a certain level abstraction did not even change them.This ensures that the transmission of one message inside another is not detected by traditional methods.

As a carrier (container) of hidden information should be an object (file) that allows distortion of its own information, not violating its functionality. The introduced distortion should be below the sensitivity level of the recognition means.Typically, image files or sound files are used for this purpose. Such files are very redundant and usually large in size, providing enough space to hide plain or formatted text.

In addition to covert messaging, steganography is one of the most promising areas used for authentication and labeling of copyright products. At the same time, the date and place of creation of the product, information about the author, license number, serial number, expiration date, say shareware programs, etc. are often used as embedded information.This information is usually embedded both in graphic and audio - video works, as well as in copyrighted software products. All information entered may be considered as strong evidence and are crucial when considering questions of authorship or to prove the fact of illegal copying.

In digital steganography, there are various ways to achieve hiding the information without coding. These software tools can hide your secret message behind the image or audio file, HTML file, DOC file or any other kind of file.

Now there is already a fairly large number of programs that use steganography and computer images as containers. Let us dwell on some of the most common ones.

III.THE EFFICIENCY ANALYSIS OF A NUMBER OF STEGANOGRAPHY SOFTWARE IN HIDING A SECRET MESSAGE

Search of software for reliable concealment of transmitted information revealed a number of programs for various operating systems available on the Internet for free.Top 10 free steganography software to download includes XiaoSteganography, ImageSteganography, Steghide, Crypture, RSteg, SSuitePiscel, OurSecret, OpenStego, SteganPEG, Hide'N'Send [4].Download and installation of these programs by links was successful.

Free text selected as secret message. The image of the building of the Nukus branch of the Tashkent University of Information Technologies will play the role of the container.

Original Image	Image with a hidden document
	

Analysis of work of programs Open Stego, Xiao Steganography, SteganPEG, SteganographX Plus, SSuite Piscel, Shusssh! in hiding the secret message in images, using various algorithms, is shown in the following Table.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006336 |

TABLE 1. Results of work of the different software for embedding the secret message in the graphical file container.

Application	Application Mode	Encryption type / strength (when applicable)	Original image file type	Original size	Size of the secret document	Final size	Size Increase in KB (Original vs Final)	Size Increase in % (Original vs Final)	Comments
OpenStego	Hide Data	AES / 128	BMP	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Best encryption method today. No size or quality difference
OpenStego	Hide Data	AES / 128	JPG	691 KB	155,0 KB	2291 KB	1600 KB	231,55%	Best encryption method today. No size or quality difference
OpenStego	Hide Data	AES / 256	BMP	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Best encryption method today. Changing the encryption strength does not increase size
OpenStego	Hide Data	AES / 256	JPG	691 KB	155,0 KB	2291 KB	1600 KB	231,55%	Best encryption method today. Changing the encryption strength does not increase size
Xiao Steganography	Add Files	RC2	BMP only	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Only supports BMP and only works with TXT Files. Encryption method has no effect on size
Xiao Steganography	Add Files	RC4	BMP only	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Only supports BMP and only works with TXT Files. Encryption method has no effect on size
Xiao Steganography	Add Files	DES	BMP only	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Only supports BMP and only works with TXT Files. Encryption method has no effect on size
Xiao Steganography	Add Files	Triple DES	BMP only	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Only supports BMP and only works with TXT Files. Encryption method has no effect on size
Xiao Steganography	Add Files	Triple DES 12	BMP only	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Only supports BMP and only works with TXT Files. Encryption method has no effect on size
SteganPEG	NA	Unknown	JPG only	691 KB	155,0 KB	691 KB	0 KB	0,00%	Only works with JPG files. No size or quality difference. May not be fully secure due to encryption
SteganographX Plus	NA	Unknown	BMP only	3967 KB	155,0 KB	3967 KB	0 KB	0,00%	Image is changed to noise. Only works with BMP Files. Cannot import the file and have to copy paste. Can only use numbers in the password
SSuite Piscel	Encrypt Image	Unknown	BMP only	3967 KB	155,0 KB	5289 KB	1322 KB	33,32%	BMP only. Takes a very long time to complete and consumes a lot of CPU power
Shusssh!	Shusssh!'		BMP / JPG						Crashed. Can only accept small text. When the big text is pasted, it errors out

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 6, June 2021 ||

| DOI:10.15680/IJIRSET.2021.1006336 |

As can be seen from the table, OpenStego was better than other programs in the task of hiding information, using graphic files of both .bmp and .jpg formats.

IV.CONCLUSION

On the example of a number of software tools, the issues of using computer steganography methods to hide a secret message are considered.The techniques and algorithms for embedding textual information in graphic files are analyzed. Based on the analysis of the data, the program that most successfully completed the task was identified. All tested programs fulfilled the task, but the OpenStego program was the best among studied programsto hide and transmit text messages without losing its quality and without increasing the carrier'ssize. However, it should be noted that to complete the task the cover file (carrier) selected was required to have a large enough width and height to hide the document. We must also caution users against using online steganography tools, because of cyberattacks.

REFERENCES

[1] S. Kumar, S.K. Muttoo. A comparative study of image steganography in wavelet domain. - International Journal of Computer Science and Mobile Computing, IJCSMC, Vol 2, no. 2, 2013.
[2] GribuninV.G., OkovI.N., Turintsev I.V. Tsifrovayasteganografiya. — M.: «Solon-Press», 2002
[3] https://mind-control.fandom.com/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F
[4] https://www.compzets.com/view-upload.php?id=61&action=view

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details