Anish Malik

Steganography is hiding secret information in a non-secret object that is encrypted upon sending and decrypted upon receiving. In modern times, media such as images and audio is used. A simple example of steganography is writing a message using “invisible ink” in the form of lemon juice. The lemon juice “encrypted” the message when it was sent to the other person. The other person “decrypted” the message when they received it by applying a heat source to slightly brown the lemon juice.

The topic of steganography inspires me due to its range of simplicity and complexity and its clandestine nature. Even though steganography involves concealing information, it is not cryptography as it doesn’t involve a key or scrambling data. Rather, it involves “data hiding”. This practice doesn’t allow privacy, but it allows secrecy. To the Navy, steganography is also known as “hiding in plain sight”. To protect themselves against adversaries, Naval soldiers must upgrade their current systems for cyber resiliency and software agility.

Even though steganography has been used for years, hackers and IT professionals have digitized the word. Many apps can be used for steganography, such as Steghide, Xiao, Stegais, and Concealment. An example of this is the sender selecting a digital image and using Steghide in the command line to embed a message. When the receiver receives the message, the receiver uses the Steghide tool in the command line to view the message.

Steganography is used for attacks as well, and an example of this is an attacker embedding scripts within Word or Excel documents. Instead of the attacker using Steghide or other steganography applications, the victim himself must open the document for the attack to occur. Once the document is opened, the hidden script is executed, installing an app into the user’s computer. This process is so indistinct that it is not noticed by typical antivirus applications. Finally, the app gets updated versions of malware from the Internet to compromise the victim’s computer.

Wojciech Mazurczyk, a professor at the Warsaw Institute of Technology and head of the Computer Systems Security Group, has written many scientific articles on steganography. He has mainly focused on steganography in network traffic and IP networks. His research has inspired me because it goes deeper into steganography as a whole, and his articles include many real-life examples. As someone interested in computer science, his articles not only show steganography itself but future applications of it too.

Many adversaries use steganography to threaten US interests. Sometime after 9/11, it was believed that Osama Bin Laden was using steganography to hide maps, targets, and terrorist plans on the Internet. The steganographic files were available on many sites for terrorists to unembed and download. The FBI also discovered that three of the terrorists booked rooms in Hollywood, Florida for the sole reason that the hotel was able to provide 24-hour access.

The use of artificial intelligence in steganography is increasing as well, and it will be ubiquitous in the future. This method is also known as “deep steganography”, and it allows steganographic techniques to be modified so the attack has a less likely chance of being discovered. An example of this using a convolutional neural network, which is shown to learn structures that correspond to logical features. This example would involve getting a good idea about the patterns of natural images and showing redundant areas where more pixels can be hidden. The increase in the number of pixels also allows more information to be hidden as well.

Steganography allows information to be hidden in a non-secret medium, and it can be used in both technical and non-technical forms. It can be as simple as “invisible ink” messages, or as complex as embedding scripts in Word and Excel documents. Additionally, as steganography in the technical sense has evolved, it is becoming easier for people to use it. Hackers can use certain tools for steganography, and they can use the command line itself to embed messages. Artificial intelligence in steganography is on the increase, and it will be used greatly in the future. Artificial intelligence allows steganography to get past its “predictable” patterns and makes it harder for cybersecurity professionals to recognize them.