STRENGTHENING STEGANOGRAPHY IN DIGITAL IMAGES

Abbas Cheddad

Supervisors: Dr. Joan Condell, Dr. Kevin Curran, Prof. Paul Mc Kevitt

First Year Report

Date: July, 2007

Presented as a requirement for Ph.D. in

School of Computing and Intelligent Systems
Faculty of Engineering
University of Ulster, Magee
Email: cheddad-a@ulster.ac.uk

To my beloved mother and to the soul of my father

Acknowledgments

I would like to express my gratitude to my supervisors, Dr. Joan Condell, Dr. Kevin Curran and Prof. Paul Mc Kevitt for their guidance, kindness, suggestions and insight throughout this research.

I am also grateful to the University of Ulster for awarding me the Vice Chancellor's Research Studentship (VCRS) and for providing me with the perfect atmosphere to excel. To my colleagues at the Intelligent Systems Engineering Laboratory I offer my sincere appreciation for their friendship and the warm welcome to their group. It has been, and will remain, a great pleasure knowing you. Finally, to my family back at home, I offer my truthful thanks for their patient and unshakable faith in me.

Abstract

Steganography among other rare disciplines is honored to be described as both an “art” and “Science” field. Its history goes back deep in the ancient civilizations. During the Persian and Greek conflict around 480 B.C and during the ancient Egyptian civilization Steganography was reported to exist. However, looking at it from a purely technical angle, it has been propelled to the forefront of current security techniques by the amazing growth in computational power, the increase in security awareness e.g., Individuals, groups, agencies, Governments…etc, and by political and intellectual arising issues. Steganography is defined as the science of hiding or embedding “data” in a transmission medium. Its ultimate objectives, which are undetectability, robustness and capacity of the hidden data, are the main factors that separate it from other “sisters-in science” techniques, namely watermarking and Cryptography. This sounds abstract, but this report will shed light on this interesting yet challenging security system of Steganography.

The main lines of reasoning of successful Steganography are its resistance to major attacks and its high payload. The plan to take into account an adaptive approach at the encoder side has meant a significant advance in the expedition for better Steganographic methods. Despite that, the true impact of the advantages resulting from this groundbreaking idea has not been adequately founded in practice in the literature. When setting down the research plan for this study, the research of digital Steganography is found to be focusing on non-adaptive measures. The above challenges motivated our work to create a more fundamental approach, based on universal properties and adaptive measures. This report provides a comprehensive state-of-the-art analysis of the different existing methods and proposes a new and robust algorithm which strives to absorb the drawbacks of current systems. The computer vision area, namely human skin tone detection in color images, is applied to form an adaptive seed for an edge operator. The latter provides an excellent secure location for data hiding. The choice for the selection carrier calls upon a format that supports sequential images display (e.g., GIF animation, MPEG, flash movies…etc) which is believed to compensate for the problem of the limited payload of edge based Steganography. The evaluation of published works dictates that embedding into the discrete wavelets transform is much more robust to attacks than discrete cosine transform and provides a high quality undistorted image carrier. The obvious difficulty of our proposition, however, is to answer the hypothesis of bringing the triplet (i.e., color transformation, Wavelet decomposition and edge detection) algorithms together successfully to generate a final solid Steganographic algorithm. A basic theoretical foundation of the proposed concept is laid out in this report.

Keywords: Steganography, adaptive algorithm, spatial domain, frequency domain, security, embedding payload, Discrete Cosine coefficients, Discrete Wavelet Transform, GIF animation, file frames, skin tone, color transforms.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ACRONYM	MEANING
WYSIWYG	What You See Is What You get
HVS	Human Visual System
WWII	World War II
DSP	Digital Signal Processing
LSBs	Least Significant Bits
MSBs	Most Significant Bits
HTML	Hyper Text Mark up Language
XML	Extensible Markup Language
.EXE	Executable Files
TCP	Transmission Control Protocol
IP	Internet Protocol
JPEG	Joint Photographic Experts Group
GIF	Graphics Interchange Format
BMP	Bitmap
EOF	End Of File
EXIF	Extended File Information
DCT	Discrete Cosine Transform
FT	Fourier Transform
DWT	Discrete Wavelet Transform
PM	Perceptual Masking
AS	Adaptive Steganography
bpp	Bit Per Pixel
χ^2	Chi-Square
PSP	Preserving Statistical Properties
Em	Embedding Process
Ex	Extraction Process
MxN	The two dimensions of a given image
QT	Quantization Table
DC	The coefficient at the top left corner of an 8x8 DCT block
AC	The remaining coefficients of the block
$\lfloor . \rfloor$	Floor rounding operator
max	Maximum
FFT	Fast Fourier Transform
PDF	Probability Density Function
PSNR	Peak-Signal-to-Noise Ratio
MSE	Mean Square Error
dB	Decibels, a unit of measurement for PSNR
LBG	Linde-Buzo-Gray

|…|	Absolute difference
ANNTS	Artificial Neural Network Technology for Steganography
iDFT	Inverse Discrete Fourier Transform
STD	Standard Deviation
2D	Two Dimensional
HSV	Hue, Saturation and Value
RGB	Red, Green and Blue
YCbCr	Luminance, Chromatic Blue and Chromatic Red
ROI	Region Of Interest
CV	Computer Vision

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 (Johnson and Jajodia, 1998; Judge, 2001; Provos and Honeyman, 2003), we provide here a brief history. The remainder of this section highlights some historical facts and attacks on methods (Steganalysis).

1.1 Ancient Steganography

The word Steganography is originally a Greek word which means "*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 (Johnson and Jajodia, 1998; Judge, 2001; Provos and Honeyman, 2003; Moulin and Koetter, 2005). 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 (Sadkhan, 2004). 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 as shown in Figure 1. This method is credited to Cardan and is called Cardan Grille (Moulin and Koetter, 2005).

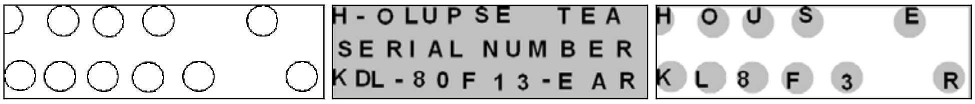


Figure 1: Cardan Grille, this is but an illustration keeping in mind that the Grill has no fixed pattern. (Left) The mask (Middle) The cover and (Right) The secret message revealed.

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*" (Judge, 2001).

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 such science. The contemporary information hiding is due to Simmons, G. J (1984) for his article titled "The prisoners' Problem and the Subliminal Channel". More recently Kurak and McHugh (1992) published their work, which resembles embedding into the 4LSBs (Least Significant Bits), discussing image downgrading and contamination which is known now by Steganography.

The distressing events that took place on 9-11-01 in the USA were the spark that irrevocably rekindled interest in digital Steganography. Cyber-terrorism, as coined recently, is believed to benefit from this digital revolution. Hence an immediate concern was shown on the possible use of Steganography by terrorists, following a report in the USA TODAY[1]. Cyber-planning, or the "*digital menace*" as Lieutenant Colonel Timothy L. Thomas defined it is difficult to control (Thomas, 2003). Provos and Honeyman, (2003) at the University of Michigan 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) (Hernandez-Castro et al., 2006).

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

[1] "Researchers: No secret bin Laden messages on sites" http://www.usatoday.com/tech/news/2001/10/17/bin-laden-site.htm#more Retrieved on: 27 November 2006 at: 18:27

advantages higher order statistics if taken into account before embedding can improve signal-to-noise ratio when dealing with Gaussian additive noise (Jakubowski et al., 2002).

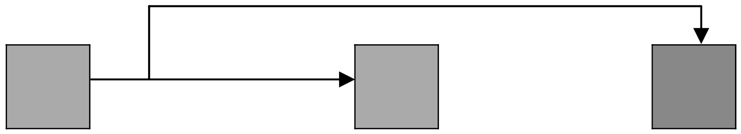
In a less legitimate manner, virus creators can exploit Steganography for their ill intention of spreading *Trojan Horses*. If that were to happen, anti-virus companies should go beyond checking simply viruses' fingerprints as they need to trace any threats embedded in image, audio or video files using 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- In order to avoid any Human Visual Perceptual attack, the generated stego image must not have visual artifacts. Alteration made up to the 5th LSBs of a given pixel will yield a dramatic change in its value, see Figure 2. Such unwise choice on the part of the Steganographer will thwart the perceptual security of the transmission.

3- Smooth homogeneous areas must be avoided (e.g., cloudless blue sky over a blanket of snow); however chaotic with natural redundant noise background and salient rigid edges should be targeted (Areepongsa et al., (2000); Da-Chun, W. and Wen-Hsiang, T., 2003; Kruus et al., 2002).



155→10011**1011**
LSBs in bold-face
MSBs in normal

1001101**0**→154
Changes made to the least
significant bit (LSB)

100**0**1011→139
Change made to the most
significant bit (MSB)

Figure 2: Visual inspection of altered least and most significant binary values of a gray color pixel.

Questions arise, such as whether child pornography exists inside innocent image or audio files? Are terrorists transmitting their secret messages in such a way? Are anti-virus systems fooled each time by the secret embedding? The answers are still not trivial.

Section 2 will look in detail with applications and methods available in the literature. The main discussions and comparisons focus on spatial domain methods, frequency domain methods and also adaptive methods. It will be shown that all of the Steganographic algorithms discussed have been detected by Steganalysis methods and thus a robust algorithm with high embedding capacity needs to be investigated. Simple edge embedding is robust to many attacks and it will be shown that this adaptive method is also an excellent means of hiding data while maintaining a good quality carrier. We intend to use human skin tone detection in a proposed edge embedding adaptive Steganographic method. Therefore Section 3 will discuss this area of computer vision and set it in context.

2 Steganography: Literature Review

In this section we attempt to give an overview of the most important Steganographic techniques in digital images. 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 (TCP/IP)[2] packets (Johnson and Jajodia, 1998), embedding Checksum (Bender et al., 2000)…etc. In a very interesting way Petitcolas, F.A.P (2000) 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 we quote here an issue in the public domain regarding patients' data confidentiality[3]; 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 embedded as part of the normal printing process, Japanese firm Fujitsu[4] 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 as exemplified in Figure 3a and shown in action in Figure 3b. 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). Then embed into the Hue domain to which human eyes are not sensitive. However mobile cameras can see coded data and retrieve it.

[2] For instance a unique ID can be embedded into an image to analyze the network traffic of particular users.
[3] The Guardian Unlimited: "Lives ruined as NHS leaks patients' notes" By Anthony Browne, Health Editor. Sunday June 25, 2000. Accessed from: http://observer.guardian.co.uk/uk_news/story/0,6903,336271,00.html on: Thursday, January 25, 2007
[4] http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6361891.stm Retrieved on: 15-02-2007 at: 14:17

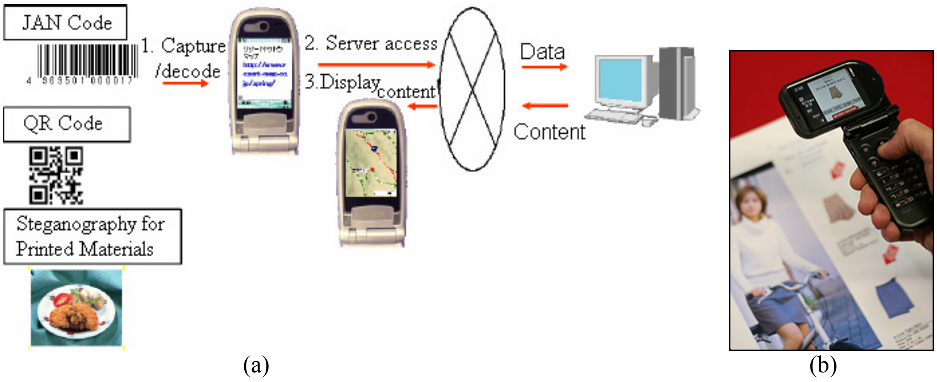


Figure 3: Fujitsu exploitation of Steganography: (a) a sketch representing the concept and (b) the idea deployed into a mobile phone shown at an exhibition recently.

The favorite image formats of the internet are constrained to the Graphics Interchange Format (GIF) and the Joint Photographic Experts Group (JPEG). Most of the techniques developed were set up to exploit the structures of these formats with some exceptions in the literature that use the Bitmap format (BMP).

We define the general process of embedding images as follows:

> Let C denote the cover carrier (i.e., image A) and C' the Stego-image, let K represent an optional key (a seed used to encrypt the message or to generate a pseudorandom noise which can be set to {ø} for simplicity) and let M be the message we want to communicate (i.e., image B). *Em* is an acronym for embedding and *Ex* for Extraction.
>
> $$Em : C \oplus K \oplus M \rightarrow C' \qquad (1)$$
>
> $$Ex(Em(c,k,m)) \approx m, \forall c \in C, k \in K, m \in M \qquad (2)$$

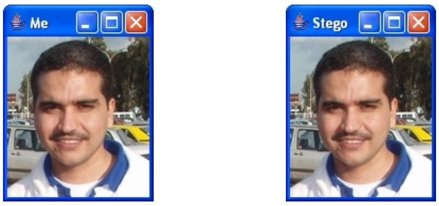
We will first discuss briefly some methods which exploit image formats. Then we will examine some of the dominant techniques. For a comprehensive survey on Steganographic techniques in digital images and other carriers the reader is directed to literature (Johnson and Katzenbeisser, 2000). An evaluation of different spatial Steganographic techniques applied to GIF images is also available (Bailey and Curran, 2006). Section 2.2 discusses the Spatial Domain which generally uses a direct Least Significant Bit (LSB) replacement technique, then followed by the frequency domain based techniques such as Discrete Cosine Transform (DCT), Fourier Transform (FT) and Discrete Wavelet Transform (DWT). Finally, the third section will highlight the recent contribution in the domain which is termed as Perceptual Masking (PM) or Adaptive Steganography (AS).

2.1 Steganography Exploiting Image Format

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

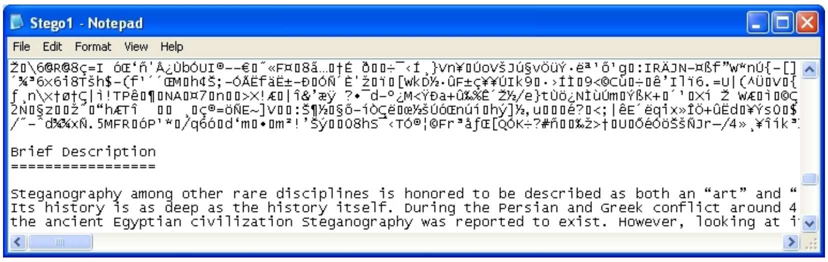
```
C:\> Copy Cover.jpg /b + Message.txt /b Stego.jpg
```

What this code does is that it 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. When *Stego.jpg* is viewed using any photo editing application, the latter will just display the picture as depicted in Figure 4 and will ignore anything coming after the *EOF* tag. However, when opened in Notepad for example, our message reveals itself after displaying some data as shown in Figure 5. The embedded message does not impair the image quality. Neither the image histograms nor the visual perception can detect any difference between the two images due to the secret message being hidden after the *EOF* tag. Whilst this method is simple, a range of Steganography software distributed online applies it (e.g., Camouflage, JpegX, Hider…etc). Unfortunately, this simple technique would not resist any kind of editing to the Stego image nor attacks by Steganalysis experts.



(a) (b)

Figure 4: The output of a simple Steganography method. (a) The cover image, (b) The resulting Stego image.



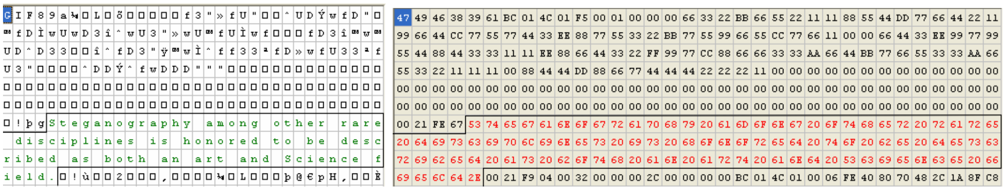
```
Ž□\6@R@8ç=I óŒ'ñ'Å¿ÙbÓUI®--€□˝«F¤□8ã…□†É ð□□÷¯‹Í¸}Vn¥□ÚoVšJú§VÖüÝ·ëª'ő'g□:IRÄJN–¤ßf"W*nÚ{-[]
´¾³6×6ì8Tšh$-(f'´´ŒM□h¢Š;-ÓÄËfäË±-Ð□ÓÑ´È'Ž□ï□[WkÐ½·ÛF±ç¥¥ÚIk9□·›Í Ì□9<©CÛ□÷□ê'Ilï6.=U|(^Ü□V□{
f¸n\×†ø†Ç|ì!TPê□¶□NA□¤7□n□□>X!Æ□|î&'æÿ ?•¯d-º¿M<ŸÐa+Û‰%Ê´Ž½/e}tÙö¿NÌùÚm□ÝßK+□´'□Xí Ž WÆ□ì□©Ç
ŽN□§z□□ž˝□"hÆTî  □□ ¸□ç®=öÑE~]V□□:Š¶½□§ő-íòÇë□œ½šÚóŒnúí□hý]½,u□□□é?□<;|êE´ëqìx»ÎÖ+ûËd□¥Ÿs□□$
/˝-ˆd%¾xÑ.5MFR□óP'*□/q6ó□d'm□•□m²!'Šý□□O8hS¯‹TÓ®¦©Fr³åƒŒ[QÓK÷?#ñ□□‰ž>†□U□ŐéÓöŠšÑJr–/4»¸¥îík³

Brief Description
=================

Steganography among other rare disciplines is honored to be described as both an "art" and "
Its history is as deep as the history itself. During the Persian and Greek conflict around 4
the ancient Egyptian civilization Steganography was reported to exist. However, looking at i
```

Figure 5: The secret message revealed when the Stego image is opened using Notepad. Note that the format of the inserted message remained intact.

Another naïve implementation of Steganography is to append hidden data into the image's Extended File Information (EXIF[5]). This is metadata information about the image and its source located at the header of the file. Special agent Paul Alvarez (Alvarez, 2004) discussed

[5] EXIF standard used by digital camera manufacturers to store information in the image file, such as, the make and model of a camera, the time the picture was taken and digitized, the resolution of the image, exposure time, and focal length.

the possibility of using such headers in digital evidence analysis to combat child pornography. Figure 6 depicts some text inserted into the comment field of a GIF image header. This method is not a reliable one as it suffers from the same drawback as the EOF method. Note that it is not always the case to hide text directly without encrypting it as we did here.



```
GIF89a¼□L□õ□□□□□f3"»fU"□□ˆUDÝwfD"□
™fDÌwUwD3îˆwU3"»wU™fUÌwf□□□fD3î™w™
UDˆD33□□îˆfD3"ÿ™wÌˆff33ªfD»wfU33ªf
U3"□□□□ˆDDÝˆfwDDD"""□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□!þgSteganography among other rare
 disciplines is honored to be desc
ribed as both an art and Science f
ield.□!ù□□2□□□,□□□□¼□L□□□þ@€pH,□□È
```

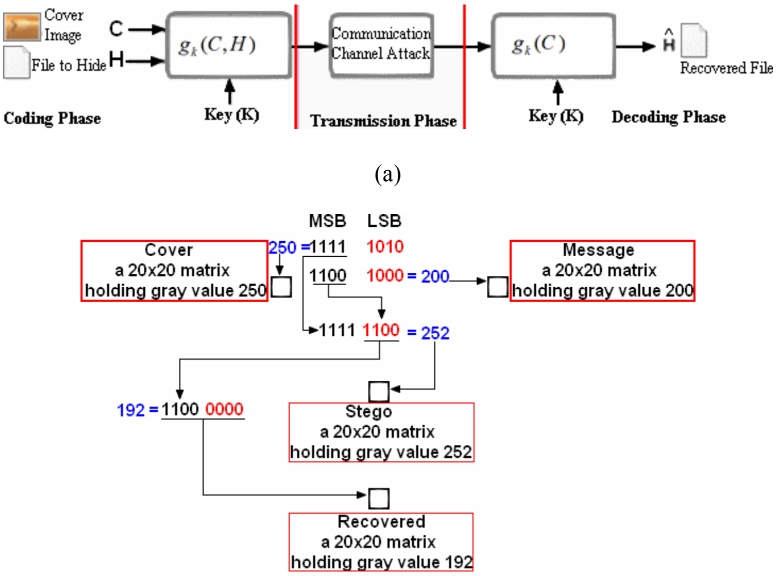
```
47 49 46 38 39 61 BC 01 4C 01 F5 00 01 00 00 00 66 33 22 BB 66 55 22 11 11 88 55 44 DD 77 66 44 22 11
99 66 44 CC 77 55 77 44 33 EE 88 77 55 33 22 BB 77 55 99 66 55 CC 77 66 11 00 00 66 44 33 EE 99 77 99
55 44 88 44 33 33 11 11 EE 88 66 44 33 22 FF 99 77 CC 88 66 66 33 33 AA 66 44 BB 77 66 55 33 33 AA 66
55 33 22 11 11 11 00 88 44 44 DD 88 66 77 44 44 44 22 22 22 11 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 21 FE 67 53 74 65 67 61 6E 6F 67 72 61 70 68 79 20 61 6D 6F 6E 67 20 6F 74 68 65 72 20 72 61 72 65
20 64 69 73 63 69 70 6C 69 6E 65 73 20 69 73 20 68 6F 6E 6F 72 65 64 20 74 6F 20 62 65 20 64 65 73 63
72 69 62 65 64 20 61 73 20 62 6F 74 68 20 61 6E 20 61 72 74 20 61 6E 64 20 53 63 69 65 6E 63 65 20 66
69 65 6C 64 2E 00 21 F9 04 00 32 00 00 00 2C 00 00 00 00 BC 01 4C 01 00 06 FE 40 80 70 48 2C 1A 8F C8
```

Figure 6: Text insertion into EXIF header: (Left) the inserted text string highlighted in a box and (Right) its corresponding hexadecimal chunk.

2.2 Steganography in the Image 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. We state with full confidence that this method has the largest impact compared to the other two methods even though it is known for its simplicity (Lin and Delp, 1999; Kermani and Jamzad, 2005).

Let us walk through how Steganography in the spatial domain works. A general framework with the underlying concept is highlighted in Figure 7. While a practical example of embedding in the 1st LSB and in the 4th LSB is illustrated in Figure 8. As we can appreciate in Figure 8, embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as “non-natural”.



(a)

(b)

Figure 7: Steganography in spatial domain. (a) Communication-theoretical view of the process, C denotes cover image, H the data to hide, and $\hat{H}$ is the estimate of H. (b) the concept in action.

It is apparent to an observer that Figure 8 concludes that there is a trade off between the payload and cover image distortion, however the payload (i.e., embedding up to 1, 2, 3, or 4th LSBs) is analogous in respect to the recovered embedded image. For instance, Figure 8k (recovered from embedding into 4LSBs) is a good estimate of the hidden image (Figure 8c) but produces noticeable artifacts (Figure 8f). Figure 8j (recovered from embedding into 1LSB) has poor quality but has an almost identical carrier to the original image (compare Figure 8d with 8a).

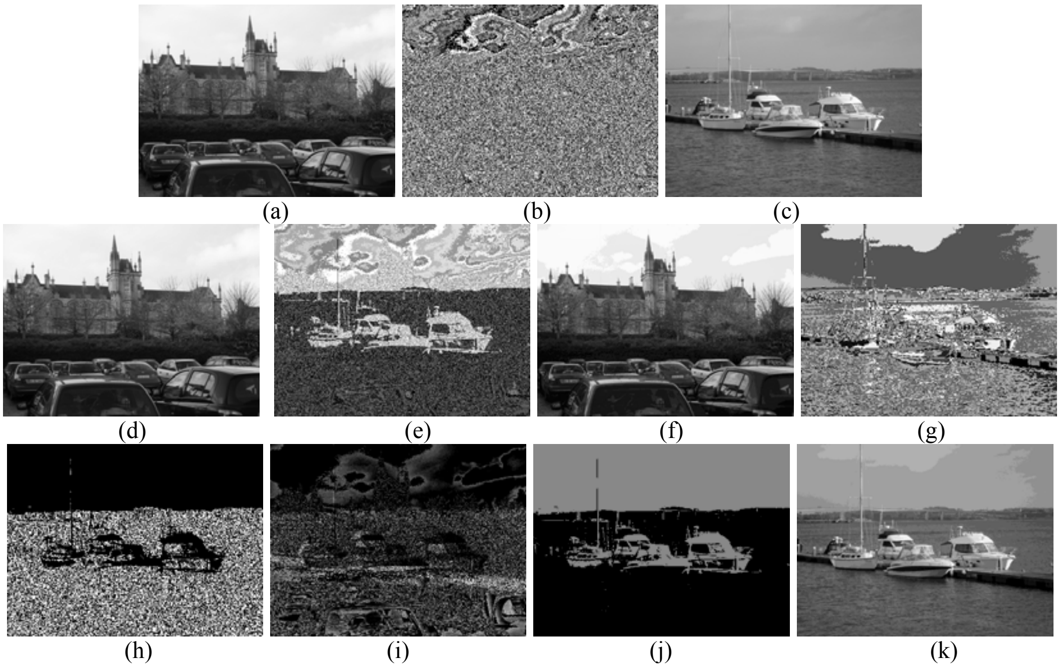


Figure 8: A plain (i.e., without encryption or pre-processing) implementation of Steganography in the spatial domain. *(a)*The cover carrier –University of Ulster- enlarged , *(b)* LSBs of (a) with an enhanced contrast for better visualization, *(c)* The image to hide –Londonderry's river- , *(d)* Stego-image 1 LSB replaced, image enlarged, *(e)* LSBs of (d) , *(f)* Stego-image 4 LSBs replaced, image enlarged *(g)* LSBs of (f) , *(h)* Difference between (a) and (d), *(i)* Difference between (a) and (f), *(j)* Hidden image extracted from (d), *(k)* Hidden image extracted from (f).

Potdar et al., (2005b) used this technique in producing fingerprinted secret sharing Steganography for robustness against image cropping attacks. Their paper addressed the issue of image cropping effects rather than proposing an embedding technique. The logic behind their proposed work is to divide the cover image into sub-images and compress and encrypt the secret data. The resulting data is then sub-divided in turn and embedded into those images portions. To recover the data; a Lagrange Interpolating Polynomial was applied along with an encryption algorithm. The computational load was high, but their algorithm parameters, namely the number of sub-images (*n*) and the threshold value (*k*) were not set to optimal values leaving the reader to guess the values. Bear in mind also that if *n* is set, for instance, to 32 that means we are in need of 32 public keys, 32 persons and 32 sub-images, which turns out to be unpractical. Moreover, data redundancy that they intended to eliminate does occur in their stego-image.

Shirali-Shahreza, M. H. and Shirali-Shahreza, M., (2006) exploited Arabic and Persian alphabet punctuations to hide messages. While their method is not related to the LSB approach, it falls into the spatial domain. Unlike English which has only two letters with dots in their lower case format, namely "i" and "j", Persian language is rich in that 18 out of 32 alphabet letters have points. The secret message is binarized and those 18 letters' points are modified according to the values in the binary file.

Colour palette based Steganography exploits the smooth ramp transition in colours as indicated in the colour palette. The LSBs here are modified based on their positions in the said palette index. Johnson and Jajodia (1998) were in favour of using BMP (24-bit) instead of JPEG images**.** Their next-best choice was GIF files (256-color). BMP as well as GIF based Steganography apply LSB techniques, while their resistance to statistical counter attack and compression are reported to be weak (Chin-Chen et al., 2006; Ren-Junn et al., 2001; Lin and Delp, 1999; Xiangwei et al., 2005; Provos and Honeyman, 2003). BMP files are bigger compared to other formats which render them improper for network transmissions. JPEG images however, were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain[6]. The experiments on the Discrete Cosine Transform (DCT) coefficients showed promising results and redirected researchers' attention towards this type of images. In fact 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 colour palettes, relationships between indexed colours, exaggerated "noise"…etc, all of which leave traces to be picked up by Steganalysis tools. This method is very fragile (Marvel and Retter, 1998). There is a serious conclusion drawn in the literature by several authors. "*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*" (Lin and Delp, 1999). Almost any filtering process will alter the values of many of the LSBs (Anderson and Petitcolas, 1998).

By inspecting the inner structure of the LSB, J. Fridrich and her colleagues (Fridrich et al., 2001) claimed to be able to extract hidden messages as short as 0.03bpp (bit per pixel). Xiangwei et al., (2005) stated that the LSB methods can result in the "*pair effect*" in the

[6] Fridrich et al., (2002) claimed that changes as small as flipping the LSB of one pixel in a JPEG image can be reliably detected.

image histograms. As can be seen in Figure 9, this "*pair effect*" phenomenon is empirically observed in Steganography based on Modulus operator. This operator acts as a means to generate random (i.e., not sequential) locations to embed data**.** It can be a complicated process or a simple one like testing in a raster scan if a pixel value is even then embed, otherwise do nothing. Avcibas et al., (2002) apply binary similarity measures and multivariate regression to detect what they call "telltale" marks generated by the 7th and 8th bit planes of a stego image.

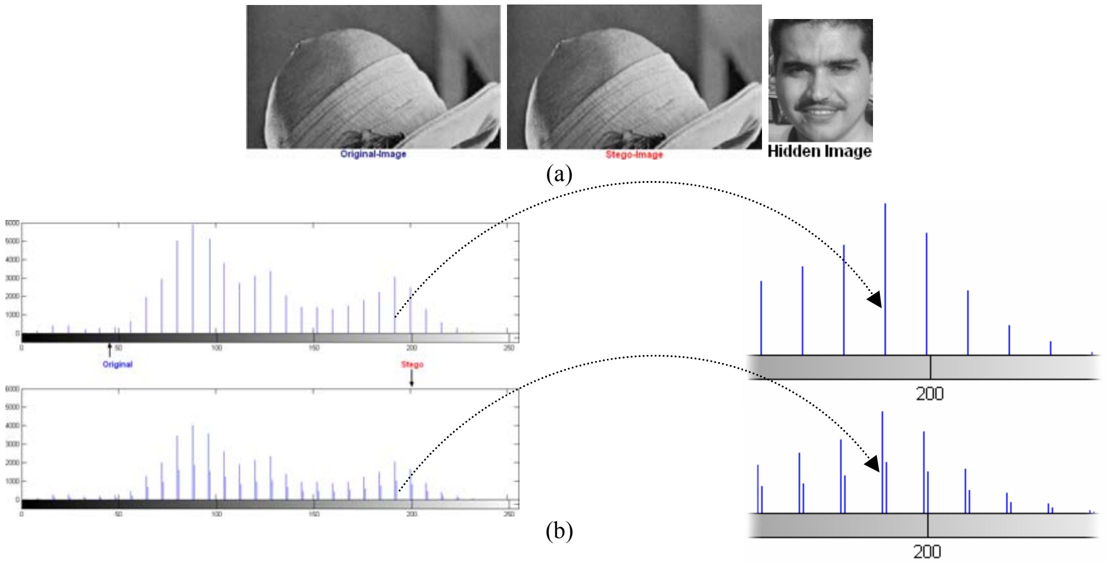
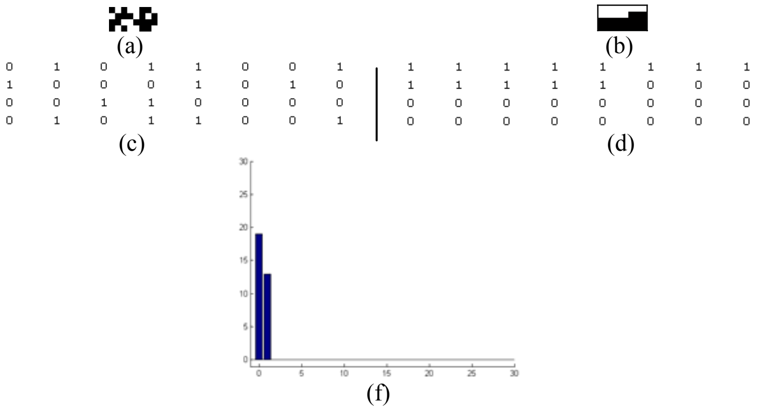


Figure 9: Steganography based on Modulus operators. (a) Lena's hat: the HVS is unable to discern between the original and the Stego image and (b) Histograms demonstrating the "*pair effect*". (b-top) Original and (b-bottom) Stego. Note that it is not always the case that Modulus Steganography produces such noticeable phenomenon.

It is the nature of standard intensity histograms of images to track and graph values in an image and not the structure of its pixels and how they are arranged, see Figure 10.



```
0  1  0  1  1  0  0  1   |   1  1  1  1  1  1  1  1
1  0  0  0  1  0  1  0   |   1  1  1  1  1  0  0  0
0  0  1  1  0  0  0  0   |   0  0  0  0  0  0  0  0
0  1  0  1  1  0  0  1   |   0  0  0  0  0  0  0  0
```

Figure 10: Standard histogram is not meant for revealing the structure of data: (a) an 8x4 matrix stored in double precision and viewed (b) another structure of (a) (c) pixel values of (a) (d) pixel values of (b) and (f) the histogram which describes both matrices.

Chi-Square (χ^2) and Pair-analysis algorithms can easily attack methods based on the spatial domain. Chi-Square is a non-parametric (a rough estimate of confidence) statistical algorithm used in order to detect whether the intensity levels scatter in a uniform distribution throughout the image surface or not (Civicioglu et al., 2004). If one intensity level has been detected as such, then the pixels associated with this intensity level are considered as corrupted pixels or in our case have a higher probability of having embedded data. The classical Chi-Square can be fooled by randomly embedded messages, thus Bohme and Westfeld (2004) developed a Steganalysis method to detect randomly scattered hidden data in LSBs spatial domain that applies the Preserving Statistical Properties (PSP) algorithm.

2.3 Steganography in the Image 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.

The description of the two-dimensional DCT for an input image *F* and output image *T* is calculated as:

$$T_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \tag{3}$$

where

$$0 \le p \le M-1$$
$$0 \le q \le N-1$$

and

$$\alpha_p = \begin{cases} 1/\sqrt{M}, p=0 \\ \sqrt{2/M}, 1 \le p \le M-1 \end{cases} \qquad \alpha_q = \begin{cases} 1/\sqrt{N}, q=0 \\ \sqrt{2/N}, 1 \le q \le N-1 \end{cases}$$

where *M, N* are the dimensions of the input image and *m*, *n* are variables ranging from 0 to M-1 and 0 to N-1 respectively.

DCT is used extensively in Video and image (i.e., JPEG) lossy compression. Each block DCT coefficients obtained from Equation (3) is quantized using a specific Quantization Table (QT). This matrix shown in Figure 11 is suggested in the Annex of the JPEG standard[7]. The

[7] Note that some Camera manufacturers have their own built-in QT and they do not necessarily conform to the standard JPEG table.

logic behind choosing such a table with such values is based on extensive experiments that tried to balance the trade off between image compression and quality factors. The HVS dictates the ratios between values in the QT.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	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 11: JPEG suggested Luminance Quantization Table used in DCT lossy compression. The value 16 (in bold-face) represents the DC coefficient and the rest represent AC coefficients.

The aim of quantization is to loose up the tightened precision produced by DCT while retaining the valuable information descriptors.

The quantization step is specified by[8]:

$$f'(\omega_x,\omega_y)=\left\lfloor \frac{f(\omega_x,\omega_y)}{\Gamma(\omega_x,\omega_y)}+\frac{1}{2}\right\rfloor, \qquad \omega_x,\omega_y \in \{0,1,...,7\} \tag{4}$$

where x and y are the image coordinates, $f'(\omega_x,\omega_y)$ denotes the result function, $f(\omega_x,\omega_y)$ is an 8x8 non-overlapping intensity image block and $\lfloor . \rfloor$ a floor rounding operator. $\Gamma(\omega_x,\omega_y)$ represents a quantization step which, in relationship to JPEG quality, is given by:

$$\Gamma(\omega_x,\omega_y)=\begin{cases} \max\left(\left\lfloor \frac{200-2Q}{100}QT(\omega_x,\omega_y)+\frac{1}{2}\right\rfloor,1\right) & , \ 50\le Q\le 100 \\ \left\lfloor \frac{50}{Q}QT(\omega_x,\omega_y)+\frac{1}{2}\right\rfloor & , \ 0\le Q\le 50 \end{cases} \tag{5}$$

where, $QT(\omega_x,\omega_y)$ is the quantization table depicted in Figure 11 and Q is a quality factor.

JPEG compression then applies entropy coding such as the Huffman algorithm to compress the resulted $\Gamma(\omega_x,\omega_y)$.

The above scenario is a discrete theory independent of Steganography. Xiaoxia Li and Jianjun Wang (2007) presented a Steganographic method that modifies the QT and inserts the hidden bits in the middle frequency coefficients. Their modified QT is shown in Figure 12. The new version of QT gives them 36 coefficients in each 8x8 block to embed their secret data into;

[8] Most of the redundant data and noise are lost in this stage hence the name lossy compression. For more details on JPEG compression the reader is directed to Popescu, A.C., (2005).

which yields a reasonable payload. Their work was motivated by a prior published work by Chin-Chen Chang el al., (2002). Steganography based on DCT JPEG compression goes through different steps as shown in Figure13.

8	1	1	1	1	1	1	1
1	1	1	1	1	1	1	55
1	1	1	1	1	1	69	56
1	1	1	1	1	87	80	62
1	1	1	1	68	109	103	77
1	1	1	64	81	104	113	92
1	1	78	87	103	121	120	101
1	92	95	98	112	100	103	99

Figure 12: The modified Quantization Table used by Xiaoxia Li and Jianjun Wang (2007).

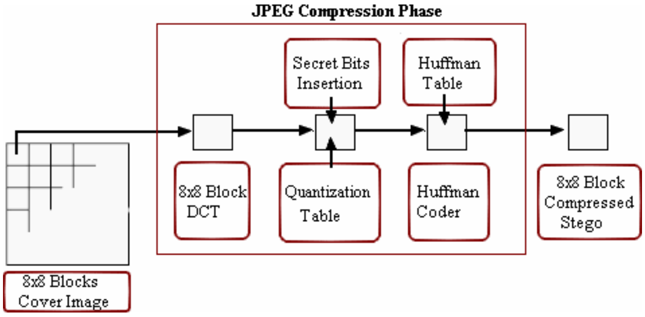
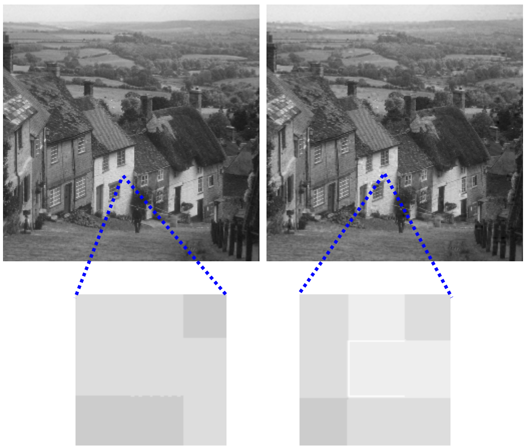


Figure 13: Data Flow Diagram showing a general process of embedding in the frequency domain.

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 (Fard et al., 2006). Since the change is operating on the frequency domain instead of the spatial domain there will be no visible changes in the cover image (Hashad et al., 2005).

According to Raja et al., (2005) Fast Fourier Transform (FFT) introduces round off errors; thus it is not suitable for hidden communication. Johnson and Jajodia (1998) included it among the used transformations in Steganography.

Choosing which values in the 8x8 DCT coefficients block to alter is very important as changing one value will affect the whole 8x8 block in the image**.** Figure 14 shows a poor implementation of such a method in which careful consideration was not given to the sensitivity of DCT coefficients.



Original 3x3 pixels block zoomed Stego 3x3 pixels block zoomed

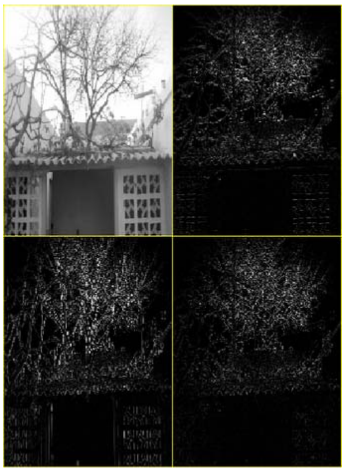
Figure 14: Even though embedding at the DCT level is a very successful and powerful tool**.** When the coefficients are not carefully selected some artifacts will be noticeable.

The JSteg algorithm was among the first algorithms to use JPEG images. Although the algorithm stood strongly against visual attacks, it was found that examining the statistical distribution of the DCT coefficients yields a proof for existence of hidden data (Provos and Honeyman, 2003). JSteg is easily detected using the X^2*-test*. Moreover, since the DCT coefficients need to be treated with sensitive care and intelligence, JSteg algorithm leaves a serious statistical signature. Wayner (2002) stated that the coefficients in JPEG compression normally fall along a bell curve and the hidden information embedded by JSteg distorts this. Manikopoulos et al., (2002) discussed an algorithm that utilizes the Probability Density Function (PDF) used to generate discriminator features fed into a neural network system to detect hidden data in this domain.

OutGuess developed by Provos and Honeyman (2003) was a better alternative as it uses a pseudo-random-number generator to select DCT coefficients. The X^2*-test* does not detect data that is randomly distributed. Strangely enough the developer of OutGuess himself suggests a counter attack against his algorithm. Provos et al., (2003, 2001a, 2001b) suggest applying an extended version of X^2-test to select Pseudo-randomly embedded messages in JPEG images.

Andreas Westfeld based his "F5" algorithm on subtraction and matrix encoding. Neither X^2*-test* nor its extended versions could break this solid algorithm. Unfortunately, F5 did not survive attacks for too long. Fridrich and her team (Fridrich et al., 2002) proposed Steganalysis that does detect F5 contents, disrupting F5's survival.

For the Discrete Wavelet Transform (DWT), the reader is directed to Wen-Yuan Chen (2007), Potdar (2005a) and Verma et al., (2005). Abdulaziz and Pang (2000) use vector quantization called Linde-Buzo-Gray (LBG) coupled with Block codes known as BCH code and 1-Stage discrete Haar Wavelet transforms. They reaffirm that modifying data using a wavelet transformation preserves good quality with little perceptual artifacts. This claim is justified based on our experiments; Figures 15 and 16 depict an implementation of this approach.



A gray scale approximation of the original image at the decomposed level	The details in the Horizontal orientation
The details in the Vertical orientation	The details in the Diagonal orientation

Figure 15: One step DWT decomposition. Images were contrast enhanced for display. The weight of Watermarking was initialised with weighting factor α= 0.01.

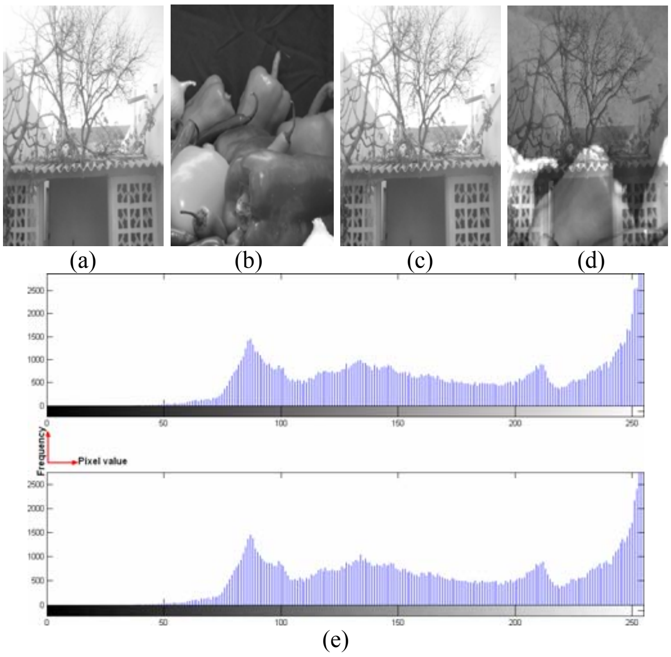


Figure 16: Single-level two-dimensional Haar wavelet decomposition with respect to low-pass and high-pass filter decompositions. (a) Cover image, (b) Secret image, (c) Stego image, (d) Absolute difference of a and c (i.e., $|a-c|$), (e) histograms seem identical too, (top) Original and (bottom) Stego.

The previous histogram is given by the following discrete function:

$$h(v_i) = n_i \qquad (6)$$

where, v_i is the ith intensity level in the interval [0, 255] and n_i is the number of pixels in the image whose intensity level is v_i.

The DWT based embedding technique is still in its infancy, Paulson (2006) report 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.

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:

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^2}{MSE}\right) \tag{7}$$

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

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \tag{8}$$

and $C_{\max}^2$ holds the maximum value in the image, for example:

$$C_{\max}^2 \le \begin{cases} \text{1 in double precision intensity images} \\ \text{255 in 8-bit unsigned integer intensity images} \end{cases}$$

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.

Many authors in the literature (Kermani et al., 2005; Besdok 2005; Hashad et al., 2005; Zhou et al., 2006; Chin-Chen Chang et al., 2006b; Yuan-Hui Yu et al., 2006; Xiaoxia Li and Jianjun Wang, 2007; Jau-Ji Shen and Po-Wei Hsu 2007…etc) consider $C_{\max}$=255 as a default value for 8-bit images. It can be the case, for instance, that the examined image has only up to 253 or fewer representations of gray colours. Knowing that C_{max} is raised to a power of 2 results in a severe change to the PSNR value. Thus we define C_{max} as the actual maximum value rather than the largest possible value.

PSNR is often expressed on logarithmic scale in decibels (dB). PSNR values falling below 30dB indicate a fairly low quality (i.e., distortion caused by embedding can be obvious); however, a high quality stego should strive for 40dB and above.

The following table (Table 1) tabulates different PSNR values spawned by some popular software applied on the images in Figure 17. Steganos appears to have a good algorithm.

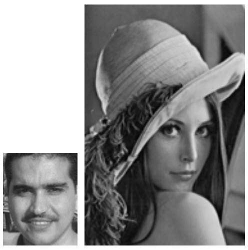


Figure 17: Images used to generate tables 1 and 2. (Left) Secret image (77x92) and (Right) Cover image (Lena 320x480).

Table 1: Summary of performance for different popular software (*) TextHide exceptionally does not support image embedding, therefore it should be noted that the secret data in this case was the abstract text of this document.

Software	PSNR	Comment
Hide&Seek	22.7408	Very clear grainy noise in the Stego image
Hide-in-Picture	28.316	Little noise
ImageHide	20.93	Very clear grainy noise in the Stego image
Steganos	**32.999**	**No visual evidence of tamper**
Stell	16.621	Works only with colour images
S-Tools	**25.208**	**No visual evidence of tamper**
TextHide(*)	22.25	Very clear grainy noise in the Stego image
Revelation	24.381	No visual evidence of tamper, but pair effect appears on the histogram
Modulus 2 Algorithm	11.749	No visual evidence of tamper

2.5 Adaptive Steganography

Adaptive Steganography is a special case of the two former methods. It is also known as "*Statistics-aware embedding*" (Provos and Honeyman, 2003) and "*Masking*" (Johnson and Jajodia, 1998). 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 (2002) 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 (Fard et al., 2006; Chin-Chen and Hsien-Wen Tseng, 2004; Franz and Schneidewind, 2004). Edge embedding follows edge segment locations of objects in the host gray scale image in a fixed block fashion each of which has its centre on an edge pixel, thus we guarantee the modifications can happen only on edge pixels or their surrounding ones. Whilst simple, edge embedding is robust to many attacks (given its nature in preserving the abrupt change in image intensities) and as shown in Table 2 it follows that this adaptive method is also an excellent means of hiding data while maintaining a good quality carrier.

Table 2: Sequential LSB and edge based embedding performances.

	MSE	**PSNR (dB)**	**Payload (bit)**
Direct-1bit	0.29208	53.476	110592
Direct-2bit	0.96099	48.304	221184
Direct-3bit	3.9054	42.214	331776
Direct-4bit	15.846	36.132	442368
Edged-1bit	0.051315	61.028	5675

Chin-Chen et al., (2004) propose an adaptive technique applied to the LSB substitution method. Their idea is to exploit the correlation between neighbouring pixels to estimate the degree of smoothness. They discuss the choices of having 2, 3 and 4 sided matches. The payload (embedding capacity) was high[9].

2.6 Comparison of Existing Methods

Table 5 compares the most popular software tools[10]. We based our comparison on the following factors: the domain on which the algorithm is applied e.g., Spatial or Frequency domain, the support for Encryption, Random bit Selection and the different image formats. We note that a majority of the Steganographic software applications running under Microsoft Windows platform use LSBs substitution algorithm. In the table, the sign (✓) indicates the characteristic is present, (-) denotes unavailability of information at present, while (x) gives the negative response. As it is clear from the table all of the mentioned Steganographic algorithms have been detected by Steganalysis methods and thus a robust algorithm with high

[9] In normal cases LSB embedding into spatial image data tends to have a higher payload but lesser robustness comparing to LSB insertion into frequency coefficients.

[10] Software websites: http://www.stegoarchive.com/
http://www.jjtc.com/mwiki/index.php?title=Main_Page
http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html
http://www.outguess.org/

embedding capacity needs to be investigated. The drawback of the current techniques is tabulated in Table 3.

Table 3: 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 compression and image filters
➢ Transform domain techniques	▪ Less prone to attacks than the former methods but that comes at the expense of capacity ▪ Breach of second order statistics ▪ Cannot resist attacks based on multiple image processing techniques

Most of the works done on Steganography in the literature have neglected the fact that object oriented Steganography can strengthen the embedding robustness. Recognising and tracking elements in a given carrier while embedding can help survive major image processing attacks and compression. This manifests itself as an adaptive intelligent type where the embedding process affects only certain 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. Here we introduce our contribution in exploiting one of the most successful face recognition algorithms in building up a robust Steganographic method. The discovery of human skin tone uniformity in some transformed color spaces introduced a great achievement in the biometric research field. It provides a simple yet a real time robust algorithm. The next section will introduce briefly the skin tone detection in the color space.

3 Skin Tone in Colour Space

For adaptive image content retrieval in sequences of images (e.g., GIF, Video) we can use color 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 space 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[11]: *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 theoretically proven that the distribution of human skin colour constantly resides in a certain range within those two spaces whilst different people differ in their skin colour (e.g, African, European, Middle Eastern, Asian...etc). A color transformation map called *HVS* (Hue, Value and Saturation) can be obtained from the RGB bases. Sobottka and Pitas (1996) define a face localization based on (*HVS*) described earlier, they found that human flesh can be an approximation from a sector out of the hexagon depicted in Figure 18a or as a 3D illustration in Figure 18b with the constraints: $S_{min}=0.23,\ S_{max}=0.68, H_{min}=0^{o}$ *and* $H_{max}=50^{0}$

- Hue (*H*) represents the color value:

$$H = \cos^{-1}\{1/2*[(R-G)+(R-B)]/[(R-G)^2+(R-B)(G-B)]^{-1/2}\} \tag{9}$$

- Intensity (*V*) is a measure of brightness:

$$V = (R+G+B)/3 \tag{10}$$

- Saturation (*S*) refers to the depth of the color:

$$S = 1 - \arg\min(R,G,B)/V \tag{11}$$

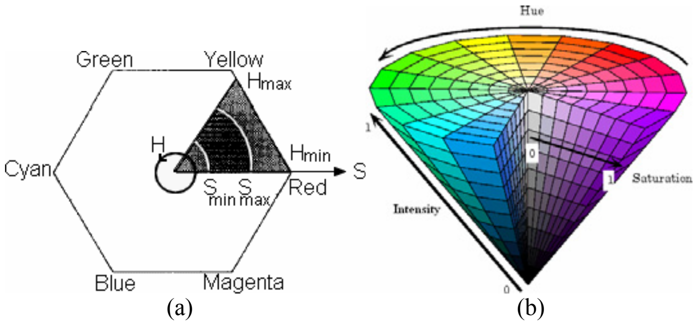


Figure 18: Skin tone colour sector. (a) Skin colour segmentation in *HVS* space (Sobottka and Pitas, 1996) and (b) Illustration of the *HVS* Colour Space (MATLAB™ documentation[12]).

[11] http://www.couleur.org/index.php?page=transformations , accessed on 13th June 2007 at 11:40am

[12] http://www.mathworks.com/access/helpdesk/help/toolbox/images/f8-20792.html, accessed on 18-06-2007 at 21:25

The other utilized colour mapping *YCbCr* (Yellow, Chromatic blue and Chromatic red) is another transformation that belongs to the family of television transmission color spaces, and which is derived from the *RGB* and calculated as follows:

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.2989 & 0.5866 & 0.1145 \\ -0.1688 & -0.3312 & 0.5000 \\ 0.5000 & -0.4184 & -0.0816 \end{bmatrix} * \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{12}$$

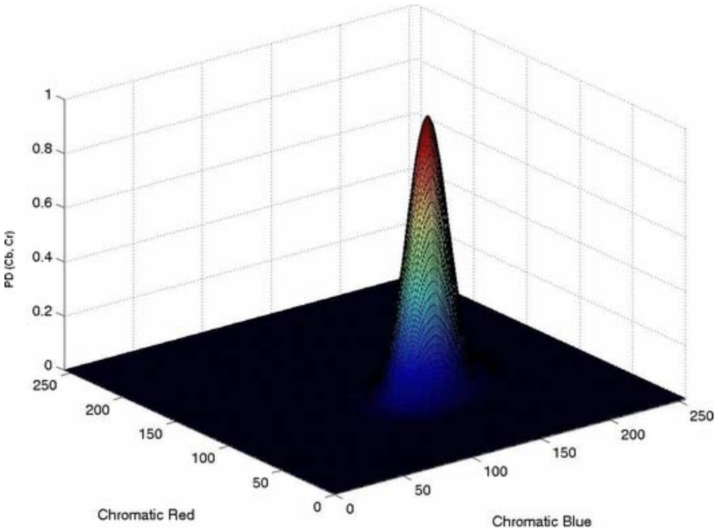


Figure 19: Skin color distribution in the YCbCr space. The graph shows the probability density distribution of Cr and Cb coordinates of pixels that belong to skin-colored areas of the image (Bae-Ho Lee et al., 2002).

Hsu et al. (2002) introduced a skin detection algorithm which starts with lighting compensation, they detect faces based on the cluster in the *(Cb/Y)-(Cr/Y)* subspace. Bae-Ho Lee et al. (2002) show that the skin-tone has a center point at (Cb, Cr) = (-24, 30) and demonstrate more precise model as depicted in Figure 20.

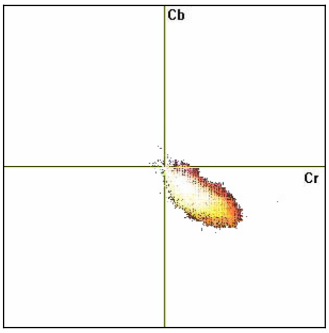


Figure 20: Sample skin-tone in the Cb-Cr plane (Bae-Ho Lee et al., 2002).

4 Project Proposal

4.1 Research Problem Statement

As is clear from the former section, there appears to be two groups in the field, one for creating Steganography algorithms and another group for creating a counter attack (Steganalysis). Fard et al., (2006) state clearly that "*there is currently no Steganography system which can resist all Steganalysis attacks*".

"*Ultimately, image understanding is important for secure adaptive Steganography. A human can easily recognize that a pixel is actually a dot above the letter "i" and must not be changed. However, it would be very hard to write a computer program capable of making such intelligent decisions in all possible cases*" (Fridrich, 1999). "*While there are numerous techniques for embedding large quantities of data in images, there is no known technique for embedding these data in a manner that is robust in light of the variety of manipulations that may occur during image manipulation*" (Bender et al., 2000).
"*Some researchers proposed to model the cover characteristics and thus create an adaptive Steganography algorithm, a goal which is not easily achieved*" (Katzenbeisser, 2000). Determining the Maximal safe bit-rate that can be embedded in a given image without introducing statistical artifacts remains a very complicated task (Fridrich and Goljan, 2002).

The above challenges motivated our work to create a more fundamental approach based on universal properties (Martin et al., 2005) and adaptive measures.

4.2 Research Objectives

The objectives of this research are:

- To investigate and evaluate existing methods of image based Steganography
- To provide the community with a state of the art survey in the field
- To enhance the available algorithms and produce a new secure and robust Steganography method (*Steganoflage)*
    - o *Investigate the use of edge embedding methods.*
    - o *Investigate the use of skin tone detection in Steganography.*
    - o *Combine edge embedding with skin tone detection to create a new adaptive Steganography method.*

4.3 Research Contribution

Based on the literature, highlighted earlier in sections 2.1, 2.2 and 2.3, we can conclude and point to the following facts:

- Algorithms F5 and Outguess are the most reliable ones although they violate the second order statistics as mentioned previously. Both utilise DCT embedding.
- Embedding in the DWT domain shows promising results and outperforms the DCT one especially in surviving compression (Wayner, 2002). A Steganographer should be cautious when embedding in the transformation domains in general; however DWT tends to be more forgiving than DCT. Unlike JPEG the newly introduced image coding system JPEG2000[13] allows for wavelets to be employed for compression in lieu of the DCT. This makes DWT based Steganography the future leading method.
- Without loss of generality; edge embedding maintains an excellent distortion free output whether it is applied in the spatial, DCT or DWT domain. However, the limited payload is its downfall.
- Most Steganographic methods do not use the actual elements of the image when hiding a message. These elements (e.g., faces in a crowd), as suggested by Kruus et al., (2002), can be adjusted in perfectly undetectable ways.

Currently we are investigating and evaluating the idea of taking into account the advantages of the techniques outlined earlier. That is embedding within the edge directions in the 2D wavelet decomposition. In this way we are guaranteed a high quality stego image. To tackle the problem of edge limited payload we choose GIF animated images. Spreading the hidden data along the frames of GIF animation will compensate for the drawback of the edge embedding technique. Note that this idea can be extended to Video image sequences too. Figure 21 provides a general outlook of the scheme.

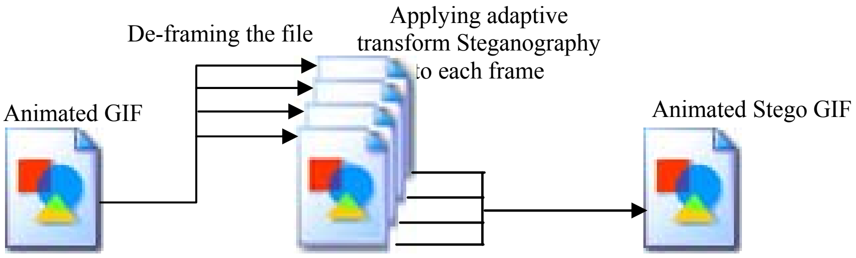


Figure 21: The proposed Steganographic method "*Steganoflage*".

[13] http://www.jpeg.org/jpeg2000/ accessed on 21-06-2007 at 17:04

We anticipate that Computer Vision can play a role here. Successful face localization algorithms for colour images exploit the fact that human skin tone can be localized within a certain range in the transform colour domain (i.e., RGB to YC_bC_r, HSV or Log-opponent[14]). Steganography can benefit from this in such a way that permits us to track and embed into the edge of sequential appearances of human skin in the frames (e.g., faces in crowd, an athlete exercising…etc) as shown in Figure 22. We can also adjust the human skin tone values, within the permissible value ranges, to embed secret data without introducing artifacts on the carrier image.

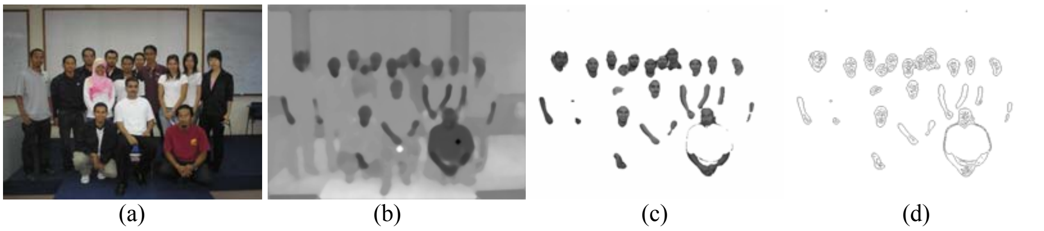


Figure 22: Skin tone detection. (a) Original colour image (b) RGB transformation to log-opponent blue (c) probable skin regions and (d) edge of (c).

[14] Log opponent conversion is given by: $l(x) = 105 * \log 10(x+1)$, x represents here the RGB matrix.

5 Project Schedule

The enclosed Gantt chart in the Appendix (Table 6) outlines the plan of work for completion of this study. Current ideas and findings have been submitted to various national conferences, international conferences and international referred Journals (see Table 4).

6 Conclusion

Digital Steganography is a fascinating scientific area which falls under the umbrella of security systems. We have presented in this work some background discussion 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. That is because they alter bits in the transform domain, thus image distortion is kept to the minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. In short there has always been a trade off between robustness and payload. Our proposed framework, *Steganoflage*, is based on edge embedding in the DWT domain using skin tone detection in RGB sequential image files. We chose to use the latter to compensate for the limited capacity that edge embedding techniques demonstrate. We use the actual elements of the image when hiding a message. Obviously, this leads to many exciting and challenging research problems.

References

Abdulaziz, N.K. and Pang, K.K., (2000). *Robust Data Hiding for Images. Proceedings of IEEE International Conference on Communication Technology, WCC - ICCT 2000, 21-25 Aug. 2000, Volume 1: 380 – 383.*

Alvarez, P., (2004). *Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis. International Journal of Digital Evidence, 2 (3). Winter 2004.*

Anderson, R. J and Petitcolas, F.A.P., (1998). *On the Limits of Steganography. IEEE journal of Selected Areas in Communications, 16(4): 474-481, May 1998.*

Areepongsa, S. Kaewkamnerd, N. Syed, Y. F. and Rao. K. R., (2000). *Exploring On Steganography For Low Bit Rate Wavelet Based Coder In Image Retrieval System. IEEE Proceedings of TENCON 2000. (3): 250-255. Kuala Lumpur, Malaysia*

Avcibas, I. Memon, N. and Sankur, B., (2002). *Image Steganalysis with Binary Similarity Measures. Proceedings of the international conference on Image Processing, 3: 645-648. 24-28 June 2002.*

Bae-Ho Lee, Kwang-Hee Kim, Yonggwan Won, and Jiseung Nam., (2002). *Efficient and Automatic Faces Detection Based on Skin-Tone and Neural Network Model. Proceedings of the 15th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, IEA/AIE 2002, Cairns, Australia, June 17-20, 2002. Lecture Notes in Computer Science (2358/2002)*

Bailey, K. and Curran, K., (2006). *An evaluation of image based steganography methods. Multimedia Tools and Applications, 30 (1): 55 – 88, July 2006.*

Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F.J. and Pogreb, S., (2000). *Applications for Data Hiding. IBM Systems Journal, 39 (3&4): 547-568*

Besdok, E (2005). *Hiding information in multispectral spatial images. Int. J. Electron. Commun. (AEÜ) 59 (2005) 15 – 24.*

Bohme, R. and Westfeld, A., (2004). *Exploiting Preserved Statistics for Steganalysis. Lecture Notes in Computer Science, (3200/2004): 82-96*

Chin-Chen Chang, Chih-Yang Lin, Yu-Zheng Wang., (2006). *New Image Steganographic Methods using Run-length Approach. Information Sciences, 176 (2006): 3393–3408.*

Chin-Chen Chang and Hsien-Wen Tseng., (2004). *A Steganographic method for digital images using side match. Pattern Recognition Letters, 25 (2004): 1431-1437.*

Chin-Chen Chang, Piyu Tsai and Min-Hui Lin., (2004). *An Adaptive Steganography for Index-Based Images Using Codeword Grouping. PCM (3) 2004: 731-738.*

Chin-Chen Chang, Tung-Shou Chen and Lou-Zo Chung., (2002). *A steganographic method based upon JPEG and quantization table modification. Information Sciences, (141) 2002: 123–138*

Chin-Chen Chang, Wei-Liang Tai, and Chia-Chen Lin, (2006b). *A Reversible Data Hiding Scheme Based on Side Match Vector Quantization. IEEE Transactions on Circuits and Systems for Video Technology, (16)10: 1301 – 1308, Oct- 2006.*

Civicioglu, P., Alci, M. and Besdok, E., (2004). *Impulsive Noise Suppression from Images with the Noise Exclusive Filter. EURASIP Journal on Applied Signal Processing, 16 (2004): 2434-2440.*

Da-Chun, Wu and Wen-Hsiang Tsai., (2003). *A Steganographic Method for Images by Pixel-value Differencing. Pattern Recognition Letters, 24 (2003): 1613-1626, Elsevier Inc.*

Fard, A. M., Akbarzadeh-T, M. and Varasteh-A, F., (2006). *A New Genetic Algorithm Approach for Secure JPEG Steganography. Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22-23 April 2006, 1- 6.*

Franz, E. and Schneidewind, A., (2004). *Adaptive Steganography Based on Dithering. Proceedings of the ACM Workshop on Multimedia and Security, September 20-21, 2004, Magdeburg, Germany, 56 – 62.*

Fridrich, J., (1999). *Application of Data Hiding in Digital Images. Tutorial for the ISSPA'99, Brisbane, Australia: August 22-25 1999.*

Fridrich, J. and Goljan, M., (2002). *Practical Steganalysis of Digital Images- State of the Art. Proceedings of SPIE Photonics West, , Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, January, 2002, Vol. 4675: pp. 1-13.*

Fridrich, J., Goljan, M. and Du, R.., (2001). *Reliable Detection of LSB Steganography in Grayscale and Color Images. Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pp. 27- 30.*

Fridrich, J., Goljan, M. and Hogeg, D., (2002). *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.*

Hashad, A.I., Madani, A.S. and Wahdan, A.E.M.A., (2005). *A Robust Steganography Technique using Discrete Cosine Transform Insertion. Proceedings of IEEE/ITI 3rd International Conference on Information and Communications Technology, Enabling Technologies for the New Knowledge Society. 5-6 Dec. 2005, 255- 264.*

Hernandez-Castro, J. C., Blasco-Lopez, I. and Estevez-Tapiador, J. M., (2006). *Steganography in Games: A general methodology and its application to the game of Go. Computers & Security, 25(2006): 64-71.*

Hsu, R., Abdel-Mottaleb, M. and Jain, A. (2002). *Face detection in color images. IEEE Transactions on Pattern Analysis and Machine Intelligence. 24(5): 696-706.*

Jakubowski, J., Kwiatos, K., Chwaleba, A. and Osowski, S. (2002). *Higher Order Statistics and Neural Network for Tremor Recognition. IEEE Transactions on Biomedical Engineering, 49 (2): February 2002.*

Jau-Ji Shen, Po-Wei Hsu (2007). *A robust associative watermarking technique based on similarity diagrams. Pattern Recognition 40 (2007) 1355 – 1367.*

Johnson, N. F. and Jajodia, S., (1998). *Exploring Steganography: Seeing the Unseen. IEEE Computer, 31 (2): 26-34, Feb 1998.*

Johnson, N. F. and Katzenbeisser, S.C., (2000). *"A Survey of Steganographic techniques". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.*

Judge, J.C., (2001). *Steganography: Past, Present, Future. SANS Institute publication, December 1, 2001. Retrieved from* http://www.sans.org/reading_room/whitepapers/stenganography/552.php

Katzenbeisser, S. C. (2000). *"Principles of Steganography". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.*

Kermani, Z. Z. and Jamzad, M., (2005). *A Robust Steganography Algorithm Based on Texture Similarity using Gabor Filter. Proceedings of IEEE 5th International Symposium on Signal Processing and Information Technology, 18-21 Dec. 2005, 578- 582.*

Kruus, P., Scace, C., Heyman, M. and Mundy, M., (2002). *A survey of Steganographic Techniques for Image Files. Advanced Security Research Journal. V(I): 41-51, Winter 2003.*

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

Lin, E. T. and Delp, E. J., (1999). *A Review of Data Hiding in Digital Images. Retrieved on 1.Dec.2006 from Computer Forensics, Cybercrime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999.*

Manikopoulos, C., Yun-Qing, S., Sui, S., Zheng, Z., Zhicheng, N. and Dekun, Z., (2002). *Detection of Block DCT-based Steganography in Gray-scale Images. Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9-11 Dec 2002,355 – 358.*

Martin, A., Sapiro, G. and Seroussi, G., (2005). *Is Image Steganography natural?. IEEE Trans on Image Processing, 14(12): 2040-2050, December 2005.*

Marvel, L. M. and Retter, C. T., (1998). *A Methodology for Data Hiding Using Images. Proceedings of IEEE Military Communications Conference (MILCOM98) Proceedings, Boston, MA, USA, 18-21 Oct 1998, 1044-1047.*

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

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

Petitcolas, F.A.P., (2000). *"Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.*

Popescu, A.C., (2005). *Statistical Tools for Digital Image Forensics. Ph.D. Dissertation, Department of Computer Science, Dartmouth College, USA, 2005. Retrieved from:* http://www.cs.dartmouth.edu/~farid/publications/apthesis05.html, *on 16-05-07 at 12:20.*

Potdar, V. M., Han, S. and Chang, E., (2005a). *A Survey of Digital Image Watermarking Techniques. Proceedings of IEEE's 3rd International Conference on Industrial Informatics (INDIN), Perth, Australia, 10-12 August 2005.*

Potdar, V. M., Han, S. and Chang, E., (2005b). *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.*

Provos, N., (2001a). *Defending Against Statistical Steganalysis. Center for Information Technology Integration, University of Michigan February 2001, [Technical Report].*

Provos, N. and Honeyman, P., (2001b). *Detecting Steganographic Content on the Internet. Center for Information Technology Integration, University of Michigan. August 31, 2001, [Technical Report].*

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

Raja, K. B., Chowdary, C.R., Venugopal, K. R. and Patnaik, L. M., (2005). *A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images. Proceedings of IEEE Third International Conference on Intelligent Sensing and Information Processing (ICISIP 2005), Bangalore, India, 14-17 Dec. 2005, 170- 176.*

Ren-Junn Hwang, Timothy K. Shih, Chuan-Ho Kao, and Tsung-Ming Chang., (2001). *Lossy Compression Tolerant Steganography. Proceedings of the First International Conference on The Human Society and the Internet - Internet Related Socio-Economic Issues, appears in Lecture Notes In Computer Science, Vol. 2105/2001: 427 – 435.*

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

Shirali-Shahreza, M. H. and Shirali-Shahreza, M., (2006). *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.*

Simmons, G. J., (1984). *The Prisoners' Problem and the Subliminal Channel. Proceedings of CRYPTO83- Advances in Cryptology, August 22-24. 1984. pp. 51.67.*

Sobottka, K. and Pitas, I. (1996). *Extraction of Facial Regions and Features Using Color and Shape Information. Proc. IEEE International Conference on Image Processing. pp. 483-486.*

Thomas, T. L., (2003). *Al Qaeda and the Internet: The Danger of "Cyberplanning". Parameters, US Army War College Quarterly - Spring 2003. Retrieved from: www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf On 22-Nov-2006.*

Verma, B., Jain, S. and Agarwal, D. P., (2005). *Watermarking Image Databases: A Review. Proceedings of the International Conference on Cognition and Recognition. Mandya, Karnataka, India 22-23 Dec 2005.*

Wayner, P. (2002). *Disappearing Cryptography. 2nd ed. USA: Morgan Kaufmann Publishers.*

Wen-Yuan Chen., (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 (2007).*

Xiangwei Kong, Ziren Wang and Xingang You., (2005). *Steganalysis of Palette Images: Attack Optimal Parity Assignment Algorithm. Proceedings of 5th IEEE International Conference on Information, Communications and Signal Processing, 860- 864, 06-09 Dec 2005.*

Xiaoxia Li and Jianjun Wang., (2007). *A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences, 177(15): 3099-31091, August 2007.*

Yuan-Hui Yu, Chin-Chen Chang and Iuon-Chang Lin (2006). A new steganographic method for color and grayscale image hiding. Computer Vision and Image Understanding [Article *In Press].*

Zhou, Z. Arce, R.G. and Di Crescenzo. G., (2006). *Halftone Visual Cryptography. IEEE Transactions on Image Processing, (15)8: August 2006.*

Appendix: **Table 4:** List of Conference and Journal Papers

CONFERENCES				
Conference name	**Status**	**Notification of acceptance**	**Conference Date**	**Venue**
● IEEE SMC UK&RI 6th Conference on Cybernetic Systems 2007	**Submitted**	June 30, 2007	September 6-7, 2007	University College Dublin. RI
● The 2nd International Symposium on Information Security (IS'07)	**Submitted**	August 22, 2007	November 26-27, 2007	Vilamoura, Algarve. Portugal
● The Seventh IT&T Conference "Digital Convergence in a Knowledge Society"	**In Process**	September 10, 2007	October 25-26, 2007	Institute of Technology Blanchardstown, Dublin , Ireland
INTERNATIONAL JOURNALS				
Journal's name	**Status**	**Notification of acceptance**	**Publishing Date**	**Publisher**
● International Journal of Computers and Electrical Engineering	**Submitted**	31st August 2007	December 2007 / Early 2008	Elsevier Ltd.

Table 5: Comparison of Different Algorithms.

Name	Creator	Year	Spatial Domain	Frequency Domain	Encryption Support	Random bit Selection	Image Format	Detected by
JSteg	Derek Upham	-	x	✓ DCT	x	x	JPEG	- X^2-test - Stegdetect -J.Fridrich's Algorithm
JSteg-Shell	John Korejwa	-	x	✓ DCT	✓ RC4	-	JPEG	- X^2-test
JPhide	Allan Latham	1999	x	✓ DCT	✓ Blowfish	x	JPEG	- X^2-test - Stegdetect
OutGuess version 0.13b	Provos and Honeyman	-	x	✓ DCT	✓ RC4	✓	JPEG	- X^2-test (extended version) - Stegdetect
OutGuess version 0.2	Provos and Honeyman	2001	x	✓ DCT	✓ RC4	✓	JPEG, PNM	-J.Fridrich's Algorithm
EZStego	Romana Machado	1996	✓	X	✓	x	BMP, GIF	-RS-Steganalysis
White Noise Storm	Ray (Arsen) Arachelian	1994	✓	X	✓	✓	PCX	- X^2-test
S-Tools	Andrew Brown	1996	✓	X	✓ IDEA, DES, 3DES,MPJ2 , NSEA	x	BMP, GIF	- X^2-test
F5	Andreas Westfeld	2001	x	✓	✓	✓	JPEG, BMP, GIF	-J.Fridrich's Algorithm

Table 6: The Research Gantt Chart.

Time Scale / Activities	2006/2007				2008				2009		
	Nov-Mar	Apr-Jun	Jul- Sep	Oct- Dec	Jan- Mar	Apr-Jun	Jul-Sep	Oct-Dec	Jan-Mar	Apr-Jun	Jul-Oct
Literature survey	░	░	░	░							
Literature Review write-up		░	░	░							
100 Day VIVA		░									
Transfer Report			░								
Strengths & weaknesses of the current methods		▒	▒	▒							
Image Database creation and algorithms testing				▒							
Enhancing current methods				▒	▒	▒	▒				
Algorithm development and coding				▓	▓	▓	▓	▓			
Optimization and adjustments								▓	▓		
Graphical User interface creation									▓		
Performance analysis against existing methods				▓	▓	▓	▓	▓	▓		
Thesis write up										▓	▓
Dissemination of research outcomes		█	█	█	█	█	█	█	█	█	█