www.ijarcsse.com

Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Various Aspects of Steganography

Dr. Govind N Sarage
Department of Computer Science,
National Defence Academy, Pune-23
Pune, India

Abstract*— Steganography focuses on hiding information in such a way that the message is undetectable for outsiders and only appears to the sender and intended recipient. It is the skill of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. This art, in contrast to cryptography, does not use ciphers or codes to scramble a message, and therefore is not obvious.Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable This paper will discuss the basic ideas and aspects of steganography and discuss the applications of stegnography. This paper will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganographic technique.*

Keywords*— Steganography, Data hiding, Cryptography, Masking, Filtering.*

I. Introduction

Steganography is the art of hiding information. It includes techniques to hide an image, a text file, and even an executable program inside a “cover" image without distorting the cover image. The word steganography comes from the Greek and literally means “hidden writing." It includes a vast array of secret communications methods that conceal the message’s very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spy craft family. People have used steganography through the centuries to hide messages. The messages are hidden in plain sight, because they are visible to people who know where to look. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. Consider the sentence “Where real interesting technical exchanges can overcome dull entertainment." The first letter of each word spells the message “write code." This is not hidden well. Better hiding methods use the second or third letter of each word or the first letter of the first word, second letter of the second word, etc. Steganography and cryptography are closely related. Cryptography scrambles a message to produce something that looks scrambled. The “write code" example could be scrambled to be “xsjuf dpef" (replace each letter with the letter that follows it in the alphabet). The scramble sometimes encourages prying eyes who see it as a challenge to unscramble. Steganography instead hides a message in a cover message. The result looks like something innocent, so prying eyes often dismiss it. Lawyers and libertarians debate if steganography is close enough to cryptography to regulate its use. To date, steganography remains unregulated.

II. Historical remarks

Throughout history, people always have aspired to more privacy and security for their communications [7, 8]. One of the first documents describing Steganography comes from *Histories* by Herodotus, the Father of History. In this work, Herodotus gives us several cases of such activities. A man named Harpagus killed a hare and hid a message in its belly. Then, he sent the hare with a messenger who pretended to be a hunter [7]. In order to convince his allies that it was time to begin a revolt against Medes and the Persians, Histaieus shaved the head of his most trusted slave, tattooed the message on his head and waited until his hair grew back. After that, he sent him along with the instruction to shave his head only in the presence of his allies. Another technique was the use of tablets covered by wax, first used by Demeratus, a Greek who wanted to report from the Persian court back to his friends in Greece that Xerxes, the Great, was about to invade them. The normal use of wax tablets consisted in writing the text in the wax over the wood. Demeratus, however, decided to melt the wax, write the message directly to the wood, and then put a new layer of wax on the wood in such a way that the message was not visible anymore. With this ingenious action, the tablets were sent as apparently blank tablets to Greece. This worked for a while, until a woman named Gorgo

guessed that maybe the wax was hiding something. She removed the wax and became the first woman cryptanalyst in History.

During the Renaissance, the Harpagus’ hare technique was “improved” by Giovanni Porta, one of the greatest cryptologists of his time, who proposed feeding a message to a dog and then killing the dog [8]. Drawings were also used to conceal information. It is a simple matter to hide information by varying the length of a line, shadings, or other elements of the picture. Nowadays, we have proof that great artists, such as Leonardo Da Vinci, Michelangelo, and Rafael, have used their drawings to conceal information [8]. However, we still do not have any means to identify the real contents, or even intention, of these messages. Sympathetic inks were a widespread technique. Who has not heard about lemon-based ink during childhood? With this type of ink, it is possible to write an innocent letter having a very different message written between its lines. Science has developed new chemical substances that, combined with other substances, cause a reaction that makes the result visible. One of them is *gallotanic acid*, made from gall nuts, that becomes visible when coming in contact with *copper sulfate* [9]. With the continuous improvement of lenses, photo cameras, and films, people were able to reduce the size of a photo down to the size of a printed period [7, 8]. One such example is micro-dot technology, developed by the Germans during the Second World War, referred to as the “enemy’s masterpiece of espionage” by the FBI’s director J. Edgar Hoover. Micro-dots are photographs the size of a printed period that have the clarity of standard sized typewritten pages. Generally, micro-dots were not hidden, nor encrypted messages. They were just so small as to not draw attention to themselves. The micro-dots allowed the transmission of large amounts of data (e.g., texts, drawings, and photographs) during the war.

There are also other forms of hidden communications, like *null ciphers*. Using such techniques, the real message is “camouflaged” in an innocuous message. The messages are very hard to construct and usually look like strange text. This strangeness factor can be reduced if the constructor has enough space and time. A famous case of a null cipher is the book *Hypteronomachia Poliphili* of 1499. A Catholic priest named Colona decided to declare his love to a young lady named Polya by putting the message “Father Colona Passionately loves Polia” in the first letter of each chapter of his book.

III. USES OF STEGANOGRAPHY

The use of steganography undeniably connotes dishonest activity, but there is a peaceful aspect to consider. Steganography is used in map making, where cartographers add a nonexistent street or lake in order to detect copyright offenders. Or similarly, fictional names are added to mailing lists to catch unauthorized resellers. Modern techniques use steganography as a watermark to inject encrypted copyright marks and serial numbers into electronic mediums such as books, audio, and video. For instance, DVD recorders detect copy protection on DVDs that contain embedded authorizations. Potential uses of steganography are undoubtedly vast. Companies could advertise public Web pages containing private, hidden text that only internal members could intercept. An attempt to decipher the hidden text would be unwarranted since no encryption (or code) was used. Steganography could also be used to hide the existence of sensitive files on storage media. This would entail a cover folder and an embedded hidden folder.

1. Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
2. It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.
3. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganographic methods can be used to hide this.

IV. SECRET CHANNELS

Digital technology offers new ways to apply steganography techniques, including the ability to hide information inside digital images1. A digital image is “an array of numbers that represent light intensities at various points” [3]. Combined, these light intensities or pixels form the image’s raster data. Images with 640 x 480 pixels and 256 colors can contain up to 300 kilobits of data. But it is more typical to see digital images in sizes of eight-bit or 24- bit files. This provides an excellent opportunity for hiding information, especially in image sizes of 24-bits. Each pixel on a computer monitor selects from three primary color variations: red, blue, and green. Each color is represented by a single storage byte. With24-bit images, three bytes are allocated for each primary color (hence eight bits per byte multiplied by three bytes). Represented in binary values, for instance, a white background is 11111111, 11111111, 11111111. Pixel representation makes up a file’s size. Thus a 24-bit image displayed in high resolution (1,024 x 768) has more than 2 million pixels, producing a file over 2MB in size. The larger the file, the greater opportunity there is to apply steganography techniques. The downside to this of course is that large file sizes might induce unwanted suspicions. To deal with this, file compression is used. There are two kinds available today: lossy and lossless. Both methods compress files to save storage space, but do so differently. This is important because certain compression applications can interfere with hidden messages. Lossy compression is the most efficient space saver, but does not retain the original image’s exactness. JPEG (Joint Photographic Experts Group) is an example of such compression. A lossless approach, in contrast, retains the integrity of the original image. Images saved as GIF (Graphic Interchange Format) or BMP (bitmap file) apply lossless compression

V. INSERTING HIDDEN DATA

Two files are required for steganography to work. The first file is an innocuous cover image that will host the second file containing hidden information. The hidden message can be anything that is embeddable into a *bit stream* such as plain text or cipher text. There are several methods to hide information in digital images, from taking advantage of *noisy* areas that draw less attention in an image, to scattering the message randomly throughout the image. A brief discussion on each of these approaches is in order before continuing.

VI. TEXT STEGANOGRAPHY

Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader. These criteria, reliable decoding and minimum visible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques. The document format file is a computer file describing the document content and page layout (or formatting), using standard format description languages such as PostScript2, TeX, @off, etc. It is from this format file that the image - what the reader sees - is generated. The three coding techniques that we propose illustrate different approaches rather than form <an exhaustive list of document marking techniques. The techniques can be used either separately or jointly. Each technique enjoys certain advantages or applicability as we discuss below.

Line-Shift Coding

This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely. This encoding may be applied either to the format file or to the bitmap of a page image. The embedded codeword may be extracted from the format file or bitmap. In certain cases this decoding can be accomplished without need of the original image, since the original is known to have uniform line spacing between adjacent lines within a paragraph.

Word-Shift Coding

This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely. This encoding can be applied to either the format file or to the bitmap of a page image. Decoding may be performed from the format file or bitmap. The method is applicable only to documents with variable spacing between adjacent words. Variable spacing in text documents is commonly used to distribute white space when justifying text. Because of this variable spacing, decoding requires the original image - or more specifically, the spacing between words in the un-encoded document.

Feature Coding

This is a coding method that is applied either to a format file or to a bitmap image of a document. The image is examined for chosen text features, and those features are altered, or not altered, depending on the codeword. Decoding requires the original image, or more specifically, a specification of the change in pixels at a feature. There are many possible choices of text features; here, we choose to alter upward, vertical endlines - that is the tops of letters, b, d, h, etc. These endlines are altered by extending or shortening their lengths by one (or more) pixels, but otherwise not changing the endline feature [7].

There is another form of text steganography which is defined by Chapman et al. as the text steganography is a method of using written natural language to conceal a secret message [8].

VII. IMAGE STEGANOGRAPHY

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make

these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.

Least Significant Bits

A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small [9]. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(0010011**1** 1110100**0** 1100100**0**)
(0010011**0** 1100100**0** 1110100**0**)
(1100100**0** 0010011**1** 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden [4]. As you see, the least significant bit of third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as "parity bit".

Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the "noise" level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used [4].

VIII. SCIENTIFIC AND COMMERCIAL APPLICATIONS

In this section, we show that there are many applications for Information Hiding.

- **Advanced data structures**. We can devise data structures to conceal unplanned information without breaking compatibility with old software. For instance, if we need extra information about photos, we can put it in the photos themselves. The information will travel with the photos, but it will not disturb old software that does not know of its existence. Furthermore, we can devise advanced data structures that enable us to use small pieces of our hard disks to secretly conceal important information [16, 17].
- **Medical imagery**. Hospitals and clinical doctors can put together patient's exams, imagery, and their information. When a doctor analyzes a radiological exam, the patient's information is embedded in the image, reducing the possibility of wrong diagnosis and/or fraud. Medical-image steganography requires extreme care when embedding additional data within the medical images: the additional information must not affect the image quality [18, 19].
- **Strong watermarks**. Creators of digital content are always devising techniques to describe the restrictions they place on their content. These technique can be as simple as the message "Copyright 2007 by someone" [20], as complex as the digital rights management system (DRM) devised by Apple Inc. in its iTunes store's contents [21], or the watermarks in the contents of the Vatican Library [22].
- **Military agencies**. Militaries' actions can be based on hidden and protected communications. Even with crypto-graphed content, the detection of a signal in a modern battlefield can lead to the rapid identification and attack of the involved parties in the communication. For this reason, military-grade equipment uses modulation and spread spectrum techniques in its communications [20].
- **Intelligence agencies**. Justice and Intelligence agencies are interested in studying these technologies, and identifying their weaknesses to be able to detect and track hidden messages [23, 2, 3].
- **Document tracking tools**. We can use hidden information to identify the legitimate owner of a document. If the document is leaked, or distributed to unauthorized parties, we can track it back to the rightful owner and perhaps discover which party has broken the license distribution agreement [20].
- **Document authentication**. Hidden information bundled into a document can contain a digital signature that certifies its authenticity [20].
- **General communication**. People are interested in these techniques to provide more security in their daily communications [10, 20]. Many governments continue to see the internet, corporations, and electronic conversations as an opportunity for surveillance [24].
- **Digital elections and electronic money**. Digital elections and electronic money are based on secret and anonymous communications techniques [5, 20].
- **Radar systems**. Modern transit radar systems can integrate information collected in a radar base station, avoiding the need to send separate text and pictures to the receiver's base stations.
- **Remote sensing**. Remote sensing can put together vector maps and digital imagery of a site, further improving the analysis of cultivated areas, including urban and natural sites, among others.

IX. PROTECTION AGAINST STEGANOGRAPHY

The proliferation of networks has added intensity to both noble and ignoble purposes of steganography. Network security analysts face an insidious foe for sure. But how is steganography detected, and why should network security analysts be alarmed and cautious? Nearly all steganography programs in use leave behind traces or fingerprints that indicate something is not right. Based on research conducted over the years, organized crime, terrorists, and various other groups operating worldwide commonly use steganography to operate via public forums, Web sites, etc. Software programs that detect steganography do exist, and enhanced iterations are under development. Neil Johnson, a graduate student at George Mason University, is developing a *stego detector*. The program, he describes, is designed to search hard drives for electronic fingerprints that typically result from steganography applications. Similar to a virus scanner, this stego detector identifies signatures. As Johnson explains: Different authors have different ways to hide information to make it less perceptible. The author may come up with ideas that nobody else is using. That tool may have a special signature. Once that signature is detected, it can be tied to a tool. [3] Johnson and other law enforcement agencies use software to locate signatures by studying the native structure of files including image, voice, text, and video files, and known software tools that implement steganography.

X. CONCLUSIONS

Steganography works as a technique to hide information in plain sight. Steganography is an instrument of security, but not exclusively secure. Almost like magic, images, executable programs, and text messages can hide in images. The cover image does not appear altered. People look at the cover image and never suspect something is hidden. Your information is hidden in plain sight. The approach steganography offers reduces the chance of a message being detected by its *inadvertent* layer of cover. However, if the hidden message is discovered, it is easily readable. For this reason, combining encryption algorithms with steganography offers a much stronger encryption routine. Although this article discusses some applications of steganography, there are many more uses in voice, media applications (such as communication channels), audio, and text, to name a few. This article unveils potential exploits of steganography regarding network security. Although awareness of steganography applications today is limited, progress is unfolding to expose the hidden art. Unfortunately, in the information age, the old adage "what you don't know can't hurt you" is not always accurate

REFERENCES

[1] R. Anderson and F. Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16:474–481, may 1998.

[2] Sara V. Hart, John Ashcroft, and Deborah J. Daniels. Forensic examination of digital evidence: a guide for law enforcement. Technical Report NCJ 199408, U.S. Department of Justice – Office of Justice Programs, Apr 2004.

[3] Sheridan Morris. The future of netcrime now (1) – threats and challenges. Technical Report 62/04, Home Office Crime and Policing Group, 2004.

[4] Niels Provos and Peter Honeyman. Hide and seek: an introduction to steganography.IEEE Security & Privacy Magazine, 1:32–44,May 2003.

[5] Andreas Pfitzmann. Information hiding terminology. In *Proceedings of the First Intl.Workshop on Information Hiding*, Cambridge, UK, May 1996. Springer–Verlag.

[6] Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. Information hiding—A survey. *Proceedings of the IEEE*, 87:1062–1078, Jul 1999.

[7] Bruce Norman. Secret warfare, the battle of Codes and Ciphers. Acropolis Books Inc., first edition, 1980. ISBN 0-87491-600-3.

[8] Marcus G. Kuhn. The history of steganography. In *Proceedings of the First Intl. Workshop on Information Hiding*, Cambridge, UK, May 1996. Springer–Verlag.

[9] Richard Popa. An analysis of steganography techniques. Master's thesis, The "Polytechnic" University of Timisoara, Timisoara, Romênia, 1998.

[10] Paul Wallich. Getting the message. In *IEEE Spectrum*, volume 40, pages 38–43, April 2003.

[11] Stephen Cass. Listening in. In *IEEE Spectrum*, volume 40, pages 32–37, April 2003.[12] Jean Kumagai. Mission impossible? In *IEEE Spectrum*, volume 40, pages 26–31, April 2003.RITA • Volume XV • Número 1 • 2008 107 Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?

[13] Anderson Rocha and Siome Goldenstein. Progressive Randomization for Steganalysis. In 8th IEEE Intl. Conf. on Multimedia and Signal Processing, 2006.

[14] USPS. USPS – US Postal Inspection Service. At www.usps.com/ postalinspectors/ar01intr.pdf, 2003.

[15] NHTCU. NHTCU – National High Tech Crime Unit. At www.nhtcu.org, 2003.

[16] H. Pang, K. L. Tan, and X. Zhou. StegFS: a steganographic file system. In 19th *Intl.* Conference on Data Engineering, pages 657–667,March 2003.

[17] Steven Hand and Timothy Roscoe. Mnemosyne: Peer-to-peer steganographic storage. In 1st *Intl. Workshop on Peer-to-Peer Systems*, volume 2429, pages 130–140, March 2002.

[18] Raúl Rodríguez-Colín, Feregrino-Uribe Claudia, and Gershom de J. Trinidad-Blas. Data hiding scheme for medical images. In 17th *IEEE Intl. Conference on Electronics, Communications and Computers*, pages 33–38, February 2007.

[19] Y. Li, C. T. Li, and C. H. Wei. Protection of mammograms using blind staganography and watermarking. In 3rd Intl. Symposium on Information Assurance and Security, August 2007.

[20] Peter Wayner. *Disappearing cryptography*. Morgan Kaufmann Publishers, San Francisco, CA, USA, second edition, 2002. ISBN 1-55860-769-2.

[21] The Electronic Frontier Foundation (EFF). The customer is always wrong: A user's guide to DRM in online music. At http://www.eff.org/IP/DRM/guide/, 2007.

[22] F. C. Mintzer, L. E. Boyle, and A. N. Cases. Toward on-line, worldwide access to vatican library materials. *IBM Journal of Research and Development*, 40:139–162,Mar 1996.

[23] Rebecca T. Mercuri. The many colors of multimedia security. *Communications of the ACM*, 47:25–29, 2004.

[24] Toby Sharp. An implementation of key-based digital signal steganography. In 4th *Intl.* Information Hiding Workshop, 2001.

[25] Anderson Rocha. Randomização Progressiva Para Esteganálise. Master's thesis, Institutode Computação – Unicamp, Campinas, SP, Brasil, 2006.

[26] Rafael C.Gonzalez and Richard E. Woods. *Digital Image Processing*. Prentice-Hall,Boston, MA, USA, second edition, 2002. ISBN 0-20118-075-8.

108 RITA • Volume XV • Número 1 • 2008 Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?

[27] Derek Upham. Jsteg shell. At http://www.tiac.net/users/korejwa/jstegshella.zip, 1999.

[28] Niels Provos. Defending against statistical steganalysis. In *Proceedings of the 10th USENIX Security Symposium*, pages 323–336, Washington, DC, USA, Aug 2001. The USENIX Association.

[29] Bruce Schneier. *Applied Cryptography*. JohnWiley & Sons, New York, 1995. ISBN 0-47111-709-9.

[30] Neil F. Johnson and Sushil Jajodia. Exploring steganography: Seeing the unseen. *IEEE Computer*, 31:26–34, Feb 1998.

[31] Andreas Westfeld and Andreas Pfitzmann. Attacks on steganographic systems. In *Proceedings* of the Third Intl.Workshop on Information Hiding, pages 61–76, London, UK, 1999. Springer Verlag.

[32] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. Springer Verlab, 2006. ISBN 0-38731-073-8.

[33] Niels Provos and Peter Honeyman. Detecting steganographic content on the internet. Technical Report CITI 01-11, University ofMichigan, Ann Arbor,MI, USA, Nov 2001.

[34] Jessica Fridrich, Miroslav Goljan, and Rui Du. Detecting LSB steganography in color and grayscale images. *IEEE Multimedia*, 8:22–28, Jan 2001.

[35] Li Shi, Sui Ai Fen, and Yang Yi Xian. A LSB steganography detection algorithm. In Proceedings of the 14th Personal, Indoor and Mobile Radio Communications, volume 3, pages 2780–2783. IEEE, Sep 2003.

[36] Siwei Lyu and Hany Farid. Detecting hidden messages using higher-order statistics and support vector machines. In Proceedings of the Fifth Intl. Workshop on Information *Hiding*, pages 340–354, Noordwijkerhout, The Netherlands, 2002. Springer-Verlag.

[37] Hany Farid. Detecting hidden messages using higher-order statistical models. In *Proceedings* of the Intl. Conference on Image Processing, volume 2, pages 905–908. IEEE,Jun 2002.

[38] Siwei Lyu. Steganalysis using color wavelet statistics and one-class support vector machines. Master's thesis, Dartmouth College, Hanover, NH, USA, 2002.

[39] Hany Farid. Detecting steganographic messages in digital images. Technical Report TR2001-412, Dartmouth College, Hanover, NH, USA, Mar 2001.RITA • Volume XV • Número 1 • 2008 109 Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?

[40] P. P. Vaidyanathan. Quadrature mirror filter banks, m-band extensions and perfect reconstruction techniques. *IEEE Signal Processing Magazine*, 4:4–20, Jul 1987.

[41] R. W. Buccigrossi and E. P. Simoncelli. Image compression via joint statistical characterization in the wavelet domain. IEEE Transactions On Image Processing, 8:1688–1701, 1998.

[42] Ismail Avcibas, Nasir Memon, and Bülent Sankur. Steganalysis using image quality metrics. IEEE Transactions On Image Processing, 12:221–229, Feb 2003.

[43] Ismail Avcibas, NasirMemon, and Bülent Sankur. Image steganalysis with binary similarity measures. In Proceedings of the Intl. Conference on Image Processing, volume 3,pages 645–648. IEEE, Jun 2002.

[44] Ismail Avcibas, Nasir Memon, and Bülent Sankur. Steganalysis based on image quality metrics. In Proceedings of the Fourth Workshop on Multimedia Signal Processing, pages 517–522. IEEE, Oct 2001.

[45] Ismail Avcibas. Steganalysis using image quality metrics. Master's thesis, Computer and Information Science Polytechnic University, Brooklyn, NY, USA, 2002.

[46] Ueli Maurer. A universal statistical test for random bit generators. *Journal of Cryptology*,5:89–105, Feb 1992.

[47] David Freedman, Robert Pisani, and Roger Purves. *Statistics*. George J. McLeod Limited, Toronto, Canadá, first edition, 1978. ISBN 0-39309-076-0.

[48] The Compuserve Group. *Specification of GIF image format*, Jul 1990. http://www.dcs.ed.ac.uk/home/mxr/gfx/2d/GIF89a.txt.

[49] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, Boston,MA, USA, 1995. ISBN 0-26274-017-6.

[50] Anderson Rocha, Siome Goldenstein, Heitor A. X. Costa, and Lucas M. Chaves. Esteganografia para proteção e privacidade digital. In 6th *SSI*, 2004.

[51] Anderson Rocha, Siome Goldenstein, Heitor A. X. Costa, and Lucas M. Chaves. Segurança e privacidade na internet por esteganografia em imagens. In *Webmedia & LA-Web* – Joint Conference 2004, 2004.

[52] Anderson Rocha. Camaleão: um software para segurança digital utilizando esteganografia, 2003. Monografia. Depto. de Ciência da Computação, Universidade Federal de Lavras.