International Journal of Cryptology Research 5(2): 15-27 (2015)

An Overview of Frequency-based Digital Image Steganography

[1]Samer Atawneh and [2]Putra Sumari

[1]College of Computing and Informatics,
Saudi Electronic University, Saudi Arabia

[2]School of Computer Sciences,
Univeristi Sains Malaysia, Malaysia

Email: satawneh@yahoo.com

ABSTRACT

Digital image steganography is the practice of concealing secret messages into digital images with the intention transmitting the secret information. Despite that the steganography existence for quite some time now, it has only become significant in today's digital world where information is frequently and easily exchanged through the Internet, emails and other ways using computers. The need for effective methods of hiding secret information into images led to the new incentive research in the area of steganography. Like any other science, steganography can be applied into several useful applications. However, it can be also exploited to transmit information for malicious reasons. Steganalysis is the antithesis of steganography and aims to disable it. This paper surveys steganography in the frequency domain of digital images in order to enlighten the reader to the key concepts behind it. Comparisons between different existing image steganographic methods in frequency domain are provided. Possible research trends, some recommendations and useful strategies to improve the security of steganography in frequency domain of digital images are also discussed.

Keywords: Digital image steganography, frequency domain, DCT, DFT, DWT, IWT.

1. INTRODUCTION

Steganography has met with success for the past centuries as secret information is valuable to those who it is hidden from. There will always be individuals or groups who will attempt to decrypt information or to find what is hidden. In this respect, governments often want to be privy to civilians or other governments' activities, and companies who want to save trade secrets from their competitors. Different motives are present to detect the steganography use, and thus, methods to do so are increasingly developed, while methods for steganography are increasingly becoming advanced. A steganographic scheme is graphically represented in Figure 1 (Atawneh and Sumari, 2014).

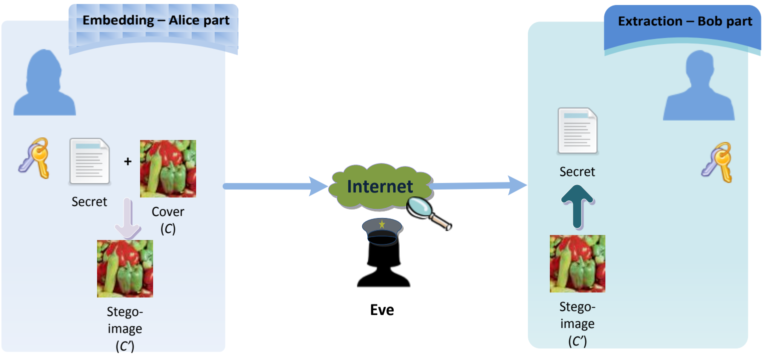


Figure 1: A general steganography approach

The primary application of steganography is the secret communication. However, steganography has a variety of other useful applications; some of the most interesting ones are file authentication, annotation, hide confidential data files (spreadsheets and documents) located inside computers, bank transactions, enhanced data structures, and protecting digital document files from forgery using self-embedding methods. Different properties characterize the performance of the steganographic method. The most important properties that contended with each other are undetectability, embedding capacity, and robustness (Al-Ani et al., 2010; Ingemar et al., 2008; Lin and Delp, 1999). The main concept of contemporary steganography was described by Simmons, 1984, when he explained how the two prisoners, Alice and Bob, were planning to escape. They are under the surveillance of Eve, the warden, and they need to communicate in a covert way with no raising suspicion. One of the earliest techniques to discuss steganography in digital media is credited to Kurak and McHugh, 1992, who developed a method to replace the 4 LSBs of 8-bit image by the 4 MSBs (most significant bits) of another. They showed that contaminating digital images with information, which can be extracted later, is extremely simple.

2. DIGITAL IMAGE STEGANOGRAPHY

The current increasing interest towards steganography can be attributed to the proliferating use of digital media and the increasing Internet development. It is now a common place for individuals to put up their pictures, videos and sounds to share with their family and friends. Such objects have become a convenient place to hide secret information for the primary reason that indicates to typical digital media files comprising a huge number of individual samples (pixels) that can be changed to embed a secret message. Compared to other digital objects, the field of image steganography is the most developed field in the current times, with various methods offered for the most common image formats. Figure 2 shows the number of steganographic applications that hide secret information in electronic media as of 2008 (Fridrich, 2009).

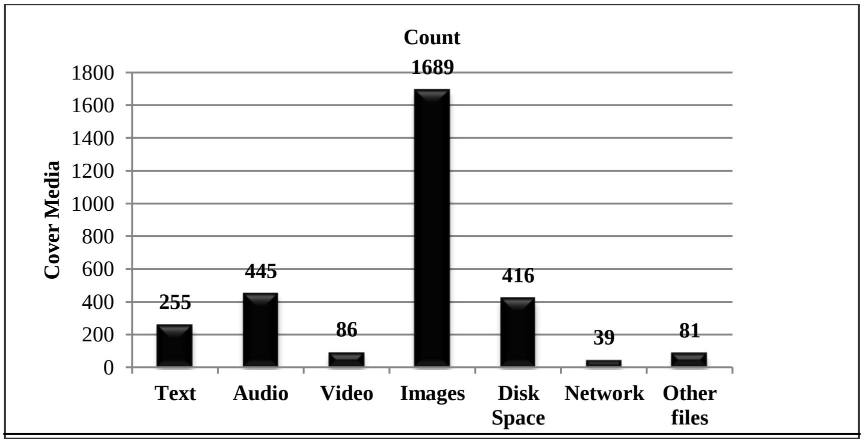


Figure 2: A pie chart showing the different carriers used in the available steganographic applications

2.1 Image Steganography Domains

Steganographic methods can be categorized in different ways. Cheddad et al., 2010, gave a standard categorization by grouping the methods into spatial domain, frequency domain, and adaptive techniques. Spatial domain steganography embeds the secret information in the LSBs of the cover image's pixels selected sequentially or randomly. These steganographic methods are widely used and are considered to act like simple systems. On the other hand, frequency domain steganography mainly embeds the secret information in the transform coefficients, and manages to satisfy the criteria of imperceptivity, as well as robustness. The development of an adaptive technique obviously requires a full knowledge of representative features of the cover image in order to decide where to make changes. Figure 3 shows the steganographic methods that utilize the spatial domain or the frequency domain of digital images, and Table 1 gives the benefits and drawbacks of the current steganography methods (Atawneh et al., 2013). This study focuses on the current methods utilizing the frequency domain of image steganography.

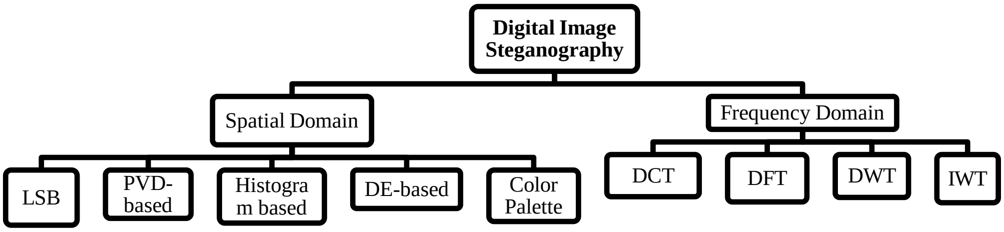


Figure 3: Digital image steganography methods

TABLE 1: The benefits and drawbacks of the current steganography methods.

Steganography Method	**Descriptions**
Spatial domain techniques	**Benefits:** High embedding capacity Simple systems; embedding information is directly carried out within the least significant bits (LSB) of the intensity values. **Drawbacks:** Typically depend on the image format The embedded information may be easily detected using statistical analysis (e.g., Chi-Square statistical test) Not robust against lossy compression and noise Not robust against cropping or rotating the image
Frequency domain techniques	**Benefits:** Typically independent of the image format Less prone to lossy compression and common image processing techniques as compared to the spatial domain methods. More robust against noise than the spatial domain techniques. **Drawbacks:** Low embedding capacity compared with spatial domain Embedding information takes place in the coefficients of the transformed image; more computations are required Not robust against second order statistical analysis

2.1.1 Frequency-domain image steganography

The most robust steganographic systems work currently in what is referred to as a frequency (transform) domain. A frequency domain method embeds secret information in specific locations of the cover image making it invulnerable to attacks, such as compression, adding noise, cropping and other image processing. Many frequency domain variations have been proposed; for instance, the use of Discrete Cosine Transformation (DCT) as a carrier to embed information in an image. DCT-based steganography is widely used due to its compatibility with JPEG compression standard. Other methods include the Discrete Fourier Transformation (DFT) methods, Discrete Wavelet Transformation (DWT) methods, and the Integer Wavelet Transformation (IWT) methods. Frequency embedding embeds secret information through the modification of selected transform coefficients of the cover image. If an attack, for example image processing, is conducted, it will mainly affect a specific band of the transform coefficient, while the remaining coefficient remains intact. Hence, frequency embedding is considered more robust compared to other embedding methods. The majority of frequency domain methods do not depend on the image format, where the message embedded may undergo lossy and lossless compressions.

A. Discrete Cosine Transformation techniques

The most widely used lossy digital image compression system currently is exemplified by the two-dimensional Discrete Cosine Transformation (DCT) in the form of the JPEG system (Johnson and Katzenbeisser, 2000; Popescu and Farid, 2005). The Jpeg-Jsteg (Upham, 2002), or shortly the JSteg, is one of the first methods that utilizing the frequency domain of JPEG images. It replaces the LSBs of the quantized DCT coefficients with the secret information, and avoids all coefficients with values of 0, 1, or -1. The OutGuess algorithm (Provos, 1999) is a two-pass process, where the first pass involves the embedding of secret message bits with a pseudo-random walk in the least significant bits of DCT coefficients, skipping those coefficients that have zero magnitude or unity. As for the second pass, it involves corrections to be performed for the coefficient magnitudes in order to guarantee that the histogram of the DCTs of the stego-image matches their counterparts in the cover image (Ingemar et al., 2008). F5 (Westfeld, 2001) is a method to embed secret information within JPEG images. In this method, instead of flipping the LSBs for the message bits encoding, F5 decrements the absolute value of the DCT coefficient by one, through a process called matrix encoding which can decrease the number of steganographic modifications and maintain coefficient histograms appearing in unchanged manners (Provos and Honeyman, 2003; Sallee, 2004). F5 algorithm involves the embedding of message bits throughout a pseudo-random path that is determined from the user pass-phrase. The DC terms and zero magnitude coefficients are overlooked and not utilized in the embedding process (Ingemar et al., 2008). PQ (Fridrich et al., 2005) is a technique that hides the secret information based on the use of a fact in which the process rounds up the coefficients with the values that are near to the middle of the quantization intervals that possess a random component as a result of a noise existing in images. PQ is considered to be the most undetectable method compared to its counterparts.

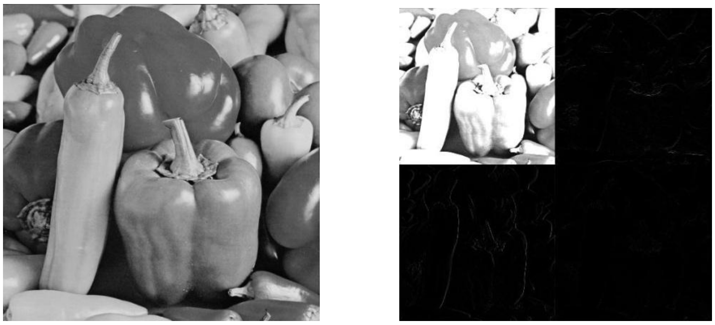
B. Discrete Fourier Transform

Fourier Transforms are important tools for image processing which are used to decompose images. The results of these transformations represent images in the frequency domain. Fourier Transforms have several applications, for example image analysis and filtering, and image compression. The DFT is based on the Fast Fourier Transform (FFT). It has been reported that the hiding methods based on the FFT are not suitable for secret communications because of the round-off errors they introduce during the extraction of embedded information (Raja et al., 2005; Wayner, 2009). Moreover, DFT-based steganography is not compatible with JPEG or JPEG2000 compression standards. However, McKeon, 2007, and Mandal and Khamrui, 2011, utilized the DFT and proposed Fourier-based hiding techniques that embed the secret payload in the coefficients of the cover image.

C. Discrete Wavelet Transform

Wavelet transforms are mathematical tools used for converting images from spatial domain into frequency domain. They are applied to different applications such as approximation theory, signal processing, and image compression. Discrete Wavelet Transform (DWT) is primarily utilized in image processing for the purpose of reducing noise, compression and edge detection. It is considered to be less resource intensive and lead to less distortion in the image compared to the DFT and DCT. Current researchers make use of the DWT owing to its widespread application in the image JPEG2000 compression standard (Ghasemi et al., 2011), and due to its fast transformation property in translating the digital image from its spatial domain to the frequency domain. The DFT and DCT are considered as full frame transforms, and as such any modification in the transform coefficients impacts the whole image (Cheddad et al., 2009). On contrary, if a digital image is embedded with secret information utilizing DWT domain, this will impact the image in a local manner. The DWT can be performed by utilizing one of the wavelet transforms (known as filter banks). There are varying filters that are available, but the most widely being used are the Haar-DWT and the Daubechies-DWT.

Upon applying the Haar-DWT on a 2-D image, the image is decomposed into one approximation sub-band known as LL sub-band and three details sub-bands namely LH, HL, and HH sub-bands (Barve et al., 2011). The smooth areas (significant part) of the image's spatial-domain exist in the approximation sub-band (LL sub-band) which holds the low-frequency coefficients, while other details of the image (the edge details) exist in the high-frequency sub-bands (LH, HL, and HH sub-bands) (Bhattacharyya and Sanyal, 2012; Nag et al., 2011). Figure 4 shows an example of decomposing a 24-bit image after applying one level Haar-DWT to it.



(a) (b)

Figure 4: (a) Original image (b) Result after one-level decomposition with 2-D Haar-DWT

Keyvanpour et al., 2013, proposed a blind hiding method in a DWT domain based on a chaotic mapping (Arnold's Cat Map (Gouxi and Min, 2010)) that is applied to the LL3 sub-band of the cover image to encode the secret bits before the embedding process starts. The cover image is first decomposed into 10 sub-bands through applying a 3-level Haar wavelet transform, and the HL3 and LH3 sub-bands are utilized for embedding the encoded secret bits using a special quantization process. In a similar way, Nag et al., 2011, proposed a hiding method based on 2-dimensional DWT. To increase the embedding capacity, the secret message bits are encoded by Huffman coding prior to the embedding phase, then the 3 LSBs of wavelet coefficients in the high frequency sub-bands of the cover image are replaced by 3 bits from the encoded secret bit stream. This method provides an embedding capacity around 24% of the cover image size where the average PSNR value is nearly 55dB.

D. Integer Wavelet Transform

Common wavelet transforms possess floating point coefficients. When the input data includes a series of integers, as in image files, the filtered outcome is no longer a series of integers. This implies that a perfect reconstruction of the original image is not enabled. As such, the inverse wavelet transform becomes lossy. However, the currently introduced Wavelet Transforms that map Integers to Integers (IWT) allow the output to be characterized by integers and accurate decompression of the original data is attained (Raja et al., 2008). The IWT produces a close copy of the original image, with a smaller scale, by adopting a technique known as Lifting scheme that converts the DWT coefficients into integers. Thanikaiselvan et al., 2011, chose to use Integer Wavelet Transform (IWT) that maps integers to integers to avoid floating point problems of the wavelet filters in DWT and proposed a steganographic technique for 24-bit images. Their technique embeds the secret information, using the LSB substitution, in non overlapping blocks of the high frequency sub-bands, i.e., LH1, HL1, and HH1, in each plane of the cover image followed by applying an optimal pixel adjustment process (OPAP) to reduce the embedding error.

3. DISCUSSIONS AND RECOMMENDATIONS

The “mutual resistance” relationship between steganography and steganalysis led to a big competition between them. While steganography aims to hide the very existence of secret information, steganalysis strives to detect the presence of this secret information. Powerful methods are developing to improve the steganography security and efficient steganalytic methods try in an increasing accuracy to disable steganography. The security of image steganographic methods in frequency domain could be influenced by some factors, such as the amount of modification to the cover image, the number of embedded locations, the features of the cover image, etc. In this section, some techniques to reduce the detectability of image steganography in frequency domain and hence improve its security are discussed.

1. Reducing the distortion

Though increasing the embedding efficiency can lead to reduce the number of locations that are changed due to embedding process, it may not minimize the distortion to the image. However, if not all LSBs or coefficients are utilized for embedding, then selecting the places that lead to the minimum distortion are adopted. This leaves minimum differences between the cover image and stego-image, and hence increasing the steganographic security. The first method handled this issue was the Perturbed Quantization (Fridrich et al., 2004; 2005).

2. Selecting a suitable cover image

Since digital images are insensitive to the HVS system and have greater levels of redundancy, they are more suitable for steganography. Moreover, selecting unsuspicious cover image to embed the secret information can improve the security of steganography. Choosing such a proper image can produce fewer changes and then the result stego-image is pretty close to the cover image.

3. Using secret-key embedding schemes

A much more secure system can be produced if a secret key that controls the embedding and extracting processes of secret information is used since only the holder of the key can recover the secret information accurately.

Possible research trends of image steganography in frequency domain are drawn below:

1. Embedding while image creation. Though most of the steganographic methods use the already generated images to embed the secret information, it has been reported that embedding the secret information during the creation process of the image can improve the security of the steganographic method. This may provide better camouflage. For example, embedding the secret information in the process of creation JPEG or JPEG2000 image versions from raw images is more secure than embedding it after the process of image creation is finished.

2. Improving the robustness. The robustness of the steganographic method could be improved by replicating the same secret information at the expense of payload. One can benefit from the redundancy in digital images to guarantee better extraction of the secret information if the payload’s size is small. Furthermore, embedding the secret information in the coefficients of the image, after transforming it into the frequency domain, can improve the correct extraction of the secret information and hence results in higher robustness than spatial domain embedding.

3. Embedding in DWT domain. DWT-based embedding methods show more encouraging results when compared to DCT especially in compression survival (Wayner, 2009). These methods lead to less distortion in the image compared to the DFT and DCT (Bachrach and Shih, 2011). In addition, if secret information is embedded in the DWT domain of a digital image, this will affect the image locally.

4. CONCLUSION

This paper presented a background on the digital image steganography in frequency domain. Frequency domain techniques, such as the DCT and

DWT techniques, embed the secret information in specific locations of the cover image making it invulnerable to attacks, especially when the size of the hidden information is small. Hence, they are considered more robust compared to other embedding methods. A trade-off between robustness and embedding capacity always exists. One of the main challenges in image steganography in frequency domain is to develop robust methods with high embedding capacity without degrading the quality of the stego-image.

REFERENCES

Al-Ani, Z. K., Zaidan, A., Zaidan, B. and Alanazi, H. (2010). Overview: Main fundamentals for steganography. *Journal of Computing.* **2**(3):158-165.

Atawneh, S., Almomani, A. and Sumari, P. (2013). Steganography in Digital Images: Common Approaches and Tools. *IETE Technical Review.* **30**(4): 344-358.

Atawneh, S., and Sumari, P. (2014). Imperceptible image-based steganographic scheme using Bit-Plane Complexity Segmentation (BPCS). *International Journal of Image Processing Techniques.* **1**: 6 - 11.

Bachrach, M., and Shih, F. Y. (2011). Image steganography and steganalysis. *Wiley Interdisciplinary Reviews: Computational Statistics.* **3**(3): 251-259.

Barve, S., Nagaraj, U. and Gulabani, R. (2011). Efficient and Secure Biometric Image Stegnography using Discrete Wavelet Transform. *International Journal of Computer Science & Communication Networks.* **1**(1): 96-99.

Bhattacharyya, S. and Sanyal, G. (2012). A Robust Image Steganography using DWT Difference Modulation (DWTDM). *International Journal of Computer Network and Information Security (IJCNIS).* **4**(7): 27-40.

Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. (2009). A secure and improved self-embedding algorithm to combat digital document forgery. *Signal Processing.* **89**(12): 2324-2332.

Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing.* **90**(3): 727-752.

Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications.* United Kingdom: Cambridge University Press.

Fridrich, J., Goljan, M. and Soukal, D. (2004). Perturbed quantization steganography with wet paper codes. Paper presented at the *Proceedings of the ACM workshop on Multimedia and security*, Magdeburg, Germany.

Fridrich, J., Goljan, M. and Soukal, D. (2005). Perturbed quantization steganography. *Multimedia Systems.* **11**(2): 98-107.

Ghasemi, E., Shanbehzadeh, J. and ZahirAzami, B. (2011). A steganographic method based on Integer Wavelet Transform and Genetic Algorithm. Paper presented at the *International Conference on Communications and Signal Processing (ICCSP)*, Calicut, India.

Gouxi, C. and Min, C. (2010). Information Hiding Algorithm Based on Transformation and Image Partition. Paper presented at the *International Conference on Computational Intelligence and Software Engineering* (CiSE), Wuhan, China.

Ingemar, J. C., Miller, M. L., Bloom, J. A., Fridrich, J. and Kalker, T. (2008). *Digital Watermarking and Steganography.* USA: Burlington, Morgan Kaufmann.

Johnson, N. F. and Katzenbeisser, S. (2000). A survey of steganographic techniques. Paper presented at the *Information Hiding Techniques for Steganography and Digital Watermarking*, Norwood, USA.

Keyvanpour, M. and Bayat, F. M. (2013). Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain. *Mathematical and Computer Modelling.* **58**(1): 56-67. doi: http://dx.doi.org/10.1016/j.mcm.2012.07.008

Kurak, C. and McHugh, J. (1992). A cautionary note on image downgrading. Paper presented at the *Eighth Annual Computer Security Applications Conference*, San Antonio, USA.

Lin, E. T. and Delp, E. J. (1999). A review of data hiding in digital images. Paper presented at the *Proceedings of the Image Processing, ImageQuality, Image Capture Systems Conference (PICS'99)*, Georgia, USA.

Mandal, J. and Khamrui, A. (2011). A Genetic Algorithm based steganography in frequency domain (GASFD). Paper presented at the *International Conference on Communication and Industrial Application (ICCIA)*, Kolkata, India.

McKeon, R. T. (2007). Strange Fourier steganography in movies. Paper presented at the *IEEE International Conference on Electro/Information Technology*, Chicago, USA.

Nag, A., Biswas, S., Sarkar, D. and Sarkar, P. P. (2011. A novel technique for image steganography based on DWT and Huffman encoding. *International Journal of Computer Science and Security*. **4**(6): 561-570.

Popescu, A. and Farid, H. (2005). Statistical tools for digital forensics. Paper presented at the *6th International Workshop on Information Hiding*, Toronto, Canada.

Provos, N. (1999). Outguess Retrieved 3 July 2012, 2012, from www.outguess.org

Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. *Security & Privacy, IEEE*. **1**(3): 32-44.

Raja, K., Chowdary, C., Venugopal, K. and Patnaik, L. (2005). A secure image steganography using LSB, DCT and compression techniques on raw images. Paper presented at the *Third International Conference on Intelligent Sensing and Information Processing (ICISIP'05)*, Bangalore, India.

Raja, K., Sindhu, S., Mahalakshmi, T., Akshatha, S., Nithin, B., Sarvajith, M., Patnaik, L. (2008). Robust image adaptive steganography using integer wavelets. Paper presented at the *3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, Bangalore, India.

Sallee, P. (2004). Model-based steganography. Paper presented at the *Proceedings of the Second International Workshop on Digital Watermarking*, Seoul, Korea.

Simmons, G. J. (1984). The prisoners' problem and the subliminal channel. Paper presented at the *Proceedings of International Conference on Advances in Cryptology (CRYPTO83),* Paris, France.

Thanikaiselvan, V., Arulmozhivarman, P., Amirtharajan, R., and Rayappan, J. (2011). Wave (let) decide choosy pixel embedding for stego. Paper presented at the *International Conference on Computer, Communication and Electrical Technology (ICCCET),* Tamilnadu, India.

Upham, D. (2002). JPEG-JSteg. Computer Software–Modification of the Independent JPEG Group's JPEG software (release 4). Retrieved 30 November 2012, 2012, from ftp://ftp.funet.fi/pub/crypt/ steganography

Wayner, P. (2009). *Disappearing cryptography: information hiding: steganography and watermarking* (3rd edition ed.). USA: Morgan Kaufmann Publishers.

Westfeld, A. (2001). F5-A Steganographic Algorithm. Paper presented at the *Proceedings of Fourth International Workshop on Information Hiding*, Pittsburgh, USA.