"Steganoflage" - A Novel Approach to Image Steganography

Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt
School of Computing and Intelligent Systems, Faculty of Computing and Engineering
Londonderry, BT48 7JL, Northern Ireland, United Kingdom
Emails: {cheddad-a, j.condell, kj.curran, p.mckevitt}@ulster.ac.uk

1. Introduction

Steganography, which is the science of concealing the very existence of data in another transmission medium, comes along not to replace Cryptography but rather to boost the security using its obscurity features. Steganography has various useful applications such as for Human rights organizations (as encryption is prohibited in some countries), Smart IDs where individuals' details are embedded in their photographs (content authentication), data integrity by embedding checksum, medical imaging and secure transmission of medical data and bank transactions to name few [1]. Conventional encryption methods suffer in the sense that any eavesdropper is able to notice the encrypted transmitted data. This carries threat of attacks such as brute force attack. Different algorithms, to date, have emerged dealing with Steganography. Some target the image spatial domain which gives a high payload capacity, while others prefer the frequency domain for robustness to attack at the expense of a small embedding space.

We believe that most of these algorithms are not resilient to image geometric distortions, such as rotation, translation and cropping [2]. Another noticeable fact is that few of them address in-depth the issue of data encryption prior to embedding, and for the ones which do they rely heavily on the conventional encryption algorithms. This dependency is due, in part, to scarce in research pertaining to image encryption. Therefore, the renowned block cipher algorithms, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), etc, are not suitable to handle bulky data, i.e., digital images, for their long computational process [3] and probability of generating repetitive patterns given their nature. We have developed a robust Steganography method with multiple layers of security to protect confidentiality and this paper outlines some of the aspects of our approach.

1.1 Aim and Contributions

Security is of utmost importance to most individuals or organisations. This work aims to enhance Steganography in digital images. Even though our research is still evolving, we have progressed far enough to bring to the domain some new and novel contributions. We summarize them below:

- A new secure and efficient bulk data encryption surpasses the previous highlighted security gaps. This scheme uses what we call *Irreversible Fast Fourier Transform (IrFFT)*.
- A highly efficient and real time skin tone detection algorithm which outperforms the state of the art.
- A new paradigm that enhances the embedding process in Steganography by incorporating computer vision. We exploit our previous published algorithm for face features extractions.
- The cost effective and highly secure ID card. This is one of our goals – a final product whose feasibility is still under investigation as we seek funding for this focused knowledge transfer application.

2. Steganoflage

2.1 Payload Encryption

We have exploited the strength of a 1D encryption algorithm namely SHA-1 and we extended it to handle 2D data such as images. The FFT is incorporated into the process to increase the disguise level and thus generate a random-like output that does not leave any distinguishable patterns of the original image. The exhaustive step by step description of our algorithm is illustrated in Fig 1. Table 1 shows comparisons of our approach to current algorithms [4].

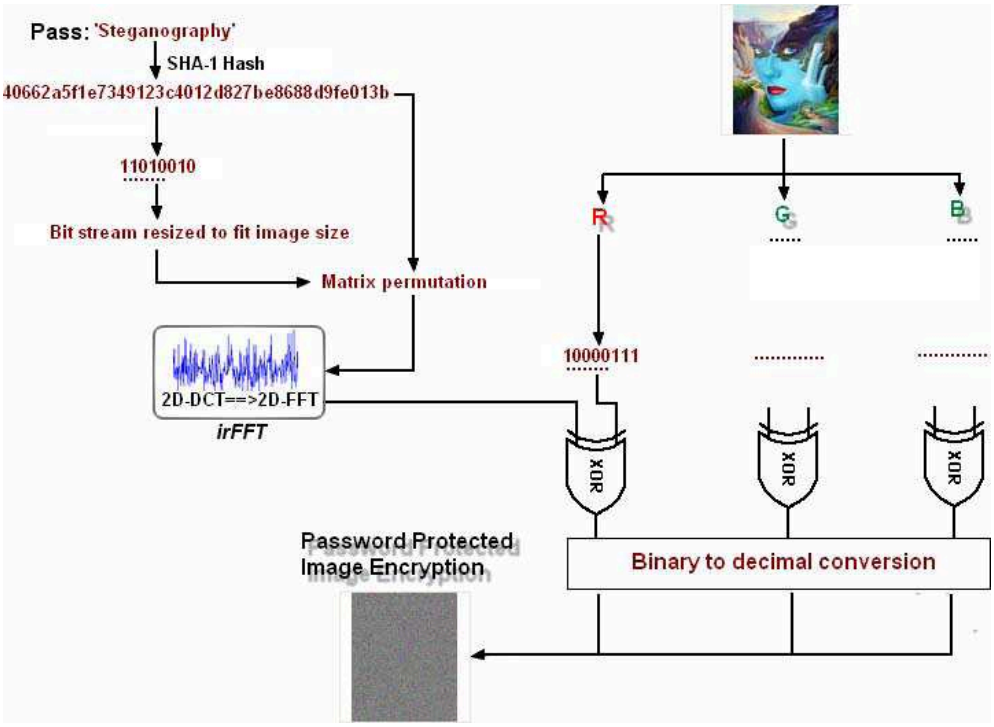

Fig. 1. Block diagram of the steps used in the proposed algorithm for image encryption.

Table. 1. Performance analysis of our proposal against recent methods using Lena image - Correlation coefficients, ranging from '1' highly correlated to '-1' highly uncorrelated, of pairs of adjacent pixels in different directions. Experiments were applied on Lena image. These coefficients ensure the two considered images are statistically independent but with different degrees.

Scan Direction	Original Image	Our Method	[5]	[6]	[7]	[8]
Horizontal	0.9851	**-0.0030**	0.006816	0.005343	0.01183	-0.0142
Vertical	0.9720	0.0015	0.007827	0.008460	0.00872	**-0.0074**
Diagonal	0.9594	**-0.0019**	0.003233	0.003557	0.01527	-0.0183

2.2 Detecting Skin Areas in the Cover Image

Detecting human skin tone is of utmost importance in numerous applications such as video surveillance, face and gesture recognition, human computer interaction, image and video indexing and retrieval, image editing, vehicle drivers' drowsiness detection, controlling users' browsing behaviour (e.g., surfing pornographic sites) and Steganography (our aimed application). We developed a novel

colour space where we believe human skin clusters can be well classified with carefully selected boundaries. We provide some examples drawn from our experiments and results which are promising (see Fig 2 and Table 2). Additionally, we have set in context and proved that our proposition is deemed true as the set of results agrees reasonably with our speculated hypothesis that says: "Unlike the common thought, luminance inclusion does increase separability of skin and non-skin clusters" [9].

Fig 2. Performance analysis of image 6: (left to right) original images, outputs of [10], [11], [12] and of our method respectively. Shown are some examples from our WWW database that appear in Table 2.

Table 2. Comparison of computational complexity of our proposal against other current methods [10], [11] and [12] on a range of 12 images obtained from WWW.
(* The Log algorithm [11] did not converge for more than 10 min which forced us to interrupt its process.)

Image #	No Elements	Time elapsed in seconds			
		[10]	[11]	[12]	Proposed
1	196608	0.2970	4.547	2.188	0.062
2	196608	0.3280	3.563	1.906	0.062
3	849162	0.5160	33.062	7.531	0.078
4	840450	0.5160	33.515	7.796	0.125
5	850545	0.6090	39	8.343	0.062
6	**478518**	**0.4060**	**22.094**	**4.156**	**0.047**
7	849162	0.6090	39.219	6.641	0.078
8	849162	0.5160	39.172	8.484	0.078
9	849162	0.6100	38.203	6	0.078
10	7750656	3.1720	> 600 *	54.86	0.562
11	982101	0.6410	79.469	7.297	0.078
12	21233664	9.3910	> 600 *	144	1.531

2.3 Object Oriented Embedding

Figure 3 demonstrates the embedding process. Whilst not shown here, due to space restrictions, we could extract efficiently the embedded data after rotation, cropping and noise addition. The embedding process took place in the 1st level wavelet decomposition to resist statistical attacks [4].

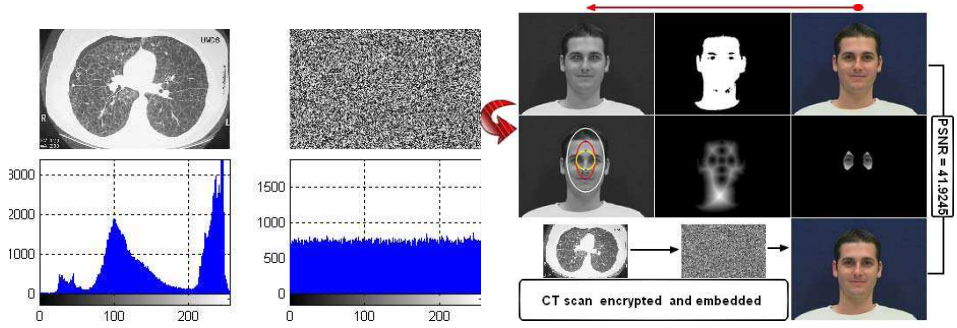

Fig. 3. Our proposed Steganography system using the aforementioned cryptography: (left) the secret data, herein CT scan of a young female[1] with chronic breathlessness disease and its encrypted version, each of which are shown with the respective histogram, (right) concealment of the medical data in a face image, note the use of biometrics facilitates embedding invariant to rotation.

[1] Lung Case Index, [online]. Available from <http://www.radiology.co.uk>, accessed on 10-07-08 at 20:15.

2.4 Secure Steganographic Identity Cards

The concept behind this application stems from our advanced research into the strengthening of digital Steganography in digital imaging. Steganography makes it possible to hide personal or sensitive data in photo images on ID cards [13].

3. Conclusion

We have presented our research to date which brings about the enhancement of Steganography in digital images. Various contributions have been highlighted briefly, while linking them whenever necessary to references for further details. These contributions are: A new secure and efficient bulk data encryption, where we generate a spatial mask from the frequency domain which we termed as Irreversible Fast Fourier Transform (*IrFFT*), a highly efficient and real time skin tone detection algorithm, a first attempt to incorporate computer vision to orient the embedding process in Steganography, and finally a cost effective and highly secure ID cards which is under investigation.

References

[1] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. (2008). Biometric Inspired Digital Image Steganography. In the proceedings of the 15th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'08). pp. 159-168. IEEE Computer Society.

[2] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. Digital Image Steganography: Survey and Analyses of Current Methods. Under review, the International Journal of Computer Standards& Interfaces, Elsevier.

[3] Usman, K., Juzoji, H., Nakajima, I., Soegidjoko, S., Ramdhani, M., Hori, Toshihiro, H. and Igi, S. (2007). Medical Image Encryption Based on Pixel Arrangement and random Permutation for Transmission Security. Proc of the 9th International Conference on e-Health Networking, Application and Services. 19-22 June 2007, pp: 244-247. IEEE DOI: 10.1109/HEALTH.2007.381640.

[4] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. On Digital Image Encryption for Secure Steganography Applications. Under review, IEEE Transactions on Information Forensics & Security.

[5] Wong, KW., Kwok, B.SH. and Law, WS. (2008). A fast image encryption scheme based on chaotic standard map. Physics Letters A, Elsevier. 372 (2008), pp: 2645-2652.

[6] Lian, SJ. and Wang. SZ. (2005). A Block Cipher Based on a Suitable Use of the Chaotic Standard Map. International Journal of Chaos, Solitons and Fractals, Elsevier. 26 (1), pp: 117-129.

[7] Zou, J., Xiong, C., Qi, D. and Ward, R.K. (2005). The application of chaotic maps in image encryption. Proc of the 3rd International IEEE-NEWCAS Conference. 19-22 June 2005, pp: 331-334.

[8] Gao, T. and Chen Z. (2008). A new image encryption algorithm based on hyper-chaos. Physics Letters A, Elsevier. 372(2008), pp: 394-400.

[9] Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P. A Real Time Colour Transformation for Effective Skin Tone Detection. Unpublished work.

[10] Hsu R.-L., Abdel-Mottaleb M. and Jain A. K. (2002). Face detection in color images. IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24(5), 696-702, 2002.

[11] Berens, J. and Finlayson, G.D. (2000). Log-opponent chromaticity coding of colour space. Proceedings of the 15th International Conference on Pattern Recognition. IEEE Computer Society. vol.1, 206-211. Barcelona, Spain.

[12] Kovač, J., Peer, P., and Solina, F., (2003). Human Skin Colour Clustering for Face Detection. EUROCON 2003. International Conference on Computer as a Tool. IEEE. Vol 2, pp: 144 - 148. Ljubljana, Slovenia, September 2003.

[13] Curran, K. Condell, J., Cheddad, A., Mc Creadie, K. and Maguire, L.M. (2009). Issues of Privacy & Surveillance. Accepted for publication in the proceedings of the 5th International Conference on Technology, Knowledge and Society. 30-Jan to 1-Feb 2009. Huntsville, Alabama, USA.