DIGITAL STEGANOGRAPHY

Abstract

Steganography derives from a Greek word and means covered writing. It is a sector of computer information security. Cryptography secures critical information. Steganography performs the function of hiding information. Cryptography changes the values of the data into unintelligible form so that apart from having the key to the algorithm no one can read it. Cryptography is a secret communication between parties that occurs by scrambling the message. Only the receiver has the key to unscramble it (Rwabutaza, Yang and Bourbakis, 2012). On the other hand, steganography hides the information in plain sight, and it is undetectable without extremely sophisticated forensic software. Steganography can be used in videos, images and plain text (Singla and Juneja, 2014).

Keywords: steganography, encryption, data, computer, security

Digital Steganography

Steganography, the art of hiding data in plain sight, has existed for centuries but is now a critical part of our digital infrastructure. Steganography began with the ancient Romans and Greeks. In Greece, the text to be hidden was written on wooden wax-covered tablets. The message avoids detection by having a second application of wax which is then removed upon receipt, and the original message is known. Today the technology has evolved. Even before steganography, microdots existed. These are the size of a simple period, but contain up to a page of data. This is the theory and basis of modern steganography.

There are over 500 known steganographic programs that can create encrypted data. With the development of the computer, digital technology has made encrypted messages a lot easier to hide. The advantage to steganography is that messages do not have to attract attention. Most encrypted messages do arouse suspicion. Steganography doesn't draw attention to its existence and stays under the radar.

The most popular formats for steganography are .doc, .bmp, .gif, .jpeg, .mp3 and .wav. Digital images are the most popular method for steganography. This exploits weaknesses in our visual system. We have a low level of sensitivity to changes in random patterns.

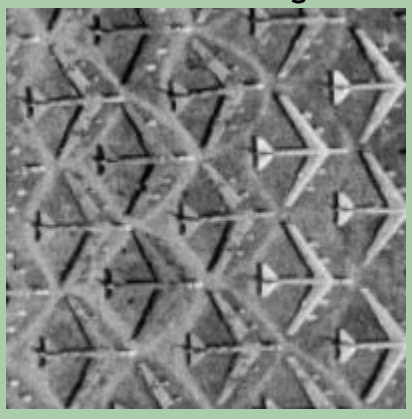
Cryptographers use keys. Steganography does not. It is based on the principle of transmission of secret messages in plain sight of the viewer. The data could be a picture of your mother. Encryption, though, is often combined with steganography.

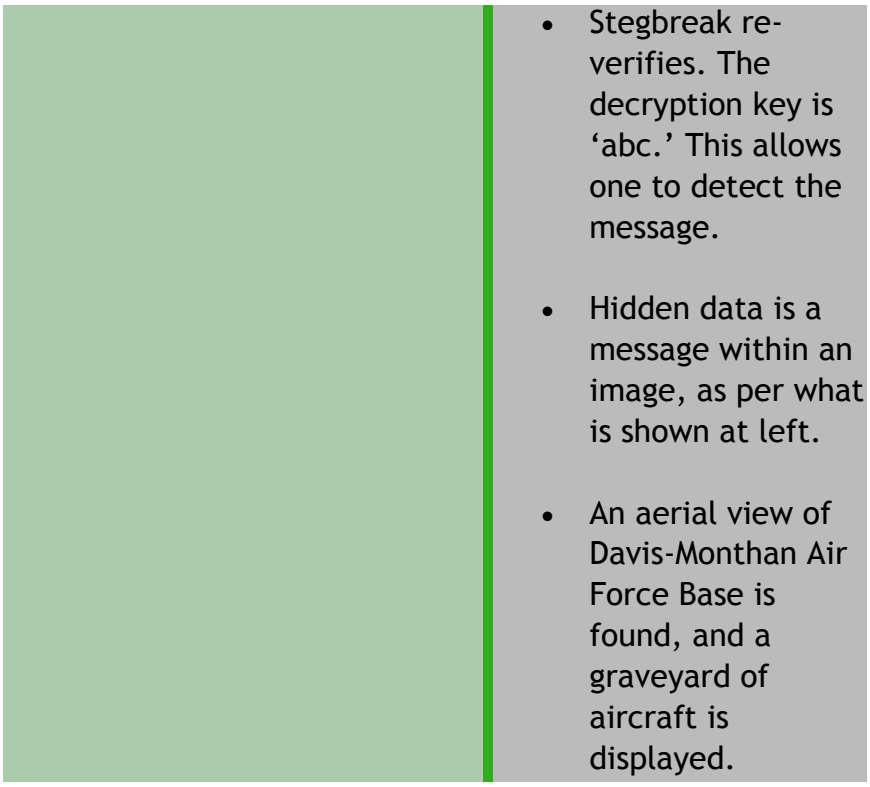
The text is stored on your relative's picture but in the remote chance it is discovered, it would also have to be decrypted. Decryption requires a key or password. That is usually transmitted separately to the receiver. In other words, the photo may be emailed, but the password to decrypt might have been innocently sent in a text message separately.

Steganography can therefore be viewed as a layered security. It protects data that one wants to be "sensitive and compartmentalized." It could be used for corporate or government purposes under this manner. However, it may also be used in illegal ways. CD-ROMs text files, photos and even music files can therefore contain hidden data. Information-hiding ability of a medium can range from ten to over fifty percent, depending on the software and techniques applied.

An example of steganography in action follows. Contained inside the image, and invisible to your naked eye, is another image – a B-52 graveyard satellite photo over an Air Force Base. Steganalysis, the investigation and forensics of hidden data, is utilized to extract this hidden photo. Remember that to the naked eye nothing at all is visible.

Table 1 – Steganography Images

Cover Image [1]	*Original Image from the ABC Network*
	• The JPEG IMAGE displayed on the left is shown during the broadcast • A hidden image, related to B-52s, is asserted to be in it • This is only a test and not an example of actual terrorist usage of the steganographic methods • Niels Provos utilized Stegdetect and Stegbreak to analyze over 2 million JPEG images
Hidden Message	*Steganographic Operation*
	• Software detection of steganographic objects is possible with the right equipment • Stegdetect is utilized to determine if hidden information exists



- Stegbreak re-verifies. The decryption key is ‘abc.’ This allows one to detect the message.
- Hidden data is a message within an image, as per what is shown at left.
- An aerial view of Davis-Monthan Air Force Base is found, and a graveyard of aircraft is displayed.

Photos courtesy of Niels Provos, http://niels.xtdnet.nl/stego/abc.html

The government is concerned about this new digital technology. If a person can hide only 5KB of data inside a picture, that hidden message could conceivably contain top secret information or dangerous instructions. The Pentagon and the CIA both fund steganalysis research, primarily at Carnegie Mellon.

Before discussing how information is hidden in an image file, it is worth a fast review of how images are stored in the first place. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image.

Hidden images are made up of 8 bit and 24 bit pixel image files. Using 8-bit color there exists a definition of up to and including 256 colors that form palettes for

images. A 24-bit color uses 24 bits per pixel, providing a better set of colors. A process called least significant bit (LSB) encoding is used for the digital images. One can store 3 bits of data in each pixel for a 24-bit image, and 1 bit per pixel in each 8-bit image. Each byte represents one of the 3 primary colors – red, green or blue (RGB).

Normal computer security protection techniques do not provide any level of protection at all to steganographic images. A firewall protects intruders, but an image delivered as part of an email is expected and received. Malware protection eliminates Trojans, worms and viruses but don't impact this method of delivery. An encrypted laptop is fine, but it still will receive these images.

Computer fraud today is often committed primarily by those inside an organization, whether it is a government or private entity. Someone can take a document, hide it inside a picture using open-source steganographic tools, and there goes confidential information to competitors or unauthorized recipients. One of the most popular tools is S-Tools v4. It hides secret files in .bmp, .gif, or .wav files. MP Stego embeds hidden data into .mp3 audio files.

The solution is on the market, but many are unaware of both the risks and the possibilities. Wetstone Technologies offers detection algorithms. These can be placed into Application Firewalls, and also Intrusion Detection Systems. They integrate the solution with the customer's existing architecture.

There will always exist individuals and groups who attempt to use these techniques for ulterior motives. Steganography, the art of concealment of information within other information so that only the intended user can decode it, is a major security issue to all owners of private and protected networks. Steganography is vastly superior to encryption since it not only prevents others from being privy to the information, but even prevents them from being aware the information has been compromised. Privacy issues in open computer systems are just one of the concerns (Atawneh, Almomani and Sumari, 2013).

Outside of the field of cryptography administration that many computer network administrators deal with everyday, steganography has emerged as the new field of computer information security that one needs to be very aware of. Some consider it only an arcane study done in the halls of academia. But in its most extreme cases of usage, it can be very dangerous. It is all too real. Some reports exist in government circles that the terrorists behind September 11th and the attacks in New York and Washington, D.C. used steganography as a means of communication (Kessler, 2001). The repercussions of not having adequate computer and network countermeasures in place can thus be very serious indeed.

References

Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. IETE Technical Review, 30(4), 344. Retrieved from http://edb.pbclibrary.org:2077/ps/i.do?id=GALE%7CA341728377&v=2.1&u=d0_mlpbcls&it&p=AONE&sw=w&asid=d81249802f2ab2833f56b488ea60388f

Kessler, G. (2001, September 1). Steganography: Hiding Data Within Data. Retrieved December 11, 2014, from http://www.garykessler.net/library/steganography.html

Provos, N. (2001, October 12). Contribution to Information Attrition. *First Steganographic Image in the Wild.* Retrieved December 11, 2014, from http://niels.xtdnet.nl/stego/abc.html

Rwabutaza, A., Yang, M., & Bourbakis, N. (2012). A comparative survey on cryptology-based methodologies. International Journal of Information Security and Privacy, 6(3), 1+. Retrieved from http://edb.pbclibrary.org:2077/ps/i.do?id=GALE%7CA311851548&v=2.1&u=d0_mlpbcls&it=r&p=AONE&sw=w&asid=b6e8bafab78a5c803a7c6a8743ed7c8b

Singla, D., & Juneja, M. (2014). New information hiding technique using features of image. Journal of Emerging Technologies in Web Intelligence, 6(2), 237+. Retrieved from

http://edb.pbclibrary.org:2077/ps/i.do?id=GALE%7CA374695809&v=2.1&u=d0_mlpbcls&it=r&p=AONE&sw=w&asid=fd41a56eedcd6d701294ad7f26112e7f