Steganoflage:[1] a new digital image security strategy

Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt
School of Computing and Intelligent Systems, University of Ulster, Magee, UK

Abstract

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier. The ultimate goal is to conceal the very presence of the embedded data. Current work in the state of the art, whether in the spatial domain or the frequency domain, cannot tolerate any geometrical attacks, e.g., rotation, translation or cropping. This paper discusses a novel scheme whereby computer vision, particularly skin tone detection, is incorporated into the process of steganography to yield an object oriented embedding mechanism. Skin tone information is deemed to be psycho-visually redundant. The paper also discusses two applications of steganography in digital image forensics and the secure transmission of electronic patient records.

1 Introduction

For decades people strove to develop innovative methods for secret communication: steganography, as an example, came to life under the assumption that if the feature is visible, the point of attack is evident. Steganography is the art and science of hiding data in a transmission medium. It is a sub-discipline of security systems. Although the term steganography has existed for thousands of years, its digital version has come to public consciousness of late. With the boost in computer power, the Internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, steganography has gone 'Digital'. In the realm of this digital world, steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed.

[1] See: http://www.infm.ulst.ac.uk/~abbasc/index.html.

Digital steganography refers to the science that involves communicating secret data in an appropriate multimedia carrier in an undetectable manner, e.g., in image, audio, or video files. Here we concentrate on digital images where human visual perception is exploited. The ultimate goal here is to conceal the very presence of the embedded data. Steganalysis, which is the official counter attack science, has challenged steganographic algorithms whether they are based on the spatial domain or the transform domain.

Inspired by the notion that steganography can be embedded as part of the normal printing process, Japanese firm, Fujitsu[2], is developing a technology to encode data into a printed picture that is invisible to the human eye, which can be decoded by a mobile phone with a camera. The process takes less than one 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 colour 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. Mobile cameras are able to ‘see’ the coded data and retrieve it. This application can be used for 'Doctor’s prescriptions, food wrappers, billboards, business cards and printed media such as magazines and pamphlets' or to replace barcodes.

Most of the steganography research to date has 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 rather than the entire image. With the advances in computer vision 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 was a key achievement in the biometric research field. It provides a simple yet real time and robust algorithm. In this work we examine the state of the art and we look at our scientific contributions

[2] Hiding messages in plain sight. Available from: <http://news.bbc.co.uk/go/pr/fr//1/hi/technology/6361891.stm>.

along with various frameworks of security applications in which steganography can play a major role.

2 Proposed method

For colour face images, we use the algorithm described in Cheddad et al. (2009). A skin probability map is created from a special non-linear transformation that injects a zeroed R, the red component in RGB (Red, Green, Blue) images, into its formulation. The central focus of this paper is to embed the secret message in the first-level 2D Haar DWT (Discrete Wavelet Transformation) with the symmetric-padding mode guided by the detected skin tone areas.

Algorithms based on DWT experience some data loss since the reverse transform truncates the values if they go beyond the lower and upper boundaries (i.e., 0 - 255). Knowing that human skin tone resides along the middle range in the chromatic red of *YCbCr* colour space allows us to embed in the DWT of the *Cr* channel without worrying about the truncation. This would leave the perceptibility of the stego-image virtually unchanged since the changes made in the chrominance will be spread among the *RGB* colours when transformed. We choose wavelets over DCT (Discrete Cosine Transform) because the wavelet transform mimics the Human Vision System (HVS) more closely than the DCT does. Also, visual artefacts introduced by wavelet coded images are less evident compared to DCT because the wavelets transform does not decompose the image into blocks for processing. Let *C* and *P* be the cover-image and the payload respectively. The stego-image *S* can be obtained by the following embedding procedure:

Step 1: Encrypt P using a user supplied key to yield P’

Step 2: Generate skin tone map (*skin_map*) from the cover C and determine an agreed-upon orientation, if desired, for embedding using face features as described earlier (embedding angle will be treated as an additional secret key)

Step 3: Transform *C* to *YCbCr* colour space

Step 4: Decompose the channel *Y* by one level of 2D-DWT to yield four sub-images (*CA,CH,CV,CD*)

Step 5: Resize *skin_map* to fit *CA*

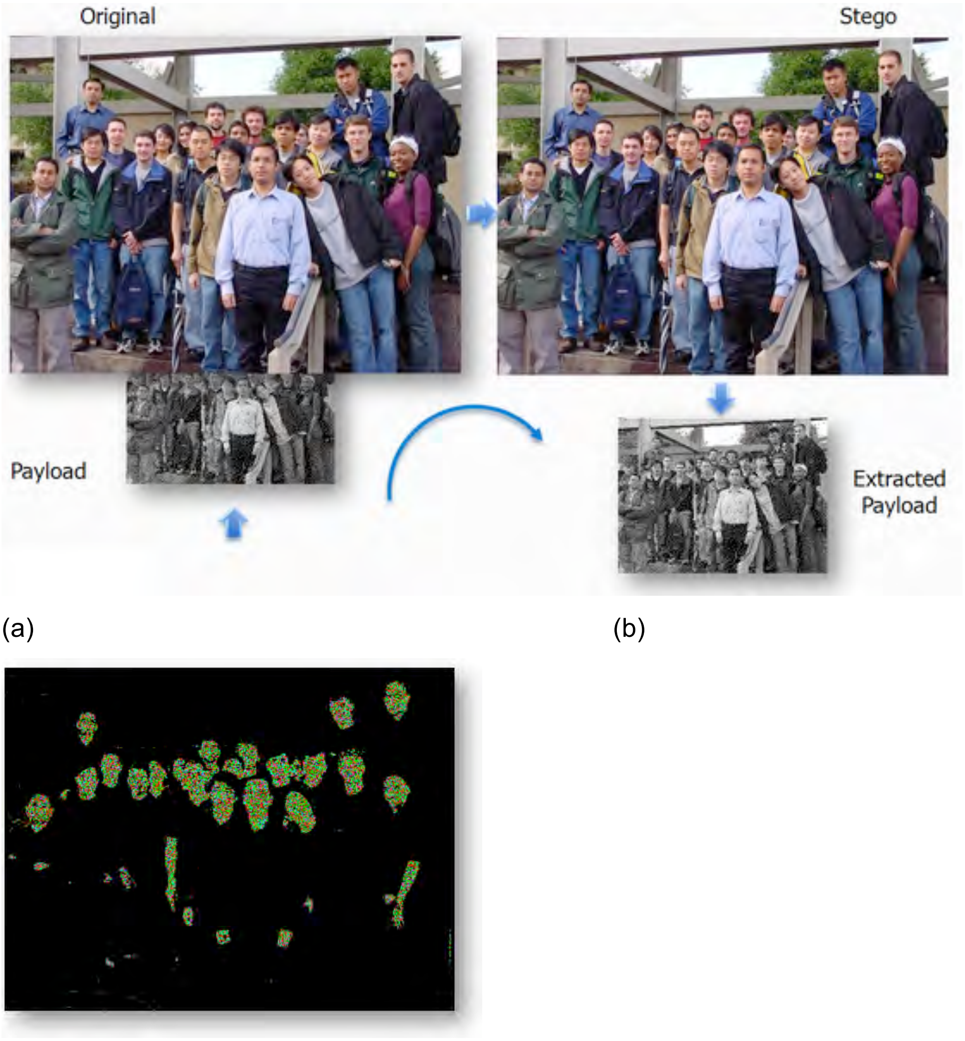
Step 6: Convert the integer part of coefficients of *CA* into the *Binary Reflected Gray Code* (*BRGC)* and store the decimal values

Step 7: Embed (the embedding location of data is also randomized using the same encryption key) the secret bits of *P'* into the *BRGC* code of skin area in *CA* guided by the *skin_map*

Step 8: Convert the modified *BRGC* code back to coefficients, restore the decimal precision andreconstruct the image *Y'*

Step 9: Convert *Y'CbCr* to *RGB* colour space and obtain the stego-image, i.e., *S*. (The effect of embedding is spread among the three RGB channels since the colour space was transformed).

The decoding stage essentially follows steps 2-6 while step 7 refers instead to the extraction phase of the secret bits before the decryption of the bit stream is performed. An example of the results obtained is shown in Figure 1.



(a) (b)

(c)

Figure 1. Hiding in human skin tone areas: (a) original image, (b) stego-image and (c) difference between original and stego-images.

3 Applications

This section deals with two applications of the aforementioned method of self-embedding, namely how to aid digital forensics experts detect forgery and recover evidences and how to secure electronic patients records' transmission and storage.

3.1 Digital forensics

Recent advances in technology and communications have resulted in increased porting of data. This however has also resulted in the need for increased vigilance with regards the security of documents. Safeguarding such digital documents is essential and we believe that steganography can play an important role here by adopting the self-embedding approach, where digital documents can be recovered after forgery by extracting the embedded data. In the search for the best way to represent the cover image with the least bit requirement for embedding we identified dithering as our ultimate pre-processing step which is the foremost task in building Steganoflage.

The process can be regarded as a distorted quantization of colours to the lowest bit rate. Meanwhile, reduction of the number of image colours is an important task for transmission, segmentation, and lossy compression of colour visual information (Farid 2008) - which is why dithering is used for printing. Dithering is a process by which a digital image with a finite number of grey levels is made to appear as a continuous-tone image (Floyd and Steinberg 1976). Jarvis and Roberts (1976) implemented dithering in the wavelet domain providing improved performance. Figure 2 illustrates the use of the proposed method to combat digital document forgery. Shown are the original image (2a), dithered version of original used as a payload (2b), Stego image after embedding (2c), extracted payload without attacks (2d), attacked Stego, i.e., face tampered with (2e), reconstructed hidden data from the attacked version (2f), inverse halftoning of (2f) shown in (2g), inverse halftoning of (2e) shown in (2h), and error signal of (2g) and (2h) with contrast being enhanced for display shown in (2i). Notice that only the tampered region, herein shown within a superimposed circle, demonstrates a coherent object in (2i).

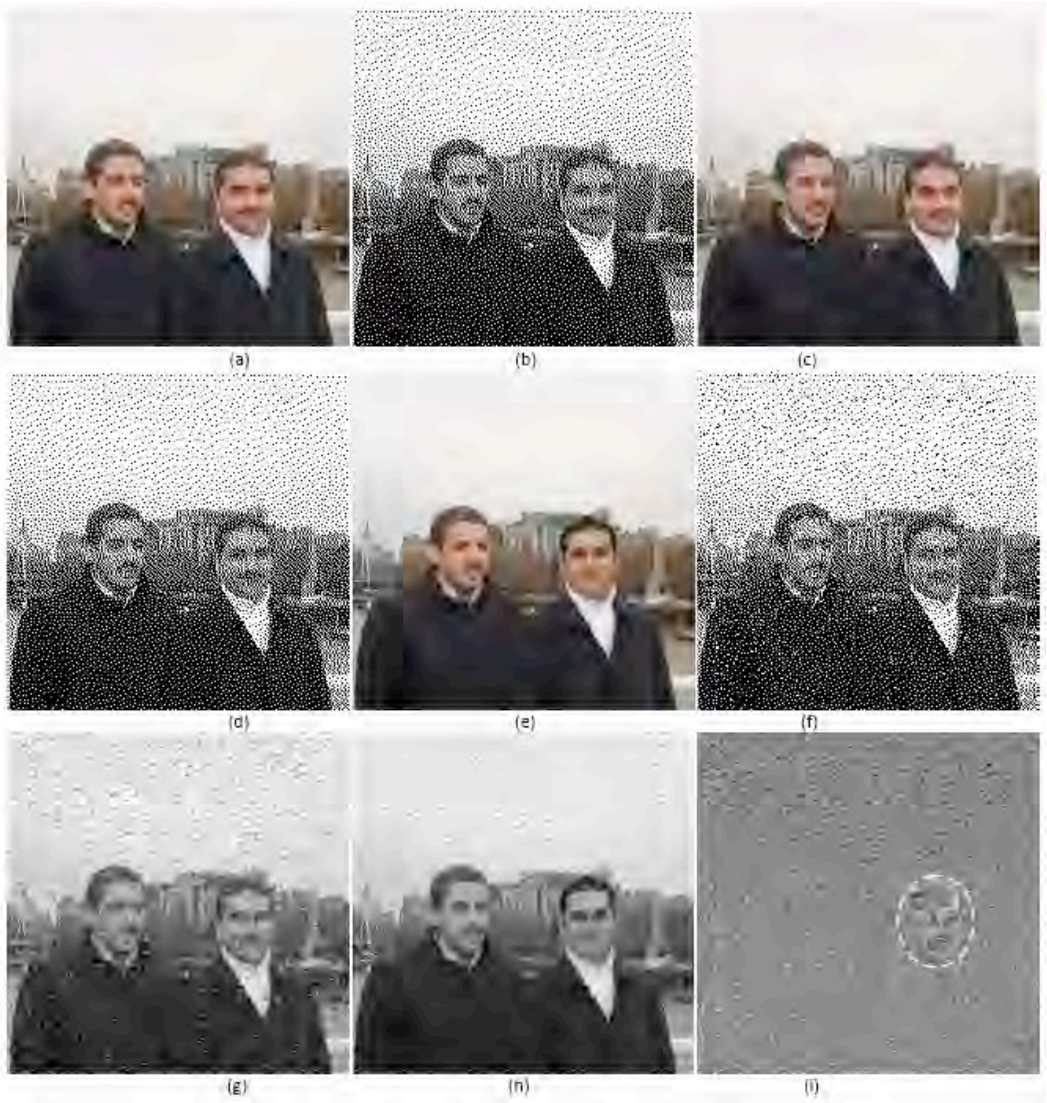
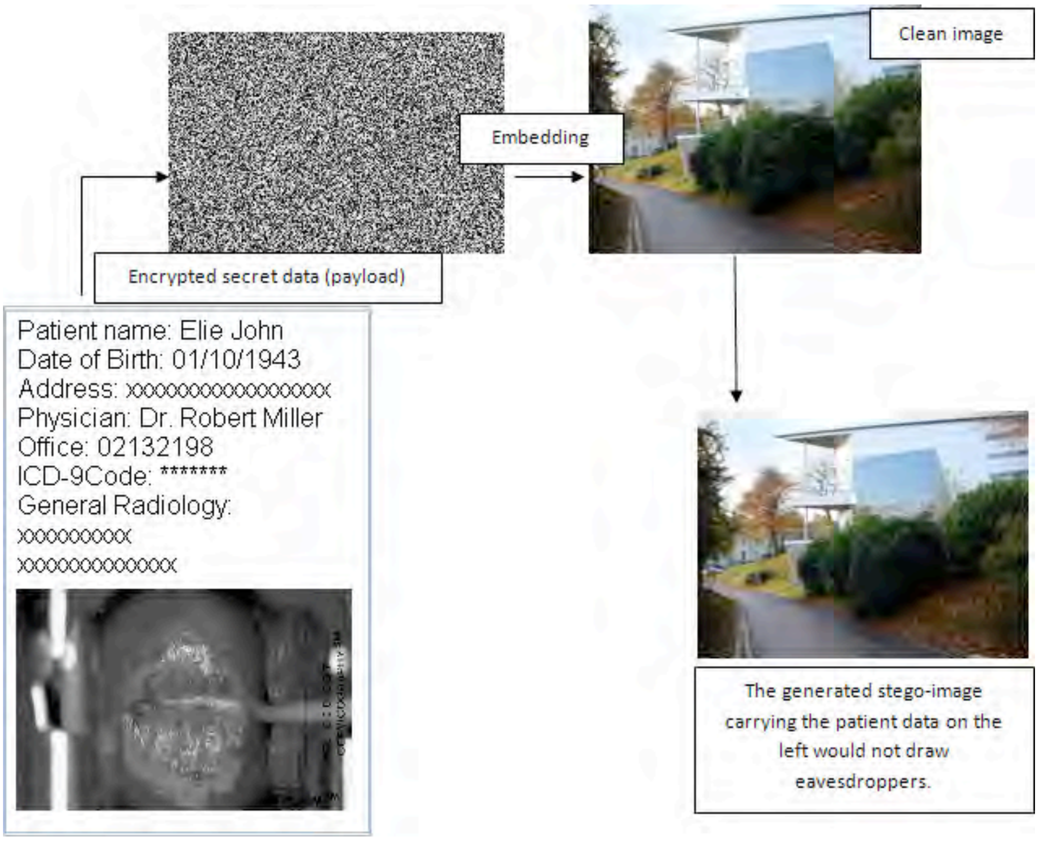


Figure 2. Performance of self-embedding algorithm on securing digital data.

3.2 Electronic patients records

Electronic patient records (EPRs) are a precious entity in health care. With the recent boost in communication technology, the massive increase in database storage and the introduction of the concept of e-Government, EPRs are more frequently stored in digital form. This goes hand in hand with the aim of the paperless workspace, but it does come at the expense of security breaches, especially if such sensitive and highly confidential information is transmitted over a network. The problem is in the security mechanism adopted to secure these documents by means of encrypted passwords. However, this security shield does not actually protect the documents that are stored intact. Encrypted passwords in fact, restrict only the access to data, a mechanism that can be bypassed by malicious attacks to get through to the real patients’ data.

Digital steganography would provide an ultimate guarantee of authentication and protection that no other security tool may ensure (see Figure 3). It is an enabling technology that can assist in transmitting EPRs across distances to hospitals and countries through the Internet without worrying about security breaches on the network (e.g., eavesdroppers’ interception). Thus, embedding the patient’s information in the image could be a useful safety measure. Medical records of patients are exceptionally sensitive and need rigid security during both storage and transmission.



Patient name: Elie John
Date of Birth: 01/10/1943
Address: xxxxxxxxxxxxxxxxxx
Physician: Dr. Robert Miller
Office: 02132198
ICD-9Code: *******
General Radiology:
xxxxxxxxxx
xxxxxxxxxxxxxx

The generated stego-image carrying the patient data on the left would not draw eavesdroppers.

Figure 3. EPRs data being concealed in an innocuous file for secure transmission.

4 Conclusion

In this paper we presented an insight into the science of steganography which can be useful to protect scanned documents from being tampered with and can help ensure the safe transmission of confidential data such as patient’s medical records through unsecure channels such as the Internet. The hidden data can be fully reconstructed after supplying the correct key. Exhaustive details of steganography and our approach can be obtained from Cheddad (2009).

References

Cheddad, A. Survey on Steganography: http://www.infm.ulst.ac.uk/~abbasc/Survey.pdf, 2009.

Cheddad, A., Condell, J., Curran, K. and McKevitt, P. "A Skin Tone Detection Algorithm for an Adaptive Approach to Steganography," *Journal of Signal Processing,* 2009, Elsevier Science. DOI: 10.1016/j.sigpro.2009.04.022.

Farid, H. Fundamentals of image processing: <http://www.cs.dartmouth.edu/farid/tutorials/fip.pdf>, tutorial, 2008: 61.

Floyd R. W. and Steinberg, L. “An adaptive algorithm for spatial grey scale,” in *Proc. Society of Information Display,* vol.17, 1976: 75-77.

Jarvis, J. and Roberts, C. “A new technique for displaying continuous tone images on a bilevel display,” *IEEE Transactions on Communications*, vol. 24, no. 8, 1976: 891-898.