Importance of Integrating Cryptography, Steganography, and Digital Watermarking for Undergraduate Curriculum

Biju Bajracharya and David Hua

Ball State University

bajracharya@bsu.edu; dhua@bsu.edu

Abstract

Cryptography is the art of obscuring information by scrambling the content of a file. Steganography, the art of information concealing information, embeds secret information into an unsuspicious carrier document without revealing its presence. Watermarking, a subarea under steganography, embeds copyright information into a document. The goal of both cryptography and steganography is to protect a message from falling into the hands of unintended third parties. The goal of watermarking is to assert copyright to protect intellectual property.

All of these technologies are advancing rapidly. Scientists and researchers are developing more secure and efficient ways to achieve its goals. At the same time, hackers, malvertisers (web advertisers that have hidden and mischievous malwares), and criminals are continuing their efforts to exploit the capabilities of cryptography and steganography for criminal intent. Criminals increasingly use these technologies for information stealing, leaking, malvertising, and intellectual rights violations.

The shortage of trained professionals has resulted in a surge in the demand for people with these skills. The issue is that academic institutions provide limited training in the field. The course content may only contain a few paragraphs or chapters. This paper presents the importance of these technologies and the need for it to be its own course. A whole course would promote a deeper understanding of these technologies needed for careers in cybersecurity.

Introduction

The rapid growth of the Internet by industry, government, researchers, and the public has generated vast amounts of data exchanged for things like communications, data sharing, and storage. While this data exchange traverses the Internet, it needs to be protected from unauthorized access. This may only be possible by concealing it either explicitly or implicitly by using innocuous carrier information.

Concealing it explicitly requires it to be transformed into unreadable and garbled content using encryption methods before transmitting data online. Once it reaches its destination, it needs to be converted back into a readable format using decryption. The process of encryption and decryption is called cryptography. An encrypted file is considered to be concealing its information explicitly because the content of the file cannot be read by anyone who does not have the encryption key needed to decrypt, or unscramble, the file. However, obtaining encryption key from any other means other than the original encrypting or authorized body is exploitation of weak encryption method.

Alternatively, information can be implicitly concealed by hiding it within an otherwise readable or viewable file. The information is transformed in such a way that it is unexposed and invisible during its transmission, which is possible only if it is carried inside another regular message called a carrier message. The intent of implicitly concealing information is to avoid the notice or suspicion of unintended parties by embedding the information in an otherwise innocuous file. Commonly used carrier messages include image, audio, video, and text files. Two methods that use carrier messages, also called cover medium, to conceal data are called steganography and digital watermarking. These strategies for data hiding can be categorized as follows:

a) Implicit Data Hiding
  i) Steganography and
  ii) Digital Watermarking
b) Explicit Data Hiding
  i) Cryptography

Steganography techniques are based on information hiding that embeds secret messages in another cover medium without revealing its existence. Only the sender and receiver of the file are aware of the presence of the data hidden within the file. For example, an individual trying to arrange a covert meeting may hide a text-based message within an image file of the Grand Canyon. In watermarking, data is hidden to convey some information about the cover medium, such as ownership and copyright. Cryptography techniques are based on rendering the content of a message unreadable to unauthorized people. Figure 1 exhibits the differences and similarities between steganography, watermarking and cryptography (Djebbar, Ayad, Meraim, & Hamam, 2012).

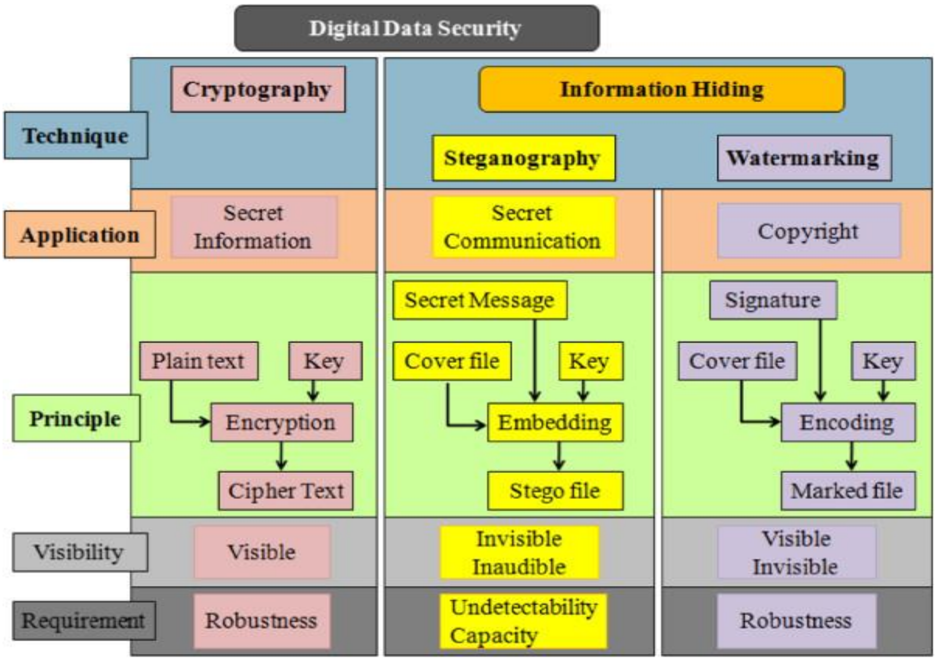

Figure 1: Digital Data Security Disciplines (Djebbar et al., 2012)

Steganography and Watermarking

Steganography is the ancient art of embedding private messages in seemingly innocuous messages in such a way that prevents the detection of the secret messages by a third party. In other words, steganography means establishing covert channels. A covert channel is a secret communication channel used for transmitting information. The other major area of steganography is copyright marking. This is when the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting. As shown in Figure 2, two general directions can be distinguished within steganography: protection against detection and protection against removal (Popa, 1998).

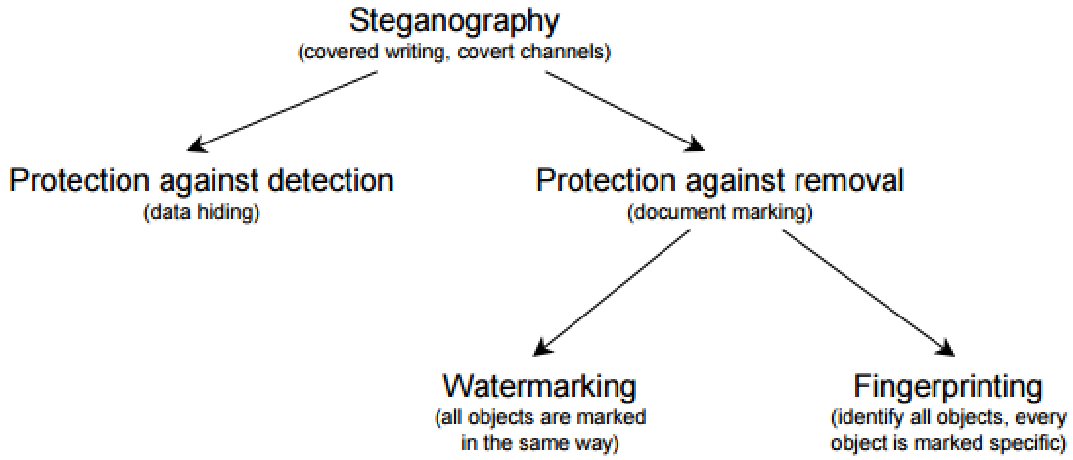
Steganography
(covered writing, covert channels)
Protection against detection
(data hiding)
Protection against removal
(document marking)
Watermarking
(all objects are marked in the same way)
Fingerprinting
(identify all objects, every object is marked specific)

Figure 2: Directions within Steganography (Popa, 1998)

Integrating Cryptography, Steganography and Watermarking

Background

There are various approaches to teach these courses for undergraduates. These three disciplines of data hiding can be integrated together as a single course. Each of this discipline can be a separate course. These disciplines can also be integrated into other courses like programming, database, or algorithm courses.

Integration of Steganography and Cryptography

Steganography is a technique used for hiding data in an array of media such as text, voice, image, and video. Cryptography re-arranges the message/data so that it cannot be interpreted (Johnson & Jajodia, 1998). Steganography can be briefly described as hiding information in plain sight while cryptography lets everyone know that the data is hidden in an unreadable message. The two concepts have multiple commonalities: secret data, computer security, computer science, and cryptography. The use of the two concepts will only increase as people use them for sharing of sensitive, private, classified, and even potentially dangerous data.

Undergraduate and graduate computer curricula should include steganography and cryptography. Such programs and courses in which the two are taught include, but not limited to, information systems, computer science, computer information systems, and computer forensics. The question to be examined is how best to incorporate the concepts into academic curricula in a way that is understandable and allows for more research and adaptation as knowledge within the field of cybersecurity.

Integrating Watermarking with Database Course

Pournaghshband, Movafaghi, Chan, and Collins (2009) briefly discussed the addition of watermarking to a database systems course in order to increase knowledge of database security. The course introduced watermarking that covered relational databases as a set of tools and techniques for protecting the ownership of relational data. The inclusion of such content would increase awareness of database ownership and protection of digital data in an era where digital information is still new and vulnerable to attack. Their database course introduced database ownership, the concept of watermarking, implementation of watermarking techniques, and discussion of future protective techniques for information technology.

Integrating Cryptography and Steganography in Introductory Programming Course

Kortsarts and Harver (2007) had a successful experience integrating cryptography into a computer forensics course for non-majors. Kortsarts and Kempner (2010) included a public-key cryptography component into a programming course. Kortsarts and Kempner (2014) embedded cryptography and steganography concepts into freshman year introductory programming courses. These courses taught Python and C without use of any image processing and graphics libraries to emphasize the merit of cryptography and steganography in programming assignments. It was noted that this created an enjoyable programming experience, sparked students' interest, and increased their engagement in the course. Students showed great interest in discovering and decrypting hidden messages. They became highly motivated in algorithmic implementation of various steganography and cryptography techniques (Kortsarts & Kempner, 2014).

Cryptography, Steganography and Digital Watermarking Curriculum

Numerous degrees, such as computer science, information technology, computer technology, information systems, cyber security, and digital forensics, offer courses that include cryptography, steganography, and watermarking. This is due to the significant increase in demand in the job market for those with these skill sets (U.S. Bureau of Labor Statistics, 2015). However, these courses vary in their objectives and goals, due to their degree programs, majors, minors, academic institutions, and faculties. Such course offerings are on theoretical aspects, programming aspects, applied concepts, algorithmic aspects, mastering operating system specific tools or online tools, and on computer forensics. The prerequisite courses may also vary. Such prerequisites may include mathematics, programming languages such as C, python, Java, Windows or Linux Operating Systems, and image processing.

Undergraduate degrees with security concentrations can offer these courses differently. Data hiding topics may be covered in individual three credit hour courses devoted to cryptography, steganography, and watermarking. The alternative is to cover a combination of two or more of these data hiding disciplines into a single three credit hour course. Some undergraduate course offerings may be limited to selected topics or a single chapter within other courses.

Data hiding technologies are delivered in various course titles such as:

a) Cryptography
b) Steganography
c) Cryptography and Steganography
d) Steganography and Digital Watermarking
e) Information Hiding Techniques, Technologies, and Investigation
f) Computer Security
g) Network Security

Importance of Cryptography, Steganography and Watermarking

The domain of cyber security is expanding almost every day. It has become a multi-disciplinary operation. The number of cyber incidents is on the rise. Several security firms have detected multiple updates to exploit kits which have recently started using steganography as a main component of their operations as they employ steganography as a way to hide exploits and malware payloads as PNG files (Cimpanu, 2016). The Stegano exploits kit (also known as Astrum) is used to transfer different malicious code via PNG banner ads. Once a web browser hits such websites, JavaScript will extract the code from the PNG file and redirect the user to a different website that will infect the computer with malware. This newly updated exploit kit was used by multiple malvertising campaigns to distribute malware. The most affected countries were Japan, Canada, and France, though Japanese users accounted for more than 30% of the total target (Paganini, 2016).

Steganography has been beneficial in protecting media copyrights (via digital watermarks). Unfortunately, there might be more downsides than benefits. On the extreme end, terrorist organizations almost completely rely on steganography as their means of communication. It is used to pass secret messages without anyone but the intended recipients being aware of it (Wall Street Pit, 2017). For example, what appears to be a family photo may surreptitiously contain the plans for a planned terrorist attack.

Unfortunately, steganography is also providing opportunities for cybercriminals. There are many steganography tools currently available ranging from opensource to commercial products. These tools give plenty of options for cybercriminals. To combat this problem, there is a need for individuals who know how to detect and decrypt this hidden data. Only a few academic institutions offer these courses that specialize in these technological areas. These technologies should not be confined to only a few paragraphs or chapters in existing courses. They should be offered as separate courses in cryptography, steganography, and watermarking.

The goal of these three technologies is the same, to secure communications to only the intended sender and receiver. These courses should be offered in a coordinated sequence that builds a comprehensive understanding of the concept, theory, and application of cryptography, steganography, and watermarking. The ability to crack encrypted files and discover messages hidden through steganography will prepare students as they enter a world in which cyber warfare has become the norm. This will serve as a gateway to more specific, specialized courses leading them to careers in steganalysis, cryptography, cryptology, digital media (audio, video, and images) forensics, and digital criminal investigation.

Conclusion

In this paper, digital data security disciplines of cryptography, steganography, and watermarking are discussed. Examples of how these technologies have been incorporated into programming courses and database courses were presented. The importance of offering integrated digital data security was discussed.

The demand for data hiding expertise and skillsets is on the rise. Academic institutions need to offer courses that address the three major digital data security disciplines. This will help students understand the fundamental knowledge of digital data security disciplines, their differences, and similarities. Students will understand these technologies as separate fields of study and lead them to careers such as digital media (image, audio, video) forensics, steganography, and cryptography.

References

Cimpanu, C. (2016, December 29). Steganography Is Very Popular with Exploit Kits All of a Sudden. Retrieved May 31, 2017, from https://www.bleepingcomputer.com/news/security/steganography-is-very-popular-with-exploit-kits-all-of-a-sudden/

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing, 2012*(1), 25. https://doi.org/10.1186/1687-4722-2012-25

Johnson, N. F., & Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. *Computer*, *31*(2), 26–34. https://doi.org/10.1109/MC.1998.10029

Kortsarts, Y., & Harver, W. (2007). Introduction to Computer Forensics for Non-Majors. In *The Proceedings of ISECON 2007*. Pittsburgh, PA.

Kortsarts, Y., & Kempner, Y. (2010). Merkle-Hellman Knapsack Cryptosystem in Undergraduate Computer Science Curriculum. In *Proceedings of the 2010 International Conference on Frontiers in Education*. CSREA Press.

Paganini, P. (2016, December 30). Sundown Exploit Kit now leverages on the steganography. Retrieved May 31, 2017, from http://securityaffairs.co/wordpress/54886/cyber-crime/sundown-exploit-kit-2.html

Popa, R. (1998). *An Analysis of Steganographic Techniques*. The “Politehnica” University of Timisoara.

Pournaghshband, H., Movafaghi, S., Chan, T., & Collins, J. S. (2009). Incorporating Watermarking in Database Systems Course - Semantic Scholar. FECS. Retrieved from /paper/Incorporating-Watermarking-in-Database-Systems-Cou-Pournaghshband-Movafaghi/90cf482a28890cb025f892e03b48010fa4798c64

U.S. Bureau of Labor Statistics. (2015). Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics. Retrieved August 20, 2017, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Wall Street Pit. (2017, March 21). New Technique Could Put An End to Photo and Video Hacking. Retrieved May 31, 2017, from http://wallstreetpit.com/113098-new-technique-end-photo-video-hacking/