International Journal of Computer Science and Informatics

Volume 1 | Issue 3 Article 12

January 2012

Digital Image Steganography

Anu Jangra
Gurgaon College of Engineering, Gurgaon, Haryana, anu.jangra@gmail.com

Available online at www.interscience.in

Digital Image Steganography

ANU, REKHA, PRAVEEN
Gurgaon College of Engineering, Gurgaon, Haryana
E-mail : anu.jangra@gmail.com

Abstract - Steganography is defined as the science of hiding or embedding data in a transmission medium. Its ultimate objectives, which are undetectability, robustness (i.e., against image processing and other attacks) and capacity of the hidden data (i.e., how much data we can hide in the carrier file), are the main factors that distinguish it from other sisters-in science. techniques, namely watermarking and Cryptography. This paper provides an overview of well known Steganography methods. It identifies current research problems in this area and discusses how our current research approach could solve some of these problems. We propose using human skin tone detection in colour images to form an adaptive context for an edge operator which will provide an excellent secure location for data hiding.

1. INTRODUCTION

The concept of "What You See Is What You get (WYSIWYG)" which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a Steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence they can convey more than merely 1000 words. For decades people strove to create methods for secret communication. Although Steganography is described elsewhere in detail [1, 2, 3], we provide here a brief history. The remainder of this section highlights some historical facts and attacks on methods (Steganalysis).

1.1 The Ancient Steganography

The word Steganography is originally made up of two Greek words which mean "*Covered Writing*". It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and was dispatched with the message after his hair grew back [1, 2, 3, 4].

In Saudi Arabia at the king Abdulaziz City of Science and Technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [5]. 500 years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing, its scenario goes as follows: A paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the letter appears as an innocuous text.

In more recent history, the Nazis invented several Steganographic methods during WWII such as Microdots, invisible ink and null ciphers. As an example of the latter a message sent by a Nazi spy that read: "Apparently neutral.s protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.. Using the 2nd letter from each word the secret message reveals: .Pershing sails from NY June 1. [2].

1.2 The Digital Era of Steganography

With the boost of computer power, the internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, Steganography went "*Digital*". In the realm of this digital world Steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications of the science. Contemporary information hiding was first discussed in the article "The prisoners' Problem and the Subliminal Channel" [6]. More recently Kurak and McHugh [7] carried out work which resembled embedding into the 4LSBs (Least Significant Bits). They discussed image downgrading and contamination which is now known as Steganography. Cyber-terrorism, as coined recently, is believed to benefit from this digital revolution.

Cyber-planning or the "*digital menace*" as Lieutenant Colonel Timothy L. Thomas defined it is difficult to control [8]. Provos and Honeyman [3] scrutinized 3 million images from popular websites looking for any trace of Steganography. They have not found a single hidden message. Despite the fact that they gave several assumptions to their failure they forget that

Steganography does not exist merely in still images. Embedding hidden messages in videos and audios is also possible and even in a simpler form such as in Hyper Text Mark up Language (HTML), executable files (.EXE) and Extensible Markup Language (XML) [11].

Steganography is employed in various useful applications e.g., Copyright control of materials, enhancing robustness of image search engines and Smart IDs where individuals' details are embedded in their photographs. Other applications are Video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, Transmission Control Protocol and Internet Protocol packets (TCP/IP) - for instance a unique ID can be embedded into an image to analyze the network traffic of particular users [1], embedding Checksum [10], etc. In a very interesting way Petitcolas [9] demonstrated some contemporary applications; one of which was in *Medical Imaging Systems* where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions e.g., Physician, Patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems. In this context this can create other issues regarding patients' data confidentiality (see the Guardian Unlimited1 (all superscripts are referenced at the internet resources): "Lives ruined as NHS leaks patients' notes" By Anthony Browne, Health Editor, Sunday June 25, 2000; Rita Pal, a hospital doctor who set up the pressure group NHS Exposed, said:

"*Medical notes are in essence your life - how many affairs you have, if you have an alcohol problem, do drugs, your sexual activity, your psychiatric state. They are all very personal issues. Yet patients have no control over their confidentiality*." Marion Chester, legal officer at the Association of Community Health Councils, said: "*Identifiable health records are flying around inside and outside the NHS at a rate of knots. It's getting worse, because of the increase in financial and clinical audit, and the increasing use of information technology. The attitude to patient confidentiality is very lax in the NHS*."

Inspired by the notion that Steganography can be Japanese firm Fujitsu2 is pushing technology to encode data into a printed picture that is invisible to the human eye (i.e., data) but can be decoded by a mobile phone with a camera. The process takes less than 1 second as the embedded data is merely 12 bytes. Hence, users will be able to use their cellular phones to capture encoded data. They charge a small fee for the use of their decoding software which sits on the firm's own servers. The basic idea is to transform the image color scheme prior to printing to its Hue, Saturation and Value components (HSV). They then embed into the Hue domain to which human eyes are not sensitive. Mobile cameras can see coded data and retrieve it.

1.3 Steganalysis

Steganalysis is the science of attacking Steganography in a battle that never ends. It mimics the already established science of Cryptanalysis. Note that a Steganographer can create a Steganalysis merely to test the strength of her algorithm. Steganalysis is achieved through applying different image processing techniques e.g., image filtering, rotating, cropping, translating, etc, or more deliberately by coding a program that examines the stego-image structure and measures its statistical properties e.g., first order statistics (histograms), second order statistics (correlations between pixels, distance, direction). Apart from many other advantages higher order statistics, if taken into account before embedding, can improve the signal-to-noise ratio when dealing with Gaussian additive noise [12]. In a less legitimate manner, virus creators can exploit Steganography for their ill intention of spreading *Trojan Horses*. If that were to happen, anti-virus companies should go beyond checking simply viruses' fingerprints as they need to trace any threats embedded in image, audio or video files using Steganalysis. Passive Steganalysis is meant to attempt to destroy any trace of secret communication whether it exists or not by using the above mentioned image processing techniques, changing the image format, flipping all LSBs or by lossy compression e.g., JPEG. Active Steganalysis however, is any specialized algorithm that detects the existence of stego-images. There are some basic notes that should be observed by a Steganographer:

1- In order to eliminate the attack of comparing the original image file with the stego image where a very simple kind of Steganalysis is essential, we can newly create an image and destroy it after generating the stego image. Embedding into images available on the World Wide Web is not advisable as a Steganalysis devotee might notice them and opportunistically utilize them to decode the stego.

2. STEGANOGRAPHY METHODS

2.1 Steganography Exploiting Image Format

Steganography can be accomplished by simply feeding into a Microsoft XP command window the following half line of code:

```
C:\> Copy Cover.jpg /b + Message.txt /b
Stego.jpg
```

This code appends the secret message found in the text file 'Message.txt' into the JPEG image file 'Cover.jpg' and produces the stego-image 'Stego.jpg'. The idea behind this is to abuse the recognition of *EOF* (End of file). In other words, the message is packed and inserted after the *EOF* tag.

2.2 Steganography in the Spatial Domain

In spatial domain methods a Steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the simplicity.

2.3 Steganography in the Frequency Domain

New algorithms keep emerging prompted by the performance of their ancestors (Spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS, its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain. DCT is used extensively in Video and image (i.e., JPEG) lossy compression.

Most of the techniques here use a JPEG image as a vehicle to embed their data. JPEG compression uses DCT to transform successive sub-image blocks (8x8 pixels) into64 DCT coefficients.

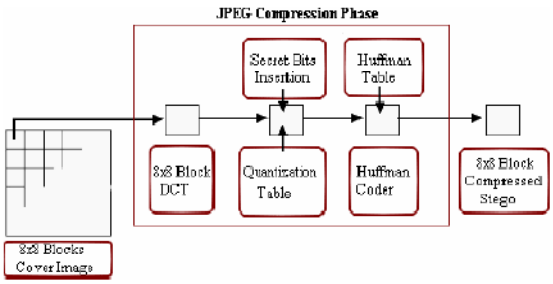


Figure 1. Data Flow Diagram showing a general process of embedding in the frequency domain.

2.4 Performance Measure

As a performance measurement for image distortion, the well known Peak-Signal-to-Noise Ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego images. It is defined as:

$$PSNR = 10 \log_{10} \left(\frac{C_{max}}{MSE} \right)$$

where *MSE* denotes the Mean Square Error which is given as:

$$MSE \quad \frac{1}{MN} \sum_{=}^{M} \sum_{=} \left({}^{N}S_{xy} - C_{xy} \right)^2$$

and holds the maximum value in the image, for example:

$$C_{max} \leq \begin{cases} 1 \text{ in double precision intensity images} \\ 255 \text{ in 8-bit unsigned integer intensity images} \end{cases}$$

x and y are the image coordinates, M and N are the dimensions of the image, $S_{xy}$is the generated stego image and $C_{xy}$is the cover image.

2.5 Adaptive Steganography

Adaptive Steganography is a special case of the two former methods. It is also known as "*Statistics-aware embedding*" [3] and "*Masking*" [1]. This method takes statistical global features of the image before attempting to interact with its DCT coefficients. The statistics will dictate where to make the changes. This method is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD *Standard Deviation* .The latter is meant to avoid areas of uniform colour e.g., smooth areas. This behaviour makes adaptive Steganography seek images with existing or deliberately added noise and images that demonstrate colour complexity. Wayner [32], dedicated a complete chapter in a book to what he called 'life in noise', pointing to the usefulness of data embedding in noise. It is proven to be robust with respect to compression, cropping and image processing [29].

Whilst simple, edge embedding is robust to many attacks (given its nature in preserving the abrupt change in image intensities) and it follows that this adaptive method is also an excellent means of hiding data while maintaining a good quality carrier.

Chang et al., [37] propose an adaptive technique applied to the LSB substitution method.

3. EMBEDDING IN THE SKIN TONE COLOUR SPACE

For adaptive image content retrieval in sequences of images (e.g., GIF, Video) we can use colour space transformations to detect and track any presence of human skin tone. The latter emerged from the field of Biometrics, where the threefold *RGB* matrix of a given image is converted into different colour spaces to yield distinguishable regions of skin or near skin tone. Colour transformations are of paramount importance in computer vision. There exist several colour spaces and here we list some of them *RGB, CMY, XYZ, xyY, UVW, LSLM, L*a*b*, L*u*v*, LHC, LHS, HSV, HSI, YUV, YIQ, YCbCr*. Mainly two kinds of spaces are exploited in the literature of biometrics which are the *HSV* and *YCbCr* spaces. It is experimentally found and

1) When the embedding is spread on the entire image (or frame), scaling, rotation or cropping will result in the destruction of the embedded data because any reference point that can reconstruct the image will be lost. However, skin tone detection in the transformed colour space ensures immunity to geometric transforms.

2) Our suggested scheme modifies only the regions of the skin tone in the colour transformed channel, this is done for imperceptibility reasons.

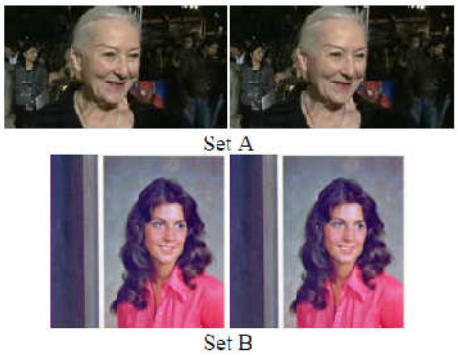
3) The skin-tone has a centre point at Cb, Cr components, it can be modelled and its range is known statistically, therefore, we can embed safely while preserving these facts. Moreover, no statistical breach occurs whether it is of first order or second order type.

4) If the image (or frame) is tampered with by a cropping process, it is more likely that our selected region will be in the safe zone, because the human faces generally demonstrate the core elements in any given image and thus protected areas (e.g., portraits).

5) Our Steganographic propos and MPEG7 standards (the concept of Video Objects (VOs) and their temporal instances, Video Object Planes (VOPs) is central to MPEG video) [41]. al is consistent with the object based coding approach followed in MPEG4

6) Intra-frame and Inter-frame properties in videos provide a unique environment to deploy a secure mechanism for image based Steganography. We could embed in any frame password and a link to the next frame holding the next portion of the hidden data in the video. Note this link does not necessarily need to be in a linear fashion (e.g., frames 100 12 3... n).

7) Videos are one of the main multimedia files available to public on the net thanks to the giant free web-hosting companies (e.g., YouTube, Google Videos, etc).



(left) Original test images and (right) Stego images

4. CONCLUSION

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. We have presented in this work some background discussions on algorithms of Steganography deployed in digital imaging. The emerging techniques such as DCT, DWT and Adaptive Steganography are not an easy target for attacks, especially when the hidden message is small.

REFERENCES

[1] Johnson, N. F. and Jajodia, S.: Exploring Steganography: Seeing the Unseen. IEEE Computer, 31 (2): 26-34, Feb 1998. [2] Judge, J.C.: Steganography: Past, Present, Future. SANS Institute publication, December 1, 2001. Retrieved from: http:// www.sans.org/reading_room/whitepapers /stenganography/ 552.php

[3] Provos, N. and Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security and Privacy, 01 (3): 32-44, May-June 2003.

[4] Moulin, P. and Koetter, R.: Data-hiding codes. Proceedings of the IEEE, 93 (12): 2083- 2126, Dec. 2005.

[5] Sadkhan, S. B.: Cryptography: Current Status and Future Trends. IEEE International Conference on Information & Communication Technologies: From Theory to Applications. Damascus. Syria: April 19 - 23, 2004.

[6] Simmons, G. J.: The Prisoners' Problem and the Subliminal Channel. Proceedings of CRYPTO83- Advances in Cryptology, August 22-24. 1984. pp. 51.67.

[7] Kurak, C. and McHugh, J.: A cautionary note on image downgrading. Proceedings of the Eighth Annual Computer Security Applications Conference. 30 Nov-4 Dec 1992 pp. 153-159.

[8] Thomas, T. L.: Al Qaeda and the Internet: The Danger of "Cyberplanning". Parameters, US Army War College Quarterly- Spring 2003.