Wayner, Peter. *Disappearing Cryptography : Information Hiding: Steganography & Watermarking*. Vol. 2nd ed, Morgan Kaufmann, 2002. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=81848&site=ehost-live.

Whitworth Library Link: (<https://librarysftp.whitworth.edu:2443/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=81848&site=ehost-live&ebv=EB&ppid=pp_COVER>)

Steganography and cryptography are hard to distinguish between. Cryptography can be described as hiding data by distinguishing it as random characters (Page 2). There are three classifications for steganographic techniques: using noise (i.e. replacing noise in an image with meaningful data), spreading out information (i.e. using set intervals between pixels to hide data), adopting a statistical profile (i.e. reformulating data to avoid typical patterns like letter frequency), replacing randomness with information (i.e some applications use random numbers to add realistic features, purposely setting these values could hold information), changing orders of lists (i.e. in many cases, the order of a list isn’t critical, so information can be hidden when a list is ordered in a certain way), splitting information (i.e. create a number of packages with portions of the data that create the initial message only when enough are combined), and hiding the source (i.e. broadcasting information anonymously).

Mazurczyk, Wojciech, et al. Information Hiding in Communication Networks : Fundamentals, Mechanisms, Applications, and Countermeasures. Hoboken, New Jersey : Wiley, 2016.

Whitworth Library Link: (<https://alliance-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=CP71248259830001451&context=L&vid=WW&lang=en_US&search_scope=WW_ALMA&adaptor=Local%20Search%20Engine&tab=default_tab&query=any,contains,steganography>)

This book describes concepts, terminology, and classifications of information hiding in communication networks along with its historical background. It introduces data concealment methods and their evolution. Chapter two discusses terminology in the field and describes different models for hidden communication. Chapters three to five present the main classes of information hiding in communication networks accompanied by a discussion of their robustness and undetectability. The book concludes with a discussion of potential countermeasures against information hiding techniques. It also highlights development trends and potential future directions of Information Hiding. Introduces a new classification and taxonomy for modern data hiding techniques. Presents different types of network steganography mechanisms. Introduces several example applications of information hiding in communication networks including some recent covert communication techniques.

Web Sources:

*The Rise of Steganography*, Alan Siper, Roger Farley and Craig Lombardo, 2005

<http://www.csis.pace.edu/~ctappert/srd2005/d1.pdf>

This source starts with a brief overview of the history of steganography, starting with its first known uses in 440 B.C. and running up through WWII. It breaks up the rest of the paper into sections including modern steganographic ciphers, the detection of steganography, also called steganalysis, risks and national security, and the ethics and legal ramifications of steganography. The only modern cipher discussed is Least Significant Bit Substitution (LSBS) which changes the LSB of some or all the pixels in a lossless image type like bmp or png. In steganalysis, the goal is to discover if a document, file, or audio source, contains a hidden message. A few simple methods are disused though not at length. In the security part, the paper talks about how most cybersecurity software applications are unable to check if an image, document, or sound file contains hidden information. This can lead to security breaches that only require a single photo to get inside the firewall. In the legal section, the use of steganography can help find illegally downloaded files by using steganographic watermarks. This can also be used to pass illicit information or pictures imbedded in seemingly mundane photos without detection.

*Steganography in contemporary cyberattacks*, Alexey Shulmin, Evgeniya Krylova, 2017

<https://securelist.com/steganography-in-contemporary-cyberattacks/79276/>

This article starts with a brief explanation of what steganography is and where the word came from. It includes a list of modern steganographic techniques and their strengths and weaknesses. This article focuses on cyberattacks and talks about malware programs that use steganography. It gives some examples of photos with and without hidden messages. These can be fairly obvious to the human eye but getting a computer to determine if there is a possible hidden message can be a lot harder. This article talks about a few different approaches and the applications in which they are useful and where they don’t fair as well. The article also talks about how DNS communication can be used to transmit data back and forth.

*Steganography in Modern Smartphones and Mitigation Techniques*, Wojciech Mazurczyk and Luca Caviglione, 2014

<https://arxiv.org/pdf/1410.6796.pdf>

This is a longer paper, about 25 pages, about steganography and its usage within smartphones. This paper covers the motivations behind why steganography is used within the smartphone ecosystem, a survey of the many different types of steganography used, how its usage has evolved over time, how the unique local abilities of smartphones (i.e. mobility, built in cameras and microphones, ect..) can be used stereographically, as well as the connectivity that smartphones have with the world around them. Even a little bit of malware on a phone can use the photos you take to hide data and pass it on.