UDC 004.056.55

METHOD OF 3D-STEGANOGRAPHY

Alexandr Kuznetsov[1], Oleh Stefanovych[1], Kateryna Kuznetsova[1], Mykola Pastukhov[2], Dmytro Prokopovych-Tkachenko[2]

[1] V. N. Karazin Kharkiv National University, Svobody Sq., 6, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, stif1304@gmail.com, kate.kuznetsova.2000@gmail.com

[2] University of Customs and Finance, Volodymyr Vernadsky St., 2/4, Dnipro, 49000, Ukraine
denart66@gmail.com, omega2@email.dp.ua

Reviewer: Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv University of Technology "STEP", Malom'yasnitska St. 9/11, Kharkiv, 61010, Ukraine
kavserg@gmail.com

Received on September 2018

Abstract: *In this work, a new direction of technical steganography related to the concealment of information in the process of layer-by-layer creation (cultivation) of a solid-state object using various 3D-printing technologies was investigated. Information data is converted into a digital 3D-model of elementary physical objects that are placed inside this 3D-model of the container product. After printing, a solid object physically contains the hidden information that cannot be deleted or distorted without damaging the container product. In addition, the applied methods do not reduce the operational, aesthetic and any other properties of the finished product. The proposed complex is invariant to the method of layer-by-layer growing, that is, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation.*

Keywords: *steganography; 3D-printing; hiding information data; 3D-model; laser scanners.*

1 Introduction

The steganography, in a broad sense, is such method of transmission of the coded information message in a case of when the fact of its existence is suppressed [1,2]. Unlike cryptography, steganography methods allow to replace unessential shares of data with confidential information so that it was impossible to suspect existence of the built-in secret message [1]. Today in connection with development of an ADP-equipment and new channels of communication there are new steganography methods, which are a cornerstone of information hiding in computer files. Computer files are containers, which possess the high level of redundancy (photo and video of the image, audio-files, text documents, etc.). Concealment is based on replacement of redundant data with information messages. Only the authorized officer who has the steganography key [1,2] can detect the fact of their existence.

In recent years there is a new direction of computer steganography based on concealment of information messages in artificially created containers in which redundancy is caused by technical features of storage, processing and/or data transfer [3-14]. Such methods of "technical" steganography are characterized on concealment of information messages in artificial containers, different by the nature. In particular, methods of network steganography as the carrier (container) use the packet transferred via network or set of data packets. Procedures of concealment and exception of information based on the use of features of functioning of network stack of data transfer protocols [3-6]. Creation of the covert cluster channels based on using of features of data storage in the modern file systems [7-9]. There are also other directions of development of technical steganography, in particular, based on using of artificial redundancy of three-dimensional (3D)-models of objects [10-14]. In recent years, three-dimensional models gained wide distribution in different branches, in particular, processing medical data, museum pieces and samples of cultural heritage, simulation models of industrial samples and productions, computer games and so forth. At the same time, steganography methods apply to protection of copyright of 3D-models, concealment of a certain information, protection against fortuitous distortions or certain errors, and so forth. So, researches of new methods of concealment of data with use 3D-technologies are perspective direction of the modern science.

This work describes new approach proposed in [15], about steganography concealment of data in solid objects using 3D-printing technology. This method transforms information messages into 3D-model, which is placed inside 3D-model of the container with subsequent printing (creation, cultivation). The appearance of the resulting solid object, its operational and aesthetic properties do not change during the process of embedding the information message. In addition, you cannot delete or distort this hidden message without destroying or significantly damaging the product. Consequently, we have new technology for steganography protection of information for covert transmission, to ensure copyright and the like.

2 Hiding Information Data

The prototype of complex of steganography protection was described in [15], in which information data hides by the process of layer-by-layer creation (cultivation) of the solid-state object using various 3D-printing technologies. The main idea is the embedding (steganography coding) of information data into digital 3D-model, whereby a solid object (a finished product or prototype for further using) creates (prints layer-by-layer). The embedding process is implemented using secret key data, excludes unauthorized access to protected information, violation of its integrity, authenticity and confidentiality. In addition, the applied steganography protection methods should not reduce the operational, aesthetic or any other properties of the finished product. So, the proposed complex (method) is invariant to the method of layer-by-layer growing, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation [15]. The main idea of data concealment is placing an information message in the middle of an arbitrary computer model of physical object that can be printed on a 3D-printer: toy, figure, souvenirs, etc. The information message is converted to a binary form and each bit becomes a specific piece of the physical model. As an example (Fig. 1), each bit can be encoded by a three-dimensional cube of the specified size. The filling of the cube corresponds to the content: "0" corresponds to the empty (*not filled*) cube, "1" - filled. An informative sign can also be another, for example, filling with different materials, or with one material, but with different density, orientation, filling, the form of elementary "bit" physical models, and the like.

For automated coding was used specialized software OpenSCAD, which is intended for creating solid-state 3D CAD-objects. It is free and available for Linux/UNIX®, Microsoft Windows® and Apple® Mac OS X.

Fig. 2 demonstrates the coding of the information message "Tomorrow never comes until it's too late". Each message character is converted to binary form using the ASCII-code. Next, for the selected cubic form of "bit" models and 3×3×3 mm in size, each information bit is coded. For this purpose, software was developed that forms the appropriate source code, which is placed in the working field of the OpenSCAD program. Now in Fig. 2 all elementary physical models are grouped into a container with the size 11×3×10 mm of the corresponding cubes (*these settings are additionally set in software*).

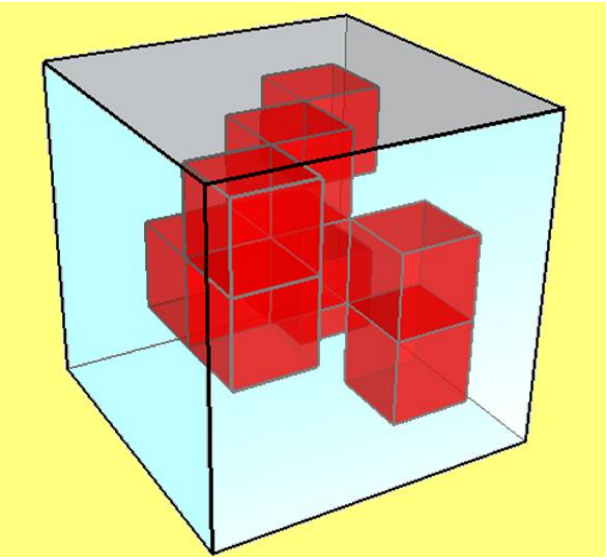


Fig.1 – Steganocoding of information message into a fragment of a computer model of physical object (*schematic representation*)

In Fig. 2 on the left, you can see the source code, which specifies the coordinates and size of three-dimensional cubes - carriers of information bits. On the right are the created three-dimensional model of the information message corresponding to all the given input parameters.

Thus, as a result of steganography coding, the information message first becomes a three-dimensional binary matrix, which turns into a computer model of physical object. The computer model of the binary matrix is placed in the middle of the basic model of the container, so that its edges do not extend beyond the outer body, as shown schematically in Fig. 3. At the same time, specialized software "MakerBot Desktop" was used for 3D-printing. The matrix in the middle of another model can be placed in different ways, for example: all filled cubes when printing on 3D-printer should be filled with different color materials; all the filled cubes should be left blank, when printing on 3D-printer. The disadvantage of the second method is the reduction of the final body weight, in a detailed analysis can give out the fact of the presence of secret message. Filling in bits with a different color (*or, for example, with another material*) reduces the probability of finding hidden message but increases the difficulty of its reading.

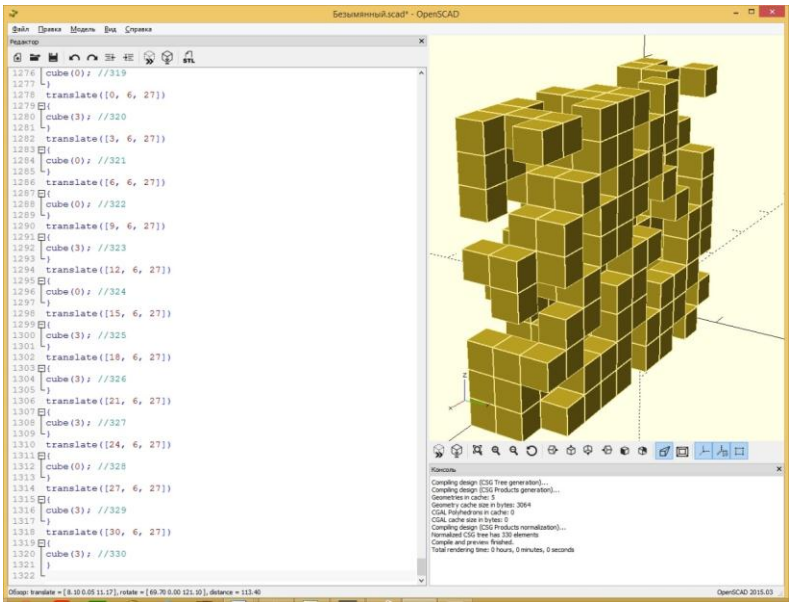


Fig. 2 – Example of steganography coding using the program OpenSCAD

Fig. 4 shows the process of layer-by-layer creation of the solid container object with built-in information message. On the left in this figure, schematic visualization of the printing process is shown, on the right - photograph of the real process on the 68th layer of 3D-printing, which was performed using the 3D-printer "Flashforge Creator Dual".

Fig. 5 shows the completion of the 3D-model printing and the finished product.

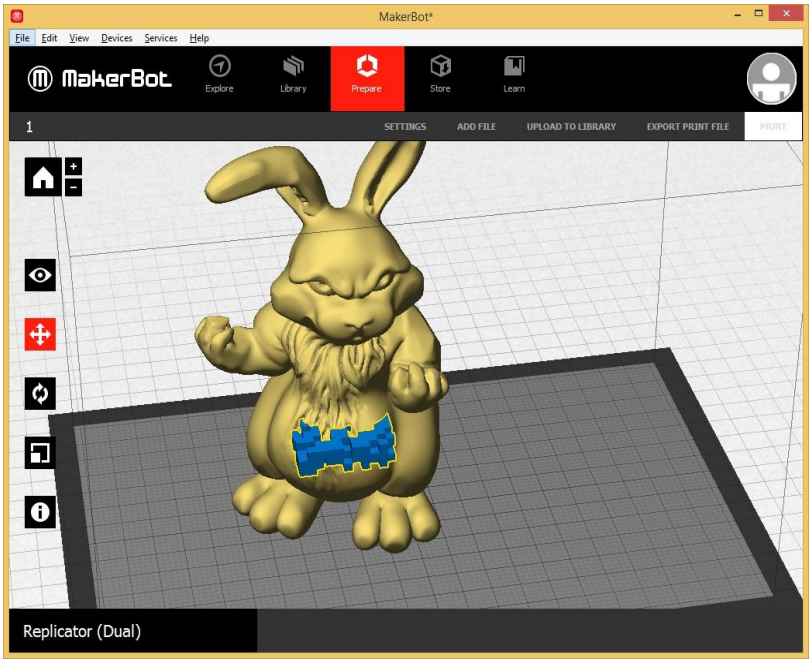


Fig. 3 – Placing three-dimensional model of the information message in the middle of the outer container model

3 Extracting of information data

The process of extracting the embedded data is performed by scanning the resulting solid object. The data received by the scanner is steganography decoded using secret key data. At this stage, various security services are provided, for example, integrity, authenticity, involvement, confidentiality and the like. To increase the reliability (*noise immunity*), the embedded data is additionally coded. As a result, it is possible to identify and/or correct the errors that occurred during layer-by-layer printing/scanning with given probability.

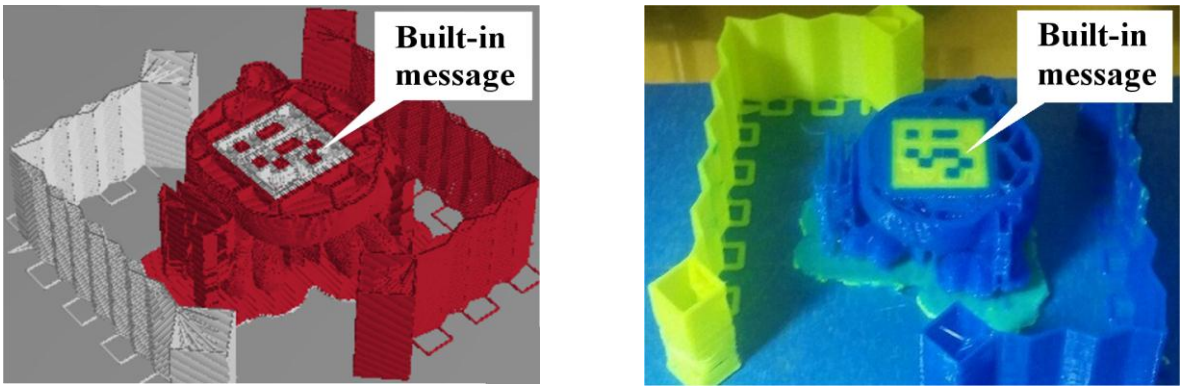
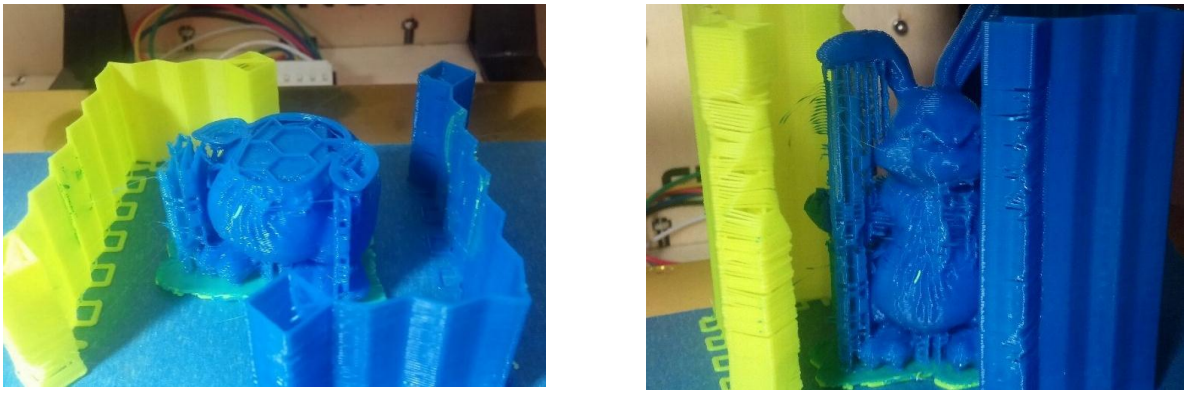


Fig. 4 – Layered creation of the solid container object with built-in information message



a) *b)*

Fig. 5 – Printing completion (*a*) and finished product (*b*) with built-in message

The proposed complex (method) can be used in various areas. For example, for the hidden transmission of information messages with the provision of various security services (*integrity, authenticity, involvement, confidentiality, etc.*). Removing, distorting or modifying embedded data is impossible without physical destruction of the finished product, the proposed complex (method) is ideally suited for ensuring the reliability of layered products, protecting them from unauthorized copying and unfair imitations, securing copyright, etc. [1,2].

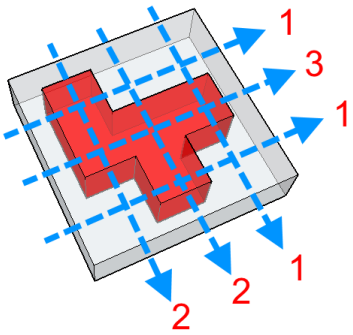
It should be noted that to date, reliable means of extracting information data have not been developed yet [15]. The main unresolved issue of the practical application of the proposed 3D-steganography complex is the uncertainty of a particular procedure of extracting embedded data by scanning the resulting solid body. In particular, the system can be completed with various peripheral devices of 3D-printing, which use different layer-by-layer technologies and different by physical properties materials. Corresponding procedures of scanning the resulting solid body must take these features into account and, if possible, ensure reliable and error-free retrieval of hidden data.

One of the possible directions in solving these problems is the use of laser scanners, in which a stream of coherent, monochromatic, polarized, and narrowly directed radiation flux is used. It decreases as a result of absorption in the medium in some pre-stipulated number of times. The following experimental studies were conducted to establish the possibility of reading of the hidden message from 3D-model that was layered (printed) on 3D-printer without damaging the model or message itself.

4 Description of the laboratory installation and experimental research

The main idea of the experiment is a narrowly focused laser irradiation of the finished product (with the built-in notification) at different angles and directions, sufficient to unambiguously determine the internal structure of the product. In this case, the initial dataset is the value of the radiation intensity, which decrease upon absorption.

The irradiation scheme of the finished product can be presented in simplified form in Fig. 6 on the left (*when encoding information bits with empty and filled cubes*). The indicated conditional value of the measurement result shown at the end of the arrows. This is a decrease in the radiation intensity (proportional to the thickness of the solid object). On the right in this figure, the values of the information bits are shown, which are expected to be extracted from the solid object.



1	0	0
1	1	1
0	1	0

a) *b)*

Fig. 6 – Simplified scheme of irradiation of the finished product (*a*) and the expected result of data extraction (*b*)

It is impossible to obtain any other information about the internal structure of the solid object. The placed filled fragments (and corresponding bits) must be uniquely extracted only from the measurement results. Represented in the figure on the left, the measurement results have two possible solutions, one of which does not correspond to the one shown on the right. This placement is a nomogram that can be used to form Japanese crossword puzzles. To simplify the experiment, a simple physical model was made in the form of stairs from ABS-plastic of yellow and blue colors. This shape allows to quickly change the thickness of the object filled with the material (Fig. 7).

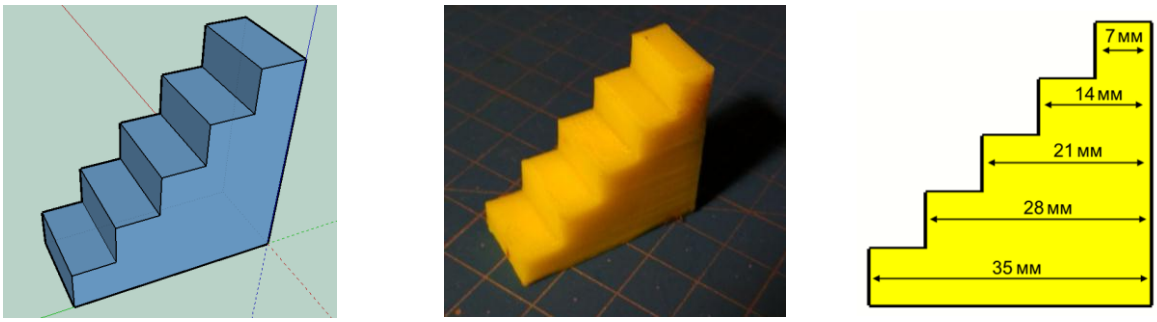


Fig. 7 – Simplified physical model of information data

In fact, there are six different values that conditionally correspond to the following information bit sequences:

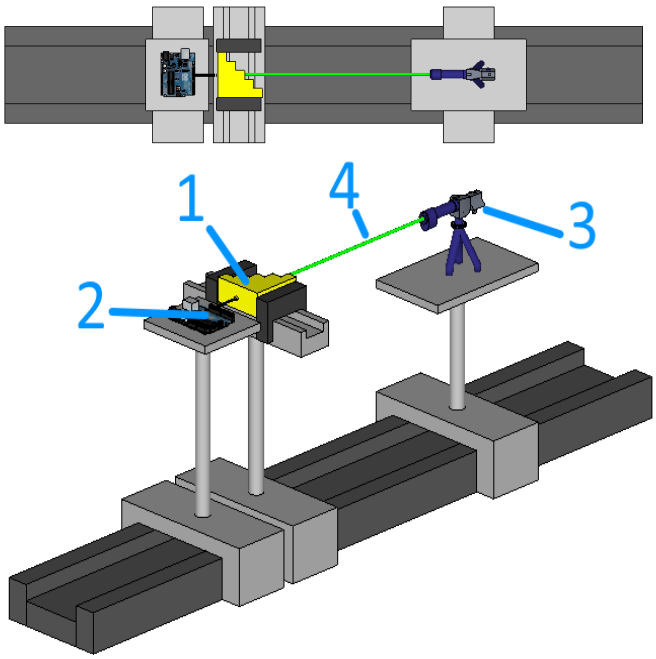
- without filling - bit sequence (00000);
- single fill (first step) - bit sequence (10000);
- two fillings (second step) - bit sequence (11000);
- three fillings (third step) - bit sequence (11100);
- four fillings (fourth step) - bit sequence (11110);
- five fillings (fifth step) - bit sequence (11111).

To conduct research, optical instruments were used from the laboratory of the Physical Optics Department of the Physics Faculty. It is known that each material has its own absorption index - the reciprocal of the distance, at which the monochromatic radiation flux forms a parallel ray, decreases as

a result of absorption in the medium to some predetermined number of times. The absorption coefficient is determined by the properties of the substance and in the general case depends on the wavelength λ of light. This dependence is the absorption spectrum of the substance. Lasers of the visible spectrum, which were in the laboratory, were used as monochromatic radiation. They are different in wavelength and radiation power. A ray of laser light passed through the body under investigation. Radiation, which was not absorbed by the plastic, fell on the photoresistor fixed on the other side. A photoresistor is a light-controlled variable resistor. The resistance of a photoresistor decreases with increasing incident light intensity. To read and process the data, the microcontroller "Arduino UNO" was used. The photoresistor was supplied with voltage 5 V. Depending on the degree of excitation of the photocell, its resistance was varied. The microcontroller measured voltage changes every 40 ms, digitized and sent them to personal computer.

Schematically, the laboratory device is shown in Fig. 8. It includes a test body made of plastic in the form of stairs (Fig. 7), laser as a source of directional irradiation of the finished product, photoresistor and microcontroller for reading scattered radiation. Photo of the collected laboratory installation and an enlarged photo of the process of optical irradiation shown in Fig. 8.

The software was developed to receive and display the current value of the photoresistor, calculate the arithmetic mean of the measurements made. Since the absorption spectrum of the substance was unknown for a solid body, all the lasers with different characteristics in the laboratory were used in the experiment (see Table 1).



1 - the solid object made of plastic in the form of stairs;
2 - photoresistor and microcontroller reading the data;
3 - laser;
4 - laser ray

Fig. 8 – The scheme of the laboratory installation

Each laser was exposed to different thicknesses of the body being examined and measurements were made of the percentage of light that passed through this section of the body. The step of variation of 7 mm was chosen considering the thickness of the laser ray, the thickness of which is within 5-6 mm. For the correctness of the experiment, the ray of laser radiation should completely fall on a section with one thickness. The microcontroller has a voltmeter, detects a voltage change in 5/1024 volts, so when digitizing an analog value, we get a number from 0 (*no light at all*) to 1024 (the max amount of light that a photoresistor can recognize).

Table 1 – Characteristics of lasers used in the experiment

Number	Wavelength, nm	Power, mW	Visible color
1	532	100	Green
2	650	25	Red
3	405	90	Violet
4	445	160	Blue
5	650	25	Red

5 The results of the experiment and their interpretation

The results of the experimental studies (*averaged over the measurements*) are presented in Table 2.

The sample from the yellow plastic absorbs less green laser radiation with a wavelength of $\lambda = 532$ nm. This is the output from the data in the table. Although both samples are made from the same kind of plastic, because of the color difference, they have completely different absorption values. The body, made of blue plastic, has a much larger absorption index. Even at the minimum thickness, the body absorbed light from each laser, which would suffice to determine the thickness.

Table 2 – Results of measurements

A sample of yellow color						
Laser number	Thickness, mm					
	0	**7**	**14**	**21**	**28**	**35**
1	1024	1001	775	162	33	4
2	1024	995	426	65	6	0
3	1024	995	97	5	1	0
4	1024	998	500	59	5	0
5	1024	995	336	57	4	0
Sample of blue color						
Laser number	Thickness, mm					
	0	**7**	**14**	**21**	**28**	**35**
1	1024	0	0	0	0	0
2	1024	0	0	0	0	0
3	1024	0	0	0	0	0
4	1024	0	0	0	0	0
5	1024	0	0	0	0	0

The obtained results for a sample of yellow material indicate that for different thicknesses we have different values of the radiation intensity and these differences are very significant. So, based on the measurement results, it is possible to recognize the thickness of the material, and, accordingly, determine the content of the hidden information bits.

6 Conclusions

In this work, a new direction of technical steganography related to the concealment of information in the process of layer-by-layer creation (cultivation) of solid-state object using various 3D-printing technologies was investigated. Information data are converted into digital 3D-model of elementary physical objects that are placed inside the 3D-model of the container product. After printing, the solid object physically contains hidden information that cannot be deleted or distorted without damaging the container. In addition, the applied methods do not reduce the operational, aesthetic and any other properties of the finished product.

The proposed complex (method) is invariant to the method of layer-by-layer growing, it can be equipped with any peripheral devices of 3D-printing of various manufacturers with any materials and principles of layer-by-layer creation. The process of extracting the embedded data is performed by scanning the resulting solid object. The uncertainty of the procedure for scanning the resulting solid body is the main unresolved issue regarding the practical application of the proposed 3D-steganography complex.

In this work, according to the results of experimental studies, it was established that it is possible in principle to read hidden message from 3D-model using laser scanners, in which the flux of coherent, monochromatic, polarized and narrowly directed radiation flux forms a parallel ray, decreases as a result of absorption in a medium into some a predetermined number of times. The obtained results for

a sample of yellow material indicate that for different thicknesses, we have different values of the radiation intensity and these differences are very significant. So, based on the measurement results, it is possible to recognize the thickness of the material, and, accordingly, determine the content of the hidden information bits. The results of the experimental studies given above are not final and need further clarification. In particular, the unresolved issue is the choice of the type and characteristics of the laser, the consistency of these characteristics with the properties of solid-state object materials, the adjustment of photoresistors, and the like. In addition, in our opinion, perspective is the conduct of experimental studies using other types of radiation, materials and colors of plastic.

References

[1] Katzenbeisser S., Petitcolas F. A. Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, MA, USA: Artech House, 2000. 220 p.
[2] Petitcolas F. A. P., Anderson R. J., Kuhn M. G. Information hiding-a survey. Proceedings of the IEEE.1999. Vol. 87, №7. P. 1062–1078.
[3] Mazurczyk W., Smolarczyk M., Szczypiorski K. Retransmission steganography and its detection. Soft Computing. 2011. Vol.15, №3. P. 505–515.
[4] Length based network steganography using UDP protocol/ Nair A. S., Kumar A., Sur A., Nandi S. 2011 IEEE 3rd International Conference on Communication Software and Networks. Xi'an, 2011. P. 726–730.
[5] Ahsan K., Kundur D. Practical data hiding in TCP/IP. ACM Workshop on Multimedia and Security, 2002. URL: https://www.gray-world.net/es/papers/acm02.pdf
[6] TCP/IP Timing Channels: Theory to Implementation / Sellke S. H., Wang C., Bagchi S., Shroff N. B. 2009. P. 2204–2212.
[7] Designing a cluster-based covert channel to evade disk investigation and forensics/ Khan H., Javed M., Khayam S.A., Mirza F. Computers & Security. 2011. Vol. 30, Issue 1. URL: https://www.sciencedirect.com/science/article/pii/ S016740481000088X
[8] Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel/ Khan H., Javed M., Khayam S.A., Mirza F. National University of Science & Technology (NUST), Islamabad 44000, Pakistan. URL: https://www.sigsac.org/ccs/CCS2009/pd/abstract_17.pdf
[9] Covert Channel for Cluster-based File Systems Using Multiple Cover Files / Morkevičius N., Petraitis G., A. Venčkauskas, J. Čeponis. Information Technology and Control. 2013. Vol. 42, №3. P. 32. URL:http://itc.ktu.lt/index.php/ITC/article/view/3328
[10] Rani R., Deep G. Digital 3D barcode image as a container for data hiding using steganography. 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC). Solan, 2017. P. 325–330.
[11] Sun Z., Lu Z. M., Li Z. Reversible Data Hiding for 3D Meshes in the PVQ-Compressed Domain. 2006 International Conference on Intelligent Information Hiding and Multimedia. Pasadena, CA, USA, 2006. P. 593–596.
[12] A Benchmark for 3D Mesh Watermarking / Wang K., Lavoué G., Denis F., Baskurt A., He X. 2010 Shape Modeling International Conference. Aix-en-Provence, 2010. P. 231–235.
[13] 3D Multimedia Protection Using Artificial Neural Network /Motwani M. C., Bryant B. D., Dascalu S. M. , Harris Jr. F. C. 2010 7th IEEE Consumer Communications and Networking Conference. Las Vegas, NV, 2010. P. 1–5.
[14] Vasić B. Annotation of cultural heritage 3-D models by robust data embedding in the object mesh. 2014 22nd Telecommunications Forum Telfor (TELFOR). Belgrade, 2014. P. 842–849.
[15] Kuznetsov A.A., Kovalenko O.Yu. Steganographic protection of information using 3D printing. Information Security of the State, Society and Personality: A Collection of Abstracts of the All-Ukrainian Scientific and Practical Conference, April 16, 2015. Kirovograd: KNTU, 2015.P. 91–92. (in Ukrainian)

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський технологічний університет "Шаг", вул. Малом'ясницька, 9/11, Харків, 61010, Україна. E-mail: kavserg@gmail.com

Надійшло: Вересень 2018.

Автори:

Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна.
E-mail: kuznetsov@karazin.ua

Олег Стефанович, студент факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна.
E-mail: stif1304@gmail.com

Катерина Кузнецова, студентка факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна.
E-mail: kate.kuznetsova.2000@gmail.com

Миколай Пастухов, к.т.н., доцент, Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, Дніпро, 49000, Україна.
E-mail: denart66@gmail.com

Дмитро Прокопович-Ткаченко, к.т.н., завідувач кафедрою кібербезпеки, Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, Дніпро, 49000, Україна.
E-mail: omega2@email.dp.ua

Метод 3D-стеганографії.

Анотація. В цій роботі досліджено новий напрямок технічної стеганографії, який пов'язаний із приховуванням інформаційних даних в процесі пошарового створення (вирощування) твердотільного об'єкта при використанні різних технологій 3D-друку. Інформаційні дані перетворюються в цифрову 3D-модель елементарних фізичних об’єктів, які розміщуються всередині 3D-моделі виробу-контейнеру. Після роздрукування твердий об'єкт фізично містить приховану інформацію, яку неможливо видалити або спотворити без пошкодження контейнеру. Крім того, застосовані методи не знижують експлуатаційних, естетичних та будь яких інших властивостей готового виробу, оскільки технології, що застосовуються для нанесення шарів, не модифікуються, а приховування є інваріантним способу пошарового вирощування, тобто можуть застосовуватися різні пристрої 3D-друку з будь-якими матеріалами і принципами пошарового створення.

Ключові слова: стеганографія; 3D-друк; приховування інформаційних даних; 3D-модель; лазерні сканери.

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский технологический университет "Шаг", ул. Маломясницкая, 9/11, Харьков, 61010, Украина. E-mail: kavserg@gmail.com

Поступила: Сентябрь 2018.

Авторы:

Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: kuznetsov@karazin.ua

Олег Стефанович, студент факультету комп’ютерних наук, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: stif1304@gmail.com

Екатерина Кузнецова, студентка факультета компьютерных наук, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина.
E-mail: kate.kuznetsova.2000@gmail.com

Николай Пастухов, к.т.н., доцент, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, Днепр, 49000, Украина.
E-mail: denart66@gmail.com

Дмитрий Прокопович-Ткаченко, к.т.н., заведующий кафедрой кибербезопасности, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, Днепр, 49000, Украина.
E-mail: omega2@email.dp.ua

Метод 3D-стеганографии.

Аннотация. В этой работе исследовано новое направление технической стеганографии, связанное с сокрытием информационных данных в процессе послойного создания (выращивания) твердотельного объекта при использовании различных технологий 3D-печати. Информационные данные преобразуются в цифровую 3D-модель элементарных физических объектов, которые размещаются внутри 3D-модели изделия-контейнера. После распечатки твердый объект физически содержит скрытую информацию, которую невозможно удалить или исказить без повреждения контейнера. Кроме того, применяемые методы не снижают эксплуатационных, эстетических и любых других свойств готового изделия, поскольку технологии, используемые для нанесения слоев, не модифицируются, а сокрытие является инвариантным к способу послойного выращивания, т.е. могут применяться различные устройства 3D-печати с любыми материалами и принципами послойного создания.

Ключевые слова: стеганография; 3D-печать; сокрытие информационных данных; 3D-модель; лазерные сканеры.