1 Introduction

A woman named Alice sends the following e-mail to her friend Bob, with whom she shares an interest in astronomy:

My friend Bob,
until yesterday I was using binoculars for stargazing. Today, I decided to try my new telescope. The galaxies in Leo and Ursa Major were unbelievable! Next, I plan to check out some nebulas and then prepare to take a few snapshots of the new comet. Although I am satisfied with the telescope, I think I need to purchase light pollution filters to block the xenon lights from a nearby highway to improve the quality of my pictures.
Cheers,
Alice.

At first glance, this letter appears to be a conversation between two avid amateur astronomers. Alice seems to be excited about her new telescope and eagerly shares her experience with Bob. In reality, however, Alice is a spy and Bob is her superior awaiting critical news from his secret agent. To avoid drawing unwanted attention, they decided not to use cryptography to communicate in secrecy. Instead, they agreed on another form of secret communication – steganography.

Upon receiving the letter from Alice, Bob suspects that Alice might be using steganography and decides to follow a prearranged protocol. Bob starts by listing the first letters of all words from Alice's letter and obtains the following sequence:

$$mfbuyiwubfstidttmnttgilaumwuniptcosnatpttafsotncaiaswttitintplpftbt$$
$$xlfanhtitqompca.$$

Then, he writes down the decimal expansion of π

$$\pi = 3.141592653589793\ldots$$

and reads the message from the extracted sequence of letters by putting down the third letter in the sequence, then the next first letter, the next fourth letter, etc. The resulting message is

$$buubdlupnpsspx.$$

Finally, Bob replaces each letter with the letter that precedes it in the alphabet and deciphers the secret message

$$attack\ tomorrow.$$

Let us take a look at the tasks that Alice needs to carry out to communicate secretly with Bob. She first encrypts her message by substituting each letter with the one that follows it in the English alphabet (e.g., a is substituted with b, b with c, ..., and z with a). Note that this simple substitution cipher could be replaced by a more secure encryption algorithm if desired. Then, Alice needs to write an almost arbitrary but meaningful(!) letter while making sure that the words whose location is determined by the digits of π start with the letters of the encrypted message. Of course, instead of the decimal expansion of π, Alice and Bob could have agreed on a different integer sequence, such as one generated from a pseudo-random number generator seeded with a shared key. The shared information that determines the location of the message letters is called the steganographic key or stego key. Without knowing this key, it is not only difficult to read the message but also difficult for an eavesdropper to prove that the text contains a secret message.

Note that the hidden message is unrelated to the content of the letter, which only serves as a decoy or "cover" to hide the very fact that a secret message is being sent. In fact, this is the defining property of steganography:

Steganography can be informally defined as the practice of undetectably communicating a message in a cover object.

We now elaborate on the above motivational example a little more. If Alice planned to send a very long message, the above steganographic method would not be very practical. Instead of hiding the message in the body of the e-mail using her creative writing skills, Alice could hide her message by slightly modifying pixels in a digital picture, such as an image of a galaxy taken through her telescope, and attach the modified image to her e-mail. Of course, that would require a different hiding procedure shared with Bob. A simple method to hide a binary message would be to encode the message bits into the colors of individual pixels in the image so that even values represent a binary 0 and odd values a binary 1. Alice could achieve this by modifying each color by at most one. Here, Alice relies on the fact that such small modifications will likely be imperceptible. This method of covert communication allows Alice to send as many bits as there are pixels in the image without the need to painstakingly form a plausible-looking cover letter. She could even program a computer to insert the message, which could be an arbitrary electronic file, into the image for her.

Digital images acquired using a digital camera or scanner provide a friendly environment to the steganographer because they contain a slight amount of noise that helps mask the modifications that need to be carried out to embed a secret message. Moreover, attaching an image to an e-mail message is commonly done and thus should not be suspicious.

This book deals with steganography of signals represented in digital form, such as digital images, audio, or video. Although the book focuses solely on images, many principles and methods can be adopted to the other multimedia objects.

1.1 Steganography throughout history

The word *steganography* is a composite of the Greek words *steganos*, which means "covered," and *graphia*, which means "writing." In other words, steganography is the art of concealed communication where the very existence of a message is secret. The term steganography was used for the first time by Johannes Trithemius (1462–1516) in his trilogy *Polygraphia* and in *Steganographia* (see Figure 1.1). While the first two volumes described ancient methods for encoding messages (cryptography), the third volume (1499) appeared to deal with occult powers, black magic, and methods for communication with spirits. The volume was published in Frankfurt in 1606 and in 1609 the Catholic Church put it on the list of "*libri prohibiti*" (forbidden books). Soon, scholars began suspecting that the book was a code and attempted to decipher the mystery. Efforts to decode the book's secret message came to a successful end in 1996 and 1998 when two researchers independently [65, 201] revealed the hidden messages encoded in numbers through several look-up tables included in the book [145]. The messages turned out to be quite mundane. The first one was the Latin equivalent of "The quick brown fox jumps over the lazy dog," which is a sentence that contains every letter of the alphabet. The second message was: "The bearer of this letter is a rogue and a thief. Guard yourself against him. He wants to do something to you." Finally, the third was the start of the 21st Psalm.

The first written evidence about steganography being used to send messages is due to Herodotus [109], who tells of a slave sent by his master, Histiæus, to the Ionian city of Miletus with a secret message tattooed on his scalp. After the tattooing of the message, the slave grew his hair back in order to conceal the message. He then traveled to Miletus and, upon arriving, shaved his head to reveal the message to the city's regent, Aristagoras. The message encouraged Aristagoras to start a revolt against the Persian king.

Herodotus also documented the story of Demeratus, who used steganography to alert Sparta about the planned invasion of Greece by the Persian Great King Xerxes. To conceal his message, Demeratus scraped the wax off the surface of a wooden writing tablet, scratched the message into the wood, and then coated the tablet with a fresh layer of wax to make it appear to be a regular blank writing tablet that could be safely carried to Sparta without arousing suspicion.

Aeneas the Tactician [226] is credited with inventing many ingenious steganographic techniques, such as hiding messages in women's earrings or using pigeons to deliver secret messages. Additionally, he described some simple methods for hiding messages in text by modifying the height of letter strokes or by marking letters in a text using small holes.

Hiding messages in text is called linguistic steganography or acrostics. Acrostics was a very popular ancient steganographic method. To embed a unique "signature" in their work, some poets encoded secret messages as initial letters of sentences or successive tercets in a poem. One of the best-known examples

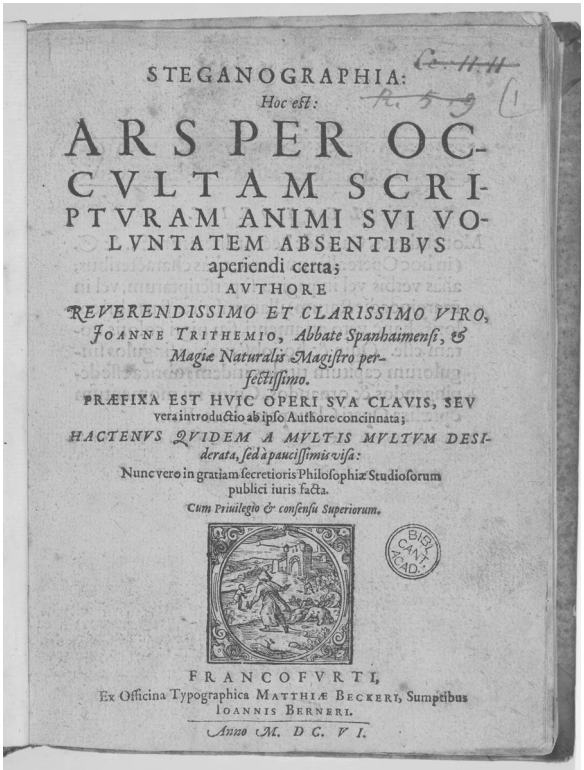
STEGANOGRAPHIA:
Hoc est:
ARS PER OC-
CVLTAM SCRI-
PTVRAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
JOANNE TRITHEMIO, Abbate Spanhaimenſi, &
Magiæ Naturalis Magiſtro per-
fectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DESI-
derata, ſed à pauciſſimis viſa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
FRANCOFVRTI,
Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus
IOANNIS BERNERI.
Anno M. D C. V I.

Figure 1.1 The title page of *Steganographia* by Johannes Trithemius, the inventor of the word "steganography." Reproduced by kind permission of the Syndics of Cambridge University Library.

is *Amorosa visione* by Giovanni Boccaccio [247]. Boccaccio encoded three sonnets (more than 1500 letters) into the initial letters of the first verse of each tercet from other poems. The linguistic steganographic scheme described at the beginning of this chapter is an example of Cardan's Grille, which was originally conceived in China and reinvented by Cardan (1501–1576). The letters of the secret message form a random pattern that can be accessed simply by placing a mask over the text. The mask plays the role of a secret stego key that has to be shared between the communicating parties.

Francis Bacon [15] described a precursor of modern steganographic schemes. Bacon realized that by using italic or normal fonts, one could encode binary representation of letters in his works. Five letters of the cover object could hold five bits and thus one letter of the alphabet. The inconsistency of sixteenth-century typography made this method relatively inconspicuous.

A modern version of this steganographic principle was described by Brassil [29]. He described a method for data hiding in text documents by slightly shifting the lines of text up or down by 1/300 of an inch. It turns out that such subtle changes are not visually perceptible, yet they are robust enough to survive photocopying.

This way, the message could be extracted even from printed or photocopied documents.

In 1857, Brewster [31] proposed a very ingenious technique that was actually used in several wars in the nineteenth and twentieth centuries. The idea is to shrink the message so much that it starts resembling specks of dirt but can still be read under high magnification. The technological obstacles to use of this idea in practice were overcome by the French photographer Dragon, who developed technology for shrinking text to microscopic dimensions. Such small objects could be easily hidden in nostrils, ears, or under fingernails [224]. In World War I, the Germans used such "microdots" hidden in corners of postcards slit open with a knife and resealed with starch. The modern twentieth-century microdots could hold up to one page of text and even contain photographs. The Allies discovered the usage of microdots in 1941. A modern version of the concept of the microdot was recently proposed for hiding information in DNA for the purpose of tagging important genetic material [45, 212]. Microdots in the form of dust were also recently proposed to identify car parts [1].

Perhaps the best-known form of steganography is writing with invisible ink. The first invisible inks were organic liquids, such as milk, urine, vinegar, diluted honey, or sugar solution. Messages written with such ink were invisible once the paper had dried. To make them perceptible, the letter was simply heated up above a candle. Later, more sophisticated versions were invented by replacing the message-extraction algorithm with safer alternatives, such as using ultraviolet light.

In 1966, an inventive and impromptu steganographic method enabled a prisoner of war, Commander Jeremiah Denton, to secretly communicate one word when he was forced by his Vietnamese captors to give an interview on TV. Knowing that he could not say anything critical of his captors, as he spoke, he blinked his eyes in Morse code, spelling out T-O-R-T-U-R-E.

Steganography became the subject of a dispute during the match between Viktor Korchnoi and Anatoly Karpov for the World Championship in chess in 1978 [117]. During one of the games, Karpov's assistants handed him a tray with yogurt. This was technically against the rules, which prohibited contact between the player and his team during play. The head of Korchnoi's delegation, Petra Leeuwerik, immediately protested, arguing that Karpov's team could be passing him secret messages. For example, a violet yogurt could mean that Karpov should offer a draw, while a sliced mango could inform the player that he should decline a draw. The time of serving the food could also be used to send additional messages (steganography in timing channels). This protest, which was a consequence of the extreme paranoia that dominated chess matches during the Cold War, was taken quite seriously. The officials limited Karpov to consumption of only one type of yogurt (violet) at a fixed time during the game. Using the terminology of this book, we can interpret this protective measure as an act of an active warden to prevent usage of steganography.

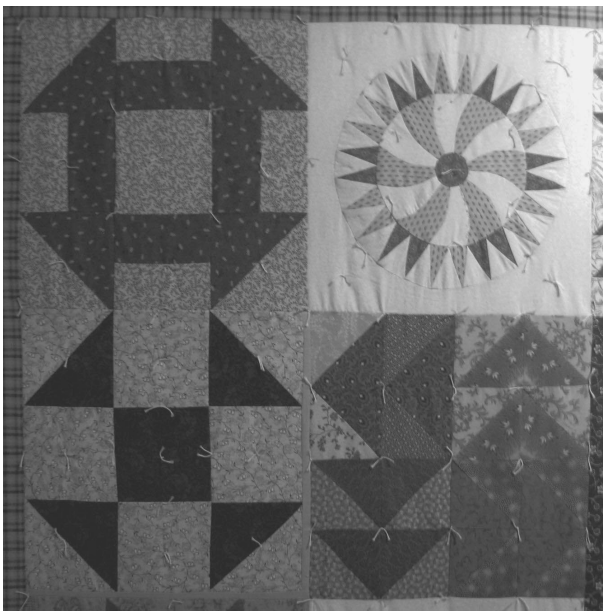

Figure 1.2 Symbols on an American patchwork quilt on display at the National Cryptologic Museum near Washington, D.C.

In the 1990s, the story of a "quilt code" allegedly used in the Underground Railroad surfaced in the media. The Underground Railroad appeared spontaneously as a clandestine network of secret pathways and safe houses that helped black slaves in the USA escape from slavery during the first part of the nineteenth century. According to the story told by a South Carolina woman named Ozella Williams [230], people sympathetic to the cause displayed quilts on their fences to non-verbally inform the escapees about the direction of their journey or which action they should take next. The messages were supposedly hidden in the geometrical patterns commonly found in American patchwork quilts (see Figure 1.2). Since it was common to air quilts on fences, the master or mistress would not be suspicious about the quilts being on display.

The recent explosion of interest in steganography is due to a rather sudden and widespread use of digital media as well as the rapid expansion of the Internet (Figure 1.3 shows the annual count of research articles on the subject of steganography published by the IEEE). It is now a common practice to share pictures, video, and sound with our friends and family. Such objects provide a very favorable environment for concealing secret messages for one good reason: typical digital media files consist of a large number of individual samples (e.g., pixels) that can be imperceptibly modified to encode a secret message. And there is no need to develop technical expertise for those who wish to use steganography because the hiding process itself can be carried out by a computer program that anyone can download from the Internet for free. As of writing this book in late 2008, one can

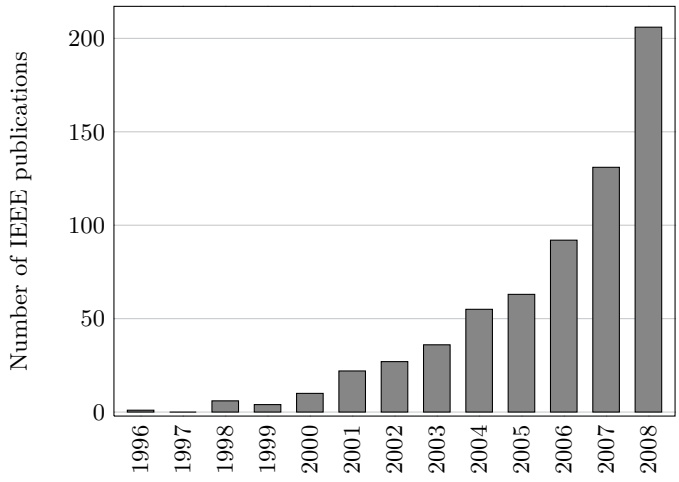

Figure 1.3 The growth of the field is witnessed by the number of articles annually published by IEEE that contain the keywords "steganography" or "steganalysis."

select from several hundreds of steganographic products available on the Internet. Figure 1.4 shows the number of newly released applications or new versions of existing programs capable of hiding data in digital media and text. Some software applications that focus on security, privacy, and anonymity offer the possibility to hide encrypted messages in pictures and music as an additional layer of protection. Examples of such programs are Steganos (`http://www.steganos.com/`) and Stealthencrypt (`http://www.stealthencrypt.com/`). An updated list of selected currently available steganographic programs for various platforms can be obtained from `http://www.stegoarchive.com/`.

In the next section, the reader is informally introduced to some key concepts and principles on which modern steganography is built. The author also feels that it is important at this point to explain the differences between steganography and other related privacy and security applications, such as cryptography and digital watermarking. No attempt is made at this point to be rigorous. The goal is to entice the reader and gently introduce some of the challenges elaborated upon in this book.

1.2 Modern steganography

Because electronic communication is very susceptible to eavesdropping and malicious interventions, the issues of security and privacy are more relevant today than ever. Traditional solutions are based on cryptography [207], which is a mature, well-developed field with rigorous mathematical foundations. The cryptographic approach to privacy is to make the exchanged information unreadable to those who do not have the right decryption key. When an encrypted message

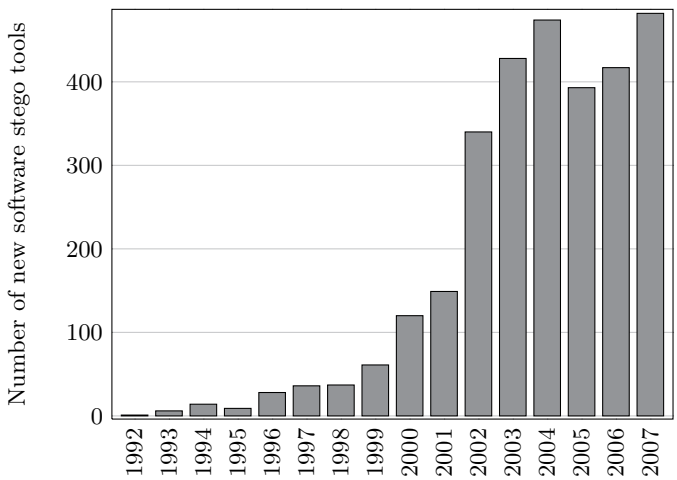

Figure 1.4 The number of newly released steganographic software applications or new versions per year. Adapted from [122] and reprinted with permission of John Wiley & Sons, Inc.

is intercepted, even though the content of the message is protected, the fact that the subjects are communicating secretly is obvious. In some situations, it may be important to avoid drawing attention and instead embed sensitive data in other objects so that the fact that secret information is being sent is not obvious in the first place. This is the approach taken by steganography.

Every steganographic system discussed in this book consists of two basic components – the embedding and extraction algorithms. The embedding algorithm accepts three inputs – the secret message to be communicated, the secret shared key that controls the embedding and extraction algorithms, and the *cover object*, which will be modified to convey the message. The output of the embedding algorithm is called the *stego object*. When the stego object is presented as an input to the message-extraction algorithm, it produces the secret message.

Steganography offers a feasible alternative to encryption in oppressive regimes where using cryptography might attract unwanted attention or in countries where the use of cryptography is legally prohibited. An interesting documented use of steganography was presented at the 4th International Workshop on Information Hiding [209]. Two subjects developed a steganographic scheme of their own to hide messages in uncompressed digital images and then used it successfully for several years when one of them was residing in a hostile country that explicitly prohibited use of encryption. The reason for their paranoia was a story told by their friend who already resided in the area, who had tried to send an encrypted e-mail only to have it returned to him by the local Internet service provider with the message appended, "Please, don't send encrypted emails – we can't read them."

In the early 1980s, Simmons [214] described intriguing political implications of the possibility to send data through a covert communication channel. According to the disarmament treaty SALT, the USA and Soviet Union mutually agreed to equip their nuclear facilities with sensors that would inform the other country about the number of missiles but not some other information, such as their location. All communications were required to be protected using standard digital signatures to prevent unauthorized modification of the sensors' readings. However, both sides quickly became concerned about the possibility to hide additional information through so-called subliminal channels that existed in most digital signature schemes at that time. This triggered research into developing digital signatures free of subliminal channels [57].

1.2.1 The prisoners' problem

The most important property of a steganographic system is undetectability, which means that it should be impossible for an eavesdropper to tell whether Alice and Bob are engaging in regular communication or are using steganography. Simmons provided a popular formulation of the steganography problem through his famous prisoners' problem [214]. Alice and Bob are imprisoned in separate cells and want to hatch an escape plan. They are allowed to communicate but their communication is monitored by warden Eve. If Eve finds out that the prisoners are secretly exchanging messages, she will cut the communication channel and throw them into solitary confinement. The prisoners resort to steganography as a means to exchange the details of their escape. Note that in the prisoners' problem, all that Eve needs to achieve is to detect the presence of secret messages rather than know their content. In other words, when Eve discovers that Alice and Bob communicate secretly, the steganographic system is considered broken. This is in contrast to encryption, where a successful attack means that the attacker gains access to the decrypted content or partially recovers the encryption key.

In the prisoners' problem, it is usually assumed that Eve has a complete knowledge of the steganographic algorithm that Alice and Bob might use, with the exception of the secret stego key, which Alice and Bob agreed upon before imprisonment. The requirement that the steganographic algorithm be known to Eve is Kerckhoffs' principle imported from cryptography. This seemingly strong and paranoid principle states that the security of the communication should not lie in the secrecy of the system but only in the secret key. The principle stems from many years of experience that taught us that through espionage the encryption (steganographic) algorithm or device may fall into the hands of the enemy and, if this happens, the security of the secret channel should not be compromised.

1.2.2 Steganalysis is the warden's job

Steganography is a privacy tool and as such it naturally provokes the human mind to attack it. The effort concerned with developing methods for detecting the presence of secret messages and eventually extracting them is called *steganalysis*. Positioning herself into the role of a *passive warden*, Eve passively monitors the communication between Alice and Bob. She is not only allowed to visually inspect the exchanged text or images, but also can apply some statistical tests to find out whether the distribution of colors in the image follows the expected statistics of natural images.

This field started developing more rapidly after the terrorist attacks of September 11, 2001, when speculations spread through the Internet that terrorists might use steganography for planning attacks [146, 48]. The only publicly documented use of a rather primitive form of steganography for planning terrorist activities was described by *The New York Times* in an article from November 11, 2006. Dhiren Barot, an Al Qaeda operative, filmed reconnaissance video between Broadway and South Street and concealed it before distribution by splicing it into a copy of the Bruce Willis movie *Die Hard: With a Vengeance*. In a different criminal case in 2000, the commercial steganographic tool S-Tools had been used for distribution of child porn.[1] The suspect was successfully prosecuted using steganalysis methods published in [119].

As we already know, steganography is considered broken even when the mere *presence* of the secret message is detected. This is because the primary goal of steganography is to conceal the communication itself. Often, identifying the subjects who are communicating using steganography can be of vital importance despite the fact that the content of the secret message may still be unknown. When the warden discovers the use of steganography, she may choose to cut the communication channel, if such an act is in her power, as in the prisoners' problem, or she may exercise other options. Eve may assume the role of an *active warden* and slightly modify the communicated objects to prevent the prisoners from using steganography. For example, if the prisoners are embedding messages in images, the warden may process the images by slightly resizing them, cropping, and recompressing in hope of preventing the recipient from reading any secret messages. She can also rephrase the content of a letter using synonyms or by changing the order of words in a sentence. During World War I, US Post Office censors used to rephrase telegrams to prevent people from sending hidden messages. In one case, the censor replaced the text "father is dead" with "father is deceased," which prompted the recipient to reply with "is father dead or deceased?" A more recent example of an active warden was given by Gina Fisk and her coworkers from Los Alamos National Laboratory [72], who described an active warden system integrated with a firewall designed to eliminate covert channels in network protocols.

[1] Personal communication by Neil F. Johnson, 2007.