DOI: https://doi.org/10.18454/RULB.2021.26.2.10

ПОНЯТИЕ «ТРИГГЕР-КОНТЕЙНЕР» В ЛИНГВИСТИЧЕСКОЙ СТЕГАНОГРАФИИ

Научная статья

Потапова Р.К.[1], Джунковский А.В.[2] *

[1] ORCID: 0000-0002-7532-9156;

[2] ORCID: 0000-0002-3761-8010;

[1, 2] Московский государственный лингвистический университет, Москва, Россия

* Корреспондирующий автор (Vetinari01[at]gmail.com)

Аннотация

В статье рассматривается авторское понятие лингвостеганографических «триггер-контейнеров», под триггер-контейнерами мы понимаем уникальные минимальные контейнеры, необходимые для внедрения конфиденциальной информации в письменные русскоязычные тексты. Необходимость введения понятия «триггер-контейнер» связана с систематическим усилием по созданию научно обоснованного метода лингвистического стеганографического сокрытия информации на основе данных лингвистических экспериментов. Одновременное использование «триггер-контейнеров» в контексте сокрытия информации на основе данных лингвистических экспериментов позволит в перспективе разработать методику сокрытия информации в естественных текстах без использования шифров и с высоким уровнем защищенности как от автоматического, так и экспертного визуального стеганоанализа. Новизна исследования состоит в создании понятия «триггер-контейнер», которое описывает еще не описанный феномен в лингвистической стеганографии. Цель работы – введение нового термина, позволяющего на его основе проводить квантитативные исследования в сфере лингвистической стеганографии. В работе предлагается новое понятие «триггер-контейнера», которое позволяет осуществлять исследования в рамках разрабатываемой авторской методики лингвистической стеганографии, основанной на перцептивных экспериментах.

Ключевые слова: экспериментальная лингвистика, экспериментальная стеганография, триггер-контейнер, текстовая стеганография, стеганография для русского языка.

TRIGGER-CONTAINERS IN LINGUISTIC STEGANOGRAPHY

Research article

Potapova R.K.[1], Dzhunkovskiy A.V.[2] *

[1] ORCID: 0000-0002-7532-9156;

[2] ORCID: 0000-0002-3761-8010;

[1, 2] Moscow State Linguistic University, Moscow, Russia

* Corresponding author (Vetinari01[at]gmail.com)

Abstract

The article deals with the new term “trigger-container” in linguistic steganography. The necessity to introduce this term was brought about by the creation a unique kind of steganographic containers of minimal possible size that would allow for insertion of confidential information into Russian written texts. The introduction of “trigger-containers” is intrinsically interwoven with our ongoing systematic attempt to create a linguistic steganographic term apparatus of describing sense information protection on the basis of linguistic experimentation with a strong scientific foundation. Concurrent use of the proposed steganographic term in praxis in conjunction with the data yielding from linguistic experiments would allow to create a method for concealing sensitive information in Russian written texts that is simultaneously highly secure against automated and expert-driven visual steganalysis as is not dependent on the usage of cryptographic cyphers. The novelty of this research is based on the introduction of the new term “trigger-containers”, which describes a phenomenon that is not touched upon in other research. The goal of the paper is, likewise, the introduction of the term, which allows one to describe the proper theoretical basis of qualitative research in the field of linguistic steganography. We introduce the term “trigger container” which allows to create the basis for our method of conducting perceptive experimental research in the field of linguistic steganography.

Keywords: experimental linguistics, experimental steganography, trigger-containers, text steganography, Russian steganography.

Introduction

There are two major ways of protecting sensitive information: cryptography and steganography. The basis of cryptography is encrypting information. The basis of steganography is the act of concealing the fact that sensitive information is being transferred. In the contemporary world steganographic methods continue gaining importance. For many purposes, the very fact that a cypher has been used to protect information is detrimental [10]. It can be altered or outright destroyed upon imminent detection [5]. Because cyphers are easily detectable, this, on a fundamental level, makes decryption a matter of time if a third party is targeting a particular information channel [2].

In our work we are currently investigating and furthering an experiment-based approach **to creating steganographic means of concealing** information [1]. While steganography itself is not a new concept, the amount of research of the efficiency of different methods is severely lacking. Furthermore, the scientific study of the subject in relation to Russian written texts is virtually nonexistent.

Methods

In our previous work we have developed a combined three-stage classification and analysis method for steganographic means in written Russian texts [4]. This taxonomy provides a robust basis for identifying alterable variables in Russian written texts and encompasses metalinguistic, linguistic and contextual variables. Each of these can be used as a steganographic container, which is a term used in steganology to describe the outer shell of the intended message. Envisaging and describing this taxonomy created a roadmap of further scientific inquiry. We posited that using linguistic experiments and testing how different variables affect the perception of texts altered via insertion of steganographic containers by native speakers would lead to discovering the most secure and robust potential steganographic containers for Russian written texts [6]. This led to the inception of a framework for exploratory visual perception linguistic experiments with the aim of finding discovery rates for different types of text alteration.

These experiments presuppose working with groups of respondents (n=100 and higher), all of them are "naive" speakers of the Russian language. They are given texts that are altered in some way. Some of these alterations include inserting grammatical, lexical, syntactic and stylistic errors, others – altering the presentation of texts removing paragraph separators, spaces between words and punctuation. When working with the former variant, the respondents are asked to highlight what they believe to be "wrong" with the text. In the latter scenario they are asked to restore the text to its original form. Let us briefly provide examples of such alterations: the word "волк" can be presented as "влок", the error consisting of a changed symbol order. The alteration for "окно" can be "оено", based on the proximity of the letters "к" and "е" in the Russian keyboard layout. Punctuation errors can simply be achieved by omitting commas in the text. For the latter case, we would alter a text in the following way and then ask the respondents to restore it:

«Небо было заполнено тучами, бегущими на север. Быстро темнело. Нужно было срочно возвращаться домой» – initial form.

«небобылозаполненотучамибегущиминасевербыстротемнелонужнобылосрочновозращатьсядомой» – altered form.

The results allow us to gather and analyze data on what types of alterations are statistically most and least noteworthy to a "naive" native speaker and to find juncture points that have an in-text spatial probability range, potentially implying that altering the text junctures (i.e. by separating the text into paragraphs at specific points) can be used as a "trigger-container".

It became apparent that the existing theoretical basis for linguistic steganography lacks the conceptual means of describing our findings and the very direction of the study. The end goal of the research is to find minimal alterations to texts that are nigh-indistinguishable to non-altered instances of the same texts.

Results

The resulting thought process that lead to introducing the notion "trigger-container" was the following one: there currently already exist **means** of concealing information that are based on "highlighting" certain letters, words, phrases or sentences. Some of these means are cryptographic and function because of an underlying mathematical model, some are combined cryptographic-steganographic means. These aforementioned combined cryptographic-steganographic means, however, are still largely dependent on their cryptographic aspects. Their main drawback is that discerning the algorithm guarantees that the container will be breached over time [7]. The concealed sense itself is "augmented" into a natural language text. The stego in these cases is similar to a map or a coordinate grid that, when overlaid over a specific text, yields a secret message [3, 9]. When such (a) text is intercepted, deciphering one hidden message endangers all other messages sent via a channel or between two parties in constant communication [8].

This drawback leads to the need and the opportunity to conceptualize a steganographic linguistic container that doesn't rely on concealing the hidden message within the text proper. The basis of such container is using minimal linguistic alterations, its theoretical functional semantic basis is a preliminary agreement between two parties. The message itself is known to both parties that try to achieve a secure transfer of sensitive information, and the appearance of the agreed-upon text alteration in the text acts as the "trigger" event that signals the receiving party that the information is to be perceived. The "trigger-container" is a sleeper message that is hidden in plain sight and activated by a minimal alteration of the text that both parties of communication are aware of.

Discussion

"Trigger-containers" in praxis allow two parties to securely relay potentially unlimited volumes of data through unsecure monitored channels as long as the information is agreed upon beforehand. Such method of hiding the information would be useful in long-term planning that requires a high degree of discretion. Let us provide an example of such a situation: two businesses are planning a merger, but the communication channels are compromised because of corporate espionage. The news that the merger is in effect becoming public too early will cause sudden oscillations of the market price of stocks of both companies and might lead to the merger becoming unprofitable. In a situation like this the use of a "trigger-container" could be an easy and efficient solution to the theoretical situation.

The very nature of "trigger-containers" makes the scenario where the stego itself is compromised nigh-impossible: the only option for third parties in this scenario is to destroy or reroute the message to prevent it reaching the receiving party. If the volume of communication between two parties is large, the third party aiming to disrupt or compromise that communication will encounter issues when trying to discover which messages contain secret information and which don't if a "trigger-container" is used. This is achieved by the "trigger-container" being identical to either a legal (from the usus standpoint) use of language means or to a random error.

Conclusion

The notion “trigger-container” represents a linguistic steganographic container that consists of a minimal alteration in the text that is identical to normal language use, but covertly refers to a message the sending and receiving parties have agreed upon beforehand.

The drawbacks of using trigger-containers are that the messages are rigid and difficult to alter. This brings about the need to create lexicons of “trigger-containers” for relaying different messages. At the same time, concurrent use of too many trigger-containers will lower the security of a message by drawing the expert’s attention to the number of anomalies in it.

Nevertheless, the use of trigger-containers can be optimal when there is need for expedient and highly secure communication of mission-critical and highly confidential messages that need to be protected both from interception and destruction by third parties. Furthermore, the introduction of this notion creates the groundwork for issues where further development of experimental methods in the field of linguistic steganography is necessary.

Финансирование

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-312-90066.

Funding

The reported study was funded by RFBR, project number 19-312-90066.

Конфликт интересов

Не указан.

Conflict of Interest

None declared.

Список литературы / References

1. Потапова Р.К. Перспективы использования стеганографических технологий в звучащей речи на современном этапе развития / Р.К. Потапова, А.В. Джунковский // Вестник МГЛУ. Гуманитарные науки. – 2019. – № 5 (821). – С. 206–211.

2. Салагай М.О. Просодические средства защиты смысловой информации (экспериментально-фонетическое исследование в области стеганографии) : дис. … канд. филол. наук : 10.02.21 : защищена 14.11.2011 / Салагай Марина Олеговна. – Москва: ФГБОУ ВПО МГЛУ, 2011. – 203 с.

3. Bennet K. Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text / K. Bennet // CERIAS Tech Report. – 2013. – № 4. – pp. 1–30.

4. Dzhunkovskiy A.V. Steganography: Three-Stage Analysis Methodology Applied to Russian Written Texts / A.V. Dzhunkovskiy // Вестник МГЛУ. Гуманитарные науки. – 2018. – № 6 (797). – pp. 117–123.

5. Johnson N.F. Exploring Steganography: Seeing the Unseen / N.F. Johnson, J. Sushil // IEEE Computer. – 2020. – № 32(2). – pp. 26–34.

6. Potapova R. Preliminary Investigation of Potential Steganographic Container Localization / R. Potapova, A. Dzhunkovskiy // Lecture Notes in Artificial Intelligence. – 2020. – vol. 12335. – pp. 389–398.

7. Provos N. Defending Against Statistical Steganalysis / N. Provos // Michigan: University of Michigan Press, 2001. – 343 p.

8. Ross A. On the Limits of Steganography / A. Ross, F. Petitcolas // IEEE Journal of Selected Areas in Communications. – 1998. – № 4(16). – pp. 474–481.

9. Taskiran C.M. Attacks on Lexical Natural Language Steganography Systems / C.M. Taskiran, U. Topkara, M. Toplara // Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, February 15-19, 2006. – pp. 122–130.

10. Wayner P. Disappearing Cryptography: Information Hiding & Steganography and Watermarking / P. Waner. – San Francisco: Morgan Kaufmann, 2009. – 456 p.

Список литературы на английском / References in English

1. Potapova R.K. Perspektivy ispol’zovanija steganograficheskih tehnologij v zvuchashhej rechi na sovremennom jetape razvitija [Prospects of using modern steganographic technologies in spoken speech] / R.K. Potapova, A.V. Dzhunkovskij // Vestnik MGLU. Gumanitarnye nauki [Vestnik MSLU. Humanitarian sciences]. – 2019. – № 5 (821). – pp. 206–211. [in Russian]

2. Salagaj M.O. Prosodicheskie sredstva zashhity smyslovoj informacii (jeksperimental’no-foneticheskoe issledovanie v oblasti steganografii) [Prosodic means of information protection (experimental phonetic inquiry in the field of steganography)]: dis. … kand. filol. nauk [Dissertation of a PhD in Philology] : 10.02.21 : zashhishhena 14.11.2011 / Salagaj Marina Olegovna. – M.: FGBOU VPO MGLU [MSLU], 2011. – 203 p. [In Russian]

3. Bennet K. Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text / K. Bennet // CERIAS Tech Report. – 2013. – № 4. – pp. 1–30.

4. Dzhunkovskiy A.V. Steganography: Three-Stage Analysis Methodology Applied to Russian Written Texts / A.V. Dzhunkovskiy // Вестник МГЛУ. Гуманитарные науки. – 2018. – № 6 (797). – pp. 117–123.

5. Johnson N.F. Exploring Steganography: Seeing the Unseen / N.F. Johnson, J. Sushil // IEEE Computer. – 2020. – № 32(2). – pp. 26–34.

6. Potapova R. Preliminary Investigation of Potential Steganographic Container Localization / R. Potapova, A. Dzhunkovskiy // Lecture Notes in Artificial Intelligence. – 2020. – vol. 12335. – pp. 389–398.

7. Provos N. Defending Against Statistical Steganalysis / N. Provos // Michigan: University of Michigan Press, 2001. – 343 p.

8. Ross A. On the Limits of Steganography / A. Ross, F. Petitcolas // IEEE Journal of Selected Areas in Communications. – 1998. – № 4(16). – pp. 474–481.

9. Taskiran C.M. Attacks on Lexical Natural Language Steganography Systems / C.M. Taskiran, U. Topkara, M. Toplara // Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents, San Jose, CA, February 15-19, 2006. – pp. 122–130.

10. Wayner P. Disappearing Cryptography: Information Hiding & Steganography and Watermarking / P. Waner. – San Francisco: Morgan Kaufmann, 2009. – 456 p.