Information hiding-enabled data transmission framework

Abbas Cheddad, Joan Condell, Kevin Curran Paul Mc Kevitt
School of Computing and Intelligent Systems, Faculty of Computing and Engineering
University of Ulster at Magee, BT48 7JL, Northern Ireland, United Kingdom
cheddad-a@email.ulster.ac.uk

ABSTRACT: *The concept behind this study stems from advanced research into the strengthening of digital steganography in digital imaging, a science that deals with imperceptibly embedding secret data within data. This is a fascinating scientific area which falls under the umbrella of security systems research. This paper exploits a developed information hiding technique tailored specially for the protection of digital data. We have achieved promising results which give direct solutions to real world problems. Particularly, our method not only detects forgery but also provides a good approximation of the original data.*

Keywords: Information hiding, Self - embedding, Steganography, Forgery detection.

Received 1 March 2009; Revised 3 April 2009; Accepted 11 April 2009

1. Introduction

The recent digital revolution has facilitated communication, data portability and on-the-fly manipulation. The ease of editing visual data in the digital domain has aided unauthorized tampering performed without leaving any perceptible trace. Steganography can be used to send sensitive information over open communications lines. More specifically digital watermarks are defined as data embedded directly within content which are imperceptible to humans but readable by computers. This particular study represents a foundation technology which enables unique and enhanced applications and services. It can authenticate, enhance security and has obvious potential real-world applications. Watermarks can be recognized by enabled software or hardware to provide copyright information, authenticate, track, monitor, enhance security and enable access to additional data, information and ecommerce opportunities across devices and networks.

Documents are more and more being stored in a digital form. This goes hand in hand with the aim of the paperless workspaces, but it does come at the expense of security breaches especially if the document is transmitted over a network. Document forgery is a worry for a range of organisations, i.e., Governments, Universities, Hospitals and Banks. The ease of digital document reproduction and manipulation has certainly attracted many eavesdroppers.

Relational Database Management Systems (RDBMS) secure scanned documents through the use of a password in the database. This means that scanned documents are stored with a “String” encrypted password. The main issue here is if a hacker is able to crack the password then they may be able to modify any document digitally and log out as if nothing has happened.

This paper unveils two systems: one to combat digital document forgery and the other a new method to authenticate CCTV (closed-circuit television) footage. In July 2005, it was discovered that a number of 2nd World War files held at the National Archives in the UK contained forged documents. An internal investigation found that the forgery took place during or after the year 2000 [1]. Additionally, recorded CCTV video frames will not stand up in court as reliable evidence since they are prone to tampering.

2. Methodology

The proposed method relies on a special case of information hiding known as self-embedding. This entails embedding a low bit rate of the carrier file into itself. It lends itself to forensics as a useful tool for digital inspection [2]. A generic dataflow of the method is provided in Figure 1.

The next section will discuss the ‘low-bit copy’ (the payload) and how to extract it. A discussion will also be provided on the secure and efficient image encryption method as well as the associated embedding procedures.

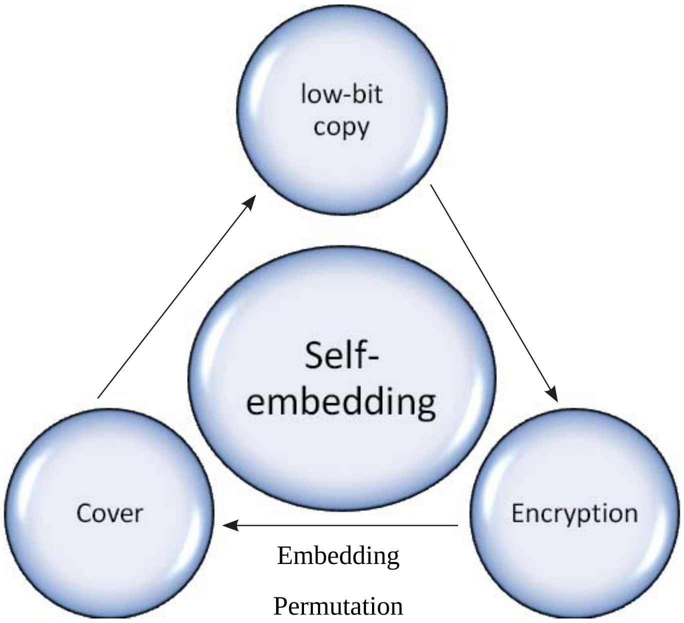


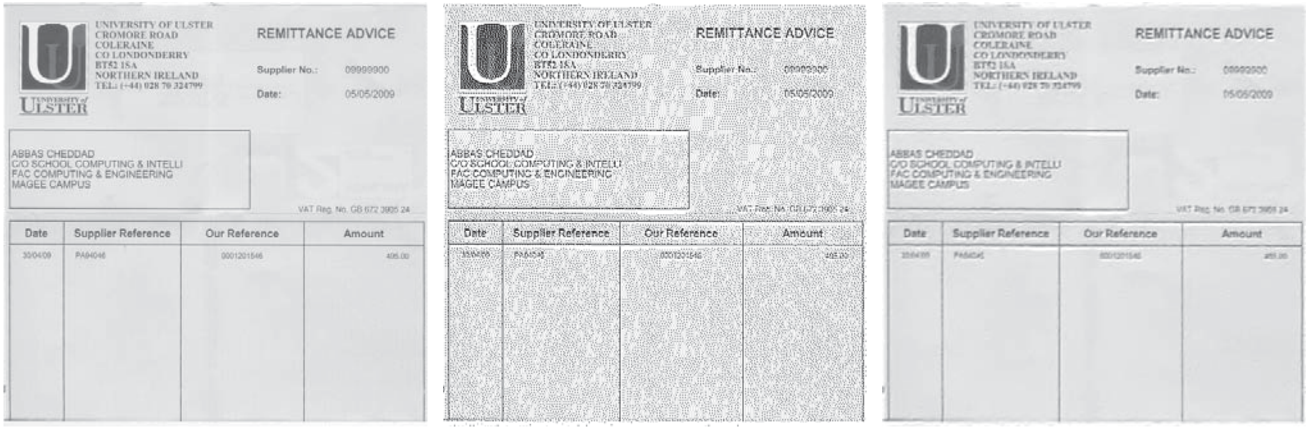
Figure 1. A generic scenario of the self-embedding technique

2.1. Payload construction

Since this study is about self-embedding, one can expect that the payload be extracted from the original file itself. After extensive investigations into the best manner in which to represent an image file the decision was made to use error diffusion. This was found the best fit to capturing graphics as well as text contents in a given image. The obvious merit of incorporating this method is its low embedding space requirement unlike for example the full continuous tone copy (grayscale). The second advantage is the possibility of reconstructing a good approximation of the continuous tone image from this binary version, a process known as inverse half-toning, see Figure 2. This work exploits Jarvis' kernel to generate the error diffusion signal and the Wavelet-based Inverse Half-toning via De-convolution (WInHD) to recover the approximation of the original signal.

2.2. Payload Encryption

The encryption method takes advantage of the sensitivity of the SHA (secure hash algorithm) on the initial condition, i.e., the key. Moreover, the compound transform of DCT (discrete cosine transform) and FFT (fast Fourier transform) are extremely sensitive to changes in 2D space. The latter transforms are used to provide confusion for the expanded map generated through SHA. More details on the algorithm formulation are available in [3]. In essence the encryption procedure is depicted in Figure 3.



UNIVERSITY OF ULSTER
CROMORE ROAD
COLERAINE
CO LONDONDERRY
BT52 1SA
NORTHERN IRELAND
TEL: (+44) 028 70 324799

UNIVERSITY of ULSTER

REMITTANCE ADVICE

Supplier No.: 09999900

Date: 05/05/2009

ABBAS CHEDDAD
C/O SCHOOL COMPUTING & INTELLI
FAC COMPUTING & ENGINEERING
MAGEE CAMPUS

VAT Reg. No. GB 672 3905 24

Date	Supplier Reference	Our Reference	Amount
30/04/09	PA84046	0001201546	405.00

Figure 2. Payload generation: (top left): Original scanned document, (top right) Half-tone version and (bottom) Inverse-half-tone version with distortion of PSNR (Peak Signal-to-Noise Ratio)=25.2257 dB.

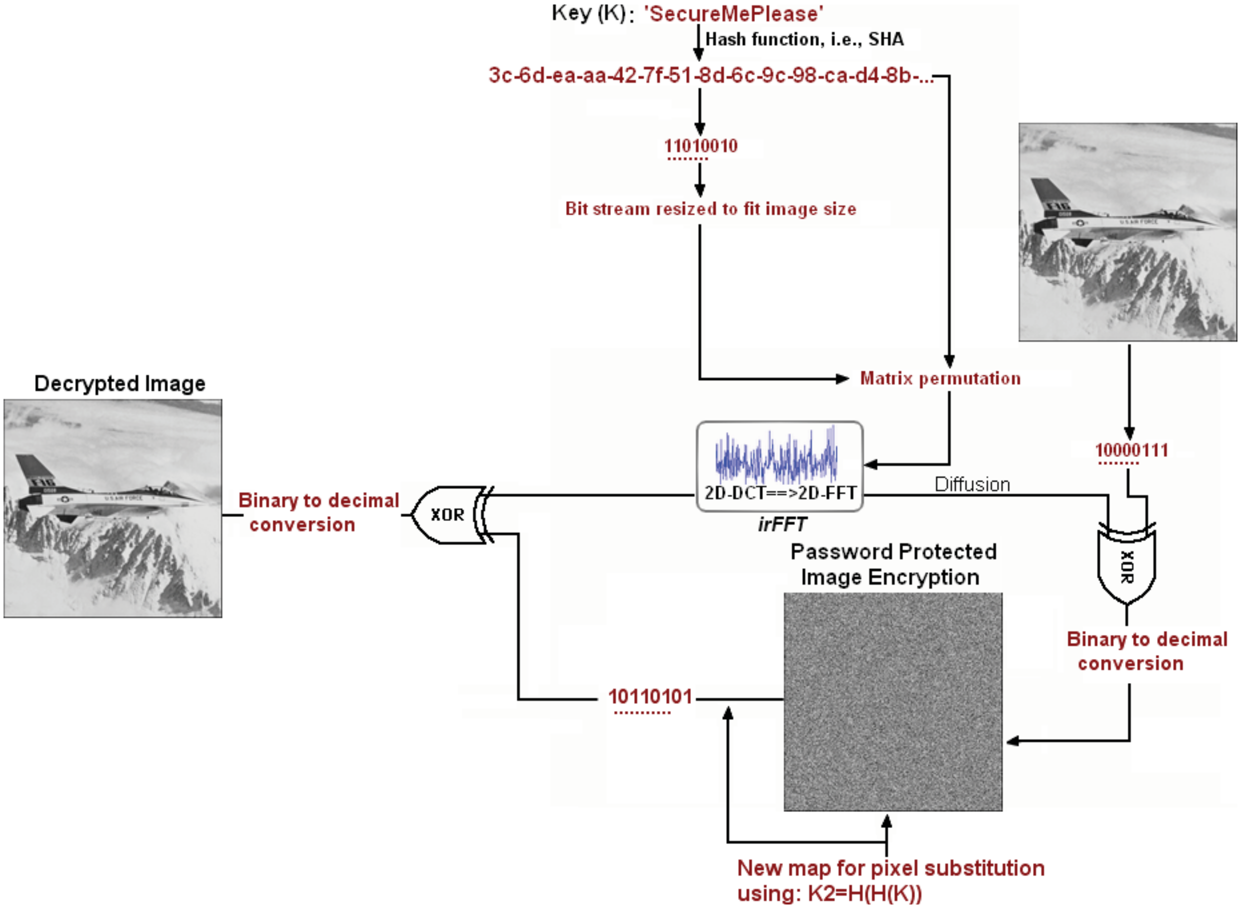

Key (K): 'SecureMePlease'
Hash function, i.e., SHA
3c-6d-ea-aa-42-7f-51-8d-6c-9c-98-ca-d4-8b-...
11010010
Bit stream resized to fit image size
Matrix permutation
Decrypted Image
2D-DCT==>2D-FFT
irFFT
Diffusion
10000111
Binary to decimal conversion
XOR
XOR
Password Protected Image Encryption
Binary to decimal conversion
10110101
New map for pixel substitution using: K2=H(H(K))

Figure 3. A framework for digital image encryption

2.3. The embedding procedure

A fundamental step in our proposal is embedding the secret message in the first level 2D Haar DWT (Discrete Wavelet Transform) with the Symmetric-padding mode, see Figure 4. DWT is a well known transformation that gained popularity among the image processing community especially those dealing with image compression. Its applications in different areas is growing however (note that JPEG2000 uses DWT to compress images). 2D DWT provides a decomposition of the approximation, and the detail in three orientations (horizontal, vertical, and diagonal) by means of a convolution-based algorithm using High and Low pass filters. In our case we compute four filters associated with the orthogonal or bi-orthogonal of the Haar wavelet.

We choose Wavelet over DCT (Discrete Cosine Transform) because the Wavelet transform understands the Human Vision System (HVS) more closely than DCT does; Visual artefacts introduced by wavelet coded images are less evident compared to DCT because the wavelet transform does not decompose the image into blocks for processing [4]. DFT (Discrete Fourier

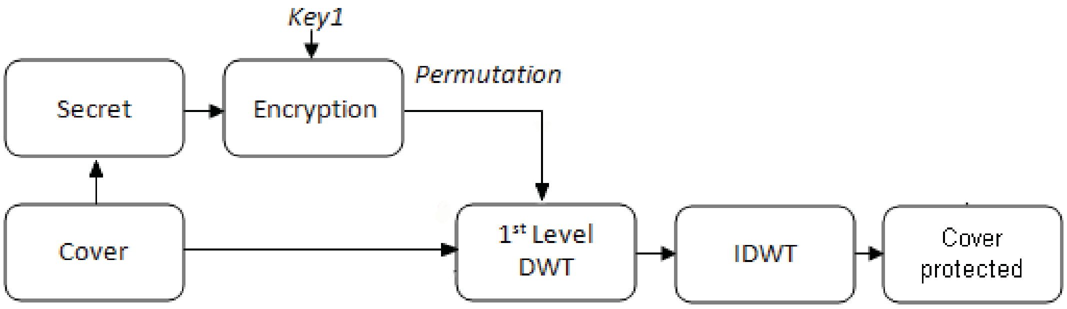


Figure 4. The embedding procedure in the wavelet domain

Transform) and DCT are full frame transforms. Hence any change in the transform coefficients affects the entire image except if DCT is implemented using a block based approach. However DWT has spatial frequency locality, which means if the signal is embedded it will affect the image locally. Hence a wavelet transform provides both frequency and spatial description for an image. More helpful to information hiding, the wavelet transform clearly separates high-frequency and low-frequency information on a pixel-by-pixel basis [5].

Obviously, there are many other existing methods for self-embedding. It is true that some, such as [6, 7], can detect a forgery's location with different degrees of efficiency but their common problem is that they are unable to provide an actual visualization of the original image. In some cases, for instance in court, it is not sufficient to just be able to tell that the image/document has been tampered with (which can be caused by colour changes) without giving the jury a tool to actually extract the original document. On the other hand, Luo et al. [8] suggest a recovery of an approximation of the original with a self-embedding

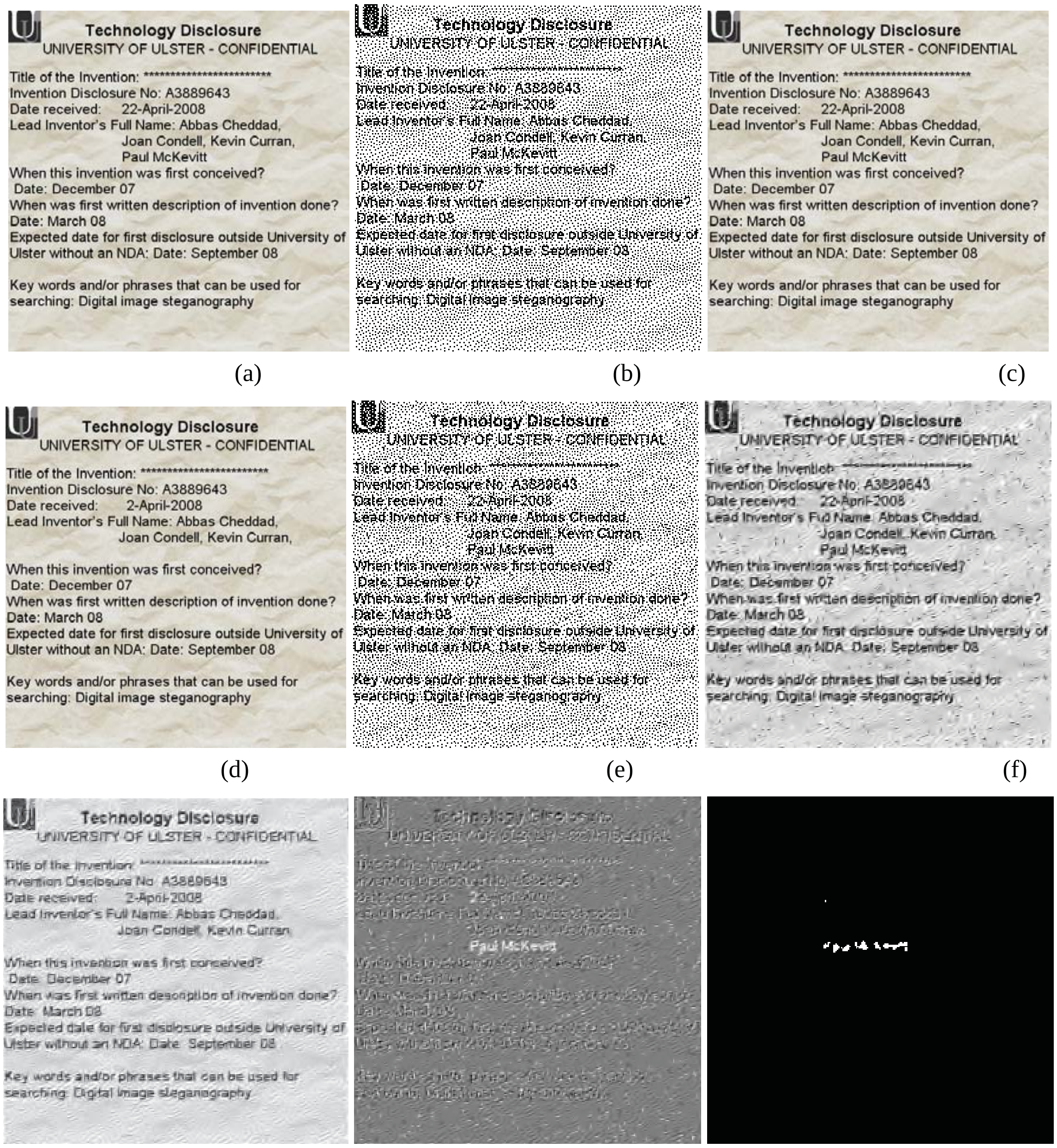


Figure 5. Performance of proposed algorithm on digital document: (a) The original document, (b) Dithered version of original used as a payload, (c) Stego image after embedding, (d) Attacked Stego, i.e., date received has changed and the 4th lead inventor's name has been removed, (e) Reconstructed hidden data from the attacked version, (f) Inverse halftoning of *(e)*, (g) Inverse halftoning of *(d)*, (h) error signal of *(f)* and *(g)*, and (i) shows *(h)* after undergoing binary thresholding

scheme, but since they embedded a continuous tone copy, their algorithm causes more distortion to the carrier file then our algorithm does. Additionally most methods are sensitive to natural processing, for example a JPEG compression of an image would trigger an alarm of forgery.

3. Applications

This section deals with two applications of the aforementioned method of self-embedding, namely how to aid detect forgery and recover evidences and how to secure CCTV footage transmission and storage.

3.1 Scanned document forgery

One of the investigated applications is combating digital document forgery such as scanned documents and digital personal images. Figure 5 shows a practical remedy to photo illegal tampering.

3.2 CCTV footage authentication

An extension to the previous application is its applicability in video streaming. CCTV recording is the primary target and the scheme can successfully eradicate any source of forgery. Various possibilities of eavesdroppers' attacks are illustrated in Figure 6.

4. Conclusion

As organisations go towards paperless workspaces, document forgery becomes an issue. The effortlessness of digital document reproduction and manipulation has undoubtedly contributed to forgery attacks. In this paper we present some applications of information hiding to combat digital tampering. The scheme allows for reconstruction of a quasi-original of the carrier even after undergoing a forgery, furthermore, its distortion effects on the cover file is minimised by using error diffusion.

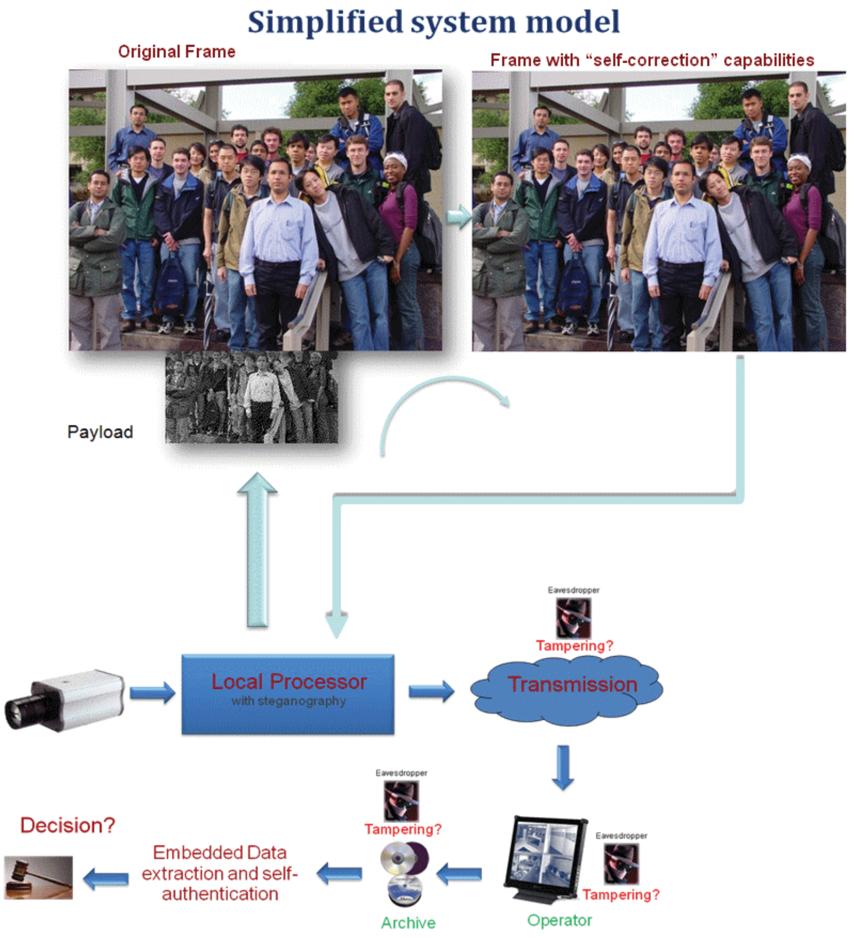


Figure 6. CCTV footage authentication using self-embedding

References

[1] The national Archives (UK government's records and information management), available from: <http://www.nationalarchives.gov.uk/news/stories/195.htm?homepage=news>. Retrieved on 09-06-2008 at 11:23.

[2] Cheddad, A., Condell, J., Curran, K., McKevitt, P (2009). Data hiding tools for digital forensic experts, In: Proceedings of Digital Forensics, Security and Law, May 20-22, 2009, Burlington, Vermont, USA, pp. 111-113, ADFSL (Association of Digital Forensics, Security and Law).

[3] Cheddad, A ., Condell, J., Curran, K., McKevitt, P (2008). Securing information content using new encryption method and steganography, In: Proceedings of the 3rd IEEE International Conference on Digital Information Management, 2008, University of East London. UK. p: 563-568.

[4] Potdar V. M., Song Han and Chang E. (2005). A Survey of Digital Image Watermarking Techniques, 3rd IEEE International Conference on Industrial Informatics (INDIN), p: 709-716.

[5] Raja K. B., Vikas, Venugopal K. R., Patnaik L.M., (2006). High Capacity Lossless Secure Image Steganography using Wavelets. International Conference on Advanced Computing and Communications, ADCOM 2006, p: 230-235.

[6] Caldellia, R., Filippinia, F., Barni, M (2006). Joint near-lossless compression and watermarking of still images for authentication and tamper localization, *Signal Processing: Image Communication*, 890-903.

[7] Yafei, S. li, Z.. Guoweim W., Xinggang, L (2001). Reconstruction of Missing Blocks In Image Transmission by Using Self-Embedding, *In*: Processdings of Proceedings of 2001 International Symposium on Intelligent Multimedia, Video and Speech Processing, May 2-4 2001, Hong Kong, p.535-538.

[8] Luo, H., Chu, S.C., Lu, Z.M (2008). Self Embedding Watermarking Using Halftoning Technique, *Circuits Syst Signal Process*, 27: 155–170.