Category: Concepts, Trends, and Challenges

Evolution of Information-Hiding Technology

Der-Chyuan Lou
National Defense University, Taiwan

Jiang-Lung Liu
National Defense University, Taiwan

Hao-Kuan Tso
National Defense University, Taiwan

INTRODUCTION

Information-hiding technology is an ancient art and has existed for several centuries. In the past, messages could easily be intercepted because there was no technology of secret communication. Hence, a third party was able to read the message easily. This was all changed during 440 B.C., that is, the Greek Herod's era. The Greek historian Herodotus in his writing of histories stated that Demaratus was the first person who used the technique of information hiding. Demaratus, a Greek who lived in Persia, smuggled a secret message to Sparta under the cover of wax. The main intent was to warn Sparta that Xerxes, king of Persia, was planning an invasion on Greece by using his great naval fleet. He knew it would be very difficult to send the message to Sparta without it being intercepted. Hence, he came up with the idea of using a wax tablet to hide the secret message. In order to hide the secret message, he removed all the wax from the tablet, leaving only the wood underneath. He then wrote the secret message into the wood and recovered the tablet with the wax. The wax covered his message to make the wax tablet look like a blank one. Demaratus' message was hidden and never discovered by the Persians. Hence, the secret message was sent to Sparta successfully. Greece was able to defeat the invading Persians by using the secret message.

Another example of information hiding was employed by another Greek named Histaiaeus. Histaiaeus wanted to instigate a revolt against the Persian king and had to deliver a secret message about the revolt to Persia. He came up with the shaved-head technique. Histaiaeus decided to shave the head of his most trusted slave and then tattooed the secret message on his bald scalp. When the hair grew back, the secret message was covered, and then Histaiaeus ordered the slave to leave for Persia. When the slave reached his destination, his head was shaved, showing the secret message to the intended recipient.

Around 100 A.D., transparent inks made it into the secret field of information hiding. Pliny discovered that the milk of the thithymallus plant could easily be used as transparent ink. If a message was written with the milk, it would soon evaporate and left no residue. It seemed that the message was completely erased. But once the completely dried milk was heated, it would begin to char and turned to a brown color. Hence, the secret message could be written on anything that was not too flammable. The reason it turned brown was because the milk was loaded with carbon, and when carbon was heated, it tended to char.

Information hiding became downfallen and won no respect until World Wars I and II. Invisible inks, such as milk, vinegar, fruit juices, and urine, were extensively used during the wars. All of them would darken when they were heated. The technology was quite simple and noticeable. Furthermore, World War II also brought about two inventions of new technologies. The first one was the invention of the microdot technology. The microdot technology was invented by the Germans to convey secret messages to their allies. The microdot was basically a highly detailed picture shrunk to about the size of a period or dot, which permitted hiding large amounts of data into the little microdot. By using a microscope, the hidden message would be revealed. The Germans would put their dots into their letters, and they were almost undetectable to the naked eye.

The other technology was the use of open-coded messages. For open-coded messages, certain letters of each word were used to spell out the secret message. Open-coded messages used normal words and messages to write the buffer text that hid the message. Because they seemed normal, they often passed the check of security. For example, the following message was a common example of open-coded messages and was actually sent by a German spy during World War II.

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

By extracting the second letter in each word, the secret message was revealed:

Pershing sails from NY June 1.
This technique was effective because it could pass through the check of security and was easy for someone to decode (Johnson, Duric, & Jajodia, 2001; Katzenbeisser & Petitcolas, 2000; Schaefer, 2001).

The technologies mentioned here are different ways of information hiding in different eras. With the development of computer technology, it is becoming hard for the third party to discover the secret message.

BACKGROUND

In recent years, information-hiding technology has become the glittering palace in multidisciplinary fields, including image and signal processing, compression, cryptography, communication and coding theory, and so forth. The characteristics of information-hiding systems also have been widely discussed, including imperceptibility, robustness, tampering resistance, low computation cost, and false-positive rate (Cox, Miller, & Bloom, 2000; Lou, Liu, & Li, 2004; Lou & Sung, 2004). Table 1 summarizes some characteristics of information-hiding technology (Lee & Chen, 2002; Lou & Liu, 2000). However, a scheme that meets all these requirements is not an easy work. Take embedding messages as an example. Such a scheme may not cause noticeable artifacts, but may be too weak to stand the attacks of signal processing. Moreover, if we want to hide a massive message in an image, the problem of low robustness will appear. Hence, it is an important issue to develop a good scheme of information hiding with a better trade-off between these characteristics.

Information-hiding technology became a remarkable field after the 9/11 attack in the United States by terrorists. U.S. officials said that Osama Bin Laden's followers downloaded easy-to-use encryption programs from the Web, then Bin Laden posted instructions for terrorist activities in chat rooms, pornographic bulletin boards, and other Web sites. The Internet has proven to be a boon for terrorists.

Table 1. A summary of characteristics of information-hiding technologies

• Imperceptibility
• Robustness
• Security
• Capacity
• Unambiguous
• Undetectable
• Blind detection
• Low computation cost
• False-positive rate
• Tamper resistance
• Multiple watermark

In general, information-hiding technology has several applications as given in Figure 1 (Petitcolas, Anderson, & Kuhn, 1999). Other applications (Anderson & Petitcolas, 1998; Cox & Miller, 2002; Katzenbeisser & Petitcolas, 2000; Maadonks, 2004) include the following.

1. **Automatic Monitoring of Copyrighted Material on the Web:** There are two technologies that can trace the use of copyrighted material. One is verifying the copyrighted material by comparing the digests of the images that are downloaded from the Internet with the ones that are registered in the database. The other is to identify illegal usage by using a robot to search the Web.
2. **Automatic Audit of Radio Transmission:** This involves using a computer to listen to a radio station and search for a special piece of advertisement or music that has been broadcast.
3. **Data Augmentation:** Information is added for the benefit of the public. This can be details about the work, annotation, other channels, or buying information so that someone listening to the radio in a car can simply press a button to order the goods that he or she wants. Moreover, in order to cause more retrieval from the database, the information can also be hidden to find pictures or music tracks.
4. **Authentication and Recovery:** A digest can be hidden into digital media to prevent or detect unauthorized tampering or destruction, and even to recover the media.
5. **Indexing for Archive:** Metadata (e.g., data about the owner, title, scene, director, cameraman, location, etc.) are added to the material for an indexing archive.
6. **Transaction Tracking:** This involves adding copyright notices, identifying recipients, and tracing the source of illegal copies.
7. **Proof of Ownership:** Copyright notices are added as proof of original ownership.
8. **Remote Control:** Information is added that will allow the triggering or control of devices in a broadcast chain.
9. **Copy Control:** Some message is added to prevent the copying of copyrighted material.
10. **Medical Safety:** The date and the patient's name are embedded in a medical image as a useful safety measure.