



## National Infrastructure Protection Center

---

### **Steganography: Implications for Law Enforcement and Counterterrorism**

August 2001

James T. Cooker, National Infrastructure Protection Center,  
and Geoffrey French, Veridian

Steganography—the ability to conceal information to prevent its detection—is becoming more commonplace as digital communication improves, and will be of greater concern to law enforcement as steganographic capabilities increase. Steganography includes a wide group of communications methods that hide the message’s very existence, such as microdots, invisible inks, and spread spectrum communications. With computer-based systems, steganography refers to the ability to hide one file (e.g., text, pictures, or audio recordings) inside another. Although it has a similar role as cryptography in safeguarding sensitive communications or information, it has a very different way of achieving that goal. Whereas cryptography scrambles a message so it cannot be understood, steganography conceals the message so it cannot be seen. Its major advantage is that a message hidden by steganographic methods may not arouse suspicion if the communication is observed, whereas a message transmitted in ciphertext might.<sup>1</sup>

A number of software programs exist that can hide one file (the message file) inside another (the cover file). One of the best descriptions of steganographic methods can be found in Neil Johnson’s and Sushil Jajodia’s article “Exploring Steganography: Seeing the Unseen,” which appeared in *IEEE Computer* in February 1998. The article describes digital steganography and evaluates three tools by hiding text and images in an image cover file. Even this, however, is just a small representation of the possibilities. Virtually any combination of formats of message and cover files (e.g., a text message hidden in an audio cover file, an image hidden in a text cover file, or an audio message hidden in an image cover file) is possible.

---

<sup>1</sup> N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” *IEEE Computer*, 1998 31(2):26–34.

Steganography does not pose a larger problem than encryption or any other type of protected communication; it is merely a different way of masking communications. Still, it does give criminals and terrorists a tool to hide their activities and connections, which may prevent investigative agencies from exploiting communications that would help avert terrorist attacks or provide evidence needed for an investigation or conviction.<sup>2</sup> Law enforcement organizations need to take steganography into account in surveillance and investigations.

## **Surveillance**

Steganography demands that those monitoring a suspect take a closer look at outgoing and incoming e-mail messages. Outgoing messages that appear innocuous, such as digital photographs of family and friends, may contain hidden messages, and must be analyzed. In one recent case, police determined that a suspect was imbedding information into seemingly harmless photographs sent to addresses that appeared to be family members. The fact that the suspect never received any replies triggered a closer examination of the e-mail attachments.<sup>3</sup> Similarly, incoming messages—including spam—must also be closely examined. One web site allows a person to send a hidden message by embedding it into what looks to be unsolicited plain text advertising. The recipient then uses the web site to view the embedded text. These examples highlight two other important implications. First, steganography is another way that cutouts can be used in cyber space, where a third party that does not know the sender's or recipient's identity relays a message. Second, an out-going e-mail is not necessary to pass a message in cyber space; a suspect who has the ability to post images to a web site or news groups may use that as a means of transmitting embedded information.

## **Forensic Investigations**

A second consequence of steganography is that any computer files taken into custody or otherwise procured must be carefully examined. Text, graphic, and audio files should be scrutinized to ensure that they do not contain important evidence or information. A recent investigation in India illustrates this. After Indian authorities arrested Ashfaq Ahmed (a member of the Kashmiri terrorist group Lashkar-e-Tayyeba), they discovered that his business computer contained a large number of pornographic image files. A specialized team is currently analyzing the files to determine if they contain embedded messages sent between Lashkar-e-Tayyeba members.<sup>4</sup> Other reporting has also suggested that terrorist groups—including Usama Bin Laden's al-Qa'ida—might hide maps and instructions in image files.<sup>5</sup> This reinforces the concept that evidence may be found in seemingly innocuous files on any disk or equipment procured in an investigation.

---

<sup>2</sup> D. Denning and W. Baugh, Jr., "Hiding crimes in cyberspace," *Information, Communication, and Society*, 1999 2(3):251–276.

<sup>3</sup> D. McCullagh, "Secret messages come in .wavs," *Wired News*, February 20, 2001.

<sup>4</sup> V. Menon, "Experts to decode Lashkar messages on porn pictures," *Hindustan Times*, March 23, 2001.

<sup>5</sup> J. Kelley, "Terrorist instructions hidden online," *USA Today*, April 13, 2001.

## Detecting Steganography

Currently, steganography is difficult to detect. Although the process does degrade the cover file, this varies depending on the quality of the steganographic tool and the sizes of the message and cover files. Some tools do leave detectable signatures. A program known as “snow” hides a message by adding extra white space at the end of each line of a text file or e-mail message.<sup>6</sup> Still, only close forensic analysis has revealed the hidden messages. Detection and recovery toolkits, however, are under development. George Mason University’s Neil Johnson, for example, is building a detector that works similar to a virus scanner by identifying the signatures sometimes left by steganographic applications. Similarly, Wetstone Technologies, a cyber forensics technology company based in Freeport, New York is developing a set of statistical tests that could lead to the detection of the cover files and identification of the steganographic method.

## Conclusions

As terrorist and criminal groups increasingly use electronic means of communications, they will also be looking for new methods of securing their communication. Although encryption is an important tool for keeping the content of the message safe from authorities, steganography can also play a significant role: keeping the entire line of communication hidden. Detecting steganography and decoding encrypted messages are both difficult tasks, especially if groups use both tools simultaneously. Still, the first step in intercepting a message, identifying the individuals involved, and preventing the criminal activities is detecting the message’s very existence.

This product was completed with support from the CRUCIAL PLAYER project. CRUCIAL PLAYER is an interagency project initiated in 1999 by the Deputy Secretary of the Department of Defense (DoD), the Deputy Director of the Federal Bureau of Investigation, and the Deputy Director of the Central Intelligence Agency, and primarily funded by DoD. The project is managed by the National Infrastructure Protection Center, Washington D.C.

---

<sup>6</sup> D. McCullagh, “Secret messages come in .wavs,” *Wired News*, February 20, 2001.