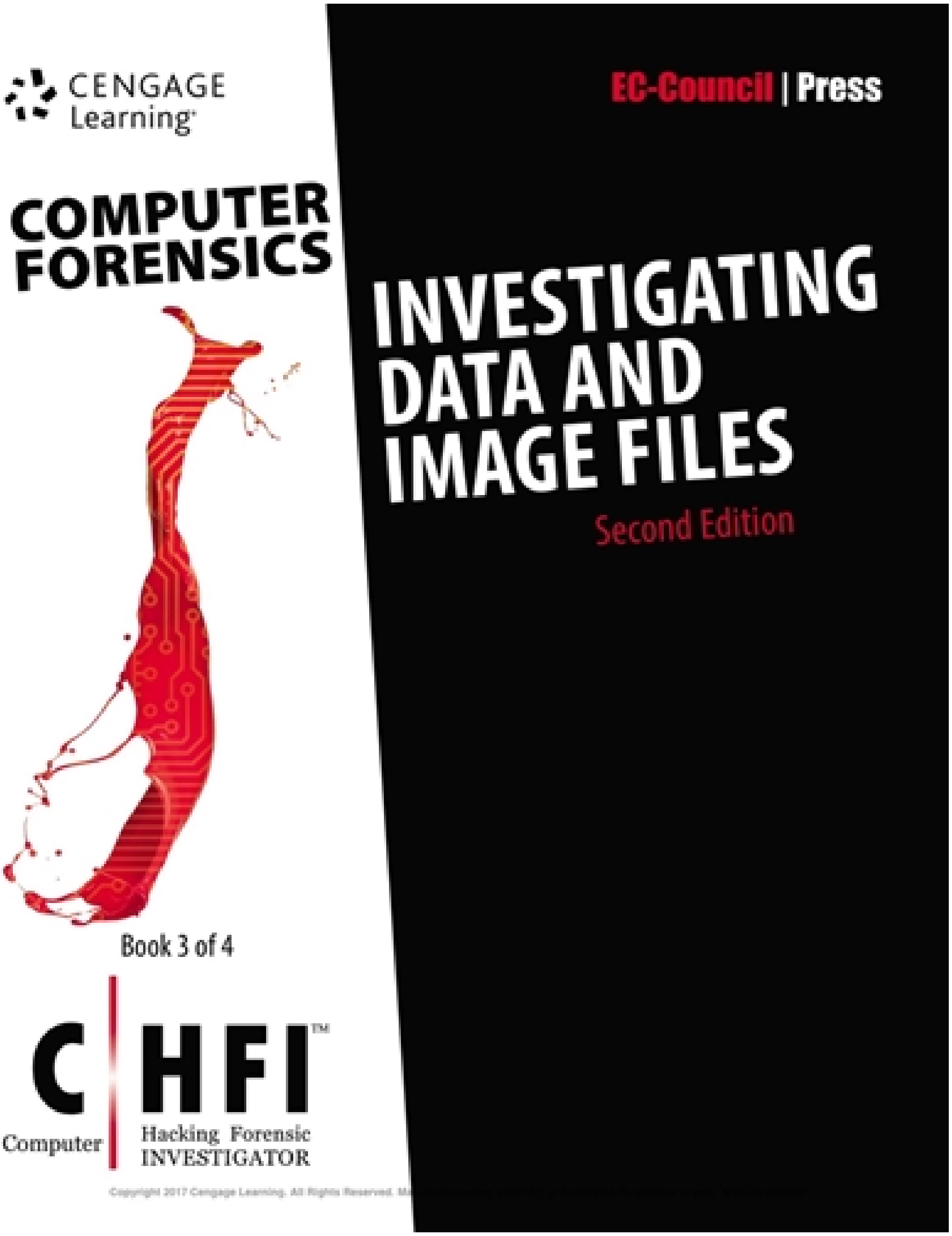
Solutions for Computer Forensics Investigating Data and Image Files CHFI 2nd Edition by EC-Council

CLICK HERE TO ACCESS COMPLETE Solutions



Solutions

Investigating Data and Image Files
Ch01-Review Question Answers

1. Define steganography.

   The practice of embedding hidden messages within a carrier medium.

2. What is a watermark?

   A digital stamp embedded into a digital signal.

3. How is steganography different from cryptography?

   In cryptography an encrypted message that is communicated can be detected but cannot be read. In steganography, the existence of the message is hidden.

4. Name the three main types of steganography.

   1. Technical steganography
   2. Linguistic steganography
   3. Digital steganography

5. How is steganography used with audio files?

   Hiding information in an audio file can be done by using either LSB or frequencies that are inaudible to the human ear. Frequencies over 20,000 Hz cannot be detected by the human ear.

   Information can also be hidden using musical tones with a substitution scheme. For example, tone F could represent 0, and tone C could represent 1. By using the substitution technique, a simple musical piece can be composed with a secret message, or an existing piece can be used with an encoded scheme that represents a message.

   Low-bit encoding replaces the LSB of information in each sampling point with a coded binary string.

   Phase coding involves substituting an initial audio segment with a reference phase that represents the data.

6. What is a cover medium?

   The medium used to hide a message with steganography.

7. Name two legal uses for steganography.

- *Medical records*: steganography is used in medical records to avoid any mix-up of patient's records.
- *Workplace communications*: steganography can be used as an efficient method for employees who desire privacy in the workplace to bypass the normal communication channels.
- *Digital music*: steganography is also used to protect music from being copied by introducing subtle changes into a music file that act as a digital signature.
- *Movie industry*: steganography can be used as copyright protection for DVDs and VCDs.

8. Explain the least-significant-bit method of steganography.

   A steganography technique in which the rightmost bit in the binary notation is substituted with a bit from the embedded message.

9. Name two technical methods used to embed messages in a text file.

   In technical steganography, physical or chemical methods are used to hide the existence of a message. Technical steganography can include the following methods:

   - *Invisible inks:* These are colorless liquids that need heating and lighting in order to be read. For example, if onion juice and milk are used to write a message, the writing cannot be seen unless heat is applied, which makes the ink turn brown.
   - *Microdots:* This method shrinks a page-sized photograph to 1 mm in diameter. The photograph is reduced with the help of a reverse microscope.

10. Explain the process of echo data hiding.

    An echo is introduced into the original signal. Three properties of this echo can then be varied to hide data:

    - Initial amplitude
    - Decay rate
    - Offset

Chapter 1

Steganography

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

Students are introduced to steganography, the technique of hiding information using various formats, tools, and methods. The first portion of Chapter 1 explains methods used to employ steganography. Next the discussion transitions to cryptography and watermarking, noting differences and similarities. The final section is a long list of tools used to employ or detect steganography.

Chapter Objectives

- Understand steganography
- Recount the history of steganography
- Explain the classifications of steganography
- Identify image steganography
- Detect steganography
- Explain the differences between steganography and cryptography
- Explain stego-forensics
- Explain watermarking
- Select appropriate steganography tools

Teaching Tips

Introduction to Steganography

1. Introduce Steganography: the centuries-old practice of embedding hidden messages within a carrier medium.
2. Emphasize that in today's world, steganography is used broadly in digital form.
3. Modern steganography works by replacing bits of useless or unused data in regular computer files with bits of different, invisible information.
4. Steganography can also be used to supplement encryption.

Stegosystem Model

1. Define stegosystem: the mechanism used in performing steganography. It consists of the following components:
   a. Embedded message: the original secret message to be hidden behind the cover medium.
   b. Cover medium: the medium used to hide the message.
   c. Stego-key: the secret key used to encrypt and decrypt the message.
   d. Stego-medium: the combined cover medium and embedded message.

Application of Steganography

1. Discuss some of the purposes, both legal and illegal, for which steganography is used:
    a. Medical records: used to avoid mix-up of patients' records. Every patient has an EPR (electronic patient record), which has examinations and other medical records stored in it.
    b. Workplace communication: can be used as a method for employees who desire privacy in the workplace to bypass normal communication channels. This can be an obstacle to network security.
    c. Digital music: used to protect music from being copied by introducing subtle changes into a music file that act as a digital signature.
        i. BlueSpike Technology removes a few select tones in a narrow band.
        ii. Verance adds signals that are out of the frequency range detectable by the human ear.
        iii. Others adjust the sound by changing the frequency slightly. Digital audio files can also be modified to carry a large amount of information.
    d. Terrorism: extremist Web sites have been known to use pictures and text to secretly communicate messages to terrorist cells operating around the world.
    e. The movie industry: copyright protection for DVDs and VCDs. The DVD copy-protection program is designed to support a copy generation management system.

Teaching Tip	Some modern computer printers use steganography. These printers add barely visible tiny yellow dots to each page. The dots contain encoded printer serial numbers and date and time stamps.

Classification of Steganography

1. Point out the three major categories of steganography, each of which is examined further:
    a. Technical steganography.
    b. Linguistic steganography.
    c. Digital steganography.

Technical Steganography

1. Technical steganography is characterized by physical or chemical methods hiding the existence of a message. It can include the following:
    a. Invisible inks: liquids that need heating and lighting in order to be read.

   b. Microdots: shrinks a page-sized photograph to 1 mm in diameter with the help of a reverse microscope.

Linguistic Steganography

1. Linguistic steganography hides messages in the carrier in several ways, primarily semagrams and open codes.
2. Semagrams hide information through the use of signs or symbols:
   a. Visual semagrams: a drawing, painting, letter, music, or any other symbol is used to hide the information.
   b. Text semagrams: a message is hidden by changing the appearance of the carrier text. Text can be changed by modifying the font size, using extra spaces between words, or by using different flourishes in letters or handwritten text.
3. Open codes make use of openly readable text. The text contains words or sentences that can be hidden in a reversed or vertical order. The letters might be in selected locations of the text. Open codes can be either jargon codes or covered ciphers.
   a. Jargon codes: a language is used that can only be understood by a particular group of people while remaining meaningless to others. A jargon message is similar to a substitution cipher in many respects, but rather than replacing individual letters the words themselves are changed.
   b. Covered ciphers: hide the message in a carrier medium that is visible to everyone. Any person who knows how the message is hidden can extract this type of message. Covered ciphers can be both null and grill ciphers.
      i. Null ciphers: hide the message within a large amount of useless data. The original data may be mixed with the unused data in any order, but only the person who knows the order can understand it.
      ii. Grill ciphers: It is possible to encrypt plaintext by writing it onto a sheet of paper through a separate pierced sheet of paper or cardboard. When an identical pierced sheet is placed on the message, the original text can be read. The grill system is difficult to crack and decipher, as only the person with the grill can decipher the hidden message.

Digital Steganography

1. In digital steganography, secret messages are hidden in a digital medium. The techniques to examine:
   a. Injection
   b. Least significant bit (LSB)
   c. Transform-domain techniques
   d. Spread-spectrum encoding
   e. Perceptual masking
   f. File generation
   g. Statistical method
   h. Distortion technique

2. Injection: the secret information is placed inside a carrier or host file. The secret message is directly inserted into a host medium, which could be a picture, sound file, or video clip.
3. Least Significant Bit: the rightmost bit in the binary notation is substituted with a bit from the embedded message. The rightmost bit has the least impact on the binary data. If an attacker knows that this technique is used, then the data are vulnerable.
4. Transform-Domain Techniques: A transformed space is generated when a file is compressed at the time of transmission. This transformed space is used to hide data. The three transform techniques used when embedding a message are:
    a. discrete cosine transform (DCT).
    b. discrete Fourier transform (DFT).
    c. discrete wavelet transform (DWT).
5. Spread-spectrum encoding encodes a small-band signal into a wide-band cover. The encoder modulates a small-band signal over a carrier. It can be used in these ways:
    a. Direct sequence: information is divided into small parts that are allocated to the frequency channel of the spectrum. The data signal is combined during transmission with a higher data-rate bit sequence that divides the data based on the predetermined spread ratio. The redundant nature of the data-rate bit sequence code is useful to the signal-resist interference, allowing the original data to be recovered.
    b. Frequency hopping: used to divide the bandwidth's spectrum into many possible broadcast frequencies. Frequency hopping devices require less power and are cheaper, but are less reliable when compared to direct sequence spectrum systems.
6. Perceptual masking: the interference of one perceptual stimulus with another, resulting in a decrease in perceptual effectiveness. This type of steganography makes one signal hard to identify due to the presence of another signal.
7. File Generation: this technique generates a new cover file solely for the purpose of hiding data. A picture is created that has a hidden message in it.
8. Statistical Method: uses a one-bit steganographic scheme. It embeds one bit of information in a digital carrier, creating a statistical change. A statistical change in the cover is indicated as a 1. A 0 indicates that a bit was left unchanged. The work is based on the receiver's ability to differentiate between modified and unmodified covers.
9. Distortion Technique: creates a change in the cover object in order to hide the information. An encoder performs a sequence of modifications to the cover that corresponds to a secret message. The secret message is recovered by comparing the distorted cover with the original. The decoder needs access to the original cover file.

Digital File Types

1. Point out that techniques used in steganography are applied differently depending on the type of file that is being used to encode the message. Each is examined: text files, audio files, and video files.

Text Files

1. First, a look at the steganography methods used in text files:
    a. Open-space
    b. Syntactic
    c. Semantic
2. Open-Space Steganography: uses white space on the printed page. Three open-space methods:
    a. Intersentence spacing: encodes a binary message by inserting one or two spaces after every terminating character. An inefficient method, since more space is required for a small message and the white space can be easily spotted.
    b. End-of-line spacing: Secret data is placed at the end of a line in the form of spaces. This allows more room to insert a message but can create problems when the program automatically removes extra spaces or the document is printed as hard copy.
    c. Interword spacing: This method uses right justification, by which the justification spaces can be adjusted to allow binary encoding. A single space between words is 0, and two spaces is 1.
3. Syntactic Steganography: manipulates punctuation to hide messages. Punctuation marks can be used to hide the message.
4. Semantic Steganography: involves changing the words. Semantic steganography assigns two synonyms primary and secondary values. When decoded, the primary value is read as 1 and the secondary as 0.

Image Files

1. Highlight common image formats:
    a. Graphics Interchange Format (GIF): compressed image files that are based on a palette of 256 colors. They are mainly used for small icons and animated images since they do not have the color ranges needed for high-quality photos.
    b. Joint Photographic Experts Group (JPEG): JPEG files are the proper format for photo images that need to be small in size. JPEG files are compressed by 90%, or to one-tenth, of the size of the data.
    c. Tagged Image File Format (TIFF): The TIFF file format was designed to minimize the problems with mixed file formats. It was made as the standard image file format for image file exchange.
2. The following steganography techniques are used to hide a message in an image file:
    a. Least-significant-bit (LSB) insertion
    b. Masking and filtering
    c. Algorithms and transformation
3. Least-Significant-Bit Insertion: Using the LSB insertion method, the binary representation of the hidden data can be used to overwrite the LSB of each byte inside the image. If the image properties indicate that the image is 24-bit color, the net change is minimal and can be indiscernible to the human eye. Describe the LSB steps:
    a. The steganography tool makes a copy of an image palette with the help of the red, green, and blue (RGB) model.

   b. Each pixel of the eight-bit binary number LSB is substituted with one bit of the hidden message.
   c. A new RGB color in the copied palette is produced.
   d. With the new RGB color, the pixel is changed to an eight-bit binary number.

4. Masking and filtering techniques are commonly used on 24-bit and grayscale images. Masking images entails changing the luminescence of the masked area. The smaller the luminescent change, the less chance there is that it can be detected. Steganography images that are masked keep a higher fidelity rate than LSB through compression, cropping, and image processing.
5. Algorithms and Transformation: mathematical functions can be used to hide data that are in compression algorithms. In this technique, the data are embedded in the cover image by changing the coefficients of an image, (e.g., discrete cosine transform coefficients).

Audio Files

1. Note the various methods for hiding information in an audio file. It can be done by:
   a. Using LSB.
   b. Utilizing frequencies that are inaudible to the human ear, i.e., over 20,000 Hz.
   c. Using musical tones with a substitution scheme.
2. Low-Bit Encoding in Audio Files: replaces the LSB of information in each sampling point with a coded binary string. The low-bit method encodes large amounts of hidden data into an audio signal at the expense of producing significant noise in the upper frequency range.
3. Phase coding: involves substituting an initial audio segment with a reference phase that represents the data. This method is carried out using the following steps:
   a. The original sound sequence is shortened into segments.
   b. Each segment creates a matrix of the phase and magnitude by using the discrete Fourier transform (DFT) algorithm.
   c. The phase difference is calculated between each adjacent segment.
   d. New phase frames are created for all other segments.
   e. A new segment is created by combining the new phase and the original magnitude.
   f. These new segments are combined together to create the encoded output.
4. Spread Spectrum: direct-sequence spread spectrum (DSSS) introduces some random noise to the signal. The encoded data is spread across as much of the frequency spectrum as possible. Spread spectrum is used in audio files both to embed data in the audio file and to send the audio file.
5. Echo Data Hiding: an echo is introduced into the original signal.

Video Files

1. Explain that techniques used in audio and image files can also be used in video files, as video consists of audio and images. Discrete cosine transform (DCT) manipulation is used to add secret data at the time of the transformation process of the video. A large

number of secret messages can be hidden in video files because a video is a moving stream of images and sound. Due to this, an individual watching the video will not observe any distortion in the video caused by the hiding of data.

Steganographic File System

1. Describe the purpose of a steganographic file system. It provides a method to store files that encrypts and hides the data within those files. It hides the user's data in other, seemingly random files, allowing users to give names and passwords for some files while keeping others secret. Two methods can be utilized to construct a steganographic file system:
    a. Method 1:
        i. Program operates using a set of cover files with initially random content.
        ii. The cover files are modified to store data files.
        iii. Cover files should be large enough to ensure that all attempts to access cover files remain computationally infeasible.
    b. Method 2:
        i. File system begins with random data.
        ii. The encrypted blocks are written to the pseudorandom locations using the key acquired from the filename and directory password to hide the file blocks in random data. When the file system continues to be written to, collisions occur and the blocks are overwritten, allowing only a small portion of the disk space to be safely utilized.
        iii. Multiple copies of each block should be written.
        iv. A method to identify the blocks when they are overwritten is also required.

Cryptography

1. Introduce cryptography: the art of writing text or data in a secret code.
2. Cryptography involves encrypting plaintext data into an unreadable format called a ciphertext. This encryption process is based on mathematical algorithms that use a secret key for secure encryption.
3. The following are three types of cryptographic schemes used:
    a. Secret-key (or symmetric) cryptography.
    b. Public-key (or asymmetric) cryptography.
    c. Hash function.

Model of a Cryptosystem

1. A cryptosystem is a pair of algorithms that use a key to convert plaintext to ciphertext and back again.

Steganography Versus Cryptography

1. Contrast steganography with cryptography.
2. As noted, steganography hides data within other data. It replaces bits of unused data from various media files with other bits that, when assembled, reveal a hidden message. The hidden data might be plaintext, ciphertext, an audio clip, or an image.
3. In cryptography an encrypted message that is communicated can be detected but cannot be read. In steganography, the existence of the message is hidden.
4. Steganography is used to hide information when encryption is not a safe option. From a security point of view, steganography is used to hide a file in an encrypted format so even if the encrypted file is decrypted, the message will remain hidden.
5. Another contrast between steganography and cryptography is that the former requires caution when reusing pictures or sound files, while the latter requires caution when reusing keys. In steganography, only one key is used to hide and extract data. In cryptography, the same key or two different keys for encryption and decryption can be used.

Public Key Infrastructure (PKI)

1. Explain the purpose of PKI and its use of the public and private key pair.
2. Next, advise how PKI provides a digital certificate that can identify an individual or organization and directory services that can store and, when necessary, revoke the certificates.
3. Identify the components of PKI:
   a. A CA that issues and verifies the digital certificate.
   b. An RA that acts as the verifier for the certificate authority before a digital certificate is issued to a request.
   c. One or more directories where the certificates (with their public keys) are held.
   d. Key management protocols.
4. Clarify purpose of and differences between session key and master key.

Watermarking

1. Define digital watermarks: digital stamps embedded into digital signals. The digital stamp can contain many kinds of data, and can be both visible and invisible. Often, the digital data found hidden in a watermark are a digital multimedia object.

Application of Watermarking

1. Watermarking is used today to facilitate the following:
   a. Embedding copyright statements into images that provide authentication to the owner of the data.
   b. Monitoring and tracking copyright material automatically on the Web.
   c. Providing automatic audits of radio transmissions. These audits show any music or advertisement that is broadcasted.

   d. Supporting data augmentation. This enables users to add more information to the existing data present on the Web.
   e. Supporting fingerprint applications.

Steganography Versus Watermarking

1. Note these methods of differentiating steganography from watermarking:
   a. The main purpose of steganography is to hide a message m in data d to form new data D, which is different from d, so that a third person cannot detect the m in D. Conversely, the main purpose of watermarking is to hide the data m in data d to form new data D so that a third person cannot remove or replace the m in D.
   b. Steganography hides the message in one-to-one communication, while watermarking hides the message in one-to-many communication.
   c. The main goal of steganography is to protect the data from detection, while that of watermarking is to protect data from distortion by others.
   d. In steganography a message of any length can be hidden, whereas in watermarking only small messages can be hidden.
   e. Steganography is used for the purpose of secret communication, while watermarking is used for authentication and copyright protection.

Categories of Watermarks

1. Watermarks are split into two categories: visible and invisible.
   a. Visible: A visible watermark is the most robust as it is not part of the foundation of the image. The watermark's presence is clearly noticeable and often difficult to remove.
   b. Invisible: The main purpose of an invisible watermark is to identify and verify a particular piece of information in data. An invisible watermark is imperceptible but can be extracted through computational methods. An invisible watermark contains information about the watermark itself or the information present in the image that is hiding the data. The data hidden in the image can be accessed with a password, termed a watermark key.

Watermarks and Compression

1. Emphasize that watermarks in the modern world primarily concern images, audio, and video. They are used in the case of MP3s and DVDs as a tool to ensure copyrights are enforced.
2. Types of watermarks:
   a. Semifragile: used at the time of soft-image authentication and integrity verifications. They are robust to any common image processing of loose compression, but are fragile in case of any malicious tampering that changes the image content.

b. Fragile: less robust when modified. A small change in the content will destroy the embedded information and show that an attack has occurred. Any tampering with the image will modify its integrity.

c. Robust: can be either visible or invisible. Robust watermarks are resistant to any kind of attack and will not affect the quality of the data. They are difficult to remove or damage. Robust watermarks are used in the case of copyright protection and access control. Most of these are found on television broadcasts during which the channels impose their logos in the corner of the screen.

Digimarc's Digital Watermarking

1. Beaverton, Ore.-based Digimarc has developed digital watermarking tools that enable users to embed a digital code into an image, audio, video, or text file. The digital code is unnoticeable in normal use and can only be detected by computers and software.
2. Digimarc's digital watermarking is the method used to embed copyright messages into the image, video, and audio files that provide authentication to the owner of the data.

Attacks on Watermarking

1. Robustness Attack: attempts to remove watermarks from an image. It can be divided into the following categories:
    a. Signal-processing attacks: apply techniques such as compression, filtering, resizing, printing, and scanning to remove the watermark.
    b. Analytical and algorithmic attacks: use algorithmic techniques of watermark insertion and detection to remove the watermark from the image.
    c. Presentation attacks: carried out to change the watermarked data in such a way that a detector cannot detect it. The watermark will appear as it did before the attack. It is not necessary to eliminate the watermark to carry out the attack.
    d. Interpretation attacks: Interpretation attacks catch the weakness of watermarks, such as wrong and multiple interpretations. A watermark can be created from the existing watermark image with the same strength as the original watermark.
    e. Legal attacks: Legal attacks mainly target digital information and copyright laws. Attackers can change the watermarked copyrights in order to create doubts about copyright in a court of law.
2. Techniques commonly attempted to remove watermarks:
    a. Collusion attack: carried out by searching for a number of different objects having the same watermark, allowing the forensic investigator to isolate and remove the watermark by comparing the copies.
    b. Jitter attack: upsets the placement of the bits that identify a watermark by applying a jitter effect to the image. By applying a jitter effect, the forensic investigator is able to gauge the integrity of the watermark.
    c. StirMark: can be applied to small distortions that are designed to simulate the printing or scanning process. If a hard-copy photograph has been scanned, it would appear obvious that subtle distortions are introduced, no matter how careful the user is.

   d. Anti–soft bot: Soft bot searches and finds a watermarked image; it can use the information to determine if there is a copyright violation.
   e. Attacks on echo hiding: Echo hiding is resistant to jitter attacks, making a removal attack the usual method for getting rid of the watermark. In echo hiding, most echo delays are between 0.5 and 3 milliseconds; in anything above 3 milliseconds the echo becomes noticeable.

3. Mosaic Attack: works by splitting an image into multiple pieces and stitching them back together using JavaScript code. In this attack the marked image can be unmarked, and later all the pixels are rendered in a similar fashion to the original marked image.

Issues in Information Hiding

1. Emphasize that there are issues that must be weighed when hiding information. The following sections raise three of them:

Level of Visibility

1. The way a message is embedded will determine whether the data is perceptible or not. To reduce the theft of data, the presence of a watermark is often publicized. However, publicizing the presence of a watermark also allows various methods to be implemented to attempt to alter or disable the watermark. When the visibility of the data is increased, the potential for manipulation of the data also increases.

Robustness Versus Payload

1. In order to have a robust method of embedding a message, redundancy should be maintained to resist changes made to the cover. However, increasing the robustness of the message means that less space is usable for the payload.

File Format Dependence

1. Conversion of files that have lossless information to compressed files with lossy information can destroy the secret information present in the cover. Some processes embed the data depending on the file format of the carrier, while others do not depend on the file format. The JPEG compression algorithm uses floating-point calculations to translate the picture into an array of integers. This conversion process can result in rounding errors that may eliminate portions of the image. This process does not result in any noticeable difference in the image. Nevertheless, embedded data could become damaged.
2. Some other popular algorithms, namely Windows Bitmap (BMP) and Graphic Interchange Format (GIF), are considered lossless compressions. The compressed image is an exact representation of the original.

Detecting Steganography

1. Highlight signs that an investigator might notice that indicate a likeliness signs of steganography:
    a. Software clues on the computer:
        i. Filenames and Web sites viewed, according to the browser's cookies or history.
        ii. Registry key entries.
        iii. Mailbox and chat or instant messaging logs.
    b. Other program files: a nonprogram file may be a cover file that hides other files inside it.
    c. Multimedia files: large files in the system can be used as carrier files for steganography. A number of large duplicate files may suggest they are used as carrier files.

Detection Techniques

1. Discuss techniques used for detecting steganography:
    a. Statistical tests: compare statistical properties of two versions of an image.
    b. Stegdetect: detects the hidden content in images.
    c. Stegbreak: breaks the encoding password with the help of dictionary guessing.
    d. Visible noise: Attacks on hidden information can employ detection, extraction, and disabling or damaging hidden information. The images that have large payloads display distortions from the hidden data.
    e. Appended spaces and invisible characters: The presence of many white spaces is an indication of steganography.
    f. Color palettes: Some application characteristics are exclusive to steganography tools. Modifications in the color palettes create a detectable steganographic signature.

Detecting Text, Image, Audio, and Video Steganography

1. Point out the different methods that must be used to expose hidden information in different types of files.
    a. Text Files: alterations are made to the character positions. They can be detected by looking for text patterns or disturbances, the language used, and an unusual number of blank spaces.
    b. Image Files: The hidden data in an image can be detected by determining changes in size, file format, last modified time stamp, and color palette of the file.
        i. Statistical analysis on the LSB also can reveal difference between random values and real values.
    c. Audio Files: statistical analysis methods can be used for audio files since LSB modifications are also used on audio. Useful techniques:
        i. Scanning information for inaudible frequencies.
        ii. Determining odd distortions and patterns that show the existence of secret data.

   d. Video Files: detecting secret data in video files uses a combination of the methods used in image and audio files.

Teaching Tip	Hiding messages dates back to 440 B.C. Early examples were messages written on wood covered with wax, and an ink message on a slave's shaved head that became hidden when his hair grew out.

Steganalysis

1. Define steganalysis: the reverse process of steganography.
2. Steganalysis detects the encoded hidden message and, if possible, recovers that message. The messages are detected by verifying the differences between bit patterns and unusually large file sizes.
3. Steganography attacks are categorized by the following seven types:
   a. Stego-only attack: only the stego-medium is used to carry out the attack. The only way to avoid this attack is by detecting and extracting the embedded message.
   b. Known-cover attack: used with the presence of both a stego-medium and a cover medium. The attacker can compare both media and detect the format change.
   c. Known-message attack: presumes that the message and the stego-medium are present and the technique by which the message was embedded can be determined.
   d. Known-stego attack: the steganography algorithm is known, and the original object and the stego-objects are available.
   e. Chosen-stego attack: takes place when the forensic investigator generates a stego-medium from the message using a special tool.
   f. Chosen-message attack: The steganalyst obtains a stego-object from a steganography tool or algorithm of a chosen message.
   g. Disabling or active attacks: These attacks are categorized into the following six types:
      i. Blurring attacks can smooth transitions and reduce contrast by averaging the pixels next to the hard edges of defined lines and the areas where there are significant color transitions.
      ii. Noise reduction: random noise in the stego-medium inserts random-colored pixels into the image. The uniform noise inserts pixels and colors that look similar to the original pixels. Noise reduction decreases the noise in the image by adjusting the colors and averaging the pixel values.
      iii. Sharpening is the opposite of the blurring effect. It increases the contrast between the adjacent pixels where there are significant color contrasts that are usually at the edge of objects.
      iv. Rotation moves the stego-medium to give its center a point.
      v. Resampling involves interpolation. It is used to reduce the raggedness associated with the stego-medium and normally is used to resize the image.

vi. Softening of the stego-medium applies a uniform blur to an image in order to smooth edges and reduce contrasts. It causes less distortion than blurring.

Stego-Forensics

1. As steganography applies to computer forensics, “stego-forensics” is the area of forensic science dealing with steganography techniques to investigate a source or cause of a crime.

Tools

1. The remainder of the chapter introduces and reviews multiple steganographic tools. It is important to note that these tools are available to law enforcement and forensic investigators, but also to potential cyber-criminals.

2Mosaic

1. 2Mosaic: a small, command-line utility for Windows that will break apart any JPEG file and generate the HTML code needed to reconstruct the picture.

BlindSide

1. BlindSide: can hide files of any file type within a Windows bitmap image. The original and the encoded image look identical to the human eye. However, when the image is executed through BlindSide, the concealed data can be extracted and retrieved. For added security, the data can be scrambled with a password so that no one will be able to access the data.

S-Tools

1. S-Tools can hide multiple files within a single object. It first compresses the individual files, which are stored with their names, and then it inserts filler on the front of the data to prevent two identical sets of files from encrypting in the same way. All files are then encrypted using the passphrase that the user generates.

StegHide

1. StegHide is able to hide information in images and audio files without changing the color or frequencies. Features include compression of the embedded data, encryption of the embedded information, and automatic integrity checking using a checksum. JPEG, BMP, and WAV file formats are supported for use as a cover file.

Snow

1. Snow is a steganography tool that exploits the nature of white space by appending it to the end of lines in ASCII text to conceal messages. It is, however, susceptible to detection by applications such as Word.

Camera/Shy

1. Camera/Shy is a simple steganography tool that allows users to encrypt information and hide it in standard GIF images. Camera/Shy is embedded in a Web browser. Other programs require users to know beforehand that an image contains embedded content. Camera/Shy however, allows users to check images for embedded messages, read them, and embed their own return messages with the click of a mouse. The Camera/Shy program allows Internet users to conceal information, viruses, or exploitative software inside graphics files on Web pages.

Steganos

1. Steganos combines cryptography and steganography to hide information. It first encrypts the information and then hides it in a file formatted as BMP, VOC, WAV, or ASCII. With Steganos, a user can store a file with a copyright and prove ownership of a picture if someone tries to use it.

Gifshuffle

1. Gifshuffle hides messages inside GIF images by mixing up the colors within the images so that it is difficult to find the original message. It supports GIF images that have features such as transparency and animation. Gifshuffle compresses the message using Huffman tables.

JPHS

1. JPHS hides files in JPEG format. For a typical visual image and a low insertion rate of up to 5%, it is nearly impossible for someone to detect that a JPEG file processed with this tool contains hidden data.

OutGuess

1. OutGuess is a steganography tool that inserts hidden information into redundant bits of data sources. During extraction, the redundant bits are extracted and written back after modification. It PNM and JPEG images. Before hiding the data, OutGuess determines the size of the hidden data and maintains the statistics. Due to this, statistical tests based on frequency counts are unable to detect the presence of steganographic content.

Invisible Secrets 4

1. Invisible Secrets 4 supports both cryptography and steganography. It first encrypts the message and then hides it behind a variety of files. The user can directly encrypt and hide files from Windows Explorer and transfer them over the Internet via e-mail. Invisible Secrets 4 can hide information behind JPEG, PNG, BMP, HTML, and WAV files. Notable features:
    a. Helps to hide files encrypt files, destroy Internet traces, shred files, make secure IP-to-IP password transfers, and even lock any application on a computer.
    b. Supports password management solutions that store all passwords.
    c. Supports a shredder that destroys files, folders, and Internet traces beyond recovery.
    d. Has a locker that allows password protection for certain applications.
    e. Creates self-decrypting packages that can be mailed over the Internet.
    f. Helps transfer passwords securely over the Internet.

Masker

1. Masker provides strong security for data. It encrypts files and hides files behind image, video, program, or sound files. The cover file remains functional, so a sound or video file can be played without causing suspicion.

Data Stash

1. Data Stash can use any large bitmap or database file as the cover file and use drag-and-drop to select the files to be hidden. The carrier file remains active. This tool supports password protection, with the help of Blowfish encryption.

StegaNote

1. StegaNote uses cryptosecure steganography that mixes up the compressed file and text from a text editor with the cover file, rendering it invisible to the human eye. It uses RPP to hide data in image files.

Stegomagic

1. Stegomagic uses text, WAV, 24-bit BMP, and 256-color BMP files to hide data. The size of the cover file remains the same except in the case of text files. Data is encrypted and protected with a password using the DES algorithm and it is subsequently hidden behind the cover file. It supports all Microsoft Windows environments.

Hermetic Stego

1. Hermetic Stego hides data files in either a single image or a set of BMP images. Valuable features:
    a. It can hide data of any type and any size.
    b. The bits of data are inserted into the bytes of image files, making it impossible to crack.
    c. Data can be transported with or without the stego-key, which encrypts the data.

StegParty

1. StegParty is a system for hiding information inside plaintext files. Unlike similar tools currently available, it does not use random gibberish to encode data. Instead, it relies on small alterations, like changes in spelling and punctuation, to the message.

Stego Suite

1. Stego Suite is a tool for blind steganography detection: the ability to identify the presence of steganography without prior knowledge of the steganography algorithm that might have been used against the target file.
2. Stego Suite is four tools:
    a. StegoHunter: designed to quickly, accurately, and easily detect steganography programs as a first step in the investigation process. With Stego Hunter, results are easily reported to the investigator of any installed or even previously installed applications. The suspected carrier types are flagged to further the investigation process. Forensic images of other popular forensic tools such as EnCase, FTK, dd, and Safeback can be scanned.
    b. StegoWatch: allows users to detect digital steganography and can use a dictionary attack to extract information that has been embedded with some of the most popular steganography tools.
    c. StegoAnalyst: a full-featured imaging and analysis tool. It allows investigators to search for visual clues that steganography has, in fact, been utilized in both image and audio files.
    d. StegoBreak: a built-in utility designed to obtain the passphrase that has been used on a file found to contain steganography

.

StegSpy

1. StegSpy detects steganography and the program used to hide the message. It also identifies the location of the hidden content. StegSpy currently can identify these programs:
    a. Hiderman
    b. JPHS
    c. Masker
    d. JPegX
    e. Invisible Secrets

WNSTORM

1. WNSTORM hides files within PCX images. A user can take the PCX image containing the hidden data and send it to any source. Only the sender and the one whom the password is shared with can get at the hidden data file.

Xidie

1. Xidie enables the user to hide and encrypt files within other files. It can encrypt sensitive information while simultaneously hiding it in a file that will not look suspicious. The carrier files are fully functional and almost identical to the original files. Include options such as encrypt and burn, hide and burn, encrypt and mail, and hide and mail.

CryptArkan

1. CryptArkan encrypts and hides data files and directories inside one or more container files. Hidden data can be directly read off an audio CD. Includes these functions:
    a. Encrypts data files to be hidden.
    b. Hides data files in multiple container files.
    c. Can hide whole directories, preserving subdirectory structure.
    d. Can use different hiding methods for separate container files.
    e. Uses different amounts of the original container file for data.

Stealth Files

1. Stealth Files takes a PGP 2.x encrypted message and strips any standard headers off to ensure that the result looks like random noise. If the PGP random number generators are secure, and if IDEA and RSA (RSA when normalized) produce good-quality random numbers, the result should look like white noise and stand up to analysis as being indistinguishable from white noise. Stealth Files can also be used to produce random numbers.

Camouflage

1. Camouflage allows the user to hide files by scrambling them and attaching them to a carrier file. A camouflaged file behaves like a normal file and can be stored, used, or e-mailed without attracting attention. It can be password protected for additional security.

CryptoBola JPEG

1. CryptoBola JPEG stores only the ciphertext without any additional information like filename, type, or length. It determines which parts (bits) of the JPEG-encoded data play the least significant role in the reproduction of the image and replaces those bits

with the bits of the ciphertext. The plaintext can be any data file or it can be entered in edit mode directly before the actual embedding takes place.

Steganosaurus

1. Steganosaurus is a plaintext steganography utility that encodes a binary file as gibberish text. Encoding is based on either a spelling dictionary or words taken from a text document.

Additional Resources

1. Gary Kessler, professor of Homeland Security at Embry-Riddle Aeronautical University in Daytona Beach, Florida, wrote "An Overview of Steganography for the Computer Forensics Examiner." See the 2015 version at: http://www.garykessler.net/library/fsc_stego.html

2. Three authors from the Warsaw University of Technology, Institute of Telecommunications in Warsaw, Poland, have written "Development Trends in Steganography." Read it at: http://arxiv.org/ftp/arxiv/papers/1202/1202.5289.pdf

3. The Computer Forensics, Cybercrime and Steganography Resources site includes links to dozens of steganography publication, papers, and resources. See: http://data-hiding.com/

Key Terms

- **Cover medium** the medium used to hide a message with steganography
- **Digital watermark** a digital stamp embedded into a digital signal
- **Least significant bit (LSB)** a steganography technique in which the rightmost bit in the binary notation is substituted with a bit from the embedded message
- **Steganography** the practice of embedding hidden messages within a carrier medium
- **Stego-key** the secret key used to encrypt and decrypt messages hidden by steganography
- **Stego-medium** the combined cover medium and embedded message used in steganography
- **Stegosystem** the mechanism used in performing steganography