Biometric Inspired Digital Image Steganography

Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt
School of Computing and Intelligent Systems, Faculty of Computing and Engineering
University of Ulster. Londonderry, Northern Ireland, United Kingdom
Emails: {cheddad-a, j.condell, kj.curran, p.McKevitt}@ulster.ac.uk}

Abstract

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

1. Introduction

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

1.1 The Ancient Steganography

The word Steganography is originally made up of two Greek words which mean "*Covered Writing*". It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and was dispatched with the message after his hair grew back [1, 2, 3, 4]. In Saudi Arabia at the king Abdulaziz City of Science and Technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [5]. 500 years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing, its scenario goes as follows: A paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the letter appears as an innocuous text. This method is credited to Cardan and is called Cardan Grille [4].

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

1.2 The Digital Era of Steganography

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

978-0-7695-3141-0/08 $25.00 © 2008 IEEE
DOI 10.1109/ECBS.2008.11

is believed to benefit from this digital revolution. Cyber-planning or the "*digital menace*" as Lieutenant Colonel Timothy L. Thomas defined it is difficult to control [8]. Provos and Honeyman [3] scrutinized 3 million images from popular websites looking for any trace of Steganography. They have not found a single hidden message. Despite the fact that they gave several assumptions to their failure they forget that Steganography does not exist merely in still images. Embedding hidden messages in videos and audios is also possible and even in a simpler form such as in Hyper Text Mark up Language (HTML), executable files (.EXE) and Extensible Markup Language (XML) [11].

Steganography is employed in various useful applications e.g., Copyright control of materials, enhancing robustness of image search engines and Smart IDs where individuals' details are embedded in their photographs. Other applications are Video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, Transmission Control Protocol and Internet Protocol packets (TCP/IP) - for instance a unique ID can be embedded into an image to analyze the network traffic of particular users [1], embedding Checksum [10], etc. In a very interesting way Petitcolas [9] demonstrated some contemporary applications; one of which was in *Medical Imaging Systems* where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions e.g., Physician, Patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems. In this context this can create other issues regarding patients' data confidentiality (see the Guardian Unlimited[1] (all superscripts are referenced at the internet resources): "Lives ruined as NHS leaks patients' notes" By Anthony Browne, Health Editor, Sunday June 25, 2000; Rita Pal, a hospital doctor who set up the pressure group NHS Exposed, said: "*Medical notes are in essence your life - how many affairs you have, if you have an alcohol problem, do drugs, your sexual activity, your psychiatric state. They are all very personal issues. Yet patients have no control over their confidentiality*." Marion Chester, legal officer at the Association of Community Health Councils, said: "*Identifiable health records are flying around inside and outside the NHS at a rate of knots. It's getting worse, because of the increase in financial and clinical audit, and the increasing use of information technology. The attitude to patient confidentiality is very lax in the NHS*."

Inspired by the notion that Steganography can be embedded as part of the normal printing process, Japanese firm Fujitsu[2] is pushing technology to encode data into a printed picture that is invisible to the human eye (i.e., data) but can be decoded by a mobile phone with a camera. The process takes less than 1 second as the embedded data is merely 12 bytes. Hence, users will be able to use their cellular phones to capture encoded data. They charge a small fee for the use of their decoding software which sits on the firm's own servers. The basic idea is to transform the image color scheme prior to printing to its Hue, Saturation and Value components (HSV). They then embed into the Hue domain to which human eyes are not sensitive. Mobile cameras can see coded data and retrieve it.

1.3 Steganalysis

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

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

2- 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. 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 [13, 14].

Section 2 will look in detail at 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 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. Section 3 will discuss this new approach in the area of computer vision and set it in context.

2. Steganography Methods

2.1 Steganography Exploiting Image Format

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

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

This code appends the secret message found in the text file ‘Message.txt’ into the JPEG image file ‘Cover.jpg’ and produces the stego-image ‘Stego.jpg’. The idea behind this is to abuse the recognition of *EOF* (End of file). In other words, the message is packed and inserted after the *EOF* tag. When *Stego.jpg* is viewed using any photo editing application, the latter will just display the picture and will ignore any data coming after the *EOF* tag. However, when opened in Notepad for example, our message reveals itself after displaying some data. 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 any attacks by Steganalysis experts.

Another naïve implementation of Steganography is to append hidden data into the image’s Extended File Information (EXIF- a 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). This is metadata information about the image and its source located at the header of the file. Special agent Paul Alvarez [15] discussed the possibility of using such headers in digital evidence analysis to combat child pornography. 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.

2.2 Steganography in the Spatial Domain

In spatial domain methods a Steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the other two methods even though it is known for its simplicity [16, 17]. Embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as “non-natural”.

Potdar et al., [18] 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 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 [19] exploited Arabic and Persian alphabet punctuations to hide messages. While 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 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 [1] 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 [16, 3]. BMP files are bigger in size than 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 (Fridrich et al., [22] claimed that changes as small as flipping the LSB of one pixel in a JPEG image can be reliably detected).

The experiments on the Discrete Cosine Transform (DCT) coefficients showed promising results and redirected researchers' attention towards this type of image. 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 [20]. 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*" [16]. Almost any filtering process will alter the values of many of the LSBs [21]. By inspecting the inner structure of the LSB, Fridrich et al., [23] claimed to be able to extract hidden messages as short as 0.03bpp (bit per pixel). Xiangwei et al., [24], stated that the LSB methods can result in the "*pair effect*" in the image histograms. This "*pair effect*" phenomenon is empirically observed in Steganography based on the 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., [25] applied 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.

2.3 Steganography in the Frequency Domain

New algorithms keep emerging prompted by the performance of their ancestors (Spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. Although it is perfect in not deceiving the HVS, its weak resistance to attacks left researchers wondering where to apply it next until they successfully applied it within the frequency domain. DCT is used extensively in Video and image (i.e., JPEG) lossy compression. Each block DCT coefficients obtained is quantized using a specific Quantization Table (QT). This matrix shown in Figure 1 is suggested in the Annex of the JPEG standard. The 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 1. JPEG suggested Luminance Quantization Table used in DCT lossy compression. The value 16 (in bold-face) represents the DC coefficient and the other values represent AC coefficients.

The aim of quantization is to loosen up the tightened precision produced by DCT while retaining the valuable information descriptors. Most of the redundant data and noise are lost at this stage hence the name lossy compression. For more papers' work on JPEG compression the reader is directed to [28]. The quantization step is specified by:

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

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 $\lfloor . \rfloor$ is a floor rounding operator. $\Gamma(\omega_x,\omega_y)$ represents a quantization step which, in relationship to JPEG quality, is given by:

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

where, $QT(\omega_x,\omega_y)$ is the quantization table depicted in (Figure 1) 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 and Jianjun [26] 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 2. The new version of QT gives them 36 coefficients in each 8x8 block to embed their secret data into, which yields a reasonable payload. Their work was motivated by a prior published work by Chang et al., [27]. Steganography based on DCT JPEG compression goes through different steps as shown in Figure 3.

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 2. The modified Quantization Table used by [26].

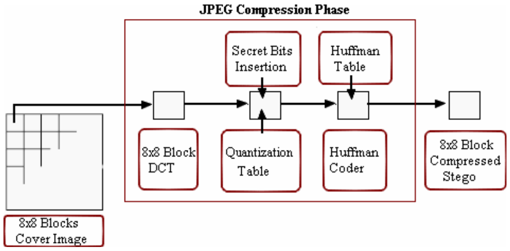


Figure 3. Data Flow Diagram showing a general process of embedding in the frequency domain.

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 [29]. Since the change is operating on the frequency domain instead of the spatial domain there will be no visible changes in the cover image [30]. According to Raja et al., [31] Fast Fourier Transform (FFT) introduces round off errors, thus it is not suitable for hidden communication. Johnson and Jajodia [1] 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. 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 [3]. JSteg is easily detected using the *X^2-test*, which 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. 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. Moreover, since the DCT coefficients need to be treated with sensitive care and intelligence, the JSteg algorithm leaves a serious statistical signature. Wayner [32] 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., [33] 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, [3] 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 and Honeyman [3], 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 et al., [22] proposed Steganalysis that does detect F5 contents, disrupting F5's survival.

For the Discrete Wavelet Transform (DWT), the reader is directed to Chen's work [34]. Abdulaziz, and Pang [35], 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.

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.

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:

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^2}{MSE}\right) \tag{3}$$

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

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \tag{4}$$

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

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

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

Many authors in the literature [17, 30, 26] 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 the 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 or higher.

2.5 Adaptive Steganography

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

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

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

Most of the works done on Steganography in the literature have neglected the fact that object oriented Steganography can strengthen the embedding robustness. Recognizing 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 colour 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 skin tone detection in the colour space.

We conclude this section by a summary of the drawback of the current techniques tabulated in
Table 1.

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 compression 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

3 Embedding in the Skin Tone Colour Space

For adaptive image content retrieval in sequences of images (e.g., GIF, Video) we can use colour space transformations to detect and track any presence of human skin tone. The latter emerged from the field of Biometrics, where the threefold *RGB* matrix of a given image is converted into different colour spaces to yield distinguishable regions of skin or near skin tone. Colour transformations are of paramount importance in computer vision. There exist several colour spaces and here we list some of them[3]: *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 as different people differ in their skin colour (e. g., African, European, Middle Eastern, Asian, etc). A colour transformation map called *HSV* (Hue, Saturation and Value) can be obtained from the RGB bases. Sobottka and Pitas [38] defined a face localization based on *HSV*. They found that human flesh can be an approximation from a sector out of a hexagon with the constraints: $S_{min}=0.23$, $S_{max}=0.68$, $H_{min}=0^{o}$ and $H_{max}=50^{0}$

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. Hsu et al., [40] introduced a skin detection algorithm which starts with lighting compensation, they detect faces based on the cluster in the *(Cb/Y)-(Cr/Y)* subspace. Lee et al., [39] showed that the skin-tone has a center point at (Cb, Cr) =
(-24, 30) and demonstrated more precise model.

Based on the literature, highlighted earlier in sections 2.1, 2.2, 2.3 and 2.5, we can conclude and point to the following facts:

- Algorithms F5 and Outguess are the most reliable methods although they violate the second order statistics as mentioned previously. Both utilize DCT embedding.
- Embedding in the DWT domain shows promising results and outperforms the DCT domain especially in surviving compression [32]. A Steganographer should be cautious when embedding in the transformation domains in general. However, DWT tends to be more tolerant to embedding than DCT. Unlike JPEG the newly introduced image coding system JPEG2000[4] allows for wavelets to be employed for compression in lieu of the DCT. This makes DWT based Steganography the future central 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) [14] can be adjusted in perfectly undetectable ways.

3.1 "*Steganoflage*"[5]- Our Proposed Framework

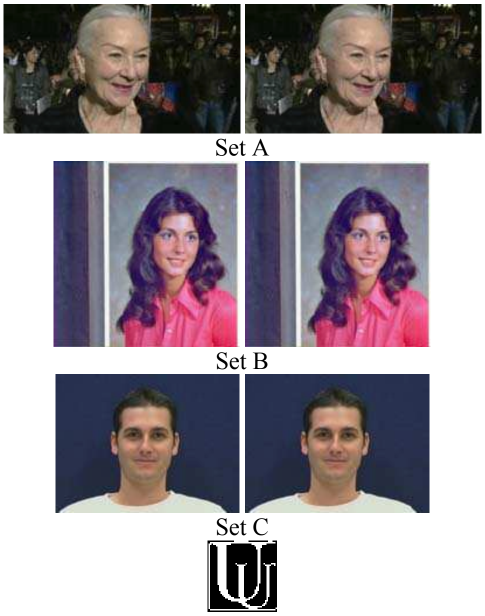
Currently we are investigating and evaluating the idea of taking into account the advantages of the techniques outlined earlier. We aim to embed within the edge directions in the 2D wavelet decomposition. In this way we are guaranteed a high quality stego image. To tackle the problem of edge limited payload we choose video files. Spreading the hidden data along the frames of the video will compensate for the drawback of the edge embedding technique.

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). 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). 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.

Video files indexing and content based retrieval applications have attracted a lot of attention during the last few years and they still are areas of active research. The core of our proposal is to find salient spatial features in image frames. We perform 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), scaling, rotation or cropping will result in the destruction of the embedded data because any reference point that can reconstruct the image will be lost. However, skin tone detection in the transformed colour space ensures immunity to geometric transforms.
2) Our suggested scheme modifies only the regions of the skin tone in the colour transformed channel, this is done for imperceptibility reasons.
3) The skin-tone has a centre point at Cb, Cr components, it can be modelled and its range is known statistically, therefore, we can embed safely while preserving these facts. Moreover, no statistical breach occurs whether it is of first order or second order type.
4) If the image (or frame) is tampered with by a cropping process, it is more likely that our selected region will be in the safe zone, because the human faces generally demonstrate the core elements in any given image and thus protected areas (e.g., portraits).
5) Our Steganographic proposal is consistent with the object based coding approach followed in MPEG4 and MPEG7 standards (the concept of Video Objects (VOs) and their temporal instances, Video Object Planes (VOPs) is central to MPEG video) [41].
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 (e.g., 100) an encrypted password and a link to the next frame holding the next portion of the hidden data in the video. Note this link does not necessarily need to be in a linear fashion (e.g., frames 100→12→3...→n).
7) Videos are one of the main multimedia files available to public on the net thanks to the giant free web-hosting companies (e.g., YouTube, Google Videos, etc). Every day a mass of these files is uploaded online and human factors are usually present.

Figure 4 shows how the proposed method preserves the quality of the original image. Table 2 shows the in comparison of our approach to F5 and S-Tools which are known as strong algorithms. The table was generated using the images shown in Figure 5. F5 and S-Tools are available online[6]. S-Tools performance was discussed in our work [42].



Set A

Set B

Set C

Figure 4. Our proposal in action. Set A,B&C: (left) Original test images and (right) Stego images 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

4 Conclusion

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

References

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

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

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

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

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

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

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

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

[9] Petitcolas, F.A.P.: "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.

[9] Petitcolas, F.A.P.: "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.

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

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

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

[13] Areepongsa, S. Kaewkamnerd, N. Syed, Y. F. and Rao. K. R.: 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. 2000.

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

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

[16] Lin, E. T. and Delp, E. J.: A Review of Data Hiding in Digital Images. Retrieved on 1.Dec.2006 from Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers, Apr 1999.

[17] Kermani, Z. Z. and Jamzad, M.: 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.

[18] 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.

[19] 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.

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

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

[22] 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.

[23] 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.

[24] 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.

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

[26] 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.

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

[28] Popescu, A.C.: 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.

[29] 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 of Intelligent Systems, 22-23 April 2006, 1- 6.

[30] Hashad, A.I., Madani, A.S. and Wahdan, A.E.M.A.: 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.

[31] Raja, K. B., Chowdary, C.R., Venugopal, K. R. and Patnaik, L. M.: 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.

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

[33] Manikopoulos, C., Yun-Qing, S., Sui, S., Zheng, Z., Zhicheng, N. and Dekun, Z.: 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.

[34] Wen-Yuan Chen.: 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).

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

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

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

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

[39] Bae-Ho Lee, Kwang-Hee Kim, Yonggwan Won, and Jiseung Nam.: 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).

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

[41] Puri, A and Eleftheriadis, A.: MPEG-4: An object-based multimedia coding standard supporting mobile applications. Mobile Networks and Applications 3 (1): 5–32. (1998). Springer Netherlands

[42] Cheddad, A., Condell, J., Curran, K and Mc Kevitt, P.: A Comparative Analysis of Steganographic Tools. Proceedings of the Seventh IT&T Conference. Institute of Technology Blanchardstown, Dublin, Ireland. 25th- 26th October 2007. pp 29-37.

Internet Resources:

[1] http://observer.guardian.co.uk/uk_news/story/0,6903,336271,00.html . Accessed on: January 25, 2007.

[2] http://news.bbc.co.uk/1/hi/technology/6361891.stm Retrieved on: 15-02-2007 at: 14:17.

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

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

[5] http://www.infm.ulst.ac.uk/~abbasc/

[6] F5: http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html, and S-Tools from: ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip