Steganographic System Model Based on Text Container

Vasilii Kozachok [1], Alexander Kozachok [1], Sergey Kopylov [1] and Evgeny Pavlenko [2]

[1] *The Academy of Federal Guard Service, 35 Priborostroitelnay st., Orel, 302015, Russia*
[2] *Peter the Great St. Petersburg Polytechnic University, 29 Polytechnicheskaya st., St. Petersburg, 195251, Russia*

Abstract

The article presents a steganography system model based on a text container resistant to format converting of an electronic text document into an image by using the "print-scan" or "print-photograph" operation. The existing protecting means limitations of text information containing confidential information and personal data from leakage through the provided channel are de-scribed. In the course of developing the model, the peculiarities analysis of the text containers presentation was carried out, the requirements and restrictions imposed on them were determined. The text container is electronic text documents prepared for printing, drawn up in the prescribed manner. The text container description, main characteristics and presentation features are presented. The main stages of the formation and transmission of a text container through a steganography sys-tem are described, possible effects on the formed container are considered. A requirement has been formed to ensure the robustness of the data embedded in the text container for the format conversion. Directions for further research are identified.

Keywords

Data leakage protection, data identification, text steganography

1. Introduction

The information technologies improvement has made possible to electronic interaction transition in all society spheres. The main direction of infotelecommunication networks development is the processing, transmission and storage integration of heterogeneous and different information services categories into a single multiservice communication network [1, 2]. A feature of such networks is the ability to simultaneously process both open and confidential information containing personal data. The presence of diverse information in multiservice networks requires the development of additional tools and systems for information protection from possible intruder destructive influences.

Security reports analysis of the InfoWatch analytical center showed that in 2020 were 1773 information leakage cases from commercial companies, government organizations and authorities around the world [3]. As a result of these leaks, more than 9.93 billion records containing personal, payment data, as well as confidential information were compiled. Moreover, in more than 79% of cases, the information security breach was carried out by insiders (internal intruder) [4]. By the type of compromised information, the leaks share of personal data and confidential information accounts for a significant part of cases (87.9%) [5]. At the same time, almost half (47.7%) of the information leaks total number was realized through paper text documents. The high percentage of leaks is due to the fact that many companies and organizations do not always follow the rules for handling paper documents [6]. In addition to the leakage of text documents physical copies there is a leak of them electronic versions, realized by scanning or photographing a printed document and sending or taking out the resulting image [7].

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: v.kozachok@academ.msk.rsnet.ru (A.1); a.kozachok@academ.msk.rsnet.ru (A.2); gremlin.kop@mail.ru (A.3); pavlenko@ibks.spbstu.ru (A.4)
ORCID: 0000-0001-5384-2269 (A.1); 0000-0002-6501-2008 (A.2); 0000-0003-2841-5243 (A.3); 0000-0003-1345-1874 (A.4)

The leaking textual information possibility through these channels is due to the presence of vulnerabilities and shortcomings inherent in the existing protection means of multiservice networks, as well as the information technologies constant improvement that make it possible to implement illegal actions bypassing protection tools. Showed features make the task of developing new and improving existing security tools ensured the security of text documents prepared for printing from leaks caused by format conversion, an actual research direction. Text steganographic methods based on the identification information embedding into the original document can be used to solve this problem [8, 9]. Identification information embedding allows ensuring the invariance of the embedded data to format conversion and to unambiguously identify the intruder or detect the fact of a leak.

As a text steganographic method an approach to information embedding based on changing the values of the intervals between words (interword spacing), can be used. The application of this approach allows the user to unnoticeably embed in the text document structure a confidentiality label of an electronic text document data, as well as information that uniquely identifies the user working with this document. In order to substantiate the possibility of using the text steganographic method based on changing interword spacing in the process of protecting text documents from leakage, it is advisable to develop a model of a steganographic system (stego system) based on a text container resistant to format transform. At the first stage of a steganographic system development, it is necessary to consider the formation and presentation features of containers describing electronic text documents prepared for printing.

This paper is organized as follows. Section 2 describes the presentation features of text containers based on electronic text documents prepared for printing. Section 3 contains a description of a steganographic system based on a text container resistant to format conversion. Finally, Section 4 presents our conclusions.

2. Text container presentation features

From the point of view of steganographic, a container (file-container) is data used to hide information (messages) in them [10, 11]. Depending on the type of data, containers can be divided into: text, graphic, audio, video or sound. Depending on the size, containers are divided into streaming and fixed [12].

A streaming container is a contiguous sequence of bits (information). Embedded information is embedded in it in real time, so it is not known in advance whether the container is large enough to embed the data. Embedded information (message) can be represented by a sequence of bits, a text document or multimedia files (image, video or audio data) [13]. In contrast to a streaming container, the dimensions and characteristics of a fixed container are known in advance. Fixed containers include electronic text documents, images, audio and video data due to the fact that the size and parameters of files are constant [14]. To describe the features of a text container, it is necessary to consider the main parameters and characteristics of electronic text documents.

In GOST R 7.0.8–2013, an electronic document is understood as a document, the information of which is presented in electronic form. Moreover, in GOST 2.105–2019, a text document is a document containing mostly solid text or text, divided into columns. Based on the considered definitions, in the context of the research, an electronic text document is understood as a document containing a solid text, a text divided into columns, as well as other text information presented in electronic form.

Electronic text documents can be divided into documents intended for printing on paper, and documents that will be used only in electronic form (prepared for visual perception). The parameters of electronic text documents prepared for visual perception are determined by the characteristics of the devices for visual display of information on the screen. These include [15, 16]:

- size (resolution) of the screen;
- number of colors reproduced by the visual output device.

Screen size – the ratio between the width and height of the screen, expressed in pixels (640x480, 800x600, 1024x768). Number of colors – a standard set of colors used by the visual display device: black and white, 16 shades of gray, 256 shades of gray, 16 colors, 256 colors, 262144 colors (high color), 67108864 colors (true color). The discrepancy between the colors specified in the text document and their number reproduced by the visual output device can lead to distortion of the original color or to its complete loss.

The parameters of electronic text documents prepared for printing are characterized by the features of the devices for outputting information to print [17, 18]:

- size of the printed sheet A;
- size of the text space (body) M;
- sizes of typographic elements F.

The presented parameters allow to describe a text container C, represented by electronic text documents prepared for printing, by the expression

$$C = \{\mathsf{A}, \mathsf{M}, \mathsf{G}\}. \quad (1)$$

The values of the following elements are used as the size of the printed sheet: paper size and sheet orientation. The following formats can be used as: described in ISO 216– A3 (297x420 mm), A4 (210x297 mm), A5 (148x210 mm), as well as – in the North American standard Letter (216x280 mm). The of the text document orientation is allowed: vertical (portrait) or horizontal (landscape). The sizes of the text space M are understood as the margins of the text document (top m_t, bottom m_b, left m_l and right m_r), text boundaries (text width, text height), headers and footers and indents from headers and footers.

Typographic elements of the text F are the following characteristics [19]: used typeface G and font size γ, spacing values (including line spacing β) and indents. An example of the main elements (parameters) of an electronic text document to be printed is shown in Figure 1.

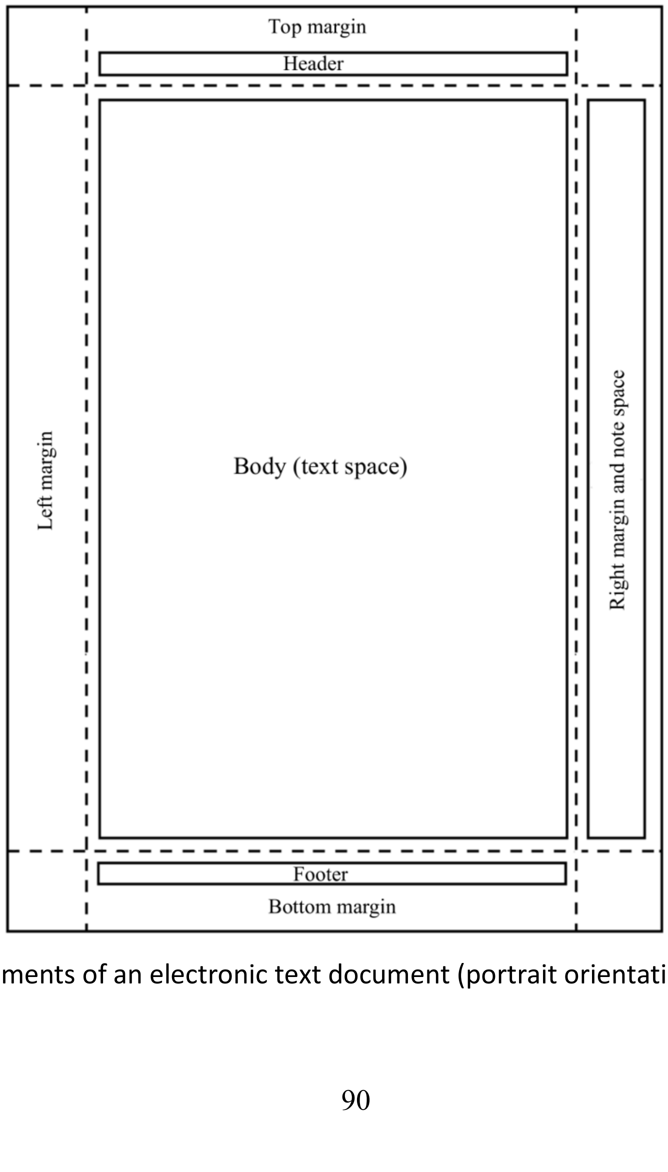

Figure 1: The basic elements of an electronic text document (portrait orientation)

Currently, electronic text documents are issued in an arbitrary way, however, in accordance with GOST R 7.0.97–2016, documents, including electronic ones, must be drawn up in accordance with the following requirements:

- paper size: A4 (210 x2 97 mm) or A5 (148 x 210 mm);
- margins of each sheet of the document must be at least 20 mm – left, 10 mm – right, 20 mm – top, 20 mm – bottom;
- freely distributed free fonts with size 12, 13, 14 pt;
- paragraph indentation – 1.25 cm;
- line spacing – 1-1.5 multiplier;
- spaces between letters in words (kerning) – normal.

The above requirements for the paperwork make it possible to describe a text container based on the use of electronic text documents prepared for printing, as

$$C = \{h, w, m_b, m_t, m_r, m_l, \gamma, \beta\}. \tag{2}$$

Expression 2 is a generalized description of a text container that meets the requirements of GOST R 7.0.97–2016 for paperwork, containing the main parameters of an electronic text document prepared for printing. The presented description of the text container allows one to proceed to the development of a steganographic system model based on a text container resistant to a format conversion of electronic text documents by using the "print-scan" or "print-photo" operation.

3. Text container presentation features

The steganographic system (stego-system) is intended for embedding and extracting (detecting) messages (data) from information of another type. In general, the steganographic system can be considered as a communication (data transmission) system [20–23]. In this case the transferring information (messages) process by means of a text container along a steganographic system consists of the following stages [24–26]:

- embedded information (messages) encoding;
- encoded information embedding into a text container (forming a text stego-container);
- format conversion of a text stego-container (an electronic text document printed out into an image containing text);
- stego-container transmission via a data transmission channel (steganographic channel);
- embedded information detection and extraction from a stego container;
- extracted information decoding.

A stego-system functional model based on a text container resistant to format conversion is shown in Figure 2.

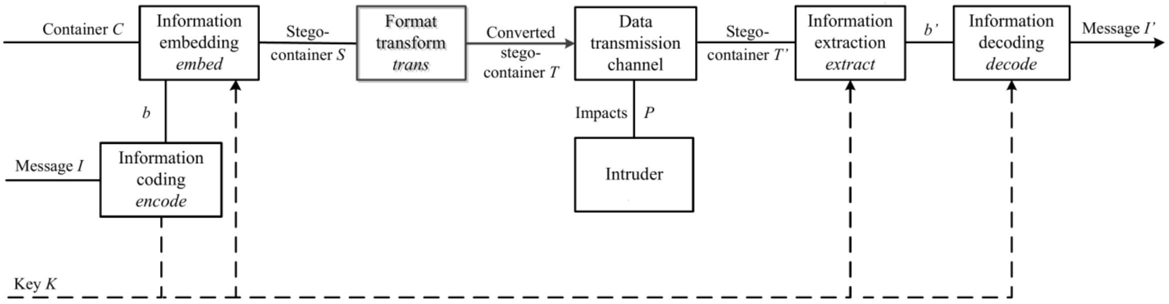
Container C
Information embedding embed
Stego-container S
Format transform trans
Converted stego-container T
Data transmission channel
Stego-container T'
Information extraction extract
b'
Information decoding decode
Message I'
b
Message I
Information coding encode
Impacts P
Intruder
Key K

Figure 2: Stego-system functional model based on a text container resistant to format conversion

In Figure 2, the following designations are adopted: C – container (electronic text document); □ – containers set ($C \in$ □); I – embedded messages (information) set ($I, I' \in \mathsf{I}$); K – keys set ($K \in \mathsf{K}$); *encode* – encoding embedded information function; B – possible code sequences set ($b, b' \in \mathsf{B}$); *embed* – function of embedding information into the container; S – steganographic container (stego-container); *trans* – format converting of a text stego container into an image; T – converted stego container; P – impacts (including intentional) ($P_L, P_D \in P$) rendered on the stego-container; T' – distorted stego-container; *extract* – function of extracting embedded information from the stego-container; b' – extracted sequence; *decode* – extracting embedded information function; I' – retrieved message (information).

At the stage of encoding the embedded information the information (message) I is converted into a form corresponding to the used embedding (embedding) algorithm. The encoding process is described as

$$b = encode(K, I). \qquad (3)$$

A secret key is used to enhance the security of embedded data. It should be noted that from the standpoint of steganography, the secret key is understood both in the broad and narrow sense. In a broad sense, this is a method (technique) of steganographic information embedding known only to legitimate users. In the narrow sense, a key is understood as a secret parameter of the applied embedding algorithm without which the embedded information extraction cannot be carried out. In view of this, all embedding algorithms can be divided into key and keyless. The secret key usage is intended to increase the security and reliability of embedded information. In addition to using the secret key in the coding process, encryption or error correction code methods can be used to increase the robustness of the embedded data.

In the encoding embedded information process the function *encode* is imposed a requirement for the embedded data invariance to carry out transformations and introduce distortions $encode(K, I) = encode(K, I')$, where $I' = I + \varepsilon$. Possible distortions and transformations (ε) of data can include: container geometric distortions, deliberate attacks and other influences (including legitimate ones) that can corrupt the container original representation.

The embedding encoded information process into a container is the formation of a steganographic container. A steganographic container S is a container containing C embedded information I. The resulting stego-container S is a mutable container that fully matches the data type of the original. In this case, the formed stego-container S should not be visually and/or statistically distinguishable from the original container C. The embedding information process is implemented by the function:

$$b = encode(K, I), \qquad (4)$$

where M – embedding mask that takes into account the characteristics of the human visual system and is designed to reduce the visibility of embedded information.

The generated stego-container must ensure invariance to format conversion due to the application of the "print-scan" or "print-photo" operation, as well as to various influences carried out both deliberately by the intruder and accidental or legitimate actions, capable of modifying or completely destroying embedded information.

In the format converting process of a text stego-container $trance: S \to T$ the presentation format of the original text document is changed. This transformation includes the "print-scan" ("print-photo") operation of an electronic text document, as well as the accompanying actions P that can be carried out in the process of said transformation. The impacts classification P that steganographic systems can be exposed to are shown in Figure 3 [27–30].

All impacts P can be divided into unintentional P_L (introducing legitimate distortions and container transforming) and deliberate P_D (attacks on embedding systems). Unintentional impacts on stego-systems are characterized by minor distortions introduction into the stego-container (container), which do not affect visual perception and can modify the stego-container (container) by the following transformations [31, 32]:

- general data processing operations – noise addition (including printer and scanner noise in printing and scanning process), brightness and contrast adjustment, histogram equalization, smoothing, filtering (median, gaussian, averaged), clarity correction (sharpness), etc.;

- geometric transformations – rotation, scaling, changing proportions (aspect ratio), shift (displacement), cropping, etc.;
- format conversion – compression (including lossy), linear conversion.

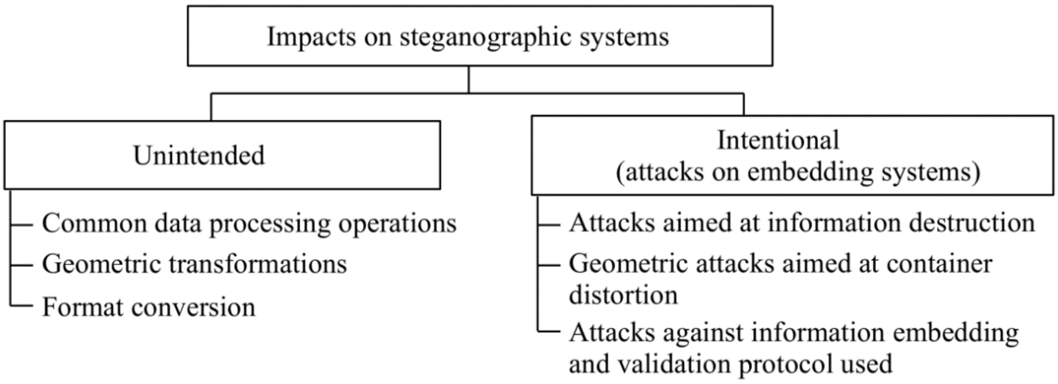
Impacts on steganographic systems
Unintended
Intentional (attacks on embedding systems)
Common data processing operations
Geometric transformations
Format conversion
Attacks aimed at information destruction
Geometric attacks aimed at container distortion
Attacks against information embedding and validation protocol used

Figure 3: Classification of impacts on steganographic systems

The minor distortions introduction into the container, which does not affect visual perception, nevertheless, affects the detection ability and the extracting accuracy of the embedded watermark from the converted stego-container (container). At the same time, the implementation of a large number of transformations and distortions can lead to destruction or erroneous extraction of information embedded in the stego-container (container).

In contrast to unintentional distortions, deliberate attacks are aimed at achieving a specific goal – the destruction, substitution, or imposition of false information [33, 34]. An attack is understood as any deliberate container transformation with or without data embedded in it, which does not degrade the container quality. The quality of the container is the container state in relation to its perceptual (connected with the human visual system) perception by the observer. Various influences can be carried out at each of the stages of an electronic text document format converting.

As the name suggests, the attacks aimed at information destruction use the container statistical characteristics changing mechanisms. The implementation of these attacks is based on the assumption that embedded information is a statistically described noise that can be removed by cleaning the container from noise, overmodulation, lossy compression (quantization), averaging and collisions. The use of these methods facilitates making changes in the container statistical characteristics without affecting the data perceptual sensation. Thus, to clear the image from noise, container filtering can be applied using the maximum likelihood or maximum a posteriori probability criterion.

In contrast to removal attacks, the geometric attacks are aimed at container modification by introducing spatial or temporal distortions. Geometric attacks are mathematically modeled as affine transformations: rotation, scaling, aspect ratio, shifting (offsetting), and cropping. These attacks are divided into global – applied to the entire container – and local – applied to a single container area or a several areas set. In particular, it is possible to implement all kinds of image geometric transformations, as well as cutting individual pixels or rows, rearranging them, etc.

Attacks against information embedding and validation protocol used are based on the fact that the intruder pretends to be a legitimate user by modifying the container with the embedded information. One of the possible options for implementing it is the use of an inverse attack, meaning that the intruder claims that false information belonging to him is in the protected container (after which he removes this data part). At the same time, there is real embedded information in the formed false original information. As a result, an unresolved problem occurs. In addition, the intruder can embed information contained in one image into other images to counter imitation protection and authentication systems.

In the electronic text document printing such geometric transformations (unintentional distortions) as a print area shift (displacement), rotation at small angles, scaling, and change in the quality (resolution) can be introduced. In addition to geometric transformations, printer noise, characterized by uneven ink distribution (general processing operations), can be introduced into the printed text document. Targeted attacks aimed at watermark removing or container modifying includes changing the printable area of an electronic text document to skip areas containing identification information.

Printed text document scanning, like printing, introduces all kinds of geometric transformations (unintentional distortions), as well as scanner noise due to wear and tear and scanner device imperfections. Additionally, in image formation process, lossy compression, filtering, adjustment of brightness, contrast and clarity (general operations of processing and format conversion) can be used. The attacks aimed at removing the marker and information contained in a text document can be a physical substitution of text areas, which consists of deleting or adding the necessary (additional) information during the scanning process.

In contrast to the scanning operation, the result a printed text document photographing (digital image) is characterized by the geometric distortions presence in three planes (Fig. 4) [35].

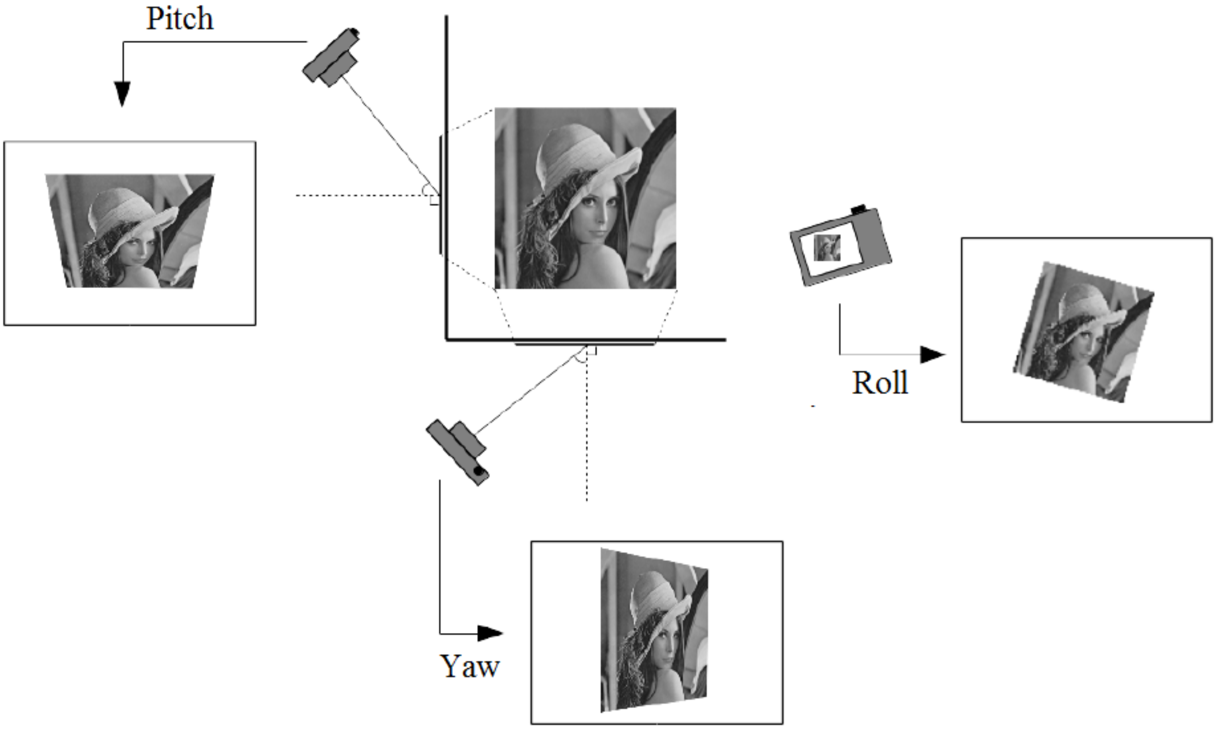

Figure 4: Geometric distortions arising in printing-photographing process

Besides geometric distortions arising in the photographing process, the following types of distortions introduced by the lens of the camera and shooting conditions are distinguished:

- distortions introduced by external lighting – image areas uneven illumination, vignetting (progressive decrease in illumination towards the image frame corners or reduction of an image's brightness or saturation toward the periphery compared to the image center);
- distortions introduced by the lens – perspective distortion (horizontal tilt and vertical camera deflection), distortion (curvature of initially straight lines inward or outward);
- distortions associated with the image formation optical features – chromatic aberrations (color fringes at contrasting boundaries), moire (a pattern that occurs when two or more periodic mesh patterns are superimposed).

As a result of format conversion and transmission via a transmission channel, an electronic text document S (stego-container) is converted into a digital image T' (converted stego-container), subjected to various types of distortions and transformations. At the stage of extracting embedded information from the transformed stego-container T' (an image containing the original text document) it's carried out using the function *extract*:

$$b' = extract(T', K) \tag{5}$$

where T' – digital image (stego-container) containing embedded data.

If the requirement for the embedded data invariance to format conversion is met, as well as the accompanying effects on the stego-container, the extracting data result from an electronic text document $b = extract(S, K)$ and the extracting data result from an image containing text $b' = extract(T', K)$ must be the same: $b = b'$, given that $S \neq T'$.

The extracted information decoding is carried out by the function *decode* as follows:

$$I' = decode(b', K) \tag{6}$$

If the requirement for the embedded data invariance is met to the format transformation of a text document in the encoding embedded information process, the result of extracting the embedded data will take the following form:

$$I' = decode(b', K) = decode(b, K) = I \tag{7}$$

Expression 7 makes it possible to characterize the developed text container as robust for an electronic text document format converting into an image by using the "print-scan" or "print-photo" operation, as well as the accompanying distortions arising in the process of these transformations. As a practical implementation of the developed steganographic system based on a text container resistant to format conversion, an algorithm for marking electronic text documents based on interwords intervals values changes can be used. This algorithm will allow the hidden (from the user) embedding of identification information, allowing to detect the leakage source of the protected document or to detect the leakage fact.

4. Conclusion

For the practical implementation of the electronic text documents marking algorithm based on changing the values of the intervals between words described by the steganographic system developed model it's necessary to justify the choice of a mathematical apparatus capable of extracting information contained in images obtained by converting the electronic format text document. In the process of choosing a mathematical apparatus, it is necessary to be guided by the developed marking approach marking, which consists in changing the values of the intervals between words to the established values in the process of embedding.

5. References

[1] D. Zegzhda, D. Lavrova, E. Pavlenko, Cyber attack prevention based on evolutionary cybernetics approach, Symmetry (2020) 1–19. doi:10.3390/sym12111931.

[2] S. Makarenko. The Steganographic System Interconnection Basic Reference Model and the Justification of New Areas of Steganography Theory's Development. Voprosy kiberbezopasnosti [Cybersecurity issues], 2014. No 2(3), pp. 24-32. (In Russ).

[3] Verizon, 2021 DBIR Master's Guide, 2021. URL: https: //www.verizon.com/business/resources/reports/dbir/2021/masters-guide.

[4] InfoWatch, A Study on Global Data Leaks in 2018, 2019. URL: https: //infowatch.com/sites/default/files/report/analytics/Global_Data_Breaches_2018.pdf.

[5] InfoWatch, A Special Report on Data Breach Penalties, 2019. URL: https: //infowatch.com/sites/default/files/report/analytics/SR_Data_Breach_Penalties.pdf.

[6] Varonis, 98 Must-Know Data Breach Statistics for 2021, 2021. URL: https: //www.varonis.com/blog/data-breach-statistics.

[7] V. Buharin, S. Karaichev, E. Pikalov. Protection Method from Destructive Software Effects in Multiservice Networks. Voprosy kiberbezopasnosti [Cybersecurity issues], 2016. No 3(16), pp. 18-24. (In Russ).

[8] S. Dhawan, R. Gupta, Analysis of various data security techniques of steganography: A survey, Information Security Journal: A Global Perspective (2021) 63–87, doi:10.1080/19393555.2020.1801911.

[9] M. Dalal, M. Juneja, Steganography and Steganalysis (in digital forensics): a Cybersecurity guide, Multimed Tools Appl (2021) 5723–5771 doi:10.1007/s11042-020-09929-9.

[10] A. V. Kozachok, S. Kopylov, A. Shelupanov, O. Evsutin, Text marking approach for data leakage prevention, Journal of Computer Virology and Hacking Techniques (2019) 219–232. doi:10.1007/s11416-019-00336-9.

[11] A. V. Kozachok, S. Kopylov, Estimation of Watermark Embedding Capacity with Line Space Shifting, in: 2020 Ivannikov Memorial Workshop (IVMEM), 2020, pp. 29–34. doi:10.1109/IVMEM51402.2020.00011.

[12] R. Anserson, Information Hiding, in: First International Workshop, Cambridge, U.K., May 30 - June 1, 1996. doi:10.1007/3-540-61996-8.

[13] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, Information hiding – A survey, in: Proceedings of the IEEE, Vol. 87, no. 7, 1999, pp. 1062-1078. doi:10.1109/5.771065.

[14] D. Salomon, Data Privacy and Security, Springer, New York, NY, 2003. doi:10.1007/978-0-387-21707-9_11.

[15] S. O. Brogain, Typographic measurement: A critique and a proposal, Professional Printer: Journal of the Institute of Printing, vol. 12, no 5 (1983) pp. 9–14.

[16] J. Tschichold, The New Typography, Berkeley: University of California Press, 2020. doi:10.1525/9780520355019.

[17] Z. Zhang, Analysis on Text Structure, in: Proceedings of the 2019 International Conference on Contemporary Education and Society Development (ICCESD 2019), 2019. doi: 10.2991/iccesd-19.2019.44.

[18] J. P. Williams, Text structure instruction: the research is moving forward, Read Writ 31 (2018), 1923–1935. doi:10.1007/s11145-018-9909-7.

[19] C. Lelis, S. Leitao, O. Mealha, B. Dunning, Typography: the constant vector of dynamic logos. Visual Communication (2020). doi: 10.1177/1470357220966775.

[20] A. V. Kozachok, S. Kopylov, R. Meshcheryakov, O. Evsutin, L. M. Tuan An approach to a robust watermark extraction from images containing text (2018) 128–155. doi:10.15622/sp.60.5. (In Russ.).

[21] M. Dalal, M. Juneja, Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimed Tools Appl 80 (2021) 5723–5771. doi:10.1007/s11042-020-09929-9.

[22] A. M. Kadhim, H. M. Jawad, Studying Audio Capacity as Carrier of Secret Images in Steganographic System (2021) 53–61. doi:10.30723/ijp.v19i49.648.

[23] X. Zhou, W. Peng, B. Yang, Linguistic Steganography Based on Adaptive Probability Distribution, in: IEEE Transactions on Dependable and Secure Computing (Early Access), 2021. doi:10.1109/TDSC.2021.3079957.

[24] S. Bajracharyaa, R. Koju, An improved DWT-SVD based robust digital image watermarking for color image, International Journal Engineering and Manufacturing (2017) 49–59. doi:10.5815/ijem.2017.01.05.

[25] W. Qi, W. Guo, T. Zhang, Y. Liu, Z. Guo, X. Fang, Robust authentication for paper-based text documents based on textwatermarking technology, Mathematical Biosciences and Engineering (2019) 2233–2249. doi:10.3934/mbe.2019110.

[26] N. Al-maweri, W. Adnan, A. Ramli, K. Samsudin, S. Rahman, Robust digital text watermarking algorithm based on Unicode extended characters, Indian Journal of Science and Technology, (2016) 1–14. doi:10.17485/ijst/2016/v9i48/87787.

[27] L. Geng, W. Zhang, H. Chen, Real-time attacks on robust watermarking tools in the wild by CNN, Journal of Real-Time Image Processing (2020) 17, 631–641. doi:10.1007/s11554-020-00941-8.

[28] K. Loukhaoukha, A. Refaey, K. Zebbiche, Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value

decomposition, Journal of Electrical Systems and Information Technology (2017), 359–368. doi:10.1016/j.jesit.2016.12.011.

[29] O. Hosam, Attacking Image Watermarking and Steganography – A Survey, Information Technology and Computer Science (2019), 3, 23–37. doi:10.5815/ijitcs.2019.03.03.

[30] D. Hitaj, B. Hitaj L. V. Mancini, Evasion Attacks Against Watermarking Techniques found in MLaaS Systems, in: 2019 Sixth International Conference on Software Defined Systems (SDS), 2019, pp. 55–63. doi:10.1109/SDS.2019.8768572.

[31] C. Wang, Y. Zhang, X. Zhou, Robust Image Watermarking Algorithm Based on ASIFT against Geometric Attacks, Applied Sciences (2018) 8(3) 410–428. doi:10.3390/app8030410.

[32] Y.Wang, J. Liu, Y. Yang, D. Ma, R. Liu, 3D model watermarking algorithm robust to geometric attacks, IET Image Processing (2017) 822–832. doi:10.1049/iet-ipr.2016.0927.

[33] S. Geetha, S. Subburam, S.Selvakumar, S. Kadry, R. Damasevicius, Steganogram removal using multidirectional diffusion in fourier domain while preserving perceptual image quality, Pattern Recognition Letters (2021) 197–205. doi:10.1016/j.patrec.2021.04.026.

[34] P. P. Amritha, M. Sethumadhavan, R. Krishnan, S. K. Pal, Anti-forensic Approach to Remove Stego Content from Images and Videos, Journal of Cyber Security and Mobility (2019) 295–320. doi:10.13052/2245-1439.831.

[35] A. Pramila, Reading watermarks with a camera phone from printed images, Master’s thesis, University of Oulu, Finland, 2018.