Advanced Science and Technology Letters
Vol.46 (Signal Processing 2014), pp.302-306
http://dx.doi.org/10.14257/astl.2014.46.63

Steganography Based Seaport Security Communication System

Yair Wiseman[1],

[1] Computer Science Department
Ramat-Gan 52900, Israel
wiseman@cs.biu.ac.il

Abstract. There is threat for any data in the hands of a port; however, there is no cybersecurity standard for the maritime industry or for enforcement agencies; though the need of secure transmission is essential. Nevertheless, using encrypted messages have a significant disadvantage. Everyone who sees the message knows there is a secret message. This paper presents a way of Steganography, to be exact - transmitting encrypted messages in images compressed by JPEG format. The algorithm actually changes the pictures a bit, but this change is unnoticeable. The image seems to be an innocent picture, while actually it does contain a data.

Keywords: Steganography, Discrete Cosine Transform, JPEG

1 Introduction

There is threat for any data in the hands of a port from vessel manifests to vessel traffic positions, particularly if it is used to perform automated tasks such as payroll, electronic alerts, bank deposits or infrastructure operations including locking gates or turning on floodlights. There is also threat for any computer-controlled functions of the port's lifelines such as water, sewer, fire or other emergency reactions. In addition, ports share data with authorities and the private sector. Storing or sending another part's data creates additional threats and have a need of an extra attention. There are no cybersecurity standards for the maritime industry or for enforcement agencies; however, there are some efforts to develop a uniform overall security system for the multifaceted connection of seaport security subsystems e. g. [1,2].
One of security main issues is encrypting messages in order to pass a financial data [3]. Our aim is showing how such a message can be smuggled in a JPEG image. This smuggling is commonly called Steganography [4,5]. Hiding a message can be very efficient in a financial or a martial community. A third person, who listens to the transmission, can think that just an innocent picture was transfer. This third person will not even try to break the code, because he will think there is no secret message in this message.

JPEG [6,7,8] images are saved as sets of frequencies. These frequencies are not accurate. They use to be saved as approximate values. Actually, some numbers divide the values. Then, the values are rounded, so the values can be saved in a less space.

ISSN: 2287-1233 ASTL

This approximation gives JPEG the ability of compressing images efficiently. These inaccurate values are very similar to the original values. It is very hard to notice where did JPEG change the original data. Taking one more step is using the least significant bits of the frequency values in order to save an encrypted message. The sequence values will be changed slightly, but again this change will be very hard to be distinguished.

The new sent message will be most likely much longer. Apparently, this is a disadvantage of this method [9]. However, such a cost may be worth, if being hidden is very important for the message. Nowadays, when communication lines become much faster, this disadvantage will become much less significant [10]. Downloading JPEG images from the web is a very common action. We can see that such an action does not consume a long time; so sending a JPEG image will not be a deficiency [11].

2 Steganography System Using JPEG

In the JPEG format the source image samples are grouped into 8X8 blocks, shifted from unsigned integer to signed integer, and input to Forward DCT [12,13]. In the case of JPEG format each 8X8 block of the source image samples is effectively a 64-point discrete signal which is a function of the 2D dimensional space x, and y. The FDCT takes such a signal as its input and decomposes it into 64 orthogonal basis signals. The output of the FDCT is the set of unique 64 basis signal amplitudes, which can be regarded as the relative amount of the 2D spatial frequency contained in the 64-point input signal [14,15].

The Steganography algorithm exploits the fact that JPEG values are intentionally not accurate anyway. It changes the least significant bits of the values so they will not contain a data of an image. These bits will contain an encrypted message.

The Steganography algorithm takes into account some or all of the following considerations:

- **The quality of a picture**

JPEG standard stipulates that a user can set the quality of the picture when he creates it. More qualitative image consumes more disk space [16]. The quality value is a number not less than 100. This value sets the numbers which divide the AC coefficients. When a smaller number divides an AC coefficient, more data will remain, so when reconstructing the image, the data will be more accurate and a better picture will be seen.

When using more qualitative image, the Steganography algorithm can insert more bits [17]. Almost every time a high quality image is used, the added data is redundant [18]. The Steganography algorithm can take advantage of this redundant data. It can replace the redundant data by an encrypted message.

- **Coefficients might be changed.**

Human's eye is more sensitive to first coefficients. Indeed, smaller numbers will divide the first coefficients, when JPEG performs the quantization step. On the other hand, because smaller numbers divide the first coefficients, they may have more data, which can be used by the Steganography algorithm.

The Steganography algorithm must take into account the size of the compressed data. JPEG treats the data as sequences. Each one of these sequences contains a sequence of zeros and another value at the end. When there are just zeros left in the end of a block, JPEG outputs an EOB. It is very common to find a block from a JPEG image with an EOB after about 20 coefficients or so [19,20]. The rest of the coefficients after the EOB are zeros, so they are not coded. If one of latter coefficients will be chosen and a non-zero number will be placed in it, a long sequence of zero will be added before this coefficient. The entropy encoder will recognize an irregular situation, which will yield a long code. Obviously, such codes will enlarge the space of an image.

- **The number of bits in each coefficient**

When using more bits in order to accommodate the encrypted message, fewer bits are left for the original value of the coefficient. The quality of the picture can be harmed. A poor quality picture might be suspicious. Someone might suspect that the picture passed some processing. This is exactly what we do not like to come about.

Sizes of compressed images were affected by number of non-zero values that were compressed. When we insert more bits, the chance to have a non-zero value will grow. In addition, small numbers are handled more efficiently by the compression method implemented in JPEG [21]. Usually, when there is a non-zero value in a latter coefficient, a long sequence of zeros will be before this coefficient. A long sequence of zeros before a non-zero value is a very rare case [22,23], so unlike dictionary codes [24,25] the entropy encoder will yield for this data, a long sequence of bits. This will increase the size of the compressed image.

Because of paper size constraints, the results of the experiments have been left out of this paper but can be found at this web site:

http://www.cs.biu.ac.il/~wiseman/steganography.pdf

4 Conclusions

The task of securing cyberspace has emerged as perhaps the single most important seaport security challenge of the decade [2]. An increasing number of functions are dependent on port computer systems and the Internet whereas security issues become more imperative [26,27]. JPEG takes off part of the image data, which seems to be redundant. It seems that more data can be removed; yet it will be hard to notice it. This redundant data can be exploited in order to transfer confidential messages.

References

1. Ochin, E., Dobryakova, L., Pietrzykowski, Z., and Borkowski, P., The application of cryptography and steganography in the integration of seaport security subsystems, Scientific Journals Maritime, Zeszyty Naukowe Akademia Morska w Szczecinie, 2012.
2. Musser, L., Securing Seaport Cyberspace, U.S. Department of Homeland Security, 2013.

3. Thiyagarajan, P., Aghila, G., and Venkatesan, V. P., Stepping up internet banking security using dynamic pattern based image steganography, Advances in Computing and Communications, pp. 98-112, Springer, 2011.
4. Li, B., He, J., Huang, J., and Shi, Y. Q., A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, Vol. 2(2), 142-172, 2011.
5. Cachin C., Digital steganography, Encyclopedia of Cryptography & Security, 348-352, 2011.
6. Wiseman, Y., The still image lossy compression standard – JPEG, Encyclopedia of Information and Science Technology, Third Edition, 2014.
7. Wallace G. K. The JPEG Still Picture Compression Standard Communication of the ACM 34, pp. 3-44, 1991.
8. Information Technology Digital Compression and Coding of Continuous-Tone Still Images Requirements and Guidelines International Standard ISO/IEC 10918-1, 1993.
9. Wiseman, Y., Schwan K. and Widener, P., Efficient End to End Data Exchange Using Configurable Compression, Operating Systems Review, Vol. 39(3), pp. 4-23, 2005.
10. Wiseman Y., A Pipeline Chip for Quasi Arithmetic Coding, IEICE Journal - Trans. Fundamentals, Tokyo, Japan, Vol. E84-A No.4, pp. 1034-1041, 2001.
11. Li, F., Zhang, X., Yu, J., and Shen, W.. Adaptive JPEG steganography with new distortion function. annals of telecommunications-annales des t él écommunications, pp. 1-10, 2014.
12. Wiseman Y. and Fredj E., Contour Extraction of Compressed JPEG Images, ACM - Journal of Graphic Tools, Vol. 6 No. 3, pp. 37-43, 2001.
13. Fredj E. and Wiseman Y., An O(n) Algorithm for Edge Detection in Photos Compressed by JPEG Format, Proc. IASTED International Conference on Signal and Image Processing SIP-2001, Honolulu, Hawaii, pp. 304-308, 2001.
14. Wiseman, Y., Fuselage Damage Locator System, Advanced Science and Technology Letters, Vol. 37, pp. 1-4, Jeju Island, Korea, 2013.
15. Wiseman, Y., Device for Detection of Fuselage Defective Parts, Information Journal, Tokyo, Japan, Vol. 17(6), 2014.
16. Wiseman, Y., Camera That Takes Pictures of Aircraft and Ground Vehicle Tires Can Save Lives, Journal of Electronic Imaging, Vol. 22(4), 041104, 2013.
17. Fridrich, J., Effect of cover quantization on steganographic fisher information., IEEE Transactions on Information Forensics and Security, Vol. 8(2), pp. 361-373, 2013.
18. Toor, R. K., & Kaur, R. (2012). A Steganographic Method Based Upon Jpeg and Quantization Table Modification, International Journal of Information Technology, Vol. 6(1), pp. 19-21, 2012.
19. Wiseman, Y., "Take a Picture of Your Tire!", Proc. IEEE Conference on Vehicular Electronics and Safety (IEEE ICVES-2010) Qingdao, ShanDong, China, pp. 151-156, 2010.
20. Wiseman, Y., The Effectiveness of JPEG Images Produced By a Standard Digital Camera to Detect Damaged Tyres, World Review of Intermodal Transportation Research, Vol. 4(1), pp. 23-36, 2013.
21. Wiseman Y., Burrows-Wheeler Based JPEG, Data Science Journal, Vol. 6, pp. 19-27, 2007.
22. Klein S. T. and Wiseman Y., Parallel Huffman Decoding with Applications to JPEG Files, The Computer Journal, Oxford University Press, Vol. 46(5), pp. 487-497, 2003.
23. Klein S. T. and Wiseman, Y., Parallel Huffman Decoding, Proc. Data Compression Conference DCC-2000, Snowbird, Utah, USA, pp. 383-392, 2000.
24. Klein S. T. and Wiseman Y., Parallel Lempel Ziv Coding, Journal of Discrete Applied Mathematics, Vol. 146(2), pp. 180-191, 2005.
25. Wiseman, Y., The Relative Efficiency of LZW and LZSS, Data Science Journal, Vol. 6, pp. 1-6, 2007.
26. Wiseman, Y., and Giat, Y., Multi-modal passenger security in Israel, Multimodal Security in Passenger and Freight Transportation: Frameworks and Policy Applications, Edward Elgar Publishing Limited, 2014.

27. Orosz, M. D., Milind, T., and Heather R.. Adaptive Real-Time eaport Security (DynaPortSec)-Integrated PortSec, Game Theory and Adaptive Adversary., 2013.

