International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-7,October 2015
ISSN: 2395-3470
www.ijseas.com

THE STEGANALYSIS RESULTING THROUGH JPEG CALIBRATION AND JPEG STEGOGRAMMES

J. SHAIK DAWOOD ANSARI,
Senior Lecturer - SOC
Institute of Business Studies
PO Box 2826, Boroko, National Capital District, Papua New Guinea

ABSTRACT

Perhaps the most important aspect of blind steganalysis is ensuring that we can derive an estimate of the cover image that is as accurate as possible. The attacks that follow this procedure often compare the data in the estimated cover image to that of the suspect image, so it is imperative that the data of the estimate is as sound as possible so as to not obscure the results. One of the most famous approaches for creating an estimate of the cover image is the model proposed by Jessica Fridrich in known as JPEG Calibration. The method takes advantage of the fact that most stego-systems encode the message data in the transform domain during the compression procedure to produce JPEG stegogrammes. Given that the JPEG compression algorithm operates by transforming the image into 8x8 blocks, and it is within these blocks that the encoding of the message operates, we can estimate the cover work by introducing a new block structure and comparing it with that of the suspect image.

Keywords: *Steganographic, Steganalysis, JPEG Calibration and JPEG stegogrammes*

INTRODUCTION

Steganography is the art of invisible communication. Its purpose is to hide the very presence of communication by embedding messages into innocuous-looking cover objects. In today's digital world, invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages – digital documents, images, video, and audio files. As long as an electronic document contains perceptually irrelevant or redundant information, it can be used as a "cover" for hiding secret messages. In this paper, we deal solely with covers that are digital images stored in the JPEG format. Each steganographic communication system consists of an embedding algorithm and an extraction algorithm. To accommodate a secret message, the original image, also called the cover-image, is slightly modified by the embedding algorithm. As a result, the stego-image is obtained.

Steganalysis is the art of discovering hidden data in cover objects. As in cryptanalysis, we assume that the steganographic method is publicly known with the exception of a secret key. The method is secure if the stego-images do not contain any detectable artifacts due to message embedding. In other words, the set of stegoimages should have the same statistical properties as the set of cover-images. If there exists an algorithm that can guess whether or not a given image contains a secret message with a success rate better than random guessing, the steganographic system is considered broken. For a more exact treatment of the concept of steganographic security, the reader is referred to.

The ability to detect secret messages in images is related to the message length. Obviously, the less information we embed into the cover-image, the smaller the probability of introducing detectable artifacts by the embedding process. Each steganographic method has an upper bound on the maximal safe message length (or the bit-rate expressed in bits per pixel or sample) that tells us how many bits can be safely embedded in a given image without introducing any statistically detectable artifacts. Determining this maximal safe bit-rate (or steganographic capacity) is a nontrivial task even for the simplest methods. Chandramouli et al. give a theoretical analysis of the maximal safe bit-rate for LSB embedding in the spatial domain. Recently, Fridrich et al. derived a more stringent estimate using dual statistics steganalysis. The choice of cover-images is important because it significantly influences the design of the stego system and its security. Images with a low number of colors, computer art, images with a unique semantic content, such as fonts, should be avoided. Aura recommends grayscale images as the best cover-images. He also recommends uncompressed scans of photographs or images obtained with a digital camera containing a high number of colors, and consider them safest for steganography.

The choice of the image format also makes a very big impact on the design of a secure steganographic system. Raw, uncompressed formats, such as BMP, provide the biggest space for secure steganography, but their obvious redundancy makes them very suspicious in the first place. Indeed, some researchers do not consider those formats for steganography claiming that exchanging uncompressed images is “equivalent” to using cryptography . Never the less, most steganographic products available on the Internet work with uncompressed image formats or formats that compress data losslessly (BMP, PCX, GIF, PGM, and TIFF). Fridrich et al. have recently shown that cover-images stored in the JPEG format are a very poor choice for steganographic methods that work in the spatial domain. This is because the quantization introduced by JPEG compression can serve as a "semi-fragile watermark" or a unique fingerprint that can be used for detection of very small modifications of the cover-image by inspecting the compatibility of the stegoimage with the JPEG format. Indeed, changes as small as flipping the least

significant bit (LSB) of one pixel can be reliably detected. Consequently, one should avoid using decompressed JPEG images as covers for spatial steganographic methods, such as the LSB embedding or its variants. Despite its proven insecurity, the method of choice of most publicly available steganographic tools is the LSB embedding. This paradigm can be adapted not only to raw formats but also to palette images after pre-sorting the palette (EZ Stego) and to JPEG images (J-Steg , JP Hide&Seek , and OutGuess). Fridrich et al. introduced the dual statistics steganalytic method for detection of LSB embedding in uncompressed formats. For high quality images taken with a digital camera or a scanner, the dual statistics steganalysis indicates that the safe bitrate is less than 0.005 bits per sample, providing a surprisingly stringent upper bound on steganographic capacity of simple LSB embedding. Pfitzmann and Westfeld introduced a method based on statistical analysis of Pairs of Values (PoVs) that are exchanged during message embedding. For example, grayscales that differ in the LSBs only, could form these PoVs. This method, which became known as the $\chi 2$ attack, is quite general and can be applied to many embedding paradigms besides the LSB embedding. It provides very reliable results when the message placement is known (e.g., for sequential embedding).

Pfitzmann and Provos noted that the method could still be applied to randomly scattered messages by applying the same idea to smaller portions of the image while comparing the statistics with the one obtained from unrelated pairs of values. Unfortunately, no further details regarding this generalized $\chi 2$ attack are provided in their papers, although Pfitzmann reports that messages as small as one third of the total image capacity are detectable. Farid developed a universal blind detection scheme that can be applied to any steganographic scheme after proper training on databases of original and coverimages. He uses an optimal linear predictor for wavelet coefficients and calculates the first four moments of the distribution of the prediction error. Fisher linear discriminant statistical clustering is then used to find a threshold that separates stegoimages from cover-images. Farid demonstrates the performance on J-Steg, both versions of OutGuess, EZ Stego, and LSB embedding. It appears that the selected statistics is rich enough to cover a very wide range of steganographic methods. However, the results are reported for a very limited image database of large, highquality images, and it is not clear how the results will scale to more diverse databases. Also, the authors of this paper believe that methods that are targeted to a specific embedding paradigm will always have significantly better performance than blind methods. Johnson and Jajodia pointed out that some steganographic methods for palette images that preprocess the palette before embedding are very vulnerable. For example, S-Tools or Stash create clusters of close palette colors that can be swapped for each other to embed message bits. These programs decrease the color depth and then expand it to 256 by making small perturbations to the colors.

This preprocessing, however, will create suspicious and easily detectable pairs (clusters) of close colors. Recently, the JPEG format attracted the attention of researchers as the main steganographic format due to the following reasons: It is the most common format for storing images, JPEG images are very abundant on the Internet bulletin boards and public Internet sites, and they are almost solely used for storing natural images. Modern steganographic methods can also provide reasonable capacity without necessarily sacrificing security. Pfitzmann and Westfeld proposed the F5 algorithm as an example of a secure but high capacity JPEG steganography. The authors presented the F5 algorithm as a challenge to the scientific community at the Fourth Information Hiding Workshop in Pittsburgh in 2001. This challenge stimulated the research presented in this paper.

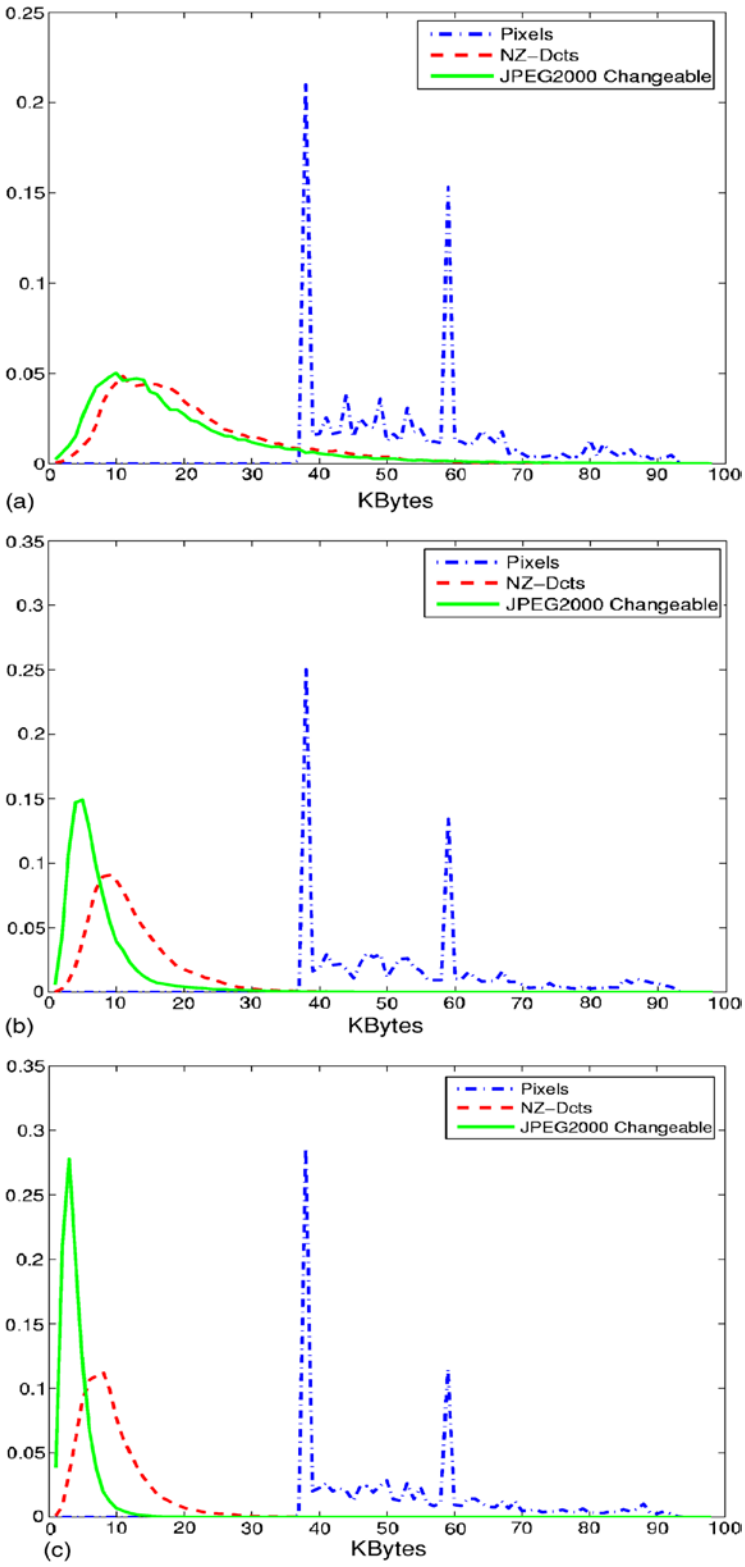
METHODS

J-Steg with sequential message embedding is detectable using the chi-square attack15. J-Steg with random straddling as well as JP Hide&Seek are detectable using the generalized chi-square attack. The chi-square attacks are not effective for F5 (because F5 does not flip LSBs) and for OutGuess (OutGuess preserves first-order statistics). The universal blind detector pioneered by Farid6 seems to be able to detect most steganographic methods after appropriate training on a database of stego and cover images. However, at the time of writing this paper, the blind detector does not naturally allow accurate estimation of the length of the embedded messages and it is not clear how its performance scales to more diverse databases. Also, this detector cannot detect messages embedded using F5 in grayscale images. The authors of this paper also believe that detection methods targeted to a specific steganographic technique will necessarily give better accuracy and detection reliability that blind approaches. Another important advantage of the approach proposed in this paper compared to previously introduced detection schemes is that one can obtain an accurate estimate for the length of the embedded secret message. In this paper, we will position ourselves into the role of a passive warden who inspects digital images and tries to identify those that contain secret messages. In particular, our goal is to estimate the number of embedding modifications (and thus the secret message length). We start the next section by introducing the concept of steganographic capacity (maximal number of bits that are “safe” to embed) in an informal manner. Then, in Section 3 we outline our strategy for design of steganalytic techniques capable of estimating the secret message length. In Section 4, we describe the steganalytic algorithm for F5 and in Section 5 the detection algorithm for OutGuess. The paper is concluded in Section 6 by outlining how the proposed methods can be used for estimating steganographic capacity. In the same section, we also state a

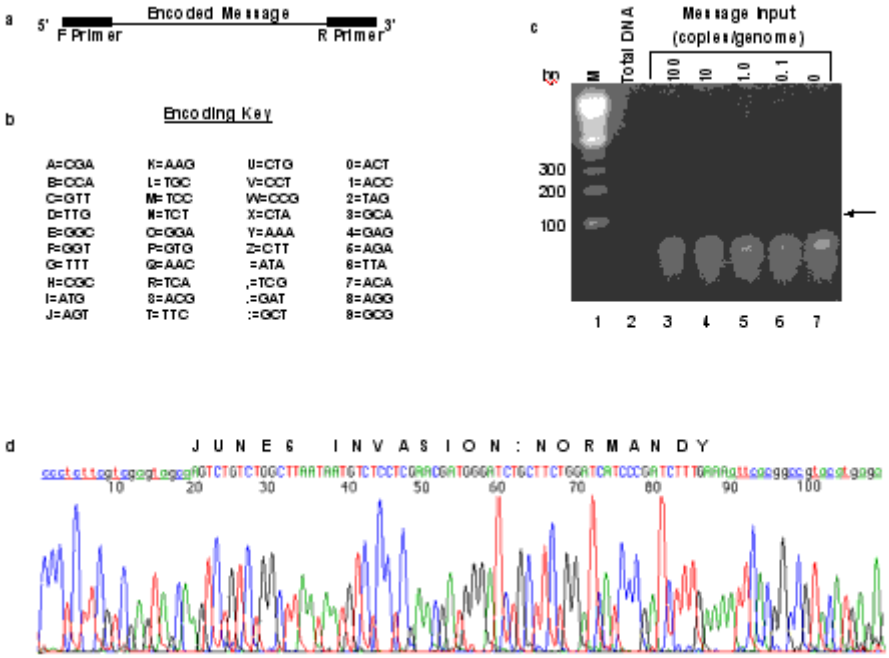
necessary condition for any high-capacity JPEG steganographic method to be secure against attacks of the kind described in this paper.

RESULTS

Result – 1



Result – 2



CONCLUSIONS

Here in this paper we have discussed various steganalysis schemes for breaking steganogrhy. We have been able to see the strengths and weaknesses of various stego-systems, not only from a steganographic viewpoint, but also in terms of how easy the artifacts of embedding can be spotted via steganalysis. By researching both sides of the field in parallel, it has been interesting to note that a trade-off seems to exist. It seems to be the case that the easiest stego-systems to implement, are also the easiest to attack, whereas the more complicated stego-systems are much harder to attack. This of course makes perfect sense as the more complex systems are likely to be so because they embed the message data in a more intricate fashion than the simpler systems.

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker. "Digital Watermarking and Steganography (Second Edition)", Morgan Kaufmann Publishers, ISBN: 978-0- 12- 372585-1, 2007.

[2] A. Dennis and B. Wixom. "Systems Analysis & Design (Second Edition)", John Wiley & Sons, Inc., ISBN: 04- 7136815-6, 2003.

[3] S. Dumitrescu, X. Wu, and Z. Wang. "Detection of LSB Steganography via Sample Pair Analysis", Lecture Notes in Computer Science, vol. 2578, pp. 355-372, 2003.

[4] H. Farid. "Detecting Hidden Messages Using HigherOrder Statistical Models", Proceedings of the International Conference on Image Processing, Rochester, NY, USA, 2002. International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012 Proceedings published by International Journal of Computer Applications® (IJCA) 15

[5] J. Fridrich, M. Goljan, and D. Hogea. "Attacking the OutGuess", Proceedings of the 3rd Information Hiding Workshop on Multimedia and Security 2002, Juan-lesPins, France, 2002.

[6] J. Fridrich, M. Goljan, and D. Hogea. "Steganalysis of JPEG Images: Breaking the F5 Algorithm", Lecture Notes in Computer Science, vol. 2578, pp. 310-323, 2003.

[7] J. Fridrich. "Feature-Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes", Lecture Notes in Computer Science, vol. 3200, pp. 67-81, 2004.