2014

Detecting covert communication channels in raster images

Brian Cusack
Auckland University of Technology, brian.cusack@aut.ac.nz

Jarrett Chambers
Auckland University of Technology,, chambers.jarrett@me.com

DOI: 10.4225/75/57a84c3abefba
15th Australian Information Warfare Conference, held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

DETECTING COVERT COMMUNICATION CHANNELS IN RASTER IMAGES

Brian Cusack; Jarrett Chambers
Auckland University of Technology, Auckland, New Zealand
brian.cusack@aut.ac.nz chambers.jarrett@me.com

Abstract

Digital image steganography is a method for hiding secret messages within everyday Internet communication channels. Such covert communications provide protection for communications and exploit the opportunities available in digital media. Digital image steganography makes the nature and content of a message invisible to other users by taking ordinary internet artefacts and using them as cover objects for the messages. In this paper we demonstrate the capability with raster image files and discuss the challenges of detecting such covert communications. The contribution of the research is community awareness of covert communication capability in digital media and the motivation for including such checks in any investigatory analysis.

Keywords

Covert, Communications, Raster, Detection, Steganography

INTRODUCTION

Steganography dates back in recorded history and is translated as covered writing; 'Steganos' meaning covered, and 'Graphy' writing (Shih & Edupuganti, 2009). Steganography has taken many forms from invisible ink, microdots, through to covert channels in digital media. The primary goal of steganography is to hide a message in plain sight, and as such messages are sent via a non-suspicious medium with the hidden message concealed within where only the sender and receiver should be aware of the presence of hidden information. Whilst the goal of Steganography and Cryptography are essentially to securely store, or send information from point *a* to point *b*, these methods contrast fundamentally. The arguably more well-known art and science of Cryptography achieves this goal by performing an operation on the data to render it illegible to eavesdroppers, and in essence by a process of either transposition, substitution or a combination. The contrast between cryptography and Steganography lies in the fact that cryptography makes no attempt to hide a secret communication, whilst Steganography hides the existence. Essentially, this means that in cryptography scenarios eavesdroppers are attracted to the secret communication, whilst such messages in Steganography scenarios must be disclosed.

Every cryptographic, information hiding scheme is theoretically susceptible to attack. It is common knowledge that the opposing side of cryptography is cryptanalysis that uses methods to decrypt an encrypted message. Synonymously, Steganalysis is the art and science of detecting and uncovering a steganographic payload. Any steganographic system is said to be broken simply if it the very existence of the payload is detected, this is regardless of whether the actual message is understood (Cogranne, Zitzmann, Fillatre, Retraint, Nikiforov, & Cornu, 2011). In our research we simply want to demonstrate the capability for covert communications in the media and then to suggest ways to detect steganography. The implication of this research are for both legitimate and illegitimate uses of the technology but principally community awareness. The paper begins with a background literature review, and elaboration of research problem areas, a demonstration of the iSteg tool for embedding covert messages and the detection of such messages. The concluding discussion reviews the importance for awareness of covert communication capability in digital media and the necessity of including such checks in any digital investigation.

BACKGROUND LITERATURE

Theoretically, the sending and storing of secret information is achievable in any digital computer generated file. However it is shown that the embedding of secret information is best suited to digital media (Singh & Siddiqui, 2012). This is because digital media files such as audio, images, and video contain a large amount of redundant information. Redundant in the sense that many of the frequencies used to render information in such files are in actuality, invisible or in audible to the human senses, as they are out of the ranges detectable by human senses. This is demonstrated in digital images whereby the noisy areas or areas in an image with more variation or

texture have a higher rate of colour changes can be used to exploit imperceptibly and hide information. In raster format images the opportunity is greater because there are more combination of colour scales to use and to manipulate for message hiding (Varsaki, Fotopoulos & Skodras, 2013). Two characteristics are of primary concern when hiding messages, the level of imperceptibility, and payload size (Li, Luo, Li & Fang, 2009). For any steganographic system to be successful, the two requirements must be satisfied. The researcher challenge is that there is a trade-off between these two characteristics, as the embedded messages size increases, the more the cover medium will degrade. Consequently when using covert channels in raster images the trade-off may be satisfied in several ways. Raster images are computer generated images which are composed of individual pixel elements. Each pixel defines the colour composition at each location in a grid like fashion and are the elemental building blocks for the digital images. Each pixel is in essence, a stored value representing the value of Red, Green, and Blue (RGB) as a ratio for every colour in the human visible spectrum that may be represented as a ratio of RGB. This ratio is then interpreted by the computer based on the image file format to render the image on the screen. Hiding information is possible in one of three methods: 1. the naïve method whereby secret information is hidden at the end of the file; 2. spatial methods using the Least Significant Bit (LSB) method, secret information is hidden in the LSB of selected pixels; and 3. Frequency domain, where images are transformed to other representative domains and information is hidden by modification of this frequency representation (Chang, Chen, & Lin, 2009).

Digital image steganography is achieved by two fundamentally differing methods: 1. In the Spatial Domain, and 2. In the Transform domain. In the spatial domain the digital image is a grid or matrix of *M x N* pixel elements, and each element is considered as a building block for the human visual impression. The individual pixel elements can be directly modified in such a way as to conceal hidden information. Whereas in the transform domain, the entire image is transformed to a frequency representation of the colour values of the image (Hemalatha, Acharya, Renuka, & Kamath, 2012). Here the frequencies can be modified in such a way as to conceal hidden information. The two methods are consequently helpful for covert communications and both must be checked in investigatory analysis. There a number of spatial methods and we use the LSB method that exploits the Human Visual System (HVS) as an example. Less distortion is created by embedding in the LSB and the colour degrades less by inserting a Most Significant Bit (MSB) (Liao, Wen, & Zhang, 2011). The LSB method considers the least significant bit plane shown in Figure 1. (Sun, Li, Zhong, & Li, 2012). The colour coded bit is the covert message.

	Pixel 1	**Pixel 2**	**Pixel 3**
R	1001010 1	00011011	11000111
G	01101001	10110111	
B			

R
G
B 11001010 11010100 10100011

Figure 1. Least significant bit plane of three pixels

In figure 2 the code of figure 1 is represented in the specified colours as a human visual representation. The encoded message is not visible to the human eye (HVS).

Figure 2. Resulting pixels from the pixel values

As there are 8 bits per Byte we may hide one Byte into these three pixels. For illustration if we take the letter A, converted to binary is 01000001. This is embedded in the LSB by literally replacing the LSB plane with this new value shown in Figure 3. Thus, it takes three bits to hide one character.

	Pixel 1	**Pixel 2**	**Pixel 3**
R	10010100	00011010	11000110
G	01101001	10110110	10101011

B 11001010 11010100 10100011

Figure 3. Least significant bit plane

Shown in Figure 4 the resulting pixel colours are imperceptible to the HVS and this is the strength of LSB steganography. Information hiding in the LSB method is very simple to achieve and has a high level of imperceptibility.

Figure 4. Resulting colours after embedding

The selection of pixels is not trivial and the selection is either based on a random key generation dispersing the hidden messages pseudo randomly, or based on the characteristics of the image such as the exploitation of the HVS by using intelligent techniques to identify the noisy sections of an image that can hold data securely without being noticed (Li, Luo, Li, & Fang, 2009).

DETECTING COVERT COMMUNICATIONS

The question arises as to how these simple methods of covert communication may be detected. Steganalysis is the art and science of uncovering Steganographic payloads, and is synonymous to the more well-known concept of Cryptanalysis. Any steganographic system is broken as soon as the presence of a Steganographic payload is detected, and the actual payload does not need to be extracted to be considered broken (Bohme, 2008). This is because various attacks may be performed on the media in order to render the hidden information unrecoverable, such as resizing, cropping and various other attacks which modify the image contents destroying any hidden messages (Kodovsky, & Fridrich, 2013). The primary objective is to hide information in plain sight so that the message is in fact invisible. In this case, therefore, clearly the uncovering of the existence of an underlying message defeats the primary purpose. Once Steganography is detected, attacks can be made to hinder communication and in this way the message is destroyed. Steganalysis may be performed by simple naïve approaches such as side by side comparison between original image and suspected Steganographic image. Side by side comparison may first begin by a visual comparison, where certain tell-tale signs occur as detected from particular Steganographic techniques, such as blockiness, areas with uncharacteristic deviations in contrast. Side by side comparisons may also consist of file size, inconsistencies and calculated pixel value histograms. However, the sophisticated algorithms being developed provide highly imperceptible differences to both the HVS and to computer assisted comparisons, and as such more sophisticated Steganalysis techniques require development.

There are two primary branches of advanced Steganalysis techniques: 1. Blind attack methods, and 2. Targeted attack methods. Both blind and targeted attack methods are achieved by comparing suspected images against known resulting statistical anomalies typical of modification by Steganographic methods; and, those which deviate past a given threshold are deemed to carry a payload. Blind methods are used to simply detect the presence of a steganographic payload potentially from any Steganographic technique (Hashemipour, & Mohammad Rahmati, 2012), however, blind attacks may be tailored for a particular file type such as JPEG (Yu, 2012). Whereas, targeted attacks are attacks targeted towards known specific Steganographic methods and techniques (Tan, 2012). There is a trade-off between using blind and targeted methods, targeted methods are more robust in instances where the Steganographic technique used is not known, or whether there is any Steganographic payload at all. Whereas, targeted attacks will typically be tailored for a specific Steganographic technique, and as such will not detect payloads which are created with different methods. To graphically demonstrate these points a hypothetical case can be developed regarding information leakage from a business or the command and control communications of a terror cell. Applying the fundamentals of spatial image Steganographic techniques and specifically the LSB method. The least significant bit of each selected pixel is replaced with one of the message. To this end the industry outguess tool is used to embed a small text file of hypothetical secret instructions called instructions.txt at 5KB in size into Lena.jpg having a resolution of 512x512 pixels in Figure 5 (a).

Figure 5 (a) Lena image before embedding process, (b) Lena image after embedding process.

Traditionally Steganalysis is performed by conducting a side by side analysis or comparison of the suspected Steganographic image with that of the original image, making note of any discrepancies. A primary mechanism used in any digital image analysis and processing field is the image histogram which represents the frequency of each colour in the image, the image histogram is used as a key mechanism to computationally describe the image. From the resulting histogram many numerical measurements may be calculated and derived to both analyse the large array of data giving a more succinct analysis than human eyes alone, but also allowing the automation of comparison.

A common practice is to average the RGB channels to obtain an intensity image by $I = (R + G + B) / 3$, the average gives an approximation. The ratio or weightings of the R, G, and B channels may be adjusted for accuracy, for simplicity of this demonstration the weightings are equal. If the intensity images is taken of both the cover image of Lena.jpg Figure 5 (a), and the Stego image Covert.jpg Figure 5 (a) shown in Figure 6 (a) and Figure 6 (b) respectively we can see slight differences in the shape that the HVS whereas the HVS Figure 5 (a) and Figure 5 (b) are indistinguishable from one another.

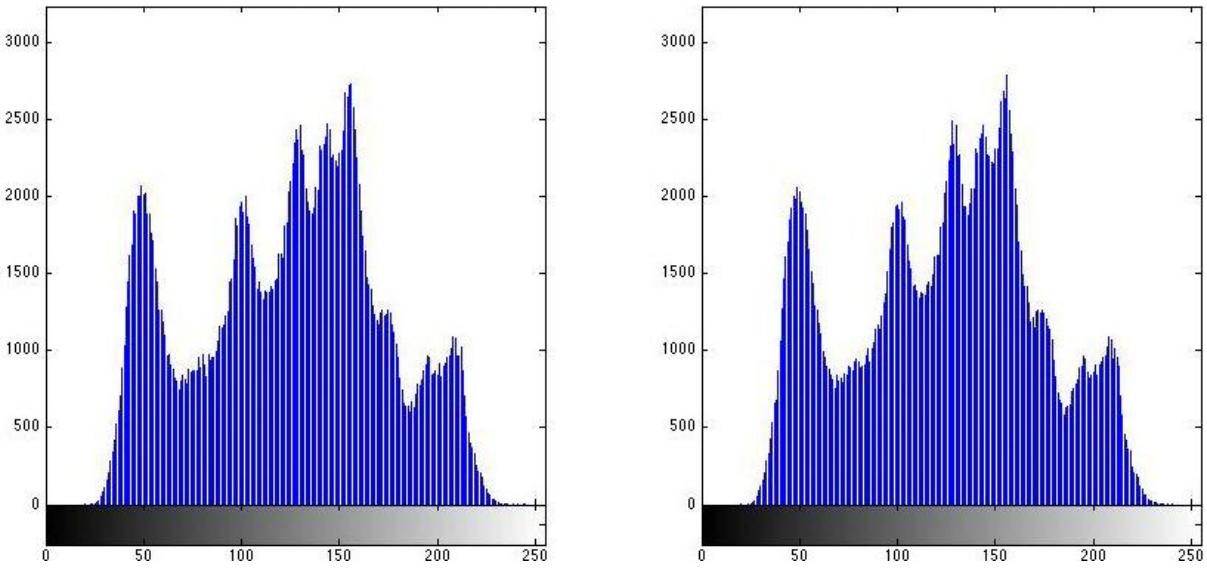

Figure 6 (a) Lena image before embedding process, (b) Lena image after embedding process.

The outguess tool is intelligent in the sense that care is taken to estimate the most unnoticeable areas to embed within. By comparing the two images alone we are unable to distinguish one from the other, however by

comparing the resulting histograms side by side there are some slight visual differences. Particularly, there are areas in the stego image histogram which has been smoothed from around the gray levels near 50. We can also see the higher frequency range has been shortened from around 248 to around 240 indicating that an even spread of embedding in light to dark areas has occurred and this fits with the idea that more advanced algorithms embed in the areas where there is a transition from light to dark. Such a histogram gives an entry point into the conclusion as to whether there exists a steganographic payload. More advanced analysis techniques may also be performed by performing histogram shape descriptors and typical statistic anomalies.

DISCUSSION

Figures 1 to 4 have demonstrated the simplicity and imperceptibility of embedding covert messages into a raster file. Imperceptibility to the HVS does not imply Steganalysis fails. As we have shown in figure 5 (b) statistical analysis of the image discloses the payload of the embedded files. The mapping of anomalies from one image to another using a variety of tools and approaches that include orchestrated attacks for zero difference assessments, can disclose hidden messages. The implications of the demonstration are twofold. One is that the community of researchers and practitioners are alerted to the fact that covert communications are easy to do and to deliver through most Internet media. Secondly we show the direction Steganalysis may go for further development. Tools and tool development are crucial in opening digital media for Steganographic scrutiny and a direction researchers may move in.

The detection of hidden messages is necessary in the fight against the distribution of dangerous material and unlawful activities, and it may also provide useful intelligence leading to further investigation. In terms of information warfare disclosure is as good as decryption. A key advantage in being able to decipher and extract such payloads provides law enforcement, and intelligence agencies with a stronger repertoire in the penetration of unlawful networks. For example, if two use case illustrations were used to elaborate the detection of covert channels in raster images, one from the corporate domain and another from the protection of public interest. Firstly, consider the scenario whereby an employee whom is contracted to work for company A on developing a ground-breaking new technology, the employee in question is approached company B and offered a considerable sum of money to provide inside information enabling an unfair technical advantage through reverse engineering. Company A stands to lose out on considerable financial gain for their effort should company B be provided with such information, Steganographic images may be used to provide company B with the desired information, and it would go unnoticed as only the employee and company B are aware of the presence of hidden information. This scenario has been popularised in a number of feature films over recent decades, and is by no means a fictional problem rather a definite reality.

Secondly, consider a scenario in the public domain that has received varying levels of media attention in recent decades. The exchange of two forms if illegal information: 1. The exchange of questionable images and information in conjunction with human trafficking, and 2. The exchange of anti-state information leading to the very real possibility of commands and directions directly leading to the harm and injury of innocent person(s). Steganography is both useful for legitimate purposes in protecting media and personal privacy, however unfortunately illegitimate and questionable uses are equally likely and are indeed a real and present threat. By utilising Steganalysis methods to detect Steganographic payloads company A may be able to improve the security intelligence posture by actively detecting possible leaks of top secret intellectual trade secrets. Similarly, state intelligence agencies, law enforcement, military and similar agencies may utilise Steganalysis techniques on key known targets in order to thwart future harm through, abuse, trafficking or terror attacks. Clearly, the legitimate use of steganography has benefits in protecting privacy and media, whilst Steganalysis protects privacy by addressing the exchange of questionable and illegal information. Clearly, there are both benefits and ill effects of both Steganographic methods and Steganalysis methods. The adoption of methods defined by the context in which such techniques are applied and for which it is within legitimate and lawful use. Steganography may be used for legitimate reasons, to protect personal privacy and protect intellectual property such as copyrighted material. Similarly, Steganography may be used for questionable and illegal purposes such as stealing, hiding, and transmitting of information such as trade secrets. Steganography may also be used to hide, and transmit questionable images and information or instructions leading to the harm of innocent person(s).

CONCLUSION

The human visual system may be exploited using Steganographic techniques to hide hidden information. This may provide covert channels for communications, for protecting privacy and providing property security. The

research focus was on raster images but any digital medial may carry covert communications, such as digital audio, game files, video, and potentially any other digital computer generated file. Covert communication unfortunately whilst it has benefits for protecting privacy and giving secure communications, it may also be used for unethical and unlawful purposes. As such it is necessary to be aware of techniques and tools that may assure adequate detection and correct usage of the digital opportunities. We have demonstrated for the purpose of community awareness the embedding techniques, the detection processes and the existence of the covert communication channel.

REFERENCES

Bhattacharyya, D., & Kim, T. (2011). Image Data Hiding Technique Using Discrete Fourier Transformation. Ubiquitous Computing and Multimedia Applications, *151*(1), 315-323. doi: 10.1007/978-3-642-20998-7_39

Bilal, M., Imtiaz, S., Abdul, W. & Ghouzali, S. (2013). Zero-steganography using DCT and Spatial domain.. 2013 ACS International Conference on Computer Systems and Applications (AICCSA), 1-7. doi:(10.1109/AICCSA.2013.6616431)

Bohme, R. (2008). Weighted Stego-Image Steganalysis for JPEG Covers. Information hiding, 5284(1), 178-194. doi:10.1007/978-3-540-88961-8_13

Chang, C., Chen, Y., & Lin, C. (2009). A data embedding scheme for color images based on genetic algorithm and absolute moment block truncation coding. Soft Computing, *3*(4), 321-331. doi: 10.1007/s00500-008-0332-x

Chen, W. (2007). Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation. Applied Mathematics and Computation, *185*(1), 432-448. doi: 10.1016/j.amc.2006.07.041

Cogranne, R., Zitzmann, C., Fillatre, L., Retraint, F., Nikiforov, I., & Cornu, P. (2011). A Cover Image Model For Reliable Steganalysis. Information hiding, *6958*(1), 178-192. doi:10.1007/978-3-642-24178-9_13

Hashemipour, S. M., & Mohammad Rahmati, M. (2012). A Statistical Blind Image Steganalysis based on Image Multi-classification. 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 150-153. doi:10.1109/IIH-MSP.2012.42

Hemalatha, S., Acharya, D., Renuka, A., & Kamath, P. (2012). A Novel Color Image Steganography using Discrete Wavelet Transform. Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology - CCSEIT '12, 223-226. doi:10.1145/2393216.2393254

Kodovsky, J., & Fridrich, J. (2013). Steganalysis in Resized Images. 2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2857-2861. doi: 10.1109/ICASSP.2013.6638179

Li, L., Luo, B., Li, Q., & Fang, X. (2009). A Color Images Steganography Method by Multiple Embedding Strategy Based on Sobel Operator. International Conference on Multimedia Information Networking and Security MINES '09, *2*(1), 118-121. doi:10.1109/MINES.2009.187

Li, X., Li, B., Luo, X., Yang, B., & Zhu, R. (2013). Steganalysis of a PVD-based content adaptive image steganography. Signal Processing, *93*(9), 2529-2538. doi: 10.1016/j.sigpro.2013.03.029

Liao, X., Wen, Q., & Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing and modified LSB substitution. Journal of Visual Communication and Image Representation, *22*(1), 1-8. doi: 10.1016/j.jvcir.2010.08.007

Liaw, J., Wang , W., & Chiu, M. (2010). A Data Hiding Method Using Secret Data Division and Pixel Value Differencing. Fourth International Conference on Genetic and Evolutionary Computing, 650-653. doi:10.1109/ICGEC.2010.166

Sathisha, N., Babu, S. k., Raja, K. B., Venugopa ,K. R., & Patnai, L. M. (2011). Covariance Based Steganography Using DCT. Information Technology and Mobile Communication, *147*(1), 636-647. doi:10.1007/978-3-642-20573-6_45

Shih, F. Y., & Edupuganti, V. G. (2009). A differential evolution based algorithm for breaking the visual steganalytic system. *Soft Computing*, *13*(4), 345–353. doi:10.1007/s00500-008-0330-z

Singh, S., & Siddiqui, T. J., V. G. (2012). Robust Image Steganography Technique Based on Redundant Discrete Wavelet Transform. 2012 2nd International Conference on Power, Control and Embedded Systems (ICPCES), *2*(1), 1-4. doi:10.1109/ICPCES.2012.650808

Sun, J., Li, Y., Zhong, X., & Li, J. (2012). A Scheme of LSB Steganography Based on Concept of Finding Optimization Pixels Selection. Software Engineering and Knowledge Engineering: Theory and Practice, *115*(1), 155-160. doi: 10.1007/978-3-642-25349-2_21

Tan, S. (2012). IEEE Signal Processing Letters. Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting, *19*(6), 336-339. doi: 10.1109/LSP.2012.2194702

Varsaki E. E., Fotopoulos, V., Skodras, A. N. (2013). Data hiding based on image texture classification. Signal, image and video processing, *7*(2), 247-253. doi:10.1007/s11760-011-0229-5

Yang, C., Weng, C., Tso, H., & Wang, S. (2011). A data hiding scheme using the varieties of pixel-value differencing in multimedia images. Journal of Systems and Software, *84*(4), 669-678. doi: 10.1016/j.jss.2010.11.889

Yu, W. (2012). Blind Detection for JPEG Steganography. 2010 International Conference on Networking and Information Technology (ICNIT), 128-132. doi:10.1109/ICNIT.2010.5508546