MULTI-CARRIER STEGANOGRAPHIC ALGORITHM USING LSB STEGANOGRAPHY

Liberios VOKOROKOS, Branislav MADOŠ, Ján HURTUK, Mária FEKOVÁ
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,
e-mail: {liberios.vokorokos, branislav.mados, jan.hurtuk}@tuke.sk, maria.fekova@student.tuke.sk

ABSTRACT

The ambition to achieve covering of secret messages into another file is implemented in many steganographic solutions, but usually the message is covered only into one file. In this paper the mechanism based on the method of steganography, with use of many cover files, is described. Proposal of the algorithm, based on Last Significant Bit method of steganography, is also described. The main contribution of this work is in the proposal of multi-carrier steganographic solution along with its implementation in the software application.

Keywords: *steganography, steganalysis, last significant bit, LSB, bmp, png*

1. INTRODUCTION

Hiding the content of personal messages is natural to mankind since the very time when writing and recording techniques started to be used. In the early days, writing was usually not known to common people, therefore there was no need to hide the written pieces of information from them. Later on, thanks to the development and increase in literacy, people started to develop and design techniques to hide contents of messages as well as to hide the existence of messages.

Today, the two terms - cryptology as a science dealing with modification of messages into unreadable form, and steganology as a science that is dealing with hiding the existence of message [1] - are relatively well known. For this reason, hiding the existence of secret messages has a significant meaning in current everyday life. A good overview of the steganography can be found in [2].

The point of this work is to give a brief overview of methods of hiding the existence of messages, to point out the advantages and disadvantages of steganographic algorithms, and to introduce the suggested algorithm of steganography which makes use of a particular method of steganography, using the least significant bits (LSB) of hiding media [3][4].

The main aim of the work is to propose and design a new algorithm for hiding information into the hiding media of raster image type. For this particular way of hiding data, a steganographic method, making use of a mechanism of hiding into the least significant bits of hiding media, is used. It is very often modified in various software implementations. However, only one hiding medium is usually used to hide the message. Algorithm that is designed in this work is using more extensive set of hiding media.

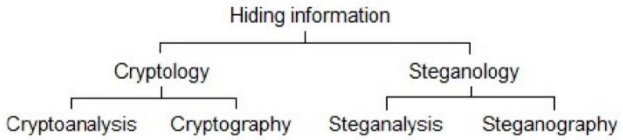

Fig. 1 Classification of information hiding

2. ANALYSIS

For the purpose of hiding private messages within the computer security, two basic approaches can be defined (Fig. 1), that is the adjustment of information assets to a form that is hidden from unauthorized persons - cryptology, and the transmission and storage of information assets in the secret and hidden way - steganology [1][5]. These two disciplines are regularly confused or their meaning is interpreted incorrectly. Both of those disciplines can be further subdivided into two areas. First is the area dealing with hiding information (cryptography, steganography) and the second area is focusing on finding the hidden content of information (cryptoanalysis, steganalysis). All those subareas can be further divided into groups on the basis of the way in which the information is processed.

Steganography as a type of hiding information can be dated as far back as to the period before the computers, as it was often used in linguistic form for visual hiding of information into written texts by using various steganographic grids that were indicating the positions of searched for characters in the text, hiding visual parts into the pictures etc.

The modern steganography, however, is closely linked to the technical computer sphere, where the emphasis is placed on hiding the secret information into commonly used graphic, sound, text or bit ?les. On the basis of graphic types of hiding files used, the steganography is divided into raster and vector steganography. Vector steganography uses images of vector format and modification of numeral data such as point coordinates, circle radii, line thickness etc. for hiding.

Raster steganography uses media in the form of raster image for hiding messages, using information on size, type, colour depth and other specific characteristics of image. One of the particular methods using raster hiding media is the LSB method. This method profits from the inability of person to visually differentiate colour shades that differ only in one unit so that the last bit of colour code is used to hide information. This method can be applied in raster monochromatic images as well as in the colourful images, where all image colour channels of RGB format are used [4][6].

3. SOLUTION AND RESULTS

This section is focused on the description of the design and implementation of the established algorithm that is based on the Last Significant Bit (LSB) steganography method.

3.1. Design of steganographic algorithm

The algorithm proposed as the part of the research uses LSB steganographic method; however, it does not use only one hiding medium for hiding the message. It uses set of hiding media K consisting of n hiding media (files) named as S_1, S_2, S_3 ... S_n as can be seen in the formula (1).

$$K = \{S_1, S_2, S_3, \dots, S_n\} \quad (1)$$

The set of files K does not inevitably have to consist only of one type of files and of the same size of files. On the other hand, various sizes of media is expected, while the total possible capacity C for hiding the message into the set of media K can be calculated on the basis of the formula (2) where the function *min(K)* determines the capacity of the smallest stegomedium from the set K and n is the number of stegomedia of the K set. Capacity of the set is determined in bites.

$$C = \min(K) * n\ [\ b\ ] \quad (2)$$

The secret message is therefore divided evenly into all stegomedia of K set where the algorithm of distribution of the message is defined in three distribution functions.

The first distribution function secures the selection of the method of division of individual bits of message into hiding media. The secret message is therefore divided into groups according to the number of media and components of RGB colour model selected within them.

The simplest distribution function is the function depicted in the image (Fig. 2), on the basis of which the message is regularly divided into individual files.

The second distribution function focuses on the method of selection of the stegomedia order, which is left to specific implementation. However, it can depend on particular hiding file parameters, such as size, file title or content aspect of hiding medium.

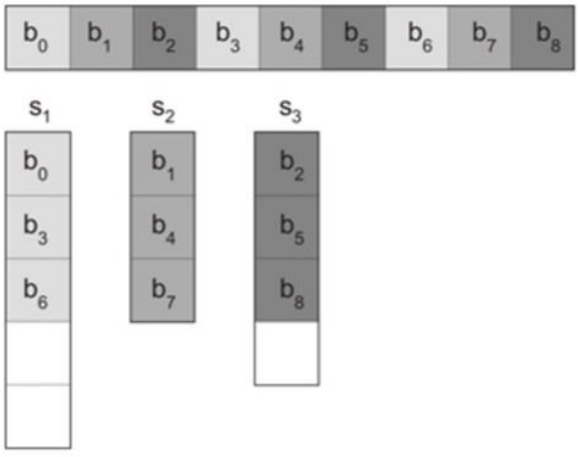

Fig. 2 First distributed function

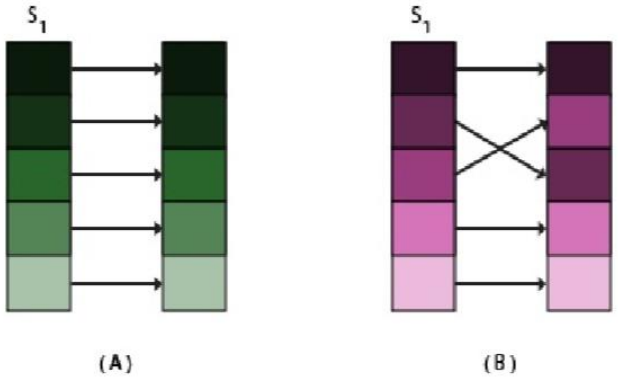

Fig. 3 Third distribution function with use of the min(K) capacity of cover medium

The third distribution function is used to distribute individual bits within the file. Insertion of bits of secret message into hiding medium can be done in different ways. To do that, either all bits of message can be used or only certain bits can be modified, resulting in not all bits changed in the file. The method of using all consecutive bits of hiding medium is depicted in the Fig. 3. Writing of the bits into the hiding medium can be in the order in which they follow in source message (Fig. 3A) or the order can be changed (Fig. 3B).

Another method can be used that is working with omitting bits. In this case not all of the bits of hiding medium are used, only those selected by particular key. This method is depicted in the image (Fig. 4). Writing of the bits into the hiding medium can be in the order in which they follow in source message (Fig. 4A) or the order can be changed (Fig. 4B).

3.2. Implementation of the algorithm

The proposed algorithm was implemented in software application, to verify its functionality. Software is using two elements set K of hiding media files in the .bmp or .png formats.

Function of the program allows to hide secret information into the components of RGB model, each component can be selected by the user. Program also gives the opportunity to process the message being saved in advance, using the encryption of the text of the message, and in this way increasing security of the application usage.

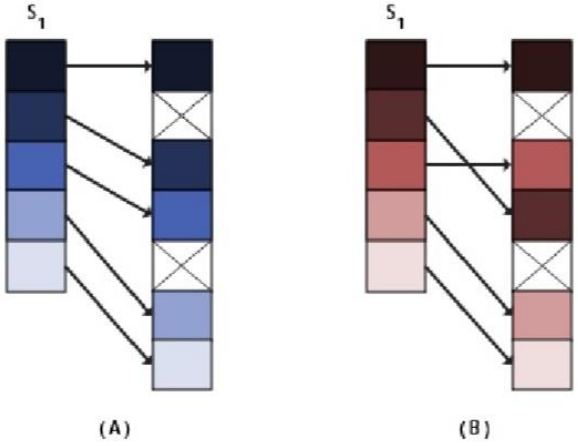

Fig. 4 Version of the third distribution function with use of omitting bits

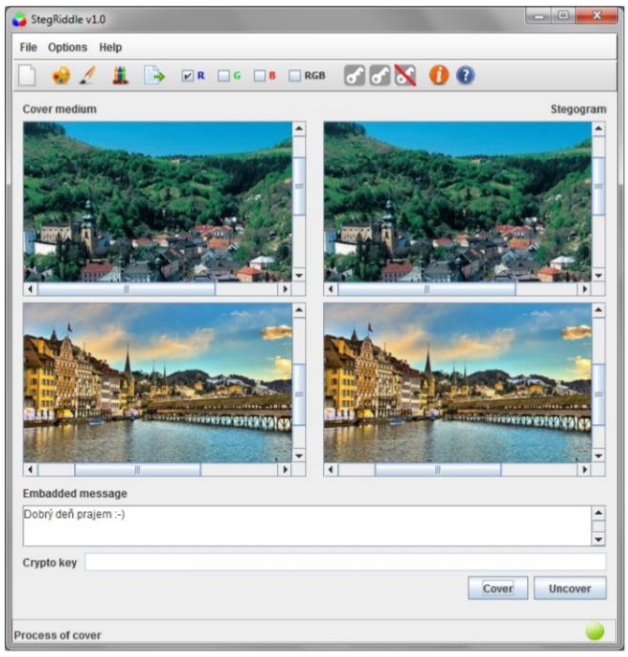

Fig. 5 Applications user interface

After processing the input message, the function of hiding secret message into two hiding media files can be used. The simplest distribution functions are used to do that:

1. the first distribution function uses even division between images and selected RGB model colour components,
2. the second distribution function uses order of images loading as a sequence of insertion,
3. the third distribution function uses direct insertion of bits in the same order as it is in source message, without omitting the bits of hiding medium.

Graphical user interface of implemented software application that is using the set of two stegomedia can be seen in the Fig. 5.

4. EXPERIMENTS AND RESULTS

The time-consuming aspect of the program was tested, as well as its functionality.

The test of time demands has shown a dependence on the input file size that is on the size of hiding media, but also on the size of input secret messages.

The time demands of processing and the size of cover media have been observed on the input cover media files of various sizes, into which a message of an invariable size was being inserted. The results of the testing can be seen in the Fig. 6. It can be derived from it that the correlation is rising linearly.

The time dependence of hiding secret messages was also tested. We used cover media of invariable size, into which the secret messages of various sizes were inserted successively. As it can be seen in the Fig. 7, the linearly rising correlation of the time of hiding the message and the size of inserted message was observed again.

5. CONCLUSIONS

The aim of this work was to design an algorithm for hiding the secret messages into the set of covering media (multi-carrier) and to implement this algorithm into the desktop software application StegRiddle, which can be widely used not only by professionals but also by the standard users.

The suggestion of this algorithm on the basis of steganographic method of the least significant bit (LSB) has brought advantages, as well as certain disadvantages.

The significant advantage is the fact that the average user is provided with an easy way to insert personal information into the set of common non-suspicious multimedia files.

The disadvantage, however, is that the end user who would like to read such a message has to know the exact settings of hiding for the message extraction.

The implementation of this algorithm shows time dependency on the size of the secret message and the size of hiding media. However, it is not a great time range, as the hiding is only a matter of few seconds and while testing, the time of hiding did not exceed 3.5 seconds in the worst case.

Since the algorithm gives the opportunity to use unlimited number of hiding media, in the future it will be necessary to create the user interface of the application that would make it possible to work with an increased number of the hiding media.

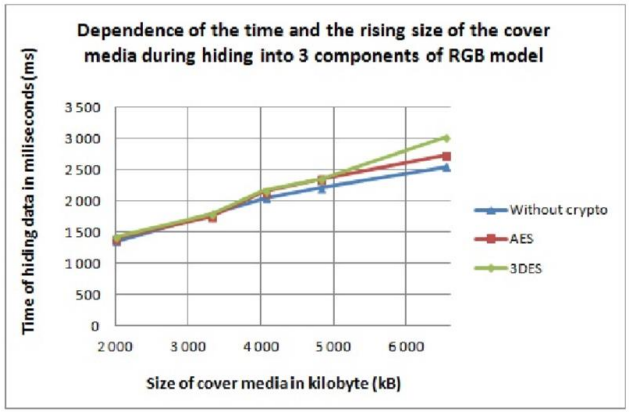

Fig. 6 Dependence of the processing time and rising size of the cover media

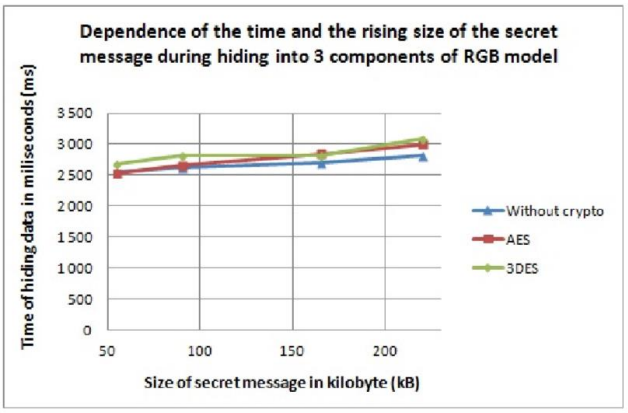

Fig. 7 Dependence of the processing time and rising size of the secret message

ACKNOWLEDGMENTS

This work was supported by the Slovak Research and Development Agency under the contract no. APVV-0008-10 and KEGA 008TUKE-4/2013 Microlearning environment for education of information security specialists. The projects are being solved at the Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice.

REFERENCES

[1] LEVICKÝ, D.: Kryptografia v informačnej bezpečnosti. Elfa Košice, 2005, 260 pp, ISBN: 80-8086-022-X.

[2] PETITCOLAS, F. – ANDERSON, R. – KUHN, M.: 1999. Information hiding a survey. Proceedings of the IEEE Vol. 87, 1062–1078.

[3] STALLINGS, W.: Cryptography and Network Security. 4th edition. Prentice Hall International, Inc., 2006, 592s, ISBN: 978-0-13-187316-2.

[4] CVEJIC, N. – SEPPANEN, T.: Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method. ITCC, Vol. 2, pp. 533-537, 2004.

[5] GOLLMANN, D.: Computer Security, 3rd edition. John Wiley Sons, 2011, 456 pp, ISBN: 978-0-470-74115-3.

[6] KATZENBEISSER, S. – PETITCOLAS, F. A. P.: Information Hiding Techniques for Steganography and Digital Watermarking. ARTECH HOUSE, Inc., Norwood, 2000, 208 pp, ISBN: 1-58053-035-4.

Received July 27, 2015 , accepted August 27, 2015

BIOGRAPHIES

Liberios Vokorokos (prof., Ing., PhD.) was born on 17. November 1966 in Greece. In 1991 he graduated (MSc.) with honours at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at Technical University in Košice. He defended his PhD. in the field of programming device and systems in 2000; his thesis title was "Diagnosis of compound systems using the Data Flow applications". He was appointed professor for Computers Science and Informatics in 2005. Since 1995 he is working as an educationist at the Department of Computers and Informatics. His scientific research focuses on parallel computers of the Data Flow type. He also investigates the questions related to the diagnostics of complex systems. He is a dean of the Faculty of Electrical Engineering and Informatics at the Technical University of Košice. His other professional interests include the membership on the Advisory Committee for Informatization at the faculty and Advisory Board for the Development and Informatization at Technical University of Košice.

Branislav Madoš (Ing., PhD.) was born on 20th May 1976 in Trebišov, Slovakia. In 2006 he graduated (Ing.) at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice. He defended his PhD. in the field of Computers and computer systems in 2009; his thesis title was "Specialized architecture of data flow computer". Since 2010 he is working as an Assistant Professor at the Department of Computers and Informatics. His scientific research is focused on the parallel computer architectures and architectures of computers with data driven computational model.

Ján Hurtuk (Ing.) was born on 4th October 1988 in Kežmarok, Slovakia. In 2013 he graduated (MSc.) at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice. Since 2014 he is studying as a PhD. student at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice. His scientific research interest is mainly focused on the computer security.

Mária Feková (Ing.) was born on 27th September 1990 in Prešov, Slovakia. In 2015 she graduated (Ing.) at the Department of Computers and Informatics at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice; her thesis title was "Design and implementation of algorithm for data hiding using steganography". Her scientific research interest is in computer security, cryptography and steganography.