

Unveiling the secret codes of

steganography

By 1st Lt. James Caldwell

752nd Communications Squadron

TINKER AIR FORCE BASE, Okla. – A type of ciphering known as steganography is the ancient art of hiding messages so that they're not detectable. Although a cousin to cryptography, steganography is not inherently obvious. So, how is steganography detected and why should network security analysts be alarmed and cautious?

Nearly all steganographic programs in use leave behind traces or fingerprints that indicate something is not right. Based on research conducted over the years, organized crime, terrorists and various other groups operating worldwide commonly use steganography to operate via public forums such

as Web sites. Software programs that detect steganography do exist and enhanced iterations are under development. Neil Johnson, graduate student at George Mason University, is developing a "stego-detector." This program, he describes, is designed to search hard drives for electronic fingerprints that typically result from steganographic applications. Similar to a virus scanner, this stego-detector identifies signatures. The Pentagon is also interested in uncovering practices of steganography, and annually funds the Naval Research Laboratory. Their interest spawns, in part, from news reports that link terrorist Osama bin Laden to steganographic communications. The concern is that data messages are being embedded in chat room messaging or bulletins unnoticed, while intelligence



"...organized crime, terrorists and various other groups operating worldwide commonly use steganography to operate via public forums such as Web sites."

agencies are off in another world monitoring [e-mail]. So far, steganography has turned up primarily on hacker Web sites, but was also found on Amazon and eBay. The Air Force and DoD have been working this since 1998, and observation by network security analysts warrants further attention.

Through the Ages

Steganography is widely employed today, but its origins trace back millennia ago. Before computers and e-mail of today, messengers had two options for delivering messages: one, to memorize the message or, two, hide it on the messenger. These early approaches were based on the principle that secret messages were hidden inside the physical object containing them. Now, digital technology offers new ways and abilities to hide information, even inside digital images. Because electronic information is sent via an array of numbers, one can hide messages randomly, or in "noisy areas" of an image that draws less attention.



▶▶ The Greek ruler Histaeus would shave the head of one of his slaves, tattoo the message onto his scalp, and send him along to deliver the message after his hair had grown back. The recipient would shave the slave's head to uncover the message and find an untainted scalp to reply by.



▶▶ Demeratus wrote a message to the Spartans warning of an invasion from Xerxes. The message was carved on a wood backing of a wax tablet, then covered in a fresh layer of wax. The seemingly blank tablet was then delivered successfully.

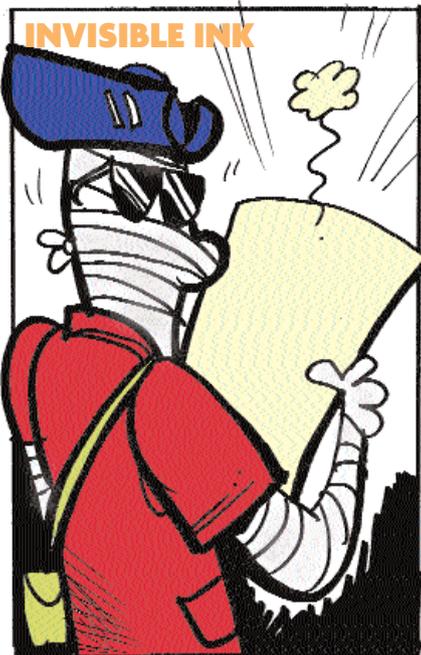
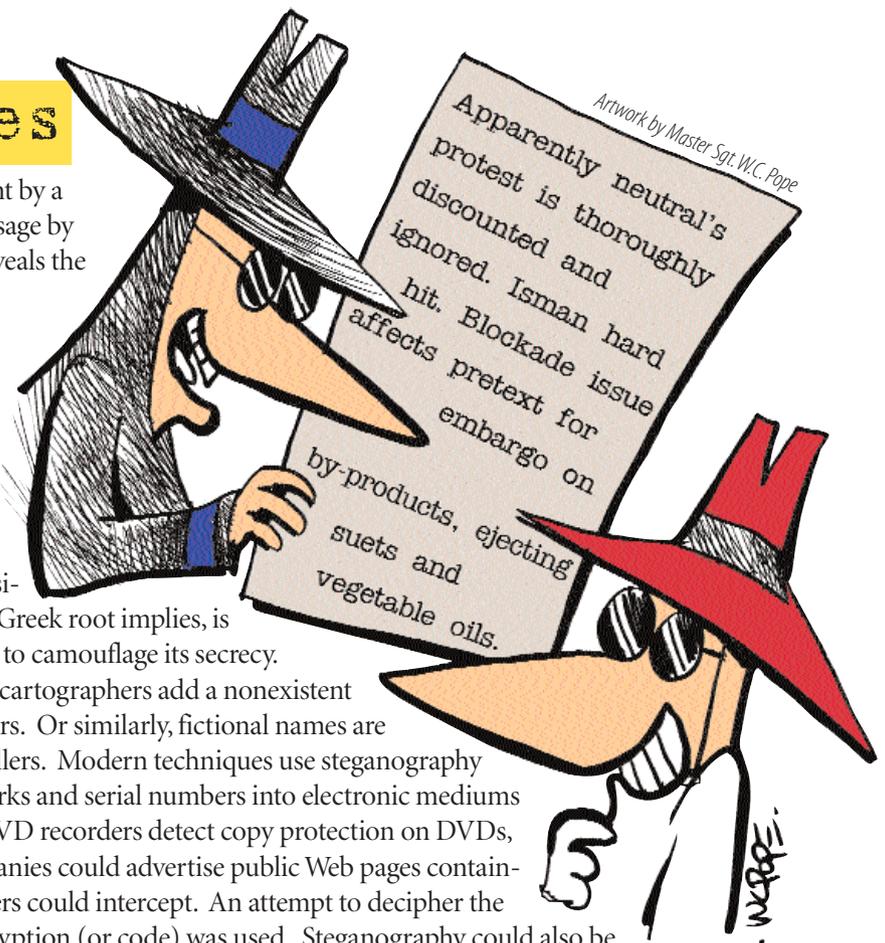
Secret Messages

The text in the cartoon contains a message sent by a German spy in World War II. Decoding the message by extracting the second character of every word reveals the following text:

Pershing sails for NY June 1.

This type of ciphering is known as steganography, which is the ancient art of hiding messages so that they're not detectable. Although a cousin to cryptography, steganography is not inherently obvious. Whereas cryptography is easily detectable as secret code, steganography, as its Greek root implies, is "covered writing," using a physical cover message to camouflage its secrecy.

Steganography is used in map making, where cartographers add a nonexistent street or lake in order to detect copyright offenders. Or similarly, fictional names are added to mailing lists to catch unauthorized resellers. Modern techniques use steganography as a watermark to inject encrypted copyright marks and serial numbers into electronic mediums such as books, audio, and video. For instance, DVD recorders detect copy protection on DVDs, which contain embedded authorizations. Companies could advertise public Web pages containing private, hidden text that only internal members could intercept. An attempt to decipher the hidden text would be unwarranted since no encryption (or code) was used. Steganography could also be used to hide the existence of sensitive files on storage media.



▶▶ During the American Revolution, the British and Americans used invisible inks extensively. They didn't have disappearing ink, but rather they used onion juice, alum, ammonia salts and several other materials that would glow dark when held over a flame.



▶▶ During World War II, the Germans used microdots, which was essentially a secret message photographed and reduced to the size of a period. FBI director J. Edgar Hoover said the microdot was, "the enemy's masterpiece of espionage."



▶▶ The advent of computers further advanced the disguise of messages. For instance, laser printers could be used to offset lines and character spaces by as little as 1/300th of an inch. A binary message could be sent easily using a normal space to represent 0s, and by offsetting characters 1/300th of an inch to represent 1s.