Digital steganography in terrorist networks

Darko Trifunović
Faculty of Security Studies, University of Belgrade, Gospodara Vučića 50, Belgrade, Serbia
galileja@yahoo.com

Abstract. As most of today's communication occurs electronically, there has been an expansion of using steganographic methods in digital multimedia contents. The main goal of using steganography is to avoid drawing attention to the transmission of hidden information. Steganography is widely used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages. The goal of the paper is to point out on the usage of digital steganography methods as a way of communication in terrorist network. Terrorists commonly scramble their messages by applying open source encryption programs that involve steganography techniques, and post hidden messages on existing photographs, text or videos on almost any website or to directly send via e-mail. This paper provides an overview of examples of using steganography methods in planning terrorist attacks. This kind of hidden communication is very easy but unfortunately very effective, and almost undetectable. This paper provides some directions in which counter-terrorism IT experts could work in preventing this kind of communication.

Keywords: Steganography, Hidden communication, Terrorist network, Counter-terrorism.

1. Introduction

Term "Steganography" comes from Greek word "steganos" which means "covered" and "graphie" or "writing". It is a secret communication hidden in non-hidden communication. The main goal is to hide secret data in an innocently looking cover, so called "carrier", and passed to receiver who is aware of its hidden content and knows how to extract that data. Steganography differs from cryptography, since a communication using cryptographic methods is evident, but the content of this communication is camouflaged. To be useful, a steganographic method needs to embed data to be transmitted imperceptibly, to allow the extraction of data, to promote a high information rate or payload, and to incorporate a certain amount of resistance to removal [2].

Various forms of steganography have been used for last 2500 years. There are numerous examples and methods used through history. First document describing steganography is written by Herodotus in ancient Greece. He explained how Demeratus wanted to notify Sparta that Xerxes intended to occupy Sparta. So he wrote a message on waxed table, covered table with a new layer of wax and message became invisible. Another example of "secret writings" is writing on already written letter with invisible ink, such as a lemon juice, milk, vinegar and urine. Later on, person who receive that letter put it above candle flame or another source of heat and hidden message becomes darken and readable. Very popular ancient way of passing secret messages was tattooing message on a human carrier's shaved head. When it's hear grown enough, carrier was sent to final destination and message was revealed after new shaving of his head. Null ciphers may be considered as form of steganography. It provides a way of concealing a message within a larger body of plain text without the need for a complicated cryptosystem. The real message is hidden in innocent looking message. Null cipher method was also commonly used by Germans during World War II. Popular example of this technique is following message.

Example 1. *“Fi**s**hing fr**e**shwater be**n**ds an**d** sa**l**twater co**a**sts re**w**ards an**y**one fe**e**ling st**r**essed. Re**s**ourceful an**g**lers us**u**ally fi**n**d ma**s**terful le**a**pers fu**n** an**d** ad**m**it sw**o**rdfish ra**n**k ov**e**rwhelming an**y**day.”*
Reading every third (bolded) letter in each word, hidden message becomes understandable: *“Send Lawyers, Guns, and Money.”*

In modern days, steganography is widely used as a very sophisticated way of secret communication, almost impossible to detect but easy to learn technique. Every person can use some of many open source software from internet and learn how to use it in within several minutes only [1]. Some of these software are: QuickStego[1], Xiao-steganography[2], Camouflage[3], SilentEye[4], Steghide[5], etc.

2. Digital steganography – the most effective technique of terrorists secret communication

Beside strong encryption, steganography is a way of secret communication that is common to Islamic terrorists. Steganography is more subtle and more effective compared to encryption and could be combined with encryption as well. For these reasons, it is widely used technique by Islamic terrorists [3], [5].

With the help of open source software, based on steganography technique, anyone can easily hide secret messages or malicious scripts into any digital format, such as: BMP, JPG, TXT, HTML/XML, PDF, PNG, GIF, AU, WAV, MP3, AVI, TIF, TGA, DLL and EXE. This technique manipulates the least significant bit of the pixels making up digital images to store hidden information. The least significant bits are those that are at the far right of a binary number. For instance, the decimal number 255 is represented in binary code as 11111111. The least significant bit is the last "1" at the far right of the number. If we change the "1" to a "0" we would get 11111110, which represents 254. The hidden file can be stored using these bits throughout the file. These minor changes cannot be perceived by viewing the image file and changes to the picture are so subtle they are impossible to detect visually [4].

There are examples of steganography usage by Islamic terrorists so far but no one really knows how many media with different formats with hidden messages are on internet

American journalist, Jack Kelley made an interview with US officials and experts and wrote an article - “Terrorist instructions hidden online”[6]on 5 February 2001 for USA Today. According to Jack's article based on relevant sources, terrorists hide maps and photographs of terrorist targets - and post instructions for terrorist activities - on sports chat rooms, pornographic bulletin boards and other popular Web sites using steganography technique. Officials and experts say the messages are scrambled using free encryption programs. Using those programs, they are able to post hidden messages on existing photographs on almost any website they choose. Ben Venzke, special projects director for iDEFENSE, a cyber-intelligence company says, "It's something the intelligence, law-enforcement and military communities are really struggling to deal with. The operational details and future targets, in many cases, are hidden in plain view on the Internet," He added, that "only the members of the terrorist organizations, knowing the hidden signals, are able to extract the information."

CIA Director George Tenet provides us an evidence for this. He said, “To a greater and greater degree, terrorist groups, including Hezbollah, Hamas, and bin Laden’s Al-Qaida group, are using computerised files, e-mail, and encryption to support their operations.”[7]

FBI Director, Louis J. Freeh explained that, “uncrackable encryption is allowing terrorists -

[1] http://quickcrypto.com/free-steganography-software.html
[2] http://xiao-steganography.en.softonic.com/
[3] http://camouflage.unfiction.com/
[4] http://www.silenteye.org/
[5] http://steghide.sourceforge.net/

[6]http://usatoday30.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm
[7] From a document Tenet wrote to the US Senate Foreign Relations Committee in March 2001.

Hamas, Hezbollah, al Qaida and others - to communicate about their criminal intentions without fear of outside intrusion…They're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."[8]

2.1 Examples of usage of of steganography in terrorist networks

There are numerous examples of terrorist attacks prepared and successfully accomplished using this method. According to former French defense ministry official, Islamic terrorists used steganography to prepare attack on the United States embassy in Paris. He said that terrorists were instructed to communicate through pictures posted on publicly on internet[9]. Jamal Beghal, leader of that terrorist plot was arrested in late July 2001 for passport fraud at Dubai International Airport in the United Arab Emirates. He was trying to travel back to Europe after receiving training in Afghanistan. Jamal revealed details of the plot after interrogation by French intelligence agents. Plan was to built a bomb out of sulfur and acetone and destroy US embassy in Paris. Former professional football player in Germany, Tunisian Nizar Trabelsi was the designated suicide bomber. He planned to strap this bomb onto himself, cover it up with a business suit and detonate himself in the U.S. embassy. Then, minivan full of explosives would be driven into the U.S. cultural center of Paris and the explosives would be detonated inside.

Next case of using this technique by Islamic terrorists was revealed when a suspected al-Qaeda member, Maqsood Lodin, a 22-year-old Austrian was arrested in Berlin in May of 2011. He was traveling to Berlin from Pakistan via Hungary when Berlin police detained him. They found in his underpants usb memory containing one video with pornographic content and a file with explicit title[10]. Computer forensics experts from German Federal Criminal Police extracted out of videos 141 hidden text files detailing al-Qaeda operations and plans for future operations[11]. Those documents contained plans to attack cruise ships as a distraction while other attacks were initiated in Europe, than PDF terrorist training manuals in German, English and Arabic were found as well. Those files were just hidden inside with digital steganography technique but not encrypted. Anyway, German specialists worked for several weeks to extract all hidden data. If those files were encrypted strong enough as well, it would be much harder or even impossible to get readable content because it would give a second layer of protection. U.S. intelligence sources told CNN that the documents uncovered are "pure gold". Another source said that they are the most important haul of al Qaeda materials in the last year, besides those found when U.S. Navy SEALs raided Osama bin Laden's compound in Abbottabad, Pakistan, a year ago and killed the al Qaeda leader.[12]

Concerning 9/11 terrorist attacks in USA, there are no clear evidences that terrorists used steganography but there are some indications. In Washington Post article (September 19, 2001.) written a week after attacks by journalists Ariana Eunjung Cha and Jonathan Krim, we can read that "Government agencies were contacting computer experts for help in understanding how Osama bin Laden and his associates may have used the Internet to send encrypted electronic messages to one another to coordinate last week's attacks on the World Trade Center and the Pentagon".[13] In the article, same source claim that federal agents had found evidences that al-Qaeda is hiding secret messages in e-mails and different web sites. Several experts of computer science

[8] Freeh's testimony was given during a closed-door hearing on terrorism before a Senate panel in March 2001.

[9] http://www.nytimes.com/2001/10/30/science/physical/30STEG.html

[10] http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future

[11] http://arstechnica.com/business/2012/05/02/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/

[12] http://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/index.html

[13] http://all.net/iwar/archive/2001Q3/0692.html

confirmed that they received calls from government officials asking them for help. One of them was asked to be available for assistance to decrypt any encoded messages if the government finds them.

3. What should counter-terrorists do?

Principe of terrorists' communication using hidden messages publicly posted on e-bay or any other website or directly send via e-mail is very easy but unfortunately very effective, and almost undetectable. Steganographic images are electronic version of Dead Drops. Dead Drops is a term from World War II used for places like common letter box or books in public library where spies left information. In electronic version of this old technique, members of terrorist organization communicate easily with each other leaving hidden messages, maps, softwares, action plans, etc. publicly without need for direct meeting or knowing each other. Perfect anonymity is one more advantage of steganography. Many people can download that picture but just few know its real content. Those who use this kind of secret communication know how to cover their real locations by changing IP address and "spoofing" other "fingerprints". They often change images - carriers of their messages and never use one or just few to develop one action plan. Complete their conversation is spread over internet in many photographs and other formats so it's almost impossible to collect every piece of information and find out what they are planning.

Counter-terrorist IT specialists have a heavy task. First, they need to find a way to scan all internet and detect all photographs and other medias with different formats containing hidden content. There are billions of uploaded content every day. For example, every single minute on the web, 216.000 photographs are shared on Instagram, 72 hours of video material are uploaded to Youtube, 204 million emails sent, 70 new domains are registered and 571 new website are created within a minute online[14]. Secondly, counter-terrorist IT specials need to find adequate working method to extract hidden content protected with passwords out of its carriers (images, music files, movie formats, pdf files, etc). If they extract content successfully, it might be encrypted so decryption is the next task. However, encryption can be 4096-bit strong and even modern super computers are not able yet to decrypt such a strong encryption.

Another way to fight against hidden content in terrorist communication is the possibility of overflowing internet with steganographic media with fake content. For example, a team of counter-terrorist IT specials can post 99.99% of fake content with only 00.01% of those with real message, then put them in at least 100 carriers in various formats. Finally, each of the contents can be encrypted with 4096-bit encryption and with different unbreakable password chosen for each of them. In addition, counter-terrorist IT team should use different fake IP address, different MAC addresses and hostnames for uploading or downloading each of them.

Acknowledgements. *This research was partially supported by Serbian Ministry of Education, Science and Technological Development under the grant no. 47017.*

References

[1] C. Abbas, J. Condell, K. Curran, P.McKevitt. Digital image steganography: Survey and analysis of current methods.*Signal processing,* 2010, 90(3) 2010, 727-752.

[2] E. Cole and R. D. Krutz. Hiding in plain sight: Steganography and the art of covert communication. *John Wiley & Sons, Inc*., 2003.

[3] M. Conway. Code wars: steganography, signals intelligence, and terrorism. *Knowledge, Technology & Policy*, 2003, 16(2), 45-62.

[4] K.Choudhary. "Image steganography and global terrorism." *International Journal of Scientific & Engineering Research* , 2012, 3(4).

[5] J.A. Matusitz. Terrorism & communication: A critical introduction. *Los Angeles: Sage*, 2013.

[14] http://www.forwardedemails.com/20948-what-happens-in-just-one-minute-on-the-internet-fwd-sharon-rajkumar