An Examination on Information Hiding Tools for Steganography

Ismail Karadogan*, Resul Das**

*Kahramanmaras Sutcu Imam Univ., Elbistan Vocational School, Department of Computer Technologies, Kahramanmaras, Turkey. e-mail: ikaradogan@gmail.com
**Firat University, Technology Faculty, Department of Software Engineering, Elazig, Turkey. e-mail: resuldas@gmail.com

Abstract— In this paper, information about the steganographic methods and tools that are used to hide important data in digital media are presented. At the same time, different aspects of these tools such as used methods, types of hidden data and cover media are examined.

Keywords- Information security; information hiding; steganography; steganography tools.

1. Introduction

Since the dawn of written communication people have been concerned with both obscuring the contents of communication (Cryptography) and obscuring the fact that communication is taking place (Steganography). As a result of the digitization of communication, new stegonagraphic approaches, protocols and applications have been developed.

Steganography is the art and science of hiding secret messages or information within innocent looking media. Because the sender and intended recipient want to communicate securely, the carrier medium in which the hidden message is embedded should not arouse the suspicion of third parties' concerning the existence of the hidden message. While cryptography encodes the message and makes it computationally impractical to decrypt, steganography hides the existence of sensitive communication. Fig. 1 shows a diagram of the simplest form of data hiding. Revealing of the hidden data is the reversal of this process.

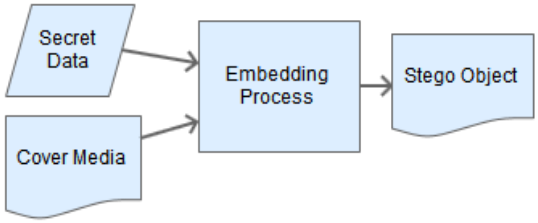

Figure 1. The data hiding diagram as a simple form

Conforming to the principle of 'Defense in Depth' it is standard practice to employ cryptography, compression, and steganography when hiding data. Even if the existence of covert communication can be determined by unwanted third parties, the encoding or the obfuscation of data complicates the retrieval of data, typically requiring access to keys. Fig. 2 shows a data hiding diagram with encryption generally.

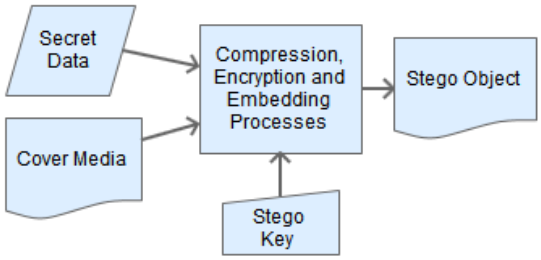

Figure 2. The data hiding diagram with encryption

The recipient party does the inverse of the process of hiding data using the stego key, thus reveals the hidden data from the stego object.

In the digital world, hiding the secret information is possible via various methods. Image-video based, audio based, text based, network based, file structure based, and document based methods are the most well known methods. The most widely used media types are image and audio file types because of their large size and frequency of use.

Steganalysis is the science (and art) of detecting whether a media file contains a covert message, extracting that covert message, and determining its content.

Many tools, applications, and techniques have been developed for steganography and steganalysis. In this paper, we will introduce and discuss some of data hiding tools that are developed and used in steganography, in particular, open source projects.

In the second section of this paper, some of the related works about steganographic tools and methods are identified. In the third section we examine well-known steganographic methods. In the fourth section some of the obtainable current tools used for steganography are investigated. Finally we offer conclusions and suggestions for further work.

2. Related Works

There is a significant body of work related to the conceptual, mathematical and procedural development of stegonagraphic techniques. Less attention has been paid to the analysis of steganographic implementations and much of the work related to such analysis is dated.

Ming et al., focused on the methods of the steganography, and partitioned its into five categories [1]. These categories are spatial domain based, transform domain based, document based, file structured based and other categories such as video compression, encoding, and spread spectrum techniques.

In [2], a number of steganographic tools were examined with respect to pricing, methodology, etc. While perhaps transiently useful this information is now 10 years old rendering its value limited except as a baseline for more up-to-date analysis.

In Johnson and Katzenbeisser [3] a classification of steganographic methods was proposed including aspects of the embedding processes as substitution systems, transform domain techniques, spread spectrum techniques, statistical methods, distortion techniques and cover generation methods.

Michaud provided a review and an analysis of several freeware steganographic tools [4]. Michaud gave information on data hiding in text, image, and audio files and examined SNOW and Steghide applications and documented how these applications are used.

Cheddad et al., provided a state-of-the-art and comprehensive review and analysis of the different methods of steganography [5]. They focused on image steganography techniques such as image spatial domain, image frequency domain, and masking.

Zax and Adelstein presented valuable results in a study of trace detection artifacts (such as files, directories, registry keys) left behind after using several freeware steganographic tools [6].

Dunbar focused on the steganographic techniques in terms of the cover media [7]. He provided a detailed look about these techniques, the secret message encoding into text, image and audio formats.

Hayati et al., surveyed and examined different steganographic and steganalytic tools including freeware, shareware, and commercial applications [8]. They provided technical specifications of typical cover media including image steganography, text, audio, video, and file system steganography etc. In each of these sections, the provided tools were compared. In the last section of that study, a number of steganalytic tools were compared.

Mathkour et al., provided a detailed investigation and comparison of a variety of image steganography techniques and tools[9]. They proposed evaluation criteria of the techniques and tools. In addition they proposed more robust steganographic techniques that takes advantage of the strengths and avoids the limitations of current systems.

In [10], more than a hundred steganographic tools were listed and introduced briefly. Also, there are links to the websites of many provided tools.

3. Steganographic Techniques

Hostiorically, steganography focused on manipulating the physical environment. With the development of technology, steganographic methods have changed depending on type of covert message and type of the utilizable digital media.

In this section, we discuss and group the steganographic methods in terms of the carrier media and the user's perspective rather than the used techniques, algorithms and the embedding process.

A. Ancient and Physical Steganography

Steganography has been widely used in historical times. In ancient Greece, people wrote messages on the wood or slate, then covered it with wax upon which an innocent covering message was written. Also in ancient Greece, an another method, a message that tattooed on the shaved head of a slave, hidden by the hair that afterwards grew over it, and exposed by shaving the slave's head again. In the years following the invention of the printing press, different typefaces on the printed page commonly were mixed due to a lack of sufficient copies of some letters enabling message embedding through the judicious use two different typefaces. Other tecniques include messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier. During captivity by the North Vitenamese Jeremiah Denton repeatedly blinked his eyes in Morse Code during a 1966 televised press conference that he was forced to participate in, spelling out the word, "t-o-r-t-u-r-e". [11]

Invisible ink and micodots were used as common steganographic forms allowing secret messages to be written in the lines of an innocent-seeming letter.

Fig. 3 shows the message that was sent by Germans during World War I as a simple approach to text steganography [12].

> President's Embargo Ruling Should Have Immediate Notice. Grave Situation Affecting International Law. Statement Foreshadows Ruin Of Many Neutrals. Yellow Journals Unifying National Excitement Immensely.
>
> The initial letters give the secret message:
> *Pershing sails from N.Y. June 1.*

Figure 3. The simplest approach to text steganography

B. Image, Audio and Video Steganography

With the advent of electronic communication modern approaches to stegonagraphy focus on embedding covert information within relatively large cover media such as images, audio and video files. The covert information embedded in the cover medium can be text, image or another file or data type. The primary restriction involved in the selection of an appropriate medium is the relative size of the cover medium and the covert message.

In image and audio steganography, the simplest and most widely used techniques are variants on spatial domain techniques such as Least Significant Bit (LSB) Replacement and LSB Matching.

LSB Replacement is a process in which the least significant bit of each pixel or byte of the cover medium is replaced by the bits of the covert message. LSB Replacement is relatively easy to implement but can be easily detected through analysis of pixel or byte asymmetry. LSB Matching differs from LSB Replacement by a small change. LSB Matching avoids the assymmetry in LSB Replacement by compensating for pixel asymmetry utilizing paired pixels, one of which carries the covert message, the other providing a negative adjustment. As a result LSB Matching is much harder to detect. [13]

Fig. 4 shows two Bitmap images of a landscape photo. The first image is original and the second one contains hidden data that consists of about 4 KB text. The sizes of both are same, 228KB. It can not be seen a noticeable difference to the human eye among these images.

Figure 4. (a) The original image of a landscape (b) The same landscape image with hidden text data.

There are a number of other approaches such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) [5] and Fast Fourier Transform (FFT) which are frequency domain techniques.

A video file consists of a sequence of images. Therefore, many of above-mentioned methods of image steganography can be applied to video steganography.

C. Text Steganography

Text steganography is less frequently used than image and video steganography due to the relatively difficulty of implementation and constraints on the volume of data that can be stored.

The use of image files has both advantages and disadvantages. The advantages include; local changes can maintain global properties of the image and it easy to make changes which are imperceptible to the human eye. Disadvantages include; the sender needs an image and needs to transmit this image completely, and without error to the receiver. In contrast text is ubiquitous. The sheer volume of text communication makes the identification of steganographed text problematic. [14].

There are a variety of approaches to text steganography. for the most part these approaches can be categorized into two groups; modifying text format, and changing the meaning of the text. Specific approaches include syntactic modifications, semantic modifications, text abbreviation and acronyms, change of spelling, line shifting, word shifting, feature coding. [15] In addition work has been done on compression-based [16] and linguistically-driven generation [17] methods.

In Arabic text, some of the steganographic methods include dots methods, pointed letters and extensions methods, Arabic diacritic methods, and Arabic Unicode texts using pseudo-space and pseudo connections. As an example, information hiding is possible using extension characters (Kashida) at suitable word positions, before or after letters. Fig. 5 shows an example of adding extensions after letters. [18-19]

Secret bits	110010
Cover-text	من حسن اسلام المرء تركه مالا يعنيه
Steganographic text	من حسن اسلام المرء تـركـه مـالا يـعنيه 1 1 0 0 1 0

Figure 5. In Arabic text, adding extensions after letters [19]

D. File Structure and Document Based Steganography

File systems can be used as a cover medium for covert messages. One of the primary methods is to utilize NTFS's Alternate Data Streams (ADS). ADS provides an opportunity for hackers to hide root kits or hacker tools on a breached system and allows them to be executed as system utilities rather than user applications and so avoid attracting attention of system administrators [20].

Covert messages can be encoded as a modified order of the attributes of HTML tags. In [21], Garg proposed a novel method for hiding data in HTML document. In this approach, predefined couples of attributes are changed mutually.

In document steganography, Microsoft Office documents and Adobe PDF files are commonly used.

E. Network Steganography

Network steganography is a process that involves the transmission of covert communication over computer networks without disturbing the flow of authorized communication.

Currently, this approach commonly involves embedding data within Transmission Control Protocol (TCP) and Internet Protocol (IP) headers. The Internet provides packet-based communication, and contains hundreds of protocols of communication, mainly IP and TCP. The described protocols specify data fields in the

packet header in order to implement communication and transmitting data aright. For example, in an IP version 4 packet, there are version, header length, type of service, total length, identification, flags, fragmentation offset, time to live, protocol, header checksum, source IP address, destination IP address, options fields. Not every field within the TCP header is used in all packets. For example the ACK sequence number and the Urgent field are only utilized if the appropriate flags are set. Unused field(s) can be manipulated and used by the sender, manually [22]. Again, if the total length of an IP packet less than the Maximum Transfer Unit (MTU) of the network, the fragmentation offset and related flags can be used as the cover of the secret data bits [23].

4. Current Tools Used For Steganography

There are a number of tools available that automate the embedding of covert data within a cover medium. These tools range from open source, freeware and commercial tools. In this section we identify, discuss and compare open source or freeware tools especially. Some of the tools which we investigated have also steganalytic properties and functions, however, we discuss them aspects of data hiding only.

A. OpenPuff

OpenPuff is an open source professional steganographic tool [24]. It is portable so doesn't require installation. As a result it does not leave artifacts such as ini files or registry keys which otherwise could provide trace information in the storage environment and evidence that could be used in stganalysis. OpenPuff supports many file types; images, audio, video, flash and Adobe. Image formats include BMP, JPG, PCX, PNG, TGA. Supported audio formats include AIFF, MP3, NEXT/SUN, WAV. Video formats include 3GP, MP4, MPG, VOB. Other formats such as FLV, SWF, PDF are also supported.

OpenPuff not only supports various encryption algorithms for security but also uses layers of security and obfuscation. These layers consist of cryptography, scrambling, whitening and encoding respectively.

B. OpenStego

OpenStego is an open source tool [25]. It supports only image files as cover media. It can encrypt and compress data, and uses a plugin based architecture. Currently, it contains two plugins, LSB and Random LSB. With plugins, it is easy to support different algorithms and different cover file types such as audio files.

C. Steganography Studio

Steganography Studio is open source project that is developed in order to aid steganographic education and the analysis of steganographic algorithms [26]. It supports BMP and PNG file formats. It is developed in Java providing cross-platform application. It also implements image analysis algorithms for detection of covert information.

D. Virtual Steganographic Laboratory

Virtual Steganographic Laboratory (VSL) is a steganographic and a steganalytic software and a block diagramming tool that aims to hide data inside digital images, and to detect its presence and testing its robustness using a variety of different techniques [27]. It is Java-based open source and cross platform software. It supports plugins. Its outputs can be JPEG, BMP, PNG and GIF formats.

E. SteganPEG

SteganPEG is an open source tool targeted specifically to the JPEG format and allows the embedding of covert data or files without changing its size and quality [28]. It can hide multiple files in a JPEG file. It supports data compression and and password protection. Covert files can be extracted separately.

F. SilentEye

SilentEye is an open source, cross-platform and easy to use application [29]. It can embed covert data in images (bmp, jpeg) and audio files (wav). With this tool, different steganographic and cryptographic algorithms can be used owing to its plug-in support.

G. F5 Steganography

F5 Steganography is a Java-based open source tool and it only deals with JPEG images as cover.

It doesn't use the metadata or the comment fields of the image file [30]. It provides password protection and the adjustment of JPEG quality. F5 is also a newly developed algorithm and unlike most other tools, it is robust against visual and statistical attacks.

H. OutGuess

OutGuess is an open source project that is developed under a BSD software license [31]. It only deals with PNM and JPEG images. It preserves statistics based on frequency counts for JPEG images rendering statistical steganalysis ineffective.

İ. Steghide

Steghide is an open source tool that hides data in a variety of image and audio files [32]. Steghide can embed covert information into JPEG, BMP, WAV and AU files. It supports compression, encryption, and embedding checksum of secret data to verify the extracted data.

Steghide is a console application, but several GUI applications were developed to improve ease of use.

J. JSteg

JSteg [33] is an obsolete steganographic tool that only uses JPEG images as carrier. It does not provide encryption or compression options.

K. Steg

Steg is a portable and cross-platform application that uses steganography and cryptography techniques [34]. It supports JPEG (JPG), TIFF, PNG and BMP image formats.

L. StegoMagic

StegoMatic [35] is a freeware program that hides a text message or any file inside many formats such as text, music (WAV) or image (BMP) files. It supports password protection and encryption.

M. wbStego

wbStego is open source project dealing with Bitmap files, text files, HTML files and PDF files [36]. It is available for Windows and Linux platforms.

N. DeepSound

DeepSound is a freeware tool that hides data into wave and flac audio file formats [37]. It might be used as a copyright marking software for wave, flac and audio CD. It also supports AES encryption.

O. MP3stego

MP3Stego hides information in MP3 audio files during the compression process [38]. The data is compressed, encrypted with password protection and hidden in MP3 bit streams respectively. It can be used as a copyright marking system for MP3 files.

P. SNOW

SNOW is an open source project that is used to hide messages in ASCII text by appending whitespace to the end of the lines [39]. Spaces and tabs are generally not visible in text viewers. Because of encryption supports of SNOW, the secret message can not be read even if it is detected.

Q. Hide In Picture

Hide In Picture uses BMP and GIF as cover and supports password protection [40]. It supports Blowfish and Rijndael encryption algorithms.

R. Hide4PGP

Hide4PGP is a freeware and open source program [41]. It supports BMP as image files but must not compressed, all formats of WAV and only 8 bit VOC as audio file formats. It is somewhat obsolete, developed for Windows 9x/NT and DOS.

S. Digital Invisible Ink Toolkit

Digital Invisible Ink Toolkit is an open source project developed with Java so it is platform independent application [42]. It can embed any file type inside 24 bit color image. Supported image file types are BMP and PNG. It can implement different algorithms and filters to conceal the data depend on the user's preference. Additionally, it gives the ability to password protect.

T. CipherTune

CipherTune is different from other tools, it creates midi files from image and text files [43]. It

encrypts a picture or a text then converts it to twelve tone midi file. In this regard, this tool can be classified in cryptography.

U. Cipher Image Free

Cipher Image is a freeware tool that hides textual information into 7 (seven) formats of image files [44]. These formats are JPEG, GIF, TIF, PCX, PNG, Windows BMP and OS/2 BMP. It can open 21 different image formats. By using it, several encrypted image files with hidden text could be saved together into one carrier file.

V. The Comparison of Steganography Tools

In Table 1, the above-mentioned tools are comparised. The information given in this table was taken from the cited works and from supporting websites. The table has been listed alphabetically by tool names.

Figure 6. The comparison of tools presented

Tool Name	Concealed Data Type	Stego Object Type				Algorithm or Approach for Data Hiding	Additional Information
		Image Files	Audio Files	Video Files	Other Files		
Cipher Image Free	Plain text	BMP, JPEG, GIF, TIF, PCX, PNG	-	-	-	-	Hiding multi-file into one, password protection, encryption
CipherTune	Text files, Image files	-	MIDI	-	-	-	Picture or text to MIDI
DeepSound	Any file type	-	WAVE, FLAC	-	-	-	Encryption, password protection, audio cd support
Digital Invisible Ink Toolkit	Any file type	BMP, PNG	-	-	-	LSB (BlindHide, HideSeek, FilterFirst, BattleSteg)	Password protection, Image Filters
F5 Steganography	Plain text	JPEG	-	-	-	DCT (F5 algorithm)	Password protection, adjusting quality
Hide In Picture	Any file type	BMP, GIF	-	-	-	-	Encryption, password protection
Hide4PGP	Plain text	BMP	WAV, VOC	-	-	LSB	PGP Encryption
Jsteg	Plain text	JPEG	-	-	-	DCT (Jsteg algorithm)	-
MP3Stego	Text files	-	MP3	-	-	-	Compression, encryption, password protection
OpenPuff	Any file type	BMP, JPG, PNG, PCX, PNG, TGA,	AIFF, MP3, Next/Sun, WAV	3GP, MP4, MPG, VOB, FLV	PDF, SWF	-	Encryption (16 algorithm), obfuscation
OpenStego	Any file type	BMP, PNG, JPEG, GIF	-	-	-	LSB, Random LSB	Compression, encryption, password protection
OutGuess	Any file type	JPEG, PNM	-	-	-	DCT (Outguess algorithm)	Encryption, password protection
SilentEye	Any file type	BMP, JPEG	WAV	-	-	LSB	Encryption, password protection, compression, plugin support, adjusting quality
Snow	Plain text	-	-	-	ASCII Text	Using whitespaces	Encryption (ICE), compression, password protection
Steg	Any file type	BMP, JPG, TIFF, PNG	-	-	-	-	Encryption, password protection,
Steganography Studio	Any file type	BMP, PNG	-	-	-	LSB (BlindHide, HideSeek, FilterFirst, BattleSteg, SLSB)	Password protection, Filters, Analysis
SteganPEG	Any file type	JPEG	-	-	-	Partial Decoding Technique	Password protection, encryption, compression, hiding multi-file into one
StegHide	Any file type	BMP, JPG	WAV, AU	-	-	Graph-theoretic approach	Password protection, compression, encryption, embedding checksum
StegoMagic	Any file type	BMP	WAV	-	Text	Whitespaces, LSB	Password protection, Encryption
VSL (Virtual Steganographic Laboratory)	Any file type	JPEG, BMP, PNG, GIF	-	-	-	Karhunen-Loeve Transform, LSB, F5 algorithm (DCT)	A block diagramming tool, compression, distortion,supports plugins
wbStego	Any file type	BMP	-	-	PDF, HTML, Text	-	Encryption

5. Conclusions and Suggestions

In this paper, we gave an overview of some of the most widely used, current, open source, freeware and commercial steganographic tools . We included information about the types of covert data, algorithms, cover media and additional capabilities such as encryption support, data compression etc.

Many of the tools mentioned embed covert messages in a variety of image formats, perhaps because of the ubiquity of images in modern electronic communication. Most steganographic tools employ compression and encryption so that even when detected, interpretation of the covert message content is problematic.

Document and text steganographic techniques allow for changes in document structure and font layout to embed covert data. For example, for HTML files, in terms of textual structure, modifying the source HTML is a form of text steganography. Additionally the use of both structural and semantic modifiers provide creative scope.

Although there have been significant advances in both steganographic and steganalysis techniques in

relation to the most common forms of electronic communication literature pertaining to the identification, classification and evaluation of steganographic tools is relatively sparse. As stegonagraphic techniques advance there is need for constantly review and revision of extant tools.

6. Future Works

The history of communication is littered with examples of the use of steganography. As the style, format, and communication media change, the potential for novel steganographic approaches will continue for legitimate purposes or otherwise.

Encrypted communication, by it's nature, represents a potential target. The combination of both encryption and steganography offers a measure of security that encryption alone cannot offer.

Steganographic techniques are a function of the technologic environment in which they reside. Current environments such as image, audio and video are very popular. However, with the advent of novel media such as 3-D and holographic transmission, advanced network protocols and peer-to-peer (mesh) communication systems, novel steganographic techniques will be in demand in the future [45].

Given the ubiquity of mobile devices, the meteoric rise of social media, and the emphasis by developers on the application rather than communication layers, it would not be surprising to see attention focused on the development of steganographic application in these areas.

There sheer volume of content generated by social networking and blogging/microblogging sites such as Facebook, Google+, Twitter, etc. provides a rich and safe environment for the communication of covert messages. Given that social media systems employ most of the cover media identified earlier it would be unsurprising for both new techniques and tools to be developed that leverage the unique opportunities that social media provides.

Most, if not all, steganography tools are traditional, desktop OS-based tools. The development of both steganographic tools for mobile devices, or potentially the development of steganographic API's for open source mobile platforms are a rich area of potential study.

References

[1] C. Ming, Z. Ru, N. Xinxin and Y. Yixian, "Analysis of current steganography tools: classifications & features", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006.

[2] Analyzing steganography softwares, URL: http://www.guillermito2.net/stegano/, Last accessed: July 2013.

[3] N.F. Johnson and S.C. Katzenbeisser, "A survey of steganographic techniques", in: S. Katzenbeisser, F.A.P. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Inc., Norwood, 2000.

[4] E. Michaud, "Current steganography tools and methods", SANS Penetration Testing, April 2003.

[5] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods", Signal Processing, 2010, pp. 727-752, doi:10.1016/j.sigpro.2009.08.010.

[6] R. Zax and F. Adelstein, "FAUST: Forensic artifacts of uninstalled steganography tools", Digital Investigation, 2009, pp. 25-38, doi:10.1016/j.diin.2009.02.002.

[7] B. Dunbar, "A detailed look at steganographic techniques and their use in an open-systems environment", SANS Institute Reading Room, 2002.

[8] P. Hayati, V. Potdar and E. Chang, "A survey of steganographic and steganalytic tools for the digital forensic investigator", In Workshop of Information Hiding and Digital Watermarking, 2007.

[9] H. Mathkour, B. Al-Sadoon and A. Touir, "A new image steganography technique", Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference, pp.I-4, 12-14 Oct. 2008.

[10] Steganography software, URL: http://www.jjtc.com/Steganography/tools.html, Last accessed: May 2013.

[11] Steganography, Wikipedia, URL: http://en.wikipedia.org/wiki/Steganography, Last accessed: June 2013

[12] D. Kahn, The Codebreakers, New York, NY: The Macmillan Company, 1967. p. 67.

[13] X. Li, B. Yang, D. Cheng and T. Zeng, "A generalization of LSB matching", IEEE Signal Processing Letters, Vol. 16, No. 2, pp. 69-72, February 2009.

[14] S. Clark and C. Chang , "Linguistic steganography: information hiding in text", URL: http://www.cl.cam.ac.uk/~sc609/talks/ed12stego.pdf, Last accessed: June 2013.

[15] P. Singh, R. Chaudhary and A. Agarwal, "A novel approach of text steganography based on null spaces", IOSR Journal of Computer Engineering, Vol. 3, Issue 4, pp. 11-17, July-Aug. 2012.

[16] E. Satir and H. Isik, "A compression-based text steganography method", The Journal of Systems and Software, 2012, pp. 2385-2394, doi: 10.1016/j.jss.2012.05.027.

[17] I. Nechta and A. Fionov, "Applying statistical methods to text steganography", arXiv:1110.2654v1 [cs.CR] 12 Oct 2011.

[18] A.F. Al-Azawi and M. A. Fadhil, "Arabic text steganography using Kashida extensions with Huffman code", Journal of Applied Sciences 10(5), pp. 436-439, 2010.

[19] A.A. Gutub, L.M. Ghouti, Y.S. Elarian, S.M. Awaideh and A.K. Alvi, "Utilizing diacritic marks for Arabic text

steganography", Kuwait Journal of Science & Engineering (KJSE), Vol. 37, No. 1, June 2010.

[20] R. Zadjmool, "Hidden threat: Alternate Data Streams", 2004, URL: http://www.windowsecurity.com/articles-tutorials/windows_os_security/Alternate_Data_Streams.html, Last accessed: June 2013.

[21] M. Garg, "A novel text steganography technique based on HTML documents", International Journal of Advanced Science and Technology, Vol. 35, Oct. 2011, pp. 129-138.

[22] I. Karadogan, R. Das, M. Baykara, "Scapy ile ağ paket manipülasyonu" (in Turkish), 1st International Symposium on Digital Forensics and Security, pp. 196-201, 20-21 May 2013.

[23] K. Ahsan, "Covert channel analysis and data hiding in TCP/IP", M.A.Sc. thesis, Dept. of Electrical and Computer Engineering, University of Toronto, 2002.

[24] OpenPuff Website, URL: http://embeddedsw.net/OpenPuff_Steganography_Home.html, Last accessed: June 2013.

[25] OpenStego Website, URL: http://www.openstego.info/, Last accessed: June 2013.

[26] Steganography Studio Website, URL: http://stegstudio.sourceforge.net/, Last accessed: June 2013.

[27] Virtual Steganographic Laboratory Website, URL: http://vsl.sourceforge.net/, Last accessed: May 2013.

[28] SteganPEG Website, URL: http://www.abhiram.tk/home/steganojpeg, Last accessed: June 2013.

[29] SilentEye Website, URL: http://www.silenteye.org/, Last accessed: June 2013.

[30] F5-Steganography Website, URL: http://code.google.com/p/f5-steganography/, Last accessed: June 2013.

[31] OutGuess Website, URL: http://www.outguess.org/, Last accessed: May 2013.

[32] Steghide Website, URL: http://steghide.sourceforge.net/, Last accessed: June 2013.

[33] D. Upham, "JSteg Steganographic Algorithm", URL: http://zooid.org/~paul/crypto/jsteg/, Last accessed: July 2013.

[34] Steg Website, URL: https://steg.drupalgardens.com/, Last accessed: June 2013.

[35] Stegomagic, URL: http://www.oocities.org/tmx575/, Last accessed: July 2013.

[36] wbStego Website, URL: http://wbstego.wbailer.com/, Last accessed: June 2013.

[37] DeepSound Website, URL: http://www.jpinsoft.net/DeepSound/, Last accessed: June 2013.

[38] MP3Stego Website, URL: http://www.petitcolas.net/fabien/steganography/mp3stego/, Last accessed: June 2013.

[39] SNOW Website, URL: http://www.darkside.com.au/snow/, Last accessed: June 2013.

[40] Hide In Picture Website, URL: http://sourceforge.net/projects/hide-in-picture/, Last accessed: June 2013.

[41] Hide4PGP Website, URL: http://www.heinz-repp.onlinehome.de/Hide4PGP.htm, Last accessed: July 2013.

[42] Digital Invisible Ink Toolkit Website, URL: http://diit.sourceforge.net/, Last accessed: July 2013.

[43] CipherTune Website, URL: http://kenjikojima.com/cipherTune/, Last accessed: June 2013.

[44] Cipher Image Website, "Software for Photographers", URL: http://www.realityinreflections.com/cipherimage.htm, Last accessed: June 2013.

[45] Baykara, M., Daş, R., "A Steganography Application for Secure Data Communication", 10th International Conference on Electronics, Computer and Computation (ICECCO 2013), Turgut Özal University, pp.309-313, 7-9 November 2013, Ankara.

Ismail Karadogan received his BS degree in Computer Engineering from Firat University, Elazig / Turkey, in 2005. He has been executing his MSc in Firat University, Department of Software Engineering since 2012. Currently, he is working as a lecturer in Kahramanmaras Sutcu Imam University, Elbistan Vocational School, Department of Computer Technologies. He is interested in Information Security, Computer Networks, Network Security.

Resul Das was born in Elazig, Turkey, 1975. He received his BS and MSc. in Computer Science from Firat University in 1999, 2002 respectively. He received PhD degree from Electrical and Electronics Engineering Department in same university in 2008. His research interests are Knowledge Discovery, Web Mining, Complex Networks, Computer Networks, Information and Network Security. Now, he is working as an assistant professor in Department of Software Engineering at Firat University.