Biometric Inspired Digital Image Steganography

Sonia Maria D'Souza
CSE
CiTech
Bangalore, India
soniamariadsouza@yahoo.com

Chris Davis Perumal
CSE
CiTech
Bangalore, India
chrisdperumal@gmail.com

Smitha H S
CSE
CiTech
Bangalore, India
Smitha.h3@gmail.com

Abstract— Steganography is defined as the science of hiding "data" in a transmission medium. The main objectives while hiding data are its undetectability, robustness against image processing and other attacks, also the capacity of the hidden data - how much data we can hide in the carrier; are the main factors that differentiate it from other similar techniques such as watermarking and cryptography. Steganography can be described as Cryptography's dark cousin. In this paper we discuss using human skin tone detection in colour images to form an adaptive context for an edge operator which will provide a secure location for data hiding.

Keywords— Cryptography, steganalysis, Data compression, Image registration, Multimedia systems,Redundancy, Quantization,Camouflage, spatial domain, Steganoflage, Watermarking.

I. INTRODUCTION

When it comes to printing images and other data, the prevalent technology is based on "What You See Is What You Get" (WYSIWYG). However, this does not always hold true and it would certainly not fool a Steganographer. Images can be more than what we see with our Human Visual System (HVS). For decades people strove to create methods to communicate secretly. The principles behind Steganography are described elsewhere [1, 2, 3], here we aim to provide a brief history of Steganography. The remainder of this section highlights some historical facts and attacks on methods (Steganalysis).

A. ANCIENT STEGANOGRAPHY

The word 'Steganography' is made up of two Greek words, *steganos* meaning *covered or concealed* and *graphei* meaning *writing.* The idea has been used in various forms for thousands of years, the earliest known record dating to the 5th Century BC, a slave Histiaeus had a message tattooed on his shaved head and was later dispatched when his hair had grown back. [1, 2, 3, 4]. In Saudi Arabia at the King Abdulaziz City of Science and Technology, a project was initiated to translate 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. A little over 500 years ago, the Italian mathematician Jerome Cardan reinvented an ancient Chinese method of secret writing. The method goes as follows: Identical paper masks with holes are shared among two parties, one of these masks is placed over a blank paper and the sender writes his secret message through the holes and then takes the mask off. The remaining blanks are filled so that the letter appears to be ordinary text. This method is credited to Cardan and is called the Cardan Grille [4].
In more recent history during World War II, the Nazis invented several Steganographic methods such as Microdots, invisible ink and null ciphers.

B. STEGANOGRAPHY IN DIGITAL ERA

With developments in Computing power, the internet and Digital Signal Processing (DSP), Information and Coding Theory, Steganography went *'Digital'.* The Digital World provided a whole realm of possibilities to the advancement of Steganography. Its existence has created various interesting applications of the science. Steganography does not necessarily exist in still images, hidden messages can be embedded in audios, videos and even in simpler formats such as Hyper Text Markup Language (HTML), Executable files (.exe), Extension Markup Language (XML). As stated earlier, steganography has very interesting applications such as in Smart IDs where the individual's details are embedded into their photographs, copyright control of materials, enhancing the robustness of image search engines, companies' circulation of secret data. Other applications include audio-video synchronization. One of these applications is the use of steganography in *Medical Imaging Systems* where there confidentiality of the patient is of the utmost importance, it is necessary to separate the patients' image data (scans, X-ray results, DNA sequences and the like) and the patient information (Name, Address and other details). However a link must be maintained between the two to avoid misreading of data. Embedding the patient data within the image could prove to be a useful safety measure. In this context, it can cause some dispute that this violates the patient's data confidentiality as it becomes common knowledge that there exists decodable data within an image. It defeats the very purpose of steganography where the idea is to hide the existence of the message itself!

Inspired by the idea that Steganography can become a part of the normal printing process a Japanese firm Fujitsu is developing technology to encode data into a printed picture that is invisible to the human eye, however this data can be decoded by a mobile phone with a camera. The entire process takes less than a second as the embedded data is 12 bytes long. In the future, users will be able to use their

cellular phones to capture hidden data. The company charges a small fee for the use of the decoding software which rests on the company servers. The basic idea is to transform the image color scheme, its Hue, Saturation and Value components (HSV) before printing the image. These changes are invisible to the human eye, mobile cameras can decode the information and retrieve it.

C. STEGANALYSIS

Steganalysis is the science of attacking steganography. Its goal is to detect and/or estimate potentially hidden information from a pile of suspected data with little or no knowledge of the steganography algorithms or the image parameters. Unlike cryptanalysis where it is obvious that the intercepted data contains a message (that needs to be decrypted), steganalysis starts with a pile of suspect data files, however there is little information as to whether the files contain a payload. The steganalyst must reduce this set of data files to a subset of files that are most likely to be altered.

Steganalysis can be achieved using different image processing techniques e.g., image filtering, rotating, cropping, translating, etc., or more deliberately by coding programs to examine the stego-image structure and measure its statistical properties e.g., first order statistics (histograms), second order statistics (correlation between pixels, distance, direction) . Virus creators can exploit Steganography for their intention of spreading *Trojan Horses.* If that were to become a reality then anti-virus companies should not only check virus's footprints on the system but also must trace any threads embedded in image, audio, video files using Steganalysis. We classify steganalysis into two categories: *Passive Steganalysis* where we detect the presence or absence of a secret message in a data file or identify the type of embedding algorithm. *Active Steganalysis* where we estimate some properties of the message or embedding algorithm to extract a (possibly approximate) version of the secret message from a stego-message. There are some basic notes that must be observed by a Steganographer.

1. In the event where we have an encoded package and the original, unmodified carrier, by comparing the package against the original file we can extract the payload by noting their differences. To avoid this situation we can create a new image and destroy it after generating the stego image. It is not advisable to embed images that are available on the World Wide Web.

2. In order to avoid Human Visual Perception attack, the generated stego image must not have visual artifacts. Alterations made up to the 5^{th} LSB of any pixel yields dramatic changes that are visible.

3. Smooth homogenous areas must be avoided (such as a cloudless blue sky over snow), however chaotic images with natural noise background and rigid edges must be targeted.

In Section 2 we look in detail at the applications and methods that are available. We focus on spatial domain methods, frequency domain methods and adaptive methods. It is also shown that all of the Steganographic algorithms discussed here have been detected by Steganalysis and thus a robust algorithm with a high-embedding capacity must be developed. Simple edge embedding is resistant to attacks and this adaptive method is an excellent means of hiding data. We also discuss the use of human skin tone detection in a proposed Edge-embedding Adaptive Steganographic Method. We discuss this approach in Section 3.

II. STEGANOGRAPHY METHODS

A. STEGANOGRAPHY BY EXPLOITING IMAGE FORMAT

A simple form of Steganography can be accomplished by feeding the following line of code into a Microsoft XP command window:

C:\> copycover.jpg /b + Message.txt /b stego.jpg

This code appends the secret message contained within the *message.txt* file into the *copycover.jpg* file and produces the stego-image *stego.jpg*. The technique behind this is to abuse the use of the EOF (End Of File). It packs the message contained within the message.txt file and *places* it after the EOF tag in the .jpg cover image. When *stego.jpg* image is opened by any photo editing application, it will just display the picture and ignore any data that comes after the EOF tag. However when it is opened in Notepad, the message is displayed after some data and can be read. This method does not affect the image quality, neither the image histograms nor the visual perception can detect any difference between the two images as the secret message is hidden after the EOF tag. While this method is simple, a range of Steganography software distributed online applies it (Camouflage, JpegX, Hider, etc.) It must be noted that this simple technique would not resist any kind of editing or any attacks by Steganalysis experts.

Another simple implementation of Steganography is to append hidden data into the image's Extend File Information (EXIF – a standard used by digital camera manufacturers to store additional information such as the make and model of the camera, the time the picture was taken, image and exposure time and focal length). This is the metadata information that is stored at the header of the file. This method too is not a reliable one as it suffers from the same drawbacks as the previous method. Note that the text hidden can also be encrypted to add another level of security.

B. STEGANOGRAPHY IN SPATIAL DOMAIN

The spatial domain methods have a Steganographer modifying the secret data and the cover medium, encoding it at the level of the LSBs (Least Significant Bits). This method has more impact compared to the above mentioned two methods, despite them being simple to implement. Embedding at the 4th LSB generates a lot of visual distortion to the cover image and it appears to be "non-natural".

Potdar et al., [5] used this technique in producing fingerprinted secret sharing Steganography for robustness against image cropping attacks. Rather than proposing an embedding technique, their paper addresses the issue of image cropping effects. The principle behind their proposed work was to divide the cover image into sub-images; compress and encrypt the secret data. The resulting data is sub-divided and then embedded into those image portions. They stated that a Lagrange Interpolating Polynomial could be applied to recover the data. This technique had high computational load, but their algorithm parameters namely, the number of sub-images (n) and the threshold value (k) were not set to the optimal values, it left the reader to guess these values.

If n is set, for instance to 32, then we need 32 public keys, 32 persons and 32 sub-images, which is quite unpractical. Moreover, their method eliminates the occurrence of data redundancy in the stego-image. Shirali-Shahreza [6] exploited the Arabic and Persian punctuations to hide messages. Though their method is not related to the LSB approach, it falls under the spatial domain. Unlike English which has only two letters with dots in the lower case format ("i" and "j"), out of 32 alphabet letters in the Persian language, 18 of them have points. The secret message is binarized, and then those 18 letters' points are modified according to the values in the binary file.

Color palette based Steganography exploits the smooth ramp transition in colors as indicated in the color palette. Here, the LSBs are modified based on their positions in the palette index. Johnson and Jajodia [1] favored the use of BMP (24-bit) instead of JPEG images. Their next-best choice was GIF files (256-color). BMP and GIF based Steganography apply LSB techniques, it must be noted that their resistance to counter attacks and compression are reported to be weak [3]. BMP files tend to be bigger in size than other formats, rendering them improper for network transmissions. JPEG images however, were avoided at the beginning because of their compression algorithm which does not support a direct LSB embedding into the spatial domain.

Experiments on the Discrete Cosine Transform (DCT) coefficients showed promising results and redirected researchers' attention towards this type of image. Acting at the level of DCT makes Steganography more robust and not as prone to many statistical attacks. Spatial Steganography generates unusual patterns such as sorting of color palettes, relationships between indexed colors, exaggerated 'noise', etc., all of which leave traces that can be picked up by Steganalysis tools. This method is quite fragile . There is a serious conclusion drawn in the literature. *"LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image"* . Almost any filtering process will alter the values of many of the LSBs[7] .

C. STEGANOGRAPHY IN FREQUENCY DOMAIN

New algorithms keep emerging prompted by the rapid development of technology and the need for enhanced security measures. The discovery of the LSB embedding mechanism was a breakthrough, although it is not perfect in deceiving the HVS. Its weak resistance to attacks left researchers wondering where to apply it until they successfully managed to apply it within the frequency domain. DCT is used extensively in video and image lossy compression. Each block DCT coefficents are quantized using a specific Quantization Table (QT).

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	5	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Figure 1. JPEG suggested Luminance Quantization Table used in DCT loss compression. The value 16 (in bold-face) represents the DC coefficient and the other values represent AC coefficients.

The process of quantization aims to loosen up the tight precision produced by DCT while still retaining valuable information descriptors. Most of the redundant data and noise is lost at this stage – hence the name lossy compression.

Steganography based on DCT JPEG compression goes through different steps as shown in Following Figure.

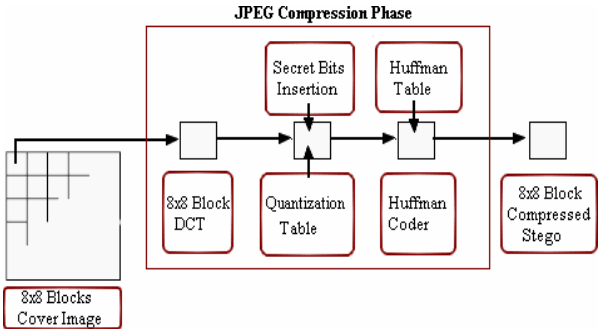

Figure 3. Data Flow Diagram showing a general process of embedding in the Frequency domain.

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) into 64 DCT coefficients. Data is inserted into these coefficients' insignificant bits. However, altering any single coefficient would affect the entire 64 block pixels [9]. Since the change is operating on the frequency domain instead of the spatial domain there will be no visible changes in the cover image [10].

The DWT based embedding technique is still in its infancy, Paulson [36] reports that a group of scientists at Iowa State University are focusing on the development of an innovative application which they called "Artificial Neural Network Technology for Steganography (ANNTS)" aimed at detecting all present Steganography techniques including DCT, DWT and DFT. The Inverse Discrete Fourier Transform (iDFT) encompasses round-off error which renders DFT improper for Steganography applications.

D. ADAPTIVE STEGANOGRAPHY

Adaptive Steganography is also known as "*Masking*" or *"Statistics-aware embedding"*. It combines the former two methods. This method takes statistical global features of the image before attempting to interact with its DCT coefficients. The statistics will determine where to make the changes. This method applies a random adaptive selection of pixels depending on the cover image. In a particular block, the pixels with a large local STD (Standard Deviation) are selected. This, in order to avoid areas of uniform color. e.g., smooth areas, blue sky. Applying such a method, makes the Adaptive Steganography algorithms seek images with existing or deliberately added noise and images with increased color complexity. Wayner dedicated a complete chapter in a book to what he called 'life in noise' where he points out the usefulness of data embedding in noise. It has proven to be robust with respect to compression, cropping and image processing [9].

Edge-embedding is robust to many attacks, therefore this method is an excellent means of hiding data while maintaining a good quality carrier.

Object oriented steganography can strengthen the edge embedding robustness. While embedding in a carrier, recognizing and tracking the elements can help in the resistance to major image processing attacks and compression. This comes across as an adaptive intelligent type where the embedding process affects only certain areas called as Regions of Interest (ROI) rather than the entire image. With the boost of Computer Vision (CV) and pattern recognition disciplines this method can be fully automated and unsupervised. Cheddad et al., [8] in their paper introduced a concept of exploiting a successful face recognition algorithm in building up a robust Stenographic method. The discovery of human skin tone uniformity in some transformed color spaces was a great achievement in the field of biometric research. It provided a simple yet real time robust algorithm. In the next section we discuss briefly skin tone detection in the color space.

Table 1. Drawback of the current methods.

METHOD	LIMITATION
File formatting techniques (i.e., Header and EXIF embedding)	-Large payload but easily detected and defeated. -Not robust against lossy compression and image filters. -Resaving the image destroys totally the hidden data.
Direct spatial LSB techniques	-Large payload but often offset the statistical properties of the image -Not robust against lossy com*pression and image filters*
Transform domain techniques	-Less prone to attacks than the former methods at the expense of capacity -Breach of second order statistics -Cannot resist attacks based on multiple image processing techniques

III. EMBEDDING IN THE SKIN TINE COLOR SPACE

For image content retrieval in sequences of images (GIF, Video and such) using adaptive methods, we can use color space transformation to detect and track the presence of human skin tone. This idea emerged from the field of Biometrics, where the threefold RGB matrix of a given image is converted into different color spaces to yield distinguishable regions of skin or near skin tone. Color transformations are of the utmost importance in computer vision. There are several color spaces that exist, some of them are: RGB, CMY, XYZ, xyY, UVW, HSV, YUV,

YCbCr and such. Mostly two kinds of spaces are exploited in biometrics namely, HSV and YCbCr spaces. It has been experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within those two spaces since different people differ in their skin color. A color transformation map, HSV (Hue, Saturation, Value) can be obtained from the RGB bases. Sobottka and Pitas defined a face localization based on HSV. They found that the human flesh could approximate a sector out of a hexagon with certain constraints.

The other utilized color mapping, YCbCr (Yellow, Chromatic blue, Chromatic red), is another transformation that belong to the family of television transmission color spaces. Hsu et al., introduced a skin detection algorithm, starting with lighting compensation, they detect faces based on the cluster in the (Cb/Y)-(Cr/Y) subspace. Lee et al., showed that the skin-tone has a center point and demonstrated a more precise model.

A. STEGANOFLAGE – A PROPOSED FRAMEWORK.

Cheddad et al., in their paper proposed the idea of embedding data within the edge directions in the 2D wavelet decomposition. This method guarantees a high quality stego image. In order to overcome the problem of edge limited payload we choose video files. Spreading the hidden data along the frames of the video compensates for the drawback of the edge embedding technique.

They anticipated that Computer Vision could play a major role in this field. Successful face localization algorithms for color images exploit the fact that the human skin tone can be localized within a certain range within the transform color domain (RGB to YcbCr, HSV or Log-opponent). Steganography can benefit from this in such a way that it permits us to track and embed into the edge sequential appearances of human skin in the frames (faces in a crowd, an athlete exercising, etc.). It could also adjust the values of the human skin tone within the permissible value ranges to embed secret data.

The core of their proposal was to find spatial features in image frames, they performed skin tone detection to embed secret data in videos for the following reasons:

1. When the embedding is spread on the entire image (or frame) then 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 color space ensures immunity to geometric transforms.
2. Their suggested scheme modifies only regions of the skin tone in the color transformed channel, this is done for imperceptibility reasons.
3. The skin-tone has a center point at Cb, Cr components, it can be modelled and its range is known statistically, therefore it could be embedded safely whilst preserving these facts. 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 the selected region will be in the safe zone, because human faces generally demonstrate the core elements in any given image and are thus protected areas (e.g. portraits).
5. Their Steganographic proposal is consistent within the object based coding approach followed in MPEG4 and MPEG7 standards.
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 an encrypted password and a link to the next frame holding the next portion of the hidden data in the video. This link need not be in a linear fashion.

Figure 4 shows how the proposed method preserves the quality of the original image.

Set A

Set B

Set C

Figure 4: Set A,B&C:(left) Original test images and (right) Stegoimages hiding UU template. Bottom: data to hide (University of Ulster's logo - 47x48).

Table 2. Comparisons of Stego images' quality

Method	PSNR(dB)
Set A	
Steganoflage	76.917
S-Tools	68.7949
F5	53.4609
Set B	
Steganoflage	71.449
S-Tools	68.144
F5	53.221
Set C	
Steganoflage	70.1268
S-Tools	68.9370
F5	48.7112

IV CONCLUSION

Digital Steganography is a fascinating scientific area that falls under the domain of security systems. In this work, we have presented some basic discussions on algorithms of Steganography 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. That is because they alter bits in the transform domain, thus image distortion is kept to a minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. There has always been a tradeoff between robustness and payload. Steganoflage, is based on edge embedding in the DWT domain using skin tone detection in RGB sequential image files. The latter compensates for the limited capacity that edge embedding techniques demonstrate. The actual elements of the image are used when hiding a message. This leads to many exciting and challenging research problems.

V. 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, December1, 2001.Retrievedfrom: 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] Potdar, V. M., Han, S. and Chang,E.: Fingerprinted Secret Sharing Steganography for Robustness against Image Cropping Attacks. Proceedings of IEEE's 3rd International Conference on Industrial Informatics (INDIN), Perth, Australia, 10-12 August 2005.

[6] Shirali-Shahreza, M. H. and Shirali-Shahreza, M.: A New Approach to Persian/Arabic Text Steganography. Proceedings of 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006), 10-12 July 2006, 310- 315.

[7] Anderson, R. J and Petitcolas, F.A.P.: On the LimitsOf Steganography. IEEE Journal of Selected Areas inCommunications, 16(4): 474-481, May 1998.

[8] Fridrich, J., Goljan, M. and Hogeg, D.: Steganalysis of JPEG Images: Breaking the F5 Algorithm. Proceedings of Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, the Netherlands, 2578/2003: 310-323, October 7-9, 2002.

[9] Fard, A. M., Akbarzadeh-T, M. and Varasteh-A, F.: A New Genetic Algorithm Approach for Secure JPEG Steganography. Proceedings of IEEE International Conference on engineering ofIntelligent Systems, 22-23 April 2006, 1- 6.

[10] Hashad, A.I., Madani, A.S. and Wahdan, A.E.M.A.: A Robust Steganography Technique using DiscreteCosine Transform Insertion. Proceedings of IEEE/ITI 3rd International Conference on Information andCommunications Technology, Enabling Technologies for the New Knowledge Society. 5-6 Dec. 2005, 255-264.

[11] Paulson, L. D.: New System Fights Steganography,"News Briefs," Computer, IEEE Computer Society, 39(8): 25-27, Aug, 2006.