SUITABLE FORMS OF STEGANOGRAPHY USAGE IN PUBLIC ADMINISTRATION

NikolaPopović
Ministry of Foreign Affairs Republic of Serbia
Belgrade, Serbia

Julijana Mirčevski
Association "Jelena Anžujska"
Belgrade, Serbia

ABSTRACT

Steganography render an unusual way to use electronic documents or public administration WEB sites for exchange lower level classified information. Several different forms of the steganography are tested and/or evaluated to envisage and enhance the capacities of the secure channels for messages exchange. Economic and security aspects of steganography usage is also encountered considering only open source software systems and selecting technological means and information resources which already exists at disposition in public administration.

I. INTRODUCTION

Today, the use of steganography take up more and more important position in the world of business and public administration also. Country in transition through the privatisation of key fields as communications and media encounter new, up to now unknown, challenges. Confidential communications and information are not more guaranteed and secured by means and instruments supplied by the state (as the national resources in developed countries). Their security are leaved to private owners or strong stakeholders of privatized communication systems. In such context there are a lot of reasons that control of comunications at strategic and tactical levels need urgent uprising to higher level, besides cryptography, by using newest steganographic methods. Besides that there is no formula for succes, contemporary steganoanalyse accomplish notable successes in detecting presence of the steganographic content and in some extent in decoding secret messages [1]. It should be noticed the statistically significant growth of scientific communications in the domain of the steganography.

In text about the steganographic sofware [2] it is shown the emerging interest in exploiting stenganography for Government administration tasks: „The U.S. Department of State is conducting market research to determine the degree of interest and capability ... in providing steganography services for the Bureau of Consular Affairs. ...for developing a card security feature (i.e. card-format passport) that uses applicant data and steganography to provide a unique authentication method, using secure software that enables embedding a Department of State derived string of characters into the printing of the bearer's photograph so that no string is detectable without decoding, but the string is readily seen with decoder, without otherwise effecting the applicant data or the rest of the personalization printing".

II. RESEARCH GOALS

The growing use of the Internet has led to a continuous increase in the amount of data that is being exchanged and storage in various digital media. This has led to some unexpected cases involving both benevolent and malevolent usage of digital data. Security and authentication techniques like digital watermarks; steganographic methods and other data embedding algorithms have contributed much to enhance the various security features and to preserve the intellectual property. In this respect, steganographic techniques have been the most successful in supporting hiding of critical information in ways that prevent the detection of hidden messages [3]. Usage of the standard official cryptographic mechanism for information exchange is a complex technological and organizational problem.

This paper is an attempt to bring out the significance of the steganographic techniques that could possible be employed in the information exchange procedures. It deals with the problem of data security, focusing mainly on texts and images, and tries to state the various properties and characteristics that the steganographic algorithms should possess. The main goal are to investigate light, short period data security mechanisms intended to apply on routinelly executed procedure like the tenders in public procurements, or messages that should not be „published" via e-mail or phone etc.

III. MATERIALS AND METHODS

In this text steganography is considered in the source form and meaning, and analyze applications domain less mentioned in the literature. There are selected and evaluated an easy-to-use and affordable non-commercial off-the-shelf software and especially open source softwares and algoritnhms for the sake of security.

Specifically the reusable and multiplied application of steganographic algorithms are analyzed. In these cases steganographic algorithms are applied not only to the primary carrier of the secret message, but to the message himself, also. The message too, may take the role of carrier of the secret message, in recursive sense. It is tested possibility to embed two (or generally more) secret messages into one outlined steganographic carrier. In this case it should be use different steganographic algorithms to escape succesive distortion of outlined carrier i.e. to avoid unreadibility one of the messages. Recursion has deficiency pertaining to the carrier capacity.

A. Recursive steganography

In the folowing section there are shown two experiments based on concept of „steganographical steganography" or formally expressed as „recursive steganography" (see Fig 1).

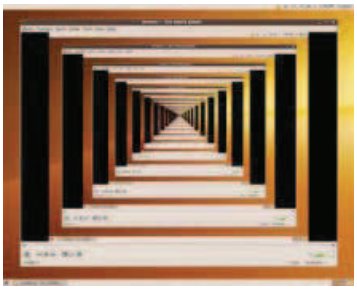

Figure 1: Visualized concept of the recursion

1) Embeding two messages into one cover image

The question: Are there possibility to embed more secret messages into one steganographic carrier and at same time maintain readibility of embeded messages.

This idea is explicitly cosidered a few years ago in paper of (Zhang 2007) [3] which have been described and analyzed process of using a multilayer embbeding steganographical messages in the image as a steganographic carrier. Later text (Al-Najjar 2008) [4] describe similar technology for multimedia steganography. Programs for image, audio and video editing consequently have the broader spectrum of capacities to apply steganography [5, 6].

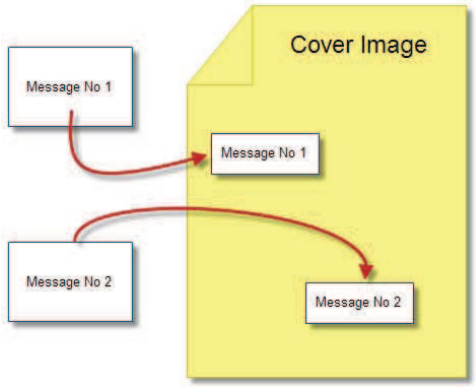

Figure 2 Embedding two messages into the cover image

Software for experiment was choosen from OpenSource domain - Digital Invisible Ink Tool (DIIT) of author Kathryn Hempstalk [7]. This software is suitable for experimenting because it has implemented six different types of steganographic algorithms and each of them are parametrized. Test messages are the following: first message Message No 1 contains only uppercase letters „A“ and other message Message No 2 contains only uppercase letters „B“. Size of both messages are 630 character in length. First message is embeded in cover image – using specified algorithm A1 and password Password No 1, other message Message No 2 is embeded into the same cover image using specified algorithm A2 and password Password No 2.

The procedure for embedding two text files into the cover image (Fig 2) is the following:

1. The cover image is Image No 1.
2. First step is to embed document Message No 1 to Image No 1 using algorithm type *BattleSteg*.
3. Result is image Image No 2
4. Second step is to embeds document Message No 2 into Image No 2 using algorithm type *FilterFirst*.
5. Final cover image is Image No 3 with embeded two messages.

Then have been applied inverse procedure – extraction messages from final cover image Image No 3:

1. Apply Decode procedure. Program require password: enter Password No 1 to extract Image No 1
2. Result is extracted Image No 1
3. Then apply Decode DIIT procedure again: Program require password: enter Password No 2 to extract Image No 2
4. Result is extracted Image No 2

Result is the same as in the case first described.

The conclusions of performed examinations of DIIT program are the following:

- it is possible to embed at least two different messages into one cover image using two different steganographic alghoritms
- exibited deterioration suggests that by repeating the same message two or more times it is possible to sustain readibility of message content
- the possibilty of embeding more messages into one steganographic layer organize higher level of the confussion to the attacker or steganoanalyzer
- when detect and decode deteriorated message then raise up new question for steganoanalyzer – is this deteriorated message – final message, or possibly exist new undetected layer of steganography

Also it is posible to confuse the steganalytic attacker by embedding one or two fake, scrambled messages and finally the actual message. It should be notice works of Davison [8] speciffically in Chapter 6. which contains source code written in Java programming language. Programs are intended to inscriptions multiplied copy of the steganographic messages into cover image. Author’s attention is dedicated to reducing possibility that image will be damaged or distorted during (eventually) image transformation (writing etc.). Instead of embeding miltiplied copies it is possible to embed several different messages.

2) Embeding two messages recursively

Test based on concept of recursive steganography is performed using the simple scheme (Fig 3):

- into the text of primary message (Message No 1) is embeded new secondary secret message using one of the simplest metods of linguistics steganography
- changed primary message is embeded into cover image using some of steganographic alghoritms
- performed inverse transformation shown that there are not specific problem during described procedure of using steganography – primary secret message is normally extracted without deterioration

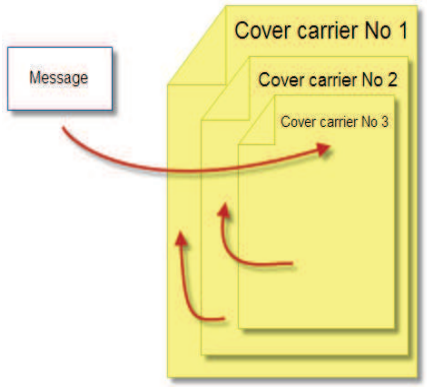

Figure 3 Model of recursive steganography

By himself performed test is not especially interesting but it can be concluded that:

- using this type of recursion („russian babushka dols" method) using simultaneosly different methods of steganography aggravate the process of steganoanalysis
- in case of multilevel steganography blind steganoanalyses require more complex testing and probably human intervention to conclude what is final message in hidden messages chain
- simultaneously applied recursion and embeding of several messages on different points of cover carrier generate significant information noise and seriously aggravated steganoanalysis

B. WEB site use as a postbox

There are major trends of using WEB technology in public services (G2G, G2C, G2B etc.). It is known that nor WEB 2 concept nor something called WEB 3 concept (unclear status) don't solve fundamental problem of WEB data security. More than 90% of all attacks are related to WEB sites. In articles of (Mills 2010) [9] and (I-Shi Lee-a 2008) [10] are considered topic about unvisible malicious usage of WEB sites i.e. using WEB site as the postbox for exchange the hidden messages. Computer forensic problem of collecting evidences in such situations requires cost and time consuming operations. Observed, analyzed person or organizations is not obliged to apply the most secure, and expensive also, measures. Intentionally or not, setting up lower security level „attacker" or „messenger" is enabled to embed secret message to files and folders of the targetted WEB site. User of embeded information has oportunity to access covered content in time period determined beforehand. More complicated problems are related to so called „invisible WEB" domain which is in wide usage also. Currently, Steganography represents a classical paradox: It is next to impossible to convince people to look for something they cannot see and do not think anyone is using because there is no large body of empirical data to prove that steganography is being used to transmit information outside of corporate or government networks.

In government and public administration domain WEB sites by himself represents very suitable places for exchange of lower classified information. For example, the sequence and contents of daily news may be used as a „public" key or pointer to access aimed segments of WEB sites. The presence of the huge number of texts formatted as pdf or docs documents give the posibility to transfer quite important quantity of information using linguistic or any other type of steganography methods.

C. Simple UNICODE Steganography

The UNICODE standard can generates a lot of the steganalysis problems. There is illustrated usage of so called *automatic font subtition* mechanism of the Microsoft Word (also can be applied in the OpenOffice, LibreOffice or similar word processing programs) to hide a message in the Word document. Using Font Design program it is maked the new font in the standard font family i.e. Times New Roman. In this case it is used High-Logic FontCreator Professional Edition Version 6. In the new font the glyphes are modified and enables the user to apply any of the classical encryption techniques (substition, Vigenere cipher etc.) or simply write needed characters in the document text in modified font. Both sides, sender and receiver, must have the same modified font installed. The word processor recognizes modified font and show exactly font family name in the respective field on the toolbar. But if the respective font it is not installed on the computer nonexistent font will be automatically replaced with similar font – steganoanalytics attacker can not be able to immediatelly visually detect different font presence. The different font presence can be registered if the respective part of Word document be analysed (depending on MS Word version in XML editor or in text editor in Hexadecimal mode better). The naming of modified font is problematic in some way. In this case it is used Unicode standard to change font name i.e. font names „Times New Roman" and „Times New Roman" are visibly equal. But differences is in the following: „Times New R*006F*man" and „Times New R*043E*man" – in the second font name letter „o" is cyrillic „o" (see extended hexadecimal codes). Modified font can be used in PowerPoint presenatations, Excel documents, Web sites pages also etc. All these documents are very present in the public administrations documents flows.

D. PDF Steganography

Steganoanalyse of the PDF documents usage as a cover document is analyzed in details in article (Zhong 2009) [11]. This type of documents are in frequently usage in public administration. PDF documents are homogenous in the sense of contents and format, so they are suitable in the role of steganographic carrier. Texts written by (Didier Steevens 2009) [12] supply source code (in Python programming language) form embeding secret message into pdf file. Programs are tested and they are functional. Well have made analyse of contradictories of the PDF proprietary format significantly spread abroad the horizont for ensuing research. Future researchs will be focused on the ODF format (ODF - Open Document Format).

E. PowerPoint Steganography

Most steganographic algorithms are mainly dedicated to images, audios, and videos as a cover media. Although the Microsoft PowerPoint file is so prevalent today, related steganographic methods have rarely been reported. Actually it is feasible to hide data in PPT files and the potential embedding capacity is considerable. Liu (2008) [13] made detailed report about using PPT files as cover media. Linguistic steganography methods are mainly used. In text of the another author (Liu 2008) [14] it is described some specificity of MS Office PowerPoint tools in final file writing phase. Secret file can be embeded in unsued or wasted space of presentation files which are regularly generated during writing. Besides textual or linguistic steganography Power Point presentations are suitable for steganography because usual presence of large number of graphical elements (images, backgrounds, diagrams, diffrent templates etc.) PowerPoint 2007 has option to write PPT in XML format. There is few years when started using steganalysis using noncontroled changes in the XML file. Not rare question on internet is:"How to embed Flash movie into PowerPoint" (i.e. Google serch machine puts 79900 hits). These information open new series of steganalytic problems [15].

Watermarking is intended to protect authenticity and validity of documents. It is not too clever to exclude presumtion that Watermark, besides original protective function, may be used as a steganographic carrier using Fingerprinting [16] option.

F. Applets and Bytecode steganography

Alvin Alexander-a (2010) [17] demonstrate several procedures for decompilation Java Applets. Program [18] j-d-gui v0.3.2 for Windows OS has been downloaded and tested. Obfuscations are no need, if the structure of applet will be periodically changed to avoid recognition of its basic function. Applets compared with computer viruses are too visible and stare and requires uploading to WEB sites. Bytecode steganography is related to exploting of unused part of applets bytecode. Applets are less immanent on government sites and therefore not too much usefull in practical sense.

G. Multifunctional viruses

Srikanth (2007) [19] give us an example of simple computer virus writen in C programming language. The program code not includes parameters or arguments. Why? If virus read a valid or targeted value of for example communication card NIC or HDD ID multifunctional virus has two options: to display secret message or in all other cases to attack computer and provocate antivirus program to „execute" him (or to activate selfdestroying intraviral mechanism – so called „suicidal virus").

Generally speaking every virus today present on internet, by nature, may be (secret) messenger! Besides demonstrating malicious behaviour by himself – virus can carry secret message hiden in internal code or programmed as a finite automata. In the case of multifunctional virus by parametrization virus code acting selectively – by using explicitly malicious mass action it hide transfer of steganographic message. Message(s) are delivered only to targeted one (or more) computers, all others attacked machines recognize received code as a virus and destroy it. In considered case fundamental operating principles are equals to those applied in domain of e-banking (managing PKI etc.). Viruses are very suitable as the messengers because they are very present on the internet, and it is tremendous job to check every possible (sended) instance of the virus. In the very near future it should be expected polymorphic steganographic viruses - messengers.

H. Social networks and Steganography

Where is the interest on considering the social networks in the context of the steganography? The contemporary steganalysis mainly use the statistical methods on the hidden messages detection. Our opinion is that Internet is too large and extremely complex object for the capacity of the contemporary statistical methods. We must notice that many high theoretical considerations of the steganalysis methods efficacy are directed to the very known steganographic algorithms (F5, JSteg etc.). Steganography by itself is much closer to the art than to the mathematics. We suppose that identification of the suspected social networks is much more rational first step to combat with potentially malpractice of the steganography. The classical problem of the Information Retrieval is how to narrow the information space for search at initial – that is the reason why we consider relationship between the steganography and the social networks.

Another aspect of social networks concept is merged to the strong contradiction between openness of the Internet idea and real national security concept. The broader aspect of the steganography itself must not be localized to the problem how to hide message but also how to hide exchange of information generally. There are three different interconnected problems:

- how to hide message in the cover document
- how to hide the exchange of information
- how to hide social network what use the steganography

Social networks appears gradually in Government and public administration affairs domain [20, 21] with functions adjusted to real requirements of administration and agencies. With officials spread across the counties (inspections, dettached departments etc.), using the network will allow employees to post requests for informations that other users can validate, as well as link to other resources, articles or posts they've contributed to other Web-based communities. Social networking has become a driving force in state administration's moves to make the government more open to the public and encourage greater public participation. It also is trying to foster greater internal collaboration by using public or internal sites to share information across departments or with the community.

Oposite to the public social networks, those who emerge in government departments and agencies obviously must hold at disposition secured, multilevel channels (Frost and Sullivan 2009) [22] for exchange information. Current research in steganography is focused on identifying various platforms through which one can hide information. Extensive analysis

in public social networks enlighten very wide spectrum of different kinds of dangers, riskiness and wickedness. Organized criminal forwarded by IT experts can be very forceful enemy. Slackly communications in government agencies (especially using e-mail, messengers, IP telephony etc.) admit the leakage of important information through "innocent" mailing, short informal questions etc. Steganographic means mentioned above are suitable for "channeled" communications including internal social networks. Unlike of the cryptography requiring specific environment and organization, usage of steganography may be much simpler but yet sufficient effective especially in temporary sense. The invisibility and sustainability of the steganography based communication channel is dependent on the two factors: a) open source software is important because the controlability is ultimate need – user must know exactly what is in use, and b) the steganography system must has form of a dynamic complex of several steganography programs which can be used interchangeably based on the specified dynamic scheme, changing algorithms and cover media also [7].

IV. Conclusions

The Steganography should be included in regular communications systems and other services of public administration. The reasons are related to the needs to protect selected parts of regular business and officials communications from intruders. Systems and networks infrastructure are the weakest chain-link in the information security chain. Same reasons is very valid on so called „outsourcing" projects. The members of localized social networks must have at disposition means to protect their „official privacy" in domain of interpersonal consulting and so on. This research are looked out to the close future – we must protect information as the national resources. The investigation of a specific cover media such as: pdf, ppt, bytecode, multifunction viruses, etc. for that there are not yet developed the steganoanalitical algorithms, is very topical. In the future research the authors will be dedicate to analyzing and evaluation of efficacy mentioned file type in a role of steganographic cariers.

V. References

[1][Online].Available:http://www.backbonesecurity.com/Latest_News/Entries/2010/4/29_Backbone_Security_Releases_New_Version_of_Popular_StegAlyzer_Tools.html[accessed 29/4/2010]

[2][Online].Available: https://www.fbo.gov/ Steganography Services, Solicitation Number: 1044006902, 21.05.2010 [accessed 21/5/2010]

[3] X Zhang, W Zhang, S Wang (2007) 'Efficient double-layered steganographic embedding', Electronics Letters

[4] AJ Al-Najaar (2008), The Decoy: Multi-Level Digital Multimedia Steganography Model, Paper Presented at 12th WSEAS International Conference on COMMUNICATIONS, Proceedings of papers (pp. 445-450), July 23-25, 2008, Heraklion, Greece,

[5] Julijana Mirčevski, Biljana Djokić, Milesa Srećković, Nikola Popović (2007), Software Tools And Technologies In Steganography, Paper Presented at the International Conference ICEST 2007. June 24-27 2007, Proceedings of papers,(pp. 543-546), Ohrid, Macedonia

[6] Nikola Popović, Julijana Mirčevski (2009) 'Mogućnosti primene virtuelizacije u sistemu državnih organa i problemi zaštite', Paper Presented at the Konferencija ISDOS 2009, septembar 2009, Beograd

[7]Kathryn Hempstalk (2007) DIIT,[Online].Available: http://diit.sourceforge.net/index.html [accessed 1/6/2010]

[8] Andrew Davison (2009) 'Java Prog. Techniques for Games. Java Art Chapter 6'. Stego, Andrew Davison©2009,Draft #1(7th June 09)

[9] Elinor Mills (2010) 'New DoS attack uses Web servers as zombies', CNET News InSecurity Complex May 12, 2010 4:12 PM PDT, [Online].Available: http://news.cnet.com/ [accessed 1/6/2010]

[10] I-Shi Leea, and Wen-Hsiang Tsai (2008) 'Secret Communication through Web Pages Using Special Space Codes in HTML Files', International Journal of Applied Science and Engineering 2008. 6, 2: 141-149

[11] Shangping Zhong, Xin Fang, and Xiangwen Liao (2009) 'Steganalysis Against Equivalent Transformation Based Steganographic Algorithm for PDF Files', Proceedings of the 2009 International Symposium on Information Processing (ISIP'09) Huangshan, P. R. China, August 21-23, 2009, pp. 075-078 [Online].Available: http://www. academypublisher.com /proc/isip09/papers/isip09p75.pdf [accessed 1/6/2010]

[12] Didier Stevens (2009) 'Embedding and hiding files in pdf documents',[Online].Available: http://blog.didierstevens.com/ 2009/07/01/embedding-and-hiding-files-in-pdf-documents [accessed 25/5/2010]

[13] Liu, Y., X. Sun, Y. Liu and C.T. Li (2008) 'MIMIC-PPT: Mimicking-based steganography for Microsoft power point document'. Inform. Technol. J., 2008, 7: 654-660.

[14] Yongping Liu, Xingming Sun, Yuling Liu, Rong Xiao (2008) 'File-Update Based Steganography for Microsoft PowerPoint Files', Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pages: 11-15.

[15] Mozo, A.J. Obien, M.E. Rigor, C.J. Rayel, D.F. Chua, K. Tangonan, G. (2009) 'Video steganography using Flash Video (FLV)', Instrumentation and Measurement Technology Conference, 2009. I2MTC '09. IEEE , pp 822 – 827.

[16] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett (2004)'Steganography and Digital Watermarking', School of Computer Science, The University of Birmingham. Copyright © 2004[Online].Available:http://www.cs.bham.ac.uk/~mdr/teaching/modules03 /security/students/SS5/Steganography.pdf [accessed 28/5/2010]

[17] Alvin Alexander (2010) 'Java decompilers and obfuscators' [Online].Available: http://www.devdaily.com/java/java-obfuscators-decompilers-class-source [accessed 28/5/2010]

[18] http://java.decompiler.free.fr/ [accessed 28/5/2010]

[19][Online]Available:http://www.gohacking.com/2007/ 12/c-program-to-demonstrate-virus-in-c.html [accessed 25/5/2010]

[20] Kathleen Hickey (2010) 'State Department social network in the Works',[Online].Available: http://gcn.com/Articles/2010/04/27/ Statebook-social-network, Apr 27, 2010 [accessed 25/5/2010]

[21] HCI (2010) 'Social Networking in Government — Part I: An Overview of Opportunities & Challenges, Part II: Diverging Patterns of Use Among Government Agencies, Part III: Closing the Satisfaction Gap in Using Social Networking Tools in Training and Development', Copyright © 2010 Human Capital Institute, January 2010

[22] Frost and Sullivan (2009) http://www.researchandmarkets.com/ research/dce9e7/steganography_fut/Steganography: Future of Information Hiding, Frost & Sullivan, Dec 2009, Pages: 66 [accessed 25/5/2010]