Nicholas Gahagen

Steganography can be defined as the placement of a concealed message within a clear message. These messages can be nearly any form of media, including digital images, sound waves, and text. The medium of the hidden message may or may not match the medium of the clearly visible message. A common characteristic of steganography lies within the fact that it is not explicitly known that a message is hidden somehow within another. Note that this is in contrast with other methods of digital encryption, in which it is often obvious that some message is concealed. While first discussed centuries ago by Greek historian Herodotus, steganography has undergone a rapid development in practical application in relatively recent years due to the expansion of the internet, and with it, the need for cyber security. The deceptive nature of steganography gives it great contrast to other methods of encryption. Rather than making an obviously hidden message hard to decrypt, like most conventional means of encryption, steganography forms the inverse, making a doubtedly hidden message relatively easy to decrypt.

The integrity of national defense is closely tied to steganography. While less common than typical encryption methods in practical use due to the volatile nature of data-hiding in which each medium requires a unique approach, it can still be used in conjunction with the aforementioned typical encryption methods to provide further defense against unintended decryption. Furthermore, steganography is essential towards the placement of effective digital decoys. For example, a standard decryption may lead to a text file with seemingly erroneous or irrelevant content, upon which point, it may be logically assumed that the decrypted message was unimportant towards the true purpose of the encrypter - potential artifact of some intended medium. By using steganography, however, an entirely different message may be hidden within the erroneous one. If done right, this may yield any other form of media containing a completely different message. However, while steganography allows for significantly improved data security, it is far more situational than standard encryption. For instance, the decoy approach to data integrity requires sufficient documentation to prevent confusion on the encryptor’s end. In addition, if one is faithful in the integrity of their encryption keys, then steganography may be irrelevant altogether.

In recent years, steganography has undergone use by the FBI and other national organizations. In 2010, a steganography method was developed by the FBI which allowed secure communication between foreign agents by hiding a text file within an image file. This text file would be covertly extracted using the given extraction method, making it very unlikely that an unintended receiver would not only assume a secret message was hidden within the image, but even less, discover the method of extracting the message from within the image. Steganographic encryption has also been of use to countries often considered to be cyber-adversaries to the United States. Russia and China, for instance, have employed similar means of steganography in recent years. This has resulted in indictments being placed against these countries by the US. In this way, a well-rounded understanding of steganography is important not only for the protection of national information, but also for the decryption of potentially-malicious external data. Compared to standard encryption methods or hashes, the data hidden within a steganographic medium is exceedingly volatile. Therefore, intelligence-gathering is perhaps the most important method to decrypt an adversary’s steganographic media. This is in contrast with key-based encryption algorithms, where simply knowing that a string of text contains an encrypted message gives little leeway in managing to successfully decrypt the string.

While it is important to recognize the use of steganography in relation to the national government, military, and defense, it may also be of benefit to analyze its public implications. Throughout history, steganography has been used in, or in relation to, literature, religion, entertainment, music, and other areas. Prior to the age of the computer, steganography was done through physical means, by using everyday items such as yarn, postage stamps, or secret pen ink. One such method, for example, involved writing over existing text using a typewriter to create a barely visible second message over the first. Musical artists have employed steganographic methods since the 1960s, when the process of backmasking was popularized by the Beatles album Revolver. This trend has stood the test of time, with artists across a great variety of genres implementing steganography in their music to this day. One such technique involves hiding an image by visualizing a portion of the song's pitch in respect to time. Private organizations have also employed steganography in recent years. Perhaps the best-known example is the mysterious Cicada 3301 puzzle, a series of cryptographic challenges posted throughout the mid-2010s by an anonymous group. These elaborate puzzles involved the use of steganographic media and steganographic decoys, as well as many other cybersecurity methods. This famous series of puzzles, which have yet to be completed today, introduced many to the topic of steganography, including myself. Because of its relative simplicity (but not necessarily or explicitly vulnerability) in comparison to key-based encryption methods, steganography has been well-received by the public, having cultural influence across several fields.

Similarly to civilian use, steganography has undergone expansive militaristic involvement, even before the introduction of the modern internet. A famous example would be the hidden message of Jeremiah Denton, an American PoW to North Korea in 1966. While forced to take part in a televised address, Denton blinked in Morse code, covertly revealing that PoWs such as himself were being tortured by North Korea. This alerted the Navy to the problem before any other means of communication, and spared Denton from suspicion by his captors. The United States military has not only been advanced by its use of steganography, however. It has also suffered because of steganography. During WWII, Japanese spy Velvalee Dickinson, who owned a doll shop in New York City, sent what appeared to be business-related documents to her colleagues in South America. However, these documents in fact contained steganographically hidden information relating to sensitive United States military information, such as ship movements. Steganography has stood the test of time in regards to its military use, and it will only continue to be an object of interest and manipulation by military leaders around the world.

The field of digital steganography has been advanced by the joint efforts of engineers and scientists in recent decades. Perhaps one of the most inspiring to me is Doctor Kamran Ahsan, who authored a thesis in 2002 through the University of Illinois on the steganographic hiding of data over the TCP/IP suite. The act of data hiding within the OSI model is particularly interesting due to the low-level operation of the steganography and the inherent networking abilities. The standardization and low level of the OSI model initially appears to suggest that a steganographic encryption would be impossible. However, Doctor Ahsan formulates an ingenious approach in which steganography is possible through two methods - packet manipulation and packet sorting. According to the thesis, these methods may be combined for additional data security, although this is not necessary. Doctor Ahsan's thesis is notable since it doesn't simply define a steganography method, but it manipulates an internet standard so that steganography would be possible, then defines the method within those constraints.

Steganography has not changed over time like many other methods of encryption. While the medium upon which steganography is conducted has modernized and digitized over the years, the abstract method of data-hiding has changed very little. This is primarily due to the strong link between the medium and the steganographic encryption, in which the method of hiding data is strongly dependent on the medium. For example, steganographically hiding data within an image file is very different from hiding data within a sound file, but neither method has changed by itself in years. The medium can only offer a certain degree of steganographic potential, and steganography simply manipulates this narrow window of manipulation.

That said, 20 years from now, I predict that the practical application of steganography will change very little. There will almost certainly be new file formats, for example, perhaps a virtual-reality-linked file type. These new files will demand a unique steganographic approach. However, for existing files, the method will change very little. I also predict that steganography will undergo a resurgence in importance as popular key-based encryption methods falter under improved cracking methods and leaps in the computing power often used to attempt to crack such methods. Steganography is immune to these methods, and will require either a human or an exceptionally powerful AI to crack. Therefore, as long as such AI remains theoretical, I predict that steganography will gradually take up popularity from key-based encryption methods. If this turns out to be true, then a massive overhaul of existing encryption algorithms will be required on the part of the government or military, replacing existing encryption methods with stronger methods, or steganographic methods.