Quest Journals
Journal of Software Engineering and Simulation
Volume 3 ~ Issue 7 (2017) pp: 22-26
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Steganographic Technique Using Instant Messaging Conversation Dynamics

*Branislav Madoš[1], Ján Hurtuk[1]
[1]*Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, tel. +421 55 602 3023,*
*Corresponding author: *Branislav Madoš*

Received 10 August, 2017; Accepted 12 August, 2017 © The author(s) 2017. Published with open access at **www.questjournals.org**

ABSTRACT : *Steganography is considered to be not only the science but also the art of hiding secret messages into other innocuous and non-secret media of different types. History of steganography started with the history of civilization and algorithms of data hiding have been constantly developed with the rise of mankind's knowledge. Some of steganographic algorithms are so close connected to the use of digital media, computers and information technology, that those algorithms do not have analogy in non-digital world. It is possible to see the use of hard disk drives (HDD), solid state discs (SSD) and file systems for the purpose of steganography, or steganography in TCP/IP networks as the example. In this paper we are concentrating on such algorithm and we are examining the possibility of the use of dynamics of conversation realized with the use of instant messaging services, which are very popular standalone services or are part of widely used social networks like Facebook. The paper discusses the possibility of hidden message encoding by the use of different parameters of conversation dynamics and introduces new algorithm and its program implementation. The last part of the paper summarizes results of its experimental use.*

Keywords: *instant messaging, IM, social network, steganography, time-stamp*

I. INTRODUCTION

Despite the fact that big attention is paid not only by scientists but also by the industry to the cryptography in the present, cryptography cannot solve all problems which are connected with information security [1]. In many cases the very existence of information stored on the media or sent through the communication channel draws undesired attention and represents some kind of information [2]. The use of cryptography even further increases suspicion. For example existence of the encrypted communication between person and foreign embassy in a time of war conflict or encrypted communication with person which is suspected as the criminal can be very dangerous if it is not concealed. This is one of reasons why information hiding techniques were invented. Classification of those techniques according [3] is depicted on the Fig. 1. One of information hiding techniques is steganography.

The word steganography comprises of the Greek words *steganos (στεγανός)*, that means covered or concealed, and the word *graphein (γράφειν)* that means writing. The word has been used in 1499 first time by Johannes Trithemius in his work *Steganographia* [4] but the first use of steganography itself can be dated back to the 440 BC, when the use of steganographic procedures have been mentioned by Herodotus in his work *Histories* [5]. Æneas the Tactician has been dealing in his work *How to survive under siege* [6] with the steganography rather than cryptography. Many works on steganography were published in 16th and 17th century, for example *Schola Stegnographica* by G. Schott [7]. Steganography was widely used also in modern age, for example in Second World War (WWII), when different modifications of grille technique were used along with others, such as microdot.

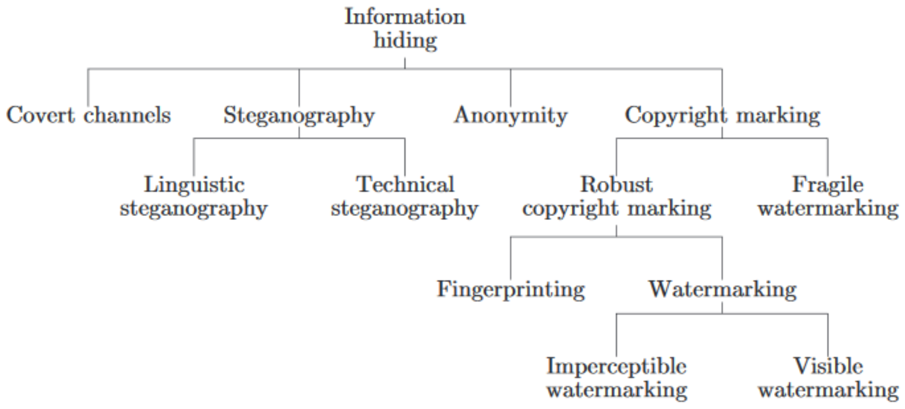

Figure 1 Information hiding techniques classification.

Microdot can be seen as the document, which is shrinked using photographic techniques to microfilm with the size of the dot on letter 'i' or the dot after sentence and consecutively those dots are replaced by this microfilm. Text messages were often hidden and sent as the part of other large and innocuous text messages in WWII.With the rise of the computers and informatics, many steganographic techniques gained their effective program implementations. There are many steganographic techniques which are based on the use of digital media, information technologies and computers and do not have counterpart in non-digital world. As an example we can see the use of computer file systems such as FAT or NTFS for hiding information using steganographic techniques [8]. Another example can be seen in the use of TCP/IP protocol [9]. That is why we can divide steganography into pre-digital and digital era.

First academic conference which was dedicated to the subject of steganography was held in Cambridge, United Kingdom in 1996 [10]. Very useful overview of the steganography can be found in Petitcolas et al. [11] and Kessler and Hosmer [12].Digital steganography can be divided according to the type of media which is using. Traditional digital media used in steganography is the text, image, audio and video sequence. Very popular and well known steganographic technique which is using raster images is Least Significant Bit (LSB) steganography. It is possible to apply this principle also to another media, for example the audio sequences [13]. Steganographic techniques which are using vector graphics can be divided by the use of jittering and embedding respectively. Jittering resembles LSB steganography, and hides information into least significant digits of numbers which are describing image. Embedding hides information by adding other redundant number codes which do not modify the visual representation of the image. Example of such algorithm for information embedding into the SVG format brings [14].

Wide range of steganographic techniques are oriented to the hiding texts into another texts. Unlike those techniques, we are examining the possibility of the use of instant messaging services as the carrier of hidden messages in this paper and our approach is not the modification of the text representation or creation of suitable artificial texts of conversations, but rather modification of the dynamics of conversation in which hidden information can be encoded.

The structure of the paper is as follows.

Section 2 of the paper discusses dynamics of instant messaging conversation and in this paper proposed possibilities of hidden information encoding in time-stamps of conversation replicas and in their ordering.Section 3 of the paper introduces designed experimental instant messenger web service solution and some details of its program implementation.Section 4 summarizes results of tests of program implementation and the last section of the paper represents conclusions and outlines of the future research in the field.

II. DYNAMICS OF INSTANT MESSAGING CONVERSATION

As the part of this research we were examining dynamics of conversation realized through instant messaging (IM) service and concluded that dynamics can be represented by two basic factors:

- Time, in which the replica of conversation was sent, resp. received.
- Order of replicas in conversation.

Time, in which the replica was sent, can be controlled precisely to the hundredths of seconds, and it is possible to include this time stamp by the IM software client of the sender of the message, consecutively it can be stored in the IM service database. At the end it is possible to send this information to the IM software client of the message receiver. It is possible to shift time in which replica was sent slightly and to encode into this shifted time part of the hidden message. For example, if last digit of seconds and digits which are representing hundredths of seconds is used, it is possible to encode three decimal digits into each replica time stamp and still the time shift of the message will be only in the range of 10 seconds. Hidden message encoding can be done as the absolute or relative encoding. If absolute mode is selected, least significant digits of time stamp immediately carry the encoded information (Fig. 2). In case of relative mode, there is operation needed for calculation of encoded information with the use of least significant digits of current and previous replicas.

Time	**Time**	**IM Message**	**Absolute encoding**
Original	**Shifted**		**of hidden message**
17:50:16:23	17:50:21:19	**Lorem ipsum dolor sit amet**	119
17:51:31:16	17:51:31:46	**consectetur adipiscing elit**	146
17:51:42:23	17:52:02:36	**Nam eu ornare**	236
17:52:47:13	17:52:48:23	**Nulla. Morbi luctus nec**	823

Figure 2 Time stamps of conversation comprising hours, minutes, seconds and hundredths of seconds and its shifted form, text of the cover IM message and encoding digits of the hidden message in absolute form.

If this steganographic technique is applied on the IM service, which is not under control of communicating parties, it is impossible to control precisely the time of sending and receiving of messages. If IM client displays the time when message was received, it is possible for example to use ranges of time to encode information. For example if it is possible to ensure that IM service will deliver message within range of ten seconds, it is possible to encode hidden information into most significant digit of seconds of time stamp, when for example even most significant digits will represent 0 and odd most significant digits will represent 1. It is possible to encode hidden message in various binary encodings. Another factor which can be used for information encoding is the order of replicas in the meaning of alternation of replicas, when after replica of one person can be sent another replica of this person or replica of the second communicating person. Many possibilities of information encoding arise from this principle.

Time stamp	**Message**	**Hidden message code**
17:50:21:19	**Lorem ipsum dolor sit amet**	119
17:51:31:46	**consectetur adipiscing elit**	146
17:52:02:36	**Nam eu ornare**	236
17:52:48:23	**Nulla. Morbi luctus nec massa**	823

Figure 3 Two way hidden communication in which green replicas encode hidden message represented by digits 119236 sent by first person and red replicas encode another independent hidden message 146823 sent by second communicating person.

For example information can be encoded in the number of replicas sent consecutively by one person. Another approach can encode digit 0 when two replicas are sent by one person consecutively and digit 1 can be encoded when replica from one person is sent after another person replica. It must be ensured that each communicating person has enough time to send as many replicas as it is needed to encode information or to wait for replica of other communicating person by particular rules. Approach to the information encoding can be combined, when rules for time stamp encoding and rules for replicas ordering can be applied in various encoding techniques. Communication in the form of the dialog allows one way hidden communication or two way communication, which can be independently held in the same time in one dialog as it is depicted in the Fig. 3.

III. SOLUTION DESIGN

For experimental verification we designed IM web service using HMTL and PHP languages and MySQL database. Designed IM client allows users to choose contacts they want to communicate with and to display the wall with replicas in the same manner as usual IM services do. Each replica is represented by the text and the time stamp, which comprises hour, minute, second and hundredths of second, when message was sent. Although full information about time stamp is sent, only information about hour, minute and second is displayed to the user in web browser user interface. Unlike other IM service, proposed service is augmented with two other input fields and one output field. In first of them user is able to choose the starting time, from which the hidden message will be encoded into or decoded from the conversation. Another field is input field where user can type his message which will be encoded and the IM client will start to encode this text into conversation time stamps from the chosen time. Another field is output field, where extracted message which was encoded by the second persons IM client is displayed in real time, as the IM client decodes it from time stamps of held conversation.

Message encoding uses alphabet which comprises small and capital alphabet letters, digits and other characters, as it is depicted in the Table 1. Each character is encoded by the use of two decimal digits, first is the number of row, second digit is the number of column in the table. Those two digits are written into the time stamp of replica as the hundredths of second. Each replica time stamp encodes one character from the table. Absolute encoding as it was described above is used. If the user wants to send not allowed character in the hidden message (character which is not in the Table 1), application prompts the user.

Table 1 Alphabet and codes of respective characters used in hidden message encoding.

	0	1	2	3	4	5	6	7	8	9
0	A	B	C	D	E	F	G	H	I	J
1	K	L	M	N	O	P	Q	R	S	T
2	U	V	W	X	Y	Z	a	b	c	d
3	e	f	g	h	i	j	k	l	m	n
4	o	p	q	r	s	t	u	v	w	x
5	y	z	0	1	2	3	4	5	6	7
6	8	9	SPC	.	,	:	;	?	!	‘
7	„	“	(	)	[	]	{	}	#	@
8	$	%	^	&	+	-	*	/	\	>
9	<	=	_	NUL	STX	ETX	LF	CR	TAB	EOT

Two-way communication is used when input message from the user is encoded in his replicas time stamps, and hidden message encoded into replicas of other user is extracted, decoded and displayed in output field of user interface. If one-way communication is needed, user leaves the input field of hidden message blank. IM client of the user is autonomously shifting time stamps of replicas to encode hidden message character by character in real time. Last character of the hidden message encodes End Of Transmission (EOT) character with the code 99. Another possibility how to start hidden communication is the use of STX character which means the start of the text and end of the hidden message is indicated by the ETX character.

IV. DISCUSSION AND RESULTS

In tests of practical usability of the IM web service it was proven that it is possible to use it for usual conversation between two users without encoding hidden messages. Algorithm that was designed as the part of this research is suitable for one way and two way hidden communication and also its program implementation in this IM web service was fully operable.Because only part of time stamps which represents hundredths of seconds is altered, the flow of conversation is modified in minor way and users are practically unable to see the difference between classical IM conversation and conversation which includes hidden message encoded.Advantage of this solution is that encoding information into conversation and decoding is autonomous, user do not need to realize any further operations, and the only assumption is that conversation will be held so long (in number of replicas) that all characters of hidden messages will be encoded. Another advantage is that algorithm does not include any additional information to the representation of the IM conversation but only modifies information that is usually included in IM conversations. Disadvantage of this steganographic technique can be seen in small speed of hidden information transmission. In tests of normal speed conversation it was possible to send a few hundreds of characters within one hour of intensive conversation. Table 2 summarizes results of four tests conducted as an example. It is possible to generate artificial conversation and send replicas automatically with the higher speed but on the other hand it is possible to develop solution which will be able to autonomously detect abnormal speed of IM conversation.

Table 2 Test of hidden information transmission speed in normal conversation with one way and two way transmission directions.

No.	Communication direction	Hidden message Length [char]	Duration [min]	Transmission speed [char/hour]
1	One way	136	50	163
2	One way	156	73	128
3	Two way	123 + 136	48	324
4	Two way	156 + 162	63	303

V. CONCLUSION

The paper deals with the problematics of steganography. The paper introduces brief history of steganography and its relationship with information hiding in the first part and division to the pre-digital and digital era of steganography is outlined. Next sections of the paper describes suggested possibilities how to encode hidden messages into dynamics of instant messaging conversations as the main contribution of this paper and describes program implementation of the web service that was established for practical experiments. Results of those experiments are summarized in the last part of the paper.It is possible to conclude that designed steganographic technique is suitable for information hiding in dynamics of instant messaging conversations, with relative disadvantage of slow speed of hidden message transmission and advantage in minimal alteration of usual instant messaging communication. This technique allows wide range of different kinds of information encoding and that is why it is possible to orient the future research in the field to optimization of information encoding. For example to allow transmission of any kind of binary files instead of text messages represented in above-mentioned characters encoding table.

ACKNOWLEDGEMENTS

This work was supported by the project 003TUKE-4/2017 Implementation of Modern Methods and Education Forms in the Area of Security of Information and Communication Technologies towards Requirements of Labour Market. The project is being solved at the Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice.

REFERENCES

[1]. E. Chovancová, N. Ádám, A. Baláž, E. Pietriková, P. Feciľák, S. Šimoňák and M. Chovanec, Securing distributed computer systems using an advanced sophisticated hybrid honeypot technology, In: Computing and Informatics, 36(10), 2017, pp. 113-139, ISSN 1335-9150.

[2]. L. Vokorokos and A. Baláž, Architecture of computer intrusion detection based on partially ordered events, In: Petri Nets: Applications, Vukovar : In-Tech, 2010 pp. 13-28, ISBN 978-953-307-047-6.

[3]. B. Pfitzmann, Information Hiding Terminology - Results of an Informal Plenary Meeting and Additional Proposals, Proceedings of the First International Workshop on Information Hiding, Springer Verlag, pp. 347-350, 1996, ISBN 3-540-61996-8.

[4]. J. Trithemius, Steganographia (written 1499, published 1606 in Frankfurt).

[5]. Herodotus, Histories (440 BC, translated by David Grene, University of Chicago Press, ISBN 0-226-32770-1).

[6]. Æ. TACTICIAN, How to survive under siege (Clarendon ancient history series, Oxford, England: Clarendon Press, 1990, ISBN 0-19-814744-9, translated by David Whitehead).

[7]. G. Schott, Schola Steganographica (Published by Johann Andreas Endter, 1665).

[8]. J. Aycock and D. Medeiros Nunes de Castro, Permutation Steganography in FAT Filesystems, Transactions on Data Hiding and Multimedia Security, Springer-Verlag Berlin Heidelberg 2015, pp. 92-105, DOI: 10.1007/978-3-66246739-8-6.

[9]. R.M. Goudar, S.J. Wagh and D.M. Goudar, Secure data transmission using steganography based data hiding in TCP/IP", In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (ICWET '11), ACM, New York, NY, USA, 974-979. DOI: http://dx.doi.org/10.1145/1980022.1980233.

[10]. R. Andersson, Proceedings of the First International Workshop on Information Hiding, Cambridge UK, May 30 – June 1, 1996, Springer-Verlag, London, UK, pp. 364, ISBN 978-3-540-61996-3.

[11]. F.A.P. Petitcolas, R. Andersson, J. Kuhn and G. Markus, Information Hiding – A Survey, In: Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062-1078, July 1999.

[12]. G. Kessler and C. Hosmer, An Overview of Steganography, In: Advances in Computers, 83(1) 51-107.

[13]. N. Cvejic and T. Seppanen, Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding, Journal of Universal Computer Science, 11(1), 56-65. doi: 10.3217/jucs011-01-0056.

[14]. Madoš, J. Hurtuk, M. Čopjak, P. Hamaš, and M. Ennert, Steganographic algorithm for information hiding using scalable vector graphics images, Acta Electrotechnica et Informatica, 14(4), 42-45. doi: 10.15546/aeei-2014-0040.

*Branislav Madoš1. "Steganographic Technique Using Instant Messaging Conversation Dynamics." Quest Journals Journal of Software Engineering and Simulation 3.7 (2017): 22-26.