Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-11, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Steganography and Terrorist Communications

Arwa Abdoun[1] & Jamaluddin Ibrahim[2]
[1](International Islamic University, Kulliyah of Information and Communication Technology)
[2](Senior Academic Fellow, KICT, International Islamic University, Kulliyah of Information and Communication Technology (Malaysia)

Abstract: *Steganography is the art and science of hiding the fact that communication is taking place by hiding information in other information' (Johnson). According to nameless "U.S. officials and experts" and "U.S. and foreign officials," terrorist groups are "hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites". This paper informs the reader how an innocent looking digital image hides a deadly terrorist plan, which can destroy the world just in a click of a mouse. It also describes and discusses the process of secret communication known as steganography. The crucial argument here is that terrorists are most likely to be employing digital steganography to facilitate secret intra-group communication as has been claimed. This is mainly because the use of digital steganography by terrorist is both technically and operationally dubious. The most important part this paper discusses is that terrorist are likely to employ low-tech steganography such as semagrams and null chippers instead. It investigates the strengths of image steganography and the reasons why terrorists are relying on it so much.*

Introduction

Stenography is the way of writing hidden messages in a way that no one will be able to know the existence of the message other than the sender and the receiver. It is based on hidden transmission and this skill attempts to conceal the existence of the message from the viewer. The earliest known stenography skill expanded in ancient Greece around 440 B.C. Herodotus's Histories explained the earliest type of stenography. It states that "The slave's head was shaved and then a Tattoo was inscribed on the scalp .When the slave's hair had grown back over the hidden tattoo, the slave was sent to the receiver. The recipient once again shaved the slave's head and retrieved the message". Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization for the best communication results. Confidentiality is a set of rules that limits the access to information or software from the person who does not have the authority to know it. Integrity involves sustaining the regularity, preciseness and reliability of data throughout its entire lifecycle. Protection happens only if data becomes secure from dependable source and regularly updated from time to time. Availability guaranteed by carefully keeping all hardware, execute hardware repairs promptly when needed and keeping a working operating system domain that does not have software dispute. It is very important to keep all software up to date. Delivering sufficient communication bandwidth and avoiding the occurrence of bottlenecks are both crucial. To accomplish this, most command and base level military communication, use hack proof dedicated Wide Area Networks based on special Mil-Grade software protocol stack and a separate hardware at the physical layer itself. All the terrorist societies need to implement CIA in their communication channels. Most of their representatives run within ordinary citizens and are not able to provide dedicated networks, used by the government counterparts. In this kind of situation, the only communication option they have is the internet (World Wide Web). In order for them to use the internet, these terror communities are expanding new kinds of software, which will allow them to communicate in private.

1.1. Stegnalysis: Techniques

Before we start with steganalysis we should know the different transmission channels and skills through which these stego-images are being used by terrorist organizations and why they are relaying so much on them.

1.2. Channels and Skills user by Terrorist organizations:

As stated earlier, for much transmission channel the CIA compliance is a necessity. In order to accomplish it terrorist use stego-images for one to one transmission via emails. Therefore, these stego-images are used as electronic Dead Drops. Dead Drop is a slang used for places suggestion such as a book in a library or any place that both parties know of where information is been left. It

assists the two parties to avoid meeting directly and they would not know each other too. Along these lines, terrorist also upload these images on public web pages and therefore keep communication without knowing who the other person is. They do not have any face-to-face meetings, E-mails or instant messaging between them. All there is that an image posted to a website or public forum, and anyone can download it if it catches his/her interests.

1.3. Advantages offered by Steganography:

A legal company never need to use dead drops. Nevertheless, terrorist need it. Therefore the feature of confidentiality makes it a powerful tool in terrorist' hands. The most important reason for using steganography is that its cost is far lower than the cost of discovering the existence of data in the same-stego image. In a few cases, it might be impossible to identify the existence of any data. For example, a one bit, "yes" or "no" massage inserted in a big image file would be impossible to find. On one hand, these files transform onto video files and collages and it can make identification more laborious. The more little the pieces of information is, the more difficult it is to be found.

1.4. Steganography: A New Age of Terrorism

Steganography is a secret way of hiding information in a way, which does not show the actual information. According to nameless "U.S. officials and experts" and "U.S. and foreign officials," these terrorist communities are " hiding all their terrorist aims and maps by posting commands for terrorist actions on sports chat rooms, pornographic bulletin boards and other Web sites". The past three years FBI director Louis Freeh attempted to persuade government that terrorist are using encryption and steganography to reinforce their communities. Free persuade legislators impose harder internet usage laws, stressing that this will not only harm the United States but it will also make fighting terrorism very difficult. Today' terrorist communities such as Hamas, Hezbollah, Al Qaeda, are engaging in modern steganography skills to move fragile information through the internet, without uncovering it. After a few highly arranged and deadly terrorist attacks, the United States government, and certainly, the world, rushed to uncover practicable techniques to identify and stop electronic deception, hoping that opposing criminal usage of the internet as their medium will provide them with preventing another attack and saving more lives.

In WWII, German secret agent used null ciphers, which "hide" the true communication within an innocent "sounding" communication. A German spy in WWII sends this message: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, discharging suites and vegetable oils. By taking the second letter in each word, it forms this message: Pershing sails from New York June. As communication recognition improved, the secret communication world was obligated to modify technologies, which may pass more communications and be less suspicious. In 1941, the very first microdots came up, "hiding information on a typed envelope carried by German agent". FBI Director, J. Edgar Hoover mentioned the microdot to be "the enemy's masterpiece of espionage." The communication that is been established, was not hidden nor encrypted but it was too small and went unnoticeable.

The microdot allowed the communication of big data including maps, photographs, documents, and drawings. With a large number of letters passing through Emails, the United States government felt alarmed. After the war has come to an end, inspectors has disallowed sending messages with flower deliveries, radio song requests, weather reports, children's drawings sent in mails, knitting instructions, and anything else that might possibly encode Axis intelligence. Adding to that, another well-known stenography incident happened during the height of the Vietnam WAR. Commander Jeremiah Denton, a naval aviator, shot down and captured by North Vietnamese forces. Denton was paraded in front of the news media; Denton, knowing he would be unable to say anything critical of his captors, spoke to the media, while speaking, he blinked his eyes in Morse code, spelling out T-O-R-T-UR-E.

1.5. Information Hiding Techniques

The most important intensions related to information hiding that one must keep in mind when thinking about the identification and recovery of hidden messages. Firstly, the most common technique for terrorist transmission protected by encryption, before it is hidden. This inspires the person transmitting with the benefit of defense in depth. "Clear encoding algorithms are the leading way to transform data into white noise". If steganography exists, it will be hard to retrieve the message because the message is been concealed by cryptography. If the correct message obtained, the attacker must crack the message, which needs the understanding of the coding algorithm used. The simplest way of hiding information in a file is to

control the least significant bits, of the color of the pixels in an image.
This is beneficial to hide the existence of the information from the eyes of humans. As with color depth at 16 or 32 bits the amendment of the least significant bit in the color will be unnoticeable. Civilized algorithms use unsystematic subdivision of pixels in the image to depot-hidden information in the same image. If there is conflict between information, (both parties use the same pixel so that the information being transmitted may be incorrect for one of the messages or both of the messages), correction codes are used to retrieve information damaged in the conflict. Some image formats (.gif, .bmp, etc.) are enhanced for using the least significant bit method of information hiding. .gif and bitmap images are stored in the same format that they are provided in, there is no constriction. The JPEG format is built using loss compression. That means that when the JPEG becomes smaller for storage and/or transmission, and then repositioned at the receiving/rendering end, this will lead to bits getting lost and therefore, the hidden message can be lost. There is a method to hide the information in JEPEG format. It uses a Discrete Cosine Transform (DCT) compression scheme. "The compressed information is kept as integers, extensive floating-point calculations are rounded at the end is involved when compressing. When rounding happens, the program makes a choice to round up or round down. By adjusting these choices, messages can be inserted in the DCT coefficients." J-Steg is one of the assets that hides data in JPEG files and is very continent to use. Finally yet importantly, there is a concept of secret sharing also involved. There are ways to crack the information, which makes the hidden information not understandable unless part of the message is reveled. Something unseen is crack able with less than required number of parts. The hidden is undiscoverable.

The easiest comparison to secrets with m parts in m-dimensional space is the example of points, lines and axis blocks. The example works as follows: the hidden information is in two sections and the point at which a line stops at an axis (x or y, it is not a great matter as long as the lines is not in the same line to one or the other axis). Both the stops are known when all the parts of the hidden information is also known. The both parts of the secrets are two points. Only one line sketched through the two points and it can only intercept each of the axes at one point each. Moreover, more than two point's coordinates are given out. These points being on the same line, so that many people can know the coordinate of a point and in this situation, any two merging their transmission can draw the line through two points and come up with the hidden message (the intercept point of the line and the axis). If the secret message is such that it needs three people, one uses other analogies (planes for 3-dimensions, and n-dimensional constructions for ndimensional secrets). This example is a simplification and an analogy for how secrets can actually be broken up, or shared. A basic stenographic file system constructed to hold m files that are n bits long.

1.6. Steganography Software

There are currently over 140 steganography programs available. The gadgets scopes from software that hides information in images to software that hides information in spam. The programs used for steganography are freely available to use. Regrettably, this has made it easy for terrorist to not only for free, but to hide their information without detection. S-Tools 4.0 is one of the stenography Tools. (S-Tools) for windows involves many programs that process GIF images, BMP images, and audio WAV files. S-Tolls is able to hide information in the empty areas on a floppy disk. On top of supporting 24-bit images, S-Tools also involves many encryption patterns including IDEA, MDC, DES, and triple DES. S-Tools applies the LSB method to both images and audio files. A useful characteristic is a status line that shows the largest message size that can be store in an open container file. This removes the chances of aiming to store information that is big for the specific container. After the messages disappear, the stenographic image shows, and the original message will stay on the screen so that the new message is compared. S-Tools is easy and secure to use, it does an amazing job to hide the information.

2.1. Different Kinds of Steganography

Nearly all digital file extensions used for steganography; the formats that are more appropriate are those with high redundancy. Redundancy is defined as the bits that contribute precision better than the user of the objects display. These bits change without being detected easily. Image and audio files especially obey this requirement, while other researchers found other file extensions that hide messages. Hiding messages in the form of text is historically the most crucial way of steganography. A clear method is to hide a secret message on the nth letter of every word of a message. It has lowered importance only since the beginning of the internet and all the different digital file extensions. Text steganography is not used because text does not have high amount of redundancy. Given the generation of images, and a

big amount of redundant bits available in the digital portrayal of an image, images are the most trendy cover object for steganography.

2.2. Image and Transform Domain

Image steganography skills are separated into two groups: those in the image domain and those in the Transform domain. Image – also known as spatial- domain skills firmly involved information in the strength of the pixels directly, while for transform – also known as frequency- domain, first images are transformed and the added in the image. Image domain involves bit-wise skills that apply bit insertion and noise manipulation and distinguished as "simple system" sometimes. Image extensions that are most appropriate for image domain steganography are free from loss and the skills are depending on image extensions. In the transform domain, manipulation of algorithms and image transforms are involved. These skills hide the image in more notable areas of the cover image, making it stronger. Most transform domain skills rely on the image extensions and the information within may survive conversion between loss and lossless compression.

2.3. Patchwork

Patchwork is a skill that uses redundant arrangement encoding to involve information in an image. The algorithm adds redundancy to the hidden message and puzzles it throughput the image. A random genitor is used to select two areas of the image, patch A and patch B. Patch A pixels are lighter than patch B. Additionally, the strengths of the pixels in a patch increased by a constant value; the other patch is decreased by the same constant value. The different changes in this patch subset encodes one bit and the changes are small and unnoticeable, while not changing the average brightness. A drawback of the patchwork skill is that only one bit is involved. More bits can be involved by first dividing the image into sub-images and the involvement of each of them. The benefit of using this skill is that secret information spread over the whole image, if one of the patches is destroyed, others may still be there. This therefore, relies on the information size, since the information is only repeated throughout the image if it is small enough. If the message is too big, it is embedded once.

2.4. Spread Spectrum

In this technique, secret data spread throughout the cover image making it more difficult to discover. A system suggested be Marvel et al. incorporates spread spectrum transmission, error control encoding, and image processing to conceal messages in images. In spread, spectrum image steganography the message embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image.

3.0. Conclusion

Although Steganography offers beneficial results to the internet privacy, it also provides a lenient way for terrorist to prepare their plans and hide their intentions. Therefore, steganography is playing a big part in the terrorist society. However, it is noticeable that the government is actually trying to eliminate the relationship between terrorists and steganography, one thing is for sure, the U.S. counter-terrorism effort failed September 11, costing many lives. Steganography has its emergence in the ancient past and in the new digital age can take many shapes. There are many different types of places and directions that can utilized to accomplish data hiding plans, any of these directions are strictly stenographic. Steganography is now been understood as the hidden information in images and sound files. The tools are highly available and cheap. The idea and proficiency of hiding communications is that, they are recorded, acknowledged and known. Information respect to these ideas and proficiencies are accessible to criminals, terrorists, and individuals who are obedient to the law and society. The use of Steganography by everyone muddles the people whose duty is to monitor terrorist transmissions.

Steganography is hard to discover, and together with the importance of cracking the encryption, as expected almost all hidden communications is encrypted so it will be difficult to extract the information. As new ways expand to trigger steganography, the software developers are writing software to add steganography information on how the current tools work and design new tools to hide the information. Therefore, the tools become stronger and more suitable for hiding the information in a way that it will reach to the other party uncovered and the detections tools are not able to detect it. Terrorist and criminals are able to construct their own information hiding ways, which are not common. This certainty makes it crucial that the analyzer runs extensive code analysis on the computers seized from terrorists. Transmissions ways that allows terrorist to propose and accomplish

attacks are very important to law enforcement and national intelligence agencies. In studying the theoretical and technical hurdles inherent in detecting steganography, it becomes necessary upon rules creator to appoint the suitable capital and apply them to solving the problem of real-time steganography detection.

References

Article, I. M. (2012, MAY). *infosecurity group*. Retrieved from Al-Qaeda uses steganography - documents hidden in porn videos found on memory stick: https://www.infosecurity-magazine.com/news/al-qaeda-uses-steganography-documents-hidden-in/

article, k. (2010, March). *Al-Qaida Goes "Old School" With*. Retrieved from Al-Qaida Goes "Old School" With: https://krypt3ia.wordpress.com/2010/03/13/al-qaida-goes-old-school-with-tradecraft-and-steganography/

Betancourt, S. R. (2004). Global Information Assurance Certification Paper. *GSEC Practical Version 1.2f*, 1-10.

Carvin, A. (2001, october). *benton foundation* . Retrieved from The Digital Beat: https://www.benton.org/archive/publibrary/digitalbeat/db103101.html

Choudhary, K. (2012). Image Steganography and Global Terrorism. *Global Security Studies, Fall 2012, Volume 3, Issue 4*, 1-21.

Cole, E. (2003). Indianapolis: Wiley Publishing. *Hiding in Plain Site. Indianapolis: Wiley Publishing*, 119.

Conway, M. (2004). Code Wars: Steganography, Signals Intelligence, and Terrorism . *C Knowledge, Technology and Policy (Special issue entitled 'Technology and Terrorism') Vol. 16, No. 2*, 171-191.

Dibbell, J. (2001, February). *feedmag*. Retrieved from "Pirate Utopia": http://www.feedmag.com/templates/default.php3?a_id=1624

Honeyman, N. P. (n.d.). *Center for Information Technology Integration*. Retrieved from University of Michigan, Detecting Steganographic Content on the Internet. The study of more than two million images downloaded from eBay auctions shows evidence that terrorists are using the images to hide encoded messages. .

Johnson, N. (1995, november). *Steganography*. Retrieved from Steganography: http://www.jjtc.com/stegdoc/index2.html

Johnson, N. (2001, November). *"Steganography."*. Retrieved from "Steganography.": http://www.jjtc.com/stegdoc/index2.html

Johnson, N. a. (1998). Steganalysis: The Investigation of Hidden Information, . *IEEE Information Technology Conference, Syracuse, New York, USA, .*

Kahn, D. (1967). The Codebreakers. *The Macmillan Company*, 67.

Morkel, T. (2005). AN OVERVIEW OF IMAGE STEGANOGRAPHY . *Information and Computer Security Architecture (ICSA) Research Group* , 12.

Petitcolas, F. A. (2002). FBI Agent Robert Hanssen using steganography as electronic dead drop tool. *Information Hiding 5th International WorkshopOct* , 20.

Schneier, B. (2001, October). *Bruce Schneier on crypto, the FBI, privacy and more*. Retrieved from A special issue of Crypto-Gram: https://www.theregister.co.uk/2001/10/03/bruce_schneier_on_crypto/

Watkins, J. (2001). Steganography . *Messages Hidden in Bits*.

Wayner. (2006). Conference on Digital Forensics, Security and Law, 2006. *Information Hiding: Steganography and Watermarking. 2nd ed. Boston: Morgan Kaufmann Publishers.*, 31.

Wayner, P. (2002). *Disappearing Cryptography.* United States of America : Edward Wade.

Wayner, P. (2002). Disappearing Cryptography . *Information Hiding: Steganography and Watermarking. 2nd ed. Boston: Morgan Kaufmann Publishers.*