A Secure and Improved Self-Embedding Algorithm To Combat Digital Document Forgery

Abbas Cheddad, Joan Condell, Kevin Curran and 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
Emails: {cheddad-a, j.condell, kj.curran, p.mckevitt}@ulster.ac.uk

Abstract. The recent digital revolution has facilitated communication, data portability and on-the-fly manipulation. Unfortunately, this has brought along some critical security vulnerabilities that put digital documents at risk. 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 which are stored intact. We propose here a solution to this real world problem through a 1D hash algorithm coupled with 2D iFFT (irreversible Fast Fourier Transform) to encrypt digital documents in the 2D spatial domain. Further by applying an imperceptible information hiding technique we can add another security layer which is resistant to noise and to a certain extent JPEG compression. We support this assertion by showing a practical example which is drawn from our set of experiments. This work exploits Jarvis' kernel to generate the error diffusion signal and the Wavelet-based Inverse Halftoning via De-convolution (WInHD) to recover the approximation of the original signal. Our method not only points out forgery but also allows legal or forensics expert gain access to the original document despite being manipulated. This would undoubtedly be very useful in cases of disputes or claims.

1. Introduction

Historically, the forgery of a document was done mechanically, however, since the recent boost in communication technology, the massive increase in databases storage and the introduction of the concept of e-Government, documents are more and more being stored in a 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 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 to 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. In July 2005 it was discovered that a number of Second World

War files held at the *National Archives* contained forged documents. An internal investigation found that the forgery took place during or after the year 2000 [1].

In this paper we propose a highly robust protection scheme which protects scanned documents from forgery. The scheme is based on an information hiding technique known as Steganography, which is the science that embeds data in a digital medium in an imperceptible manner. The advantage of this technology over the well known technique of Cryptography is that no one knows it is there. A number of Steganographic methods have been introduced; however, few authors have applied Steganography and information hiding to real world problems [2, 3, 4, 5, 6]. In the realm of content based image retrieval in databases, Li [7, 8] demonstrated a clever way to exploit watermarks. Hence, our objective is to put into context a practical application of our ongoing research on enhancing Steganography in digital images that could solve one of those problems. Our proposed algorithm is efficient, highly secure and robust against different image processing attacks.

The contributions of this paper are, a new strong digital image encryption based on SHA-1 and irreversible Fast Fourier Transform (iFFT), a new embedding process in the wavelet domain and finally combating forgery in digital scanned documents using the aforementioned information hiding methods. The remainder of this paper is organised as follows: Related work is reported in section 2; section 3 describes the methodology; experimental results are shown in section 4; and we conclude this work and discuss future work in section 5.

2. Related Work

Information hiding is used for owner identification, royalty payments, and authentication by determining whether the data has been altered in any manner from its original form [9]. Popescu [10] shows a comprehensive investigation carried out on image forensics which aims to detect forgery by means of the preserved natural image statistics. Although, they seem to have successfully created a system whereby image forgery can be detected however our method goes beyond that by showing what the original 'non-forged' image looked like. We believe 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.

Shefali et al. [11] propose a method in which the host image is converted into the YIQ colour space followed by the application of orthogonal dual domains of DCT and DWT transforms. The scheme generates an adaptive watermark based on image features which allows for tamper detection. Their method is complex in the sense

that it uses the dual domains DCT and DWT. Moreover, the method detects the tamper and does not encompass any recovery procedure.

Lukáš et al. [12] take another approach to detecting forgery through the presence of the camera pattern noise, which is a unique stochastic characteristic of imaging sensors, in individual regions in the image. The forged region is determined as the one that lacks the pattern noise. The authors assume the availability of either the same camera that took the attacked image or another image taken with the same camera. The method deals with the detection without the recovery and suffers from false alarms. As far as image forgery is concerned this approach has no practical soundness as it cannot be generalised.

Kostopoulos et al. [13] discuss image authentication by means of a watermarking scheme that embeds an approximation of the image into itself. Specifically, the luminance of the image is inserted into the three colour channels using a mapping function. The method works in the spatial domain, thus its resistance to JPEG compression is not attainable.

Shao et al. [14] propose a semi-fragile method for missing block reconstruction using the concept of self-embedding. Low quality image DCT coefficients are embedded into the LSB of the DCT blocks of the same original image, where missing blocks can be reconstructed from those embedded bits.

In a more intelligent type of self-correcting images, Fridrich and Goljan [15, 16] have proposed the extraction of 11 coefficients from each 8x8 block representing the lowest frequency and then quantizing them using a 50% JPEG quantization matrix. The binary stream of each block is embedded into distant blocks in a seemingly random fashion. Lin et al. [17] used a DCT-based image authentication using a self embedding strategy. The problem with these systems is the high likelihood of having unrecovered data if a relatively large portion of the image is tampered with [18].

Most of the preceding algorithms deal with image authentication and pay little attention to recovery. Those which address recovery use a block-wise-based recovery process. The block based recovery is based on the assumption that the forged segment will likely be a connected component rather than a collection of very small patches or individual pixels [19].

More closely related to our research, Luo et al. [18] propose a method that exploits a digital halftoning technique to transform the host image to a halftone image, in which the content features of the host image are well preserved. The embedding phase takes place in the spatial domain and therefore is not resilient to noise impulses or modest compression. Despite this, the authors claim it is impossible to destroy all the embedded content even when a large area of the watermarked image is tampered with since the content of a block is

dispersed in the whole image instead of some other blocks. Converting the watermarked image into JPEG, even with a high fidelity of Q=100%[1], will result in a complete destruction of the embedded data.

The concept behind this work stems from advanced research into the strengthening of digital Steganography in digital imaging[2]. Our approach is motivated by existing techniques to date lacking rigour and displaying security weaknesses. A core benefit of our algorithm is the low bit rate representation of the cover document allowing for higher payload embedding. The *Haar* DWT is chosen because of its superior performance and ability to adapt to the Human Visual System (HVS) [20].

3. Methodology

The fundamental concept of this paper is to embed the secret message in the 1st-level 2D Haar DWT (Discrete Wavelet Transform) with the Symmetric-padding mode. DWT is a well known transformation that gained popularity among the image processing community especially those who are dealing with image compression. The application of DWT in different areas is increasing (note that JPEG2000 uses DWT to compress images). 2D DWT provides a decomposition of the approximation, and the details 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 (see, [21]): the Wavelet transform understands the Human Vision System (HVS) more closely than does DCT; 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. DFT (Discrete Fourier 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 [22].

3.1 The payload

We refer to data that we wish to embed as payload. Since we need means of protecting scanned documents against forgery it is essential that the payload will carry as much information from the host (cover image) as

[1] Note that this kind of conversion would flag a tamper, even though it is a legitimate change, unlike in our method.
[2] Steganoflage, available from WWW: <http://www.infm.ulst.ac.uk/~abbasc/index.php>

possible. There is a trade-off between perceptual visualization and space demand for embedding (usually measured in bits). Without taking compression into account, the payload can be consistent with the cover signal; therefore, if the cover is stored as an 8-bit unsigned integer type then the payload will require 8 templates when applying the one bit substitution method. There is a high payload Steganography approach called A Block Complexity Data Embedding (ABCDE) [23], but it is prone to statistical attacks as it acts in the spatial domain; moreover it cannot resist any kind of manipulation to the Stego-image (image having embedding data).

An approximation of the cover document can be achieved by applying the gray threshold technique which results in a binary image demanding only 1 bit per pixel for storage. Some authors suggest using an edged image instead as it approximates the cover better. 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 our system. The process can be regarded as a distorted quantization of colours to the lowest bit rate. Meanwhile, reduction of the number of image colors is an important task for transmission, segmentation, and lossy compression of color visual information [24] which is why dithering is used for printing. Dithering is a process by which a digital image with a finite number of gray levels is made to appear as a continuous-tone image [25]. For instance, shown in Figure 1 (a) is a 24-bit image (i.e., RGB image). Shown in Figure 1 (b, c and d) are three 1 bit images (i.e., binary) of the grayscale version of Figure 1 (a). The first was created by thresholding, the second by an edge operator, and the third by dithering respectively. Despite, in all versions, each pixel takes on only one bit, it is apparent that the way dithering quantizes image pixels contributes a lot to the final quality of data approximation. We observed that thresholding performs better in text based documents, while in capturing graphics it is proven to be a poor performer compared to dithering. Therefore, since our aim is to produce a general workable prototype we have to take into consideration the presence of both text and graphics; subsequently we opt to use dithering. There exist different algorithms to generate an inverse halftone image, among which are: look-up table based methods [26], filtering-based methods and projection-based methods [18]. As an improved version of the filtering based methods, Neelamani et al. [27] propose an inverse halftoning in the Wavelets domain. All of the above make use of Floyd-Steinberg [28] and Jarvis [29] kernels to generate the error diffusion signal. We carried out a test to select which algorithm we can adopt. Based on the table shown below (Table 1) we can easily see that Jarvis implementation in the Wavelet domain provides better performance.

Table 1. Performance of different inverse halftoning algorithms.

Algorithm	*Performance on Lena image measured in PSNR (dB)*
Floyd: Classic raster scan	28.084
Floyd: Raster scan with edge enhancement	28.2513
Floyd: Serpent scan	27.6623
Jarvis: Serpent scan	26.6602
Jarvis: Raster scan	27.221
Jarvis: Wavelets	28.292

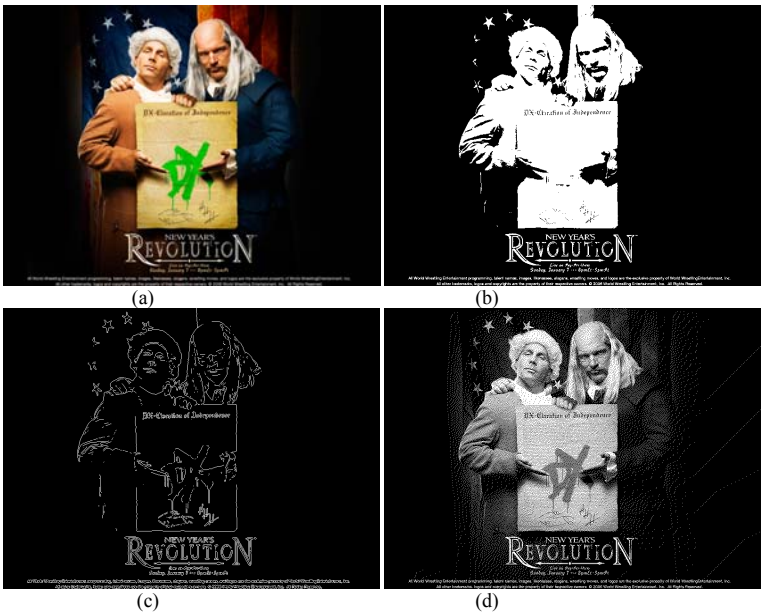

Figure 1. Image fidelity in different binary representations. Shown, top to bottom and left to right, are original image, graythreshold, edged and dithered versions respectively. An observer can determine that the dithered version retained most information from the original signal.

3.2 A new approach for payload encryption

In this work we propose adding another unit of security which encrypts the secret image before the embedding process [30]. Various hash algorithms are available such as MD family (Message Digest) and SHA-1 (Secure Hash Algorithm 1) which hash data strings, thus changing their state from being natural to a seemingly unnatural state. A hash function is more formally defined as the mapping of bit strings of an arbitrary finite length to strings of fixed length [31]. Here we attempt to extend SHA-1 (the terminology and functions used as building blocks to form SHA-1 are described in the US Secure Hash Algorithm 1, [32]) to encrypting digital 2D data. The introduction of Fast Fourier Transform (FFT) forms together with the output of SHA-1 a strong image encryption setting. Let the key bit stream be $\lambda_{k,l}$ where the subscripts *k* and *l* denote the width and height after resizing the key's bit stream respectively, i.e., 8, *N***N*, where *N*, *N* are the plain image's dimension. The FFT will operate on the DCT transform of $\lambda_{k,l}$ subject to Eq. 2.

$$f(u,v) = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} F(x,y)e^{-2\pi i(xu+yv)/N}$$
$$where, F(x,y) = DCT(\lambda_{k,l}), satisfying \quad Eq \quad 2 \tag{1}$$

Note that for the transformation at the FFT and DCT levels we do not utilise the whole coefficients. Rather, we impose the following rule, which generates at the end a binary random-like map. Given the output of Eq. 2 we can derive the binary map straightforwardly as:

$$Map(x,y) = \begin{cases} 1 & iff \quad f(u,v) > 0 \\ 0 & Otherwise \end{cases} \tag{2}$$

This map takes the positive coefficients of the imaginary part to form the ON pixels in the map. Since the coefficients are omitted the reconstruction of the password phrase is impossible, hence the name *Irreversible Fast Fourier Transform* (*IrFFT*). In other words, it is a one way function which accepts initially a user password. This map finally is XORed with the binary version of each colour component separately. Another phenomenon that we noticed and we would like to exploit is the sensitivity of the spread of the FFT coefficients to changes in the spatial domain. Therefore if we couple this with the sensitivity of the SHA-1 algorithm to changes of the initial condition, i.e., password phrase, we can meet easily the Shannon law requirements, i.e., confusion and diffusion. For instance a small change in the password string will, with overwhelming probability, result in a completely different hash and thus a different image by extension. So, the core idea here is to transform these changes into the spatial domain where we can apply 2D-DCT and 2D-FFT that introduce the aforementioned sensitivity to the two dimensional space. As such, images can be easily encoded securely with password protection.

3.3 The embedding stage

Manipulating coefficients in the wavelet domain tends to be less sensitive unlike other transformations such as DCT and FFT. There are two methods to convert decimal integer to a binary string: one is to use the conventional decimal to binary conversion and the other is termed The Binary Reflected Gray Code (BRGC)[3]. This binary mapping is the answer to the augmented embedding capacity introduced by ABCDE algorithm. There is a trade-off between robustness and distortion which is summarized in Figure 2.

[3] BRGC available from WWW: <http://mathworld.wolfram.com/GrayCode.html>. Accessed on 10-06-08, at 11:42.

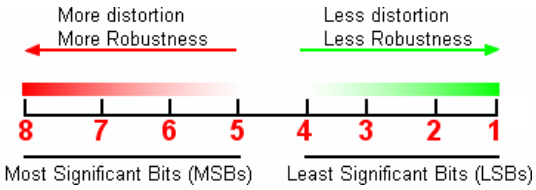

Figure 2. An 8-bit (1 byte) representation with the conventional integer to binary conversion. It is clear that choosing the right index for embedding is very crucial. This intricacy is less severe when using the RGC since it produces seemingly disordered decimal-to-binary representation.

Another trade-off that occurred during our algorithm's creation was due to the different levels wavelets can be decomposed. The lower we go the more robust we get but with less capacity for embedding. For example if the cover image is of size 512x512 (8-bit grayscale) we can embed 65536 bits in the 1st level, the second level will reduce that by ¼, i.e., 16384 bits and so on. Figure 3 depicts the recovery of the payload after compression attack with different quality factors.

In some cases the inverse transform in the wavelet domain truncates some values that fall larger or lower than the allowed limits in 8-bit type of images, the truncation occurs because of the introduction of 'non-natural bits' coming from the secret message while embedding. To cope with this rare problem we choose to transform the RGB image into the YC_bC_r colour space prior to feeding it into DWT where we embed in the luminance channel (Y). This step ensures that there will not be any data lost. Our proposed design is illustrated in Figure 4.

4. Evaluation

Here we demonstrate how efficient our algorithm is in preserving data even after the attack (forging). Figure 6 shows the encrypted dithered image carrying the most valuable information of the original document. Figure 5 (c) shows a perceptually identical copy of Figure 5 (a) but it has a duplicate of itself embedded into its pixels. Finally, Figure 5 (d) confirms that the embedded data can be retrieved intact. Our embedding scheme is robust against reasonable noise load that can be introduced for example during electronic transmission of the Stego-document. Moreover, using DWT gave us the advantage of the possibility of converting the Stego-document into lossless compressed formats, i.e., JPEG, without having to lose so much detail. Figures 5 and 7 show experiments where a Stego-image is forged and also we show the recovered embedded copy. Table 2 shows our proposed algorithm outperforming other related methods pertaining to visual distortion of the carrier image (usually image distortion is measured using specific distortion metrics such as the Peak Signal-to-Noise Ratio PSNR).

Spatial domain approaches are vulnerable to attacks for the following reasons (not exhaustive however):

1. Spatial domain techniques provide only a spatial description for an image at the pixel level, i.e., [0 255]

for 8-bit image files.

2. They can easily be fooled by any linear or non linear distortion of the image, hence they cannot tolerate compression or noise.

3. Since colour components of an RGB image are highly correlated, embedding in the spatial domain distorts the natural statistical properties of an image file more than that in the frequency domain which leaves spatial domain methods exposed to attacks.

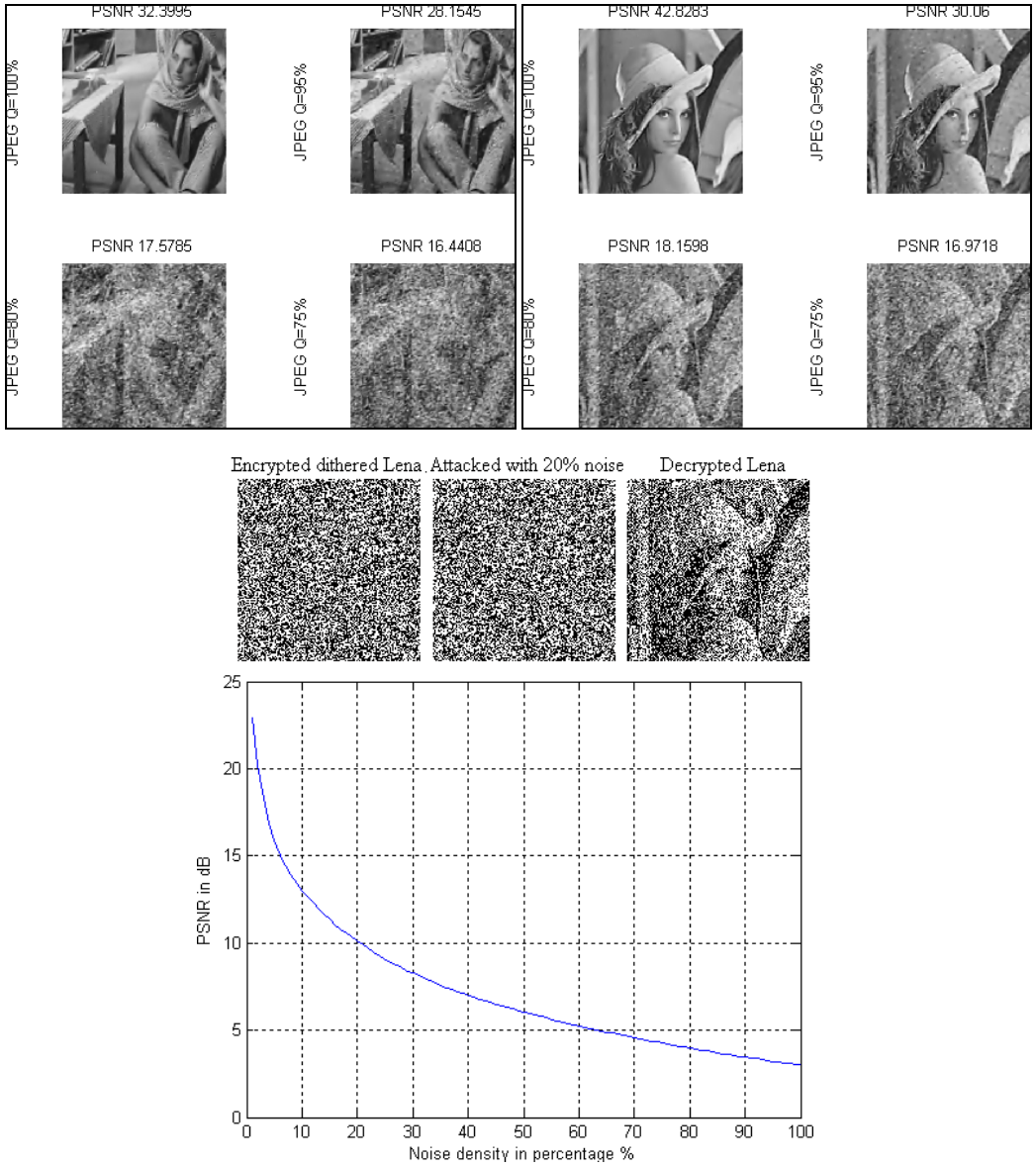

Figure 3. Performance of our self-embedding algorithm: (top-left) image recovery after JPEG attack on Barbara image, (top-right) image recovery after JPEG attack on Lena image and (bottom) decrypted image under different *Salt &Pepper* noise densities.

Table 2. Comparison of visual distortion of our algorithm and other methods in the literature.

	PSNR (dB)			
Image	Our method	[14]	[13]	[17]
Lena	41.6132	34.35	35.10	38.0164*

* We selected a balance between robustness and visual distortion in the tool's setting.

4.1 Limitations

Our scheme works on RGB images; however, there is a work around the grayscale images in the sense that we can construct a 3D matrix containing duplicates of the grayscale image. Future work will investigate whether there is a side effect with this procedure, but the initial experiments show it is a safe measure. Compression below the standard ratio of 75% will totally destroy the embedded data. The various non-oblivious watermarking techniques available, which are highly resilient to image processing and geometric attacks, aim to detect the presence of a watermark using a correlation with an original template. This can be seen for instance in the invariance in the work of [33, 34, 35]. Since our method is rather an oblivious technique certain tolerance factor in attacks must be adhered to.

5. Conclusions and Future Directions

We have outlined the leading techniques in document self-embedding and identified weaknesses among these methods. We proposed a superior approach to scanned document forgery detection and a correction method which uses an information hiding technique that is highly secure, efficient and robust to various image processing attacks. We believe it is a novel approach to allow documents to heal after any forgery attack. The payload, which is a dithered version of the cover, has a low bit rate while capturing the main image characteristics needed for reconstruction. This payload is further encrypted using a key to generate a balanced bit version which provided a balanced visual effect.

Unlike other methods, this work achieves high robustness, efficiency and capacity thanks to the compound DWT and The Binary Reflected Gray Code.

The experiments we carried out, of which a sample is reported in this paper, show promising results. The results show that the system can be relied on to combat scanned document forgery. The proposed technique was designed with the intent to serve as a practical application for our ongoing research on enhancing Steganography in digital images.

Future work will involve tackling and overcoming the problem of severe image compression. Also we need to analyse the effect of the encryption of the payload on the overall performance.

6. Acknowledgements

The work on this paper was supported by a VCRS (Vice Chancellor Research Studentship) from the University of Ulster in the UK. The authors acknowledge the constructive comments from the anonymous reviewers, with which this manuscript was further enhanced.

References

[1] The National Archives, <http://www.nationalarchives.gov.uk/news/stories/195.htm?homepage=news>, 2008.
[2] D.C. Lou, M.C. Hu, and J.L. Liu, Multiple layer data hiding scheme for medical images, Computer Standards & Interfaces, 31 (2) (2009) 329-335.
[3] D. Zou, J. Tian, J. Bloom, and J. Zhai, Data Hiding in Film Grain, in: Proceedings of International Workshop on Digital Watermarking, vol. 4283, 2006, pp. 197-211.
[4] E. Beşdok, Hiding information in multispectral spatial images, International Journal of Electronics and Communications. 59 (1) (2005) 15-24.
[5] Y. Li, C.T. Li, and C.H. Wei, Protection of Mammograms using Blind Steganography and Watermarking, in: Proceedings of International Symposium on Information Assurance and Security, 2007, pp. 496-499.
[6] A.T.S. Ho, and F. Shu, A print-and-scan resilient digital watermark for card authentication, in: Proceedings of International Conference on Information, Communications and Signal Processing, 2003, vol. 2, pp.1149-1152.
[7] X. Li, Image retrieval based on perceptive weighted color blocks, Pattern Recognition Letters, 24 (12) (2003a), 1935-1941.
[8] X. Li, Watermarking in secure image retrieval, Pattern Recognition Letters, 24 (14) (2003b) 2431-2434.
[9] Z. Zhao, N. Yu, and X. Li, A novel video watermarking scheme in compression domain based on fast motion estimation, in: Proceedings of IEEE International Conference on Communications, vol. 2, 2003, pp.1878-1882.
[10] A.C. Popescu, (2005). *Statistical Tools for Digital Image Forensics*. PhD thesis, Dartmouth College Hanover: USA.
[11] S. Shefali, S.M. Deshpande, and S.G. Tamhankar, Attack Detection through Image Adaptive Self Embedding Watermarking, International Journal of Signal Processing, 4 (4) (2008) 260-266.
[12] J. Lukáš, J. Fridrich, and M. Goljan, Detecting digital image forgeries using sensor pattern noise, in: Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, 2006, pp. 362-372.
[13] I. Kostopoulos, S.A.M. Gilani, and A.N. Skodras, Colour image authentication based on a self-embedding technique, in: Proceedings of International Conference on Digital Signal Processing, vol. 2, 2002, pp. 733-736.
[14] Y. Shao, L. Zhang, G. Wu, and X. Lin, Reconstruction of Missing Blocks In Image Transmission by Using Self-Embedding, in: Proceedings of International Symposium on Intelligent Multimedia, Video and Speech Processing, 2001, pp. 535-538.
[15] J. Fridrich, and M. Goljan, Protection of Digital Images Using Self Embedding, in: Proceedings of Symposium on Content Security and Data Hiding in Digital Media, 1999a.
[16] J. Fridrich, and M. Goljan, Images with Self-Correcting Capabilities, in: Proceedings of International Conference on Image Processing, vol. 3,1999b, pp. 792-796.
[17] C.Y. Lin, and S.F. Chang, SARI: Self-Authentication-and-Recovery Image Watermarking System, in: Proceedings of ACM International Conference on Multimedia, 2001, pp. 628-629.
[18] H. Luo, S.C. Chu, and Z.M. Lu, Self Embedding Watermarking Using Halftoning Technique, Circuits Systems and Signal Processing, 27 (2008) 155-170.
[19] J. Fridrich, D. Soukal, and J. Lukáš, Detection of Copy-Move Forgery in Digital Images, in: Proceedings of Digital Forensic Research Workshop, 2003.
[20] E.S. Silva, and S. Agaian, The Best Transform in the Replacement Coefficients and the Size of the Payload Relationship Sense, in: Proceedings of Society for Imaging Science & Technology, 2004, pp. 199-203.
[21] V.M. Potdar, H. Song and E. Chang, A Survey of Digital Image Watermarking Techniques, in: Proceedings of IEEE International Conference on Industrial Informatics, 2005, pp. 709-716.
[22] K.B. Raja, Vikas, K.R. Venugopal, and L.M. Patnaik, High Capacity Lossless Secure Image Steganography using Wavelets, in: Proceedings of International Conference on Advanced Computing and Communications, 2006, pp. 230-235.
[23] H. Hioki, A Data Embedding Method Using BPCS Principle With New Complexity Measures, in: Proceedings of Pacific Rim Workshop on Digital Steganography, 2002, pp. 30-47.
[24] X. Li, T. Yuan, N. Yu, and Y. Yuan, Adaptive color quantization based on perceptive edge protection, Pattern Recognition Letters, 24 (16) (2003) 3165-3176.
[25] H. Farid, Fundamentals of Image Processing, <http://www.cs.dartmouth.edu/farid/tutorials/fip.pdf>, Tutorial, pp. 61, accessed on 09-06-2008 at 10:00.
[26] M. Mese, P.P. and Vaidyanathan, Look-Up Table (LUT) Method for Inverse Halftoning, IEEE Transactions on Image Processing, 10 (10)(2001) 1566-1578.
[27] R. Neelamani, R. Nowak, and R. Baraniuk, Model-Based Inverse Halftoning with Wavelet-Vaguelette

Deconvolution, in: Proceedings of International Conference on Image Processing, vol. 3, 2000, pp. 973-976.
[28] R. W. Floyd, and L. Steinberg, An Adaptive Algorithm for Spatial Gray Scale, in: Proceedings of International Symposium Digest of Technical, 1975, pp. 36-37.
[29] J.F. Jarvis, C. N. Judice, and W. H. Ninke, A Survey of Techniques for the Display of Continuous-tone Pictures on Bilevel Displays, Computer Graphics and Image Processing, 5 (1) (176) 13-40.
[30] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, Securing Information Content using New Encryption Method and Steganography, in: Proceedings of IEEE International Conference on Digital Information Management, 2008, pp. 563-568.
[31] Y. Wang, X. Liao, D. Xiao, K.W. Wong, One-way hash function construction based on 2D coupled map lattices, Information Sciences, 178 (5) (2008) 1391-1406.
[32] US Secure Hash Algorithm 1, <http://www.faqs.org/rfcs/rfc3174>, 2001.
[33] C. Deng, X. Gao, D. Tao, and X. Li, Digital Watermarking in Image Affine Co-Variant Regions, in: International Conference on Machine Learning and Cybernetics, vol. 4, 2007, pp. 2125-2130.
[34] C. Deng, X. Gao, D. Tao, and X. Li, Geometrically invariant watermarking using affine covariant regions, in: Proceedings of IEEE International Conference on Image Processing, 2008a, pp. 413-416.
[35] C. Deng, X. Gao, D. Tao, and X. Li, Invariant Image Watermarking Based on Local Feature Regions, in: Proceedings of International Conference on Cyberworlds, 2008b, pp.6-10.

Appendix

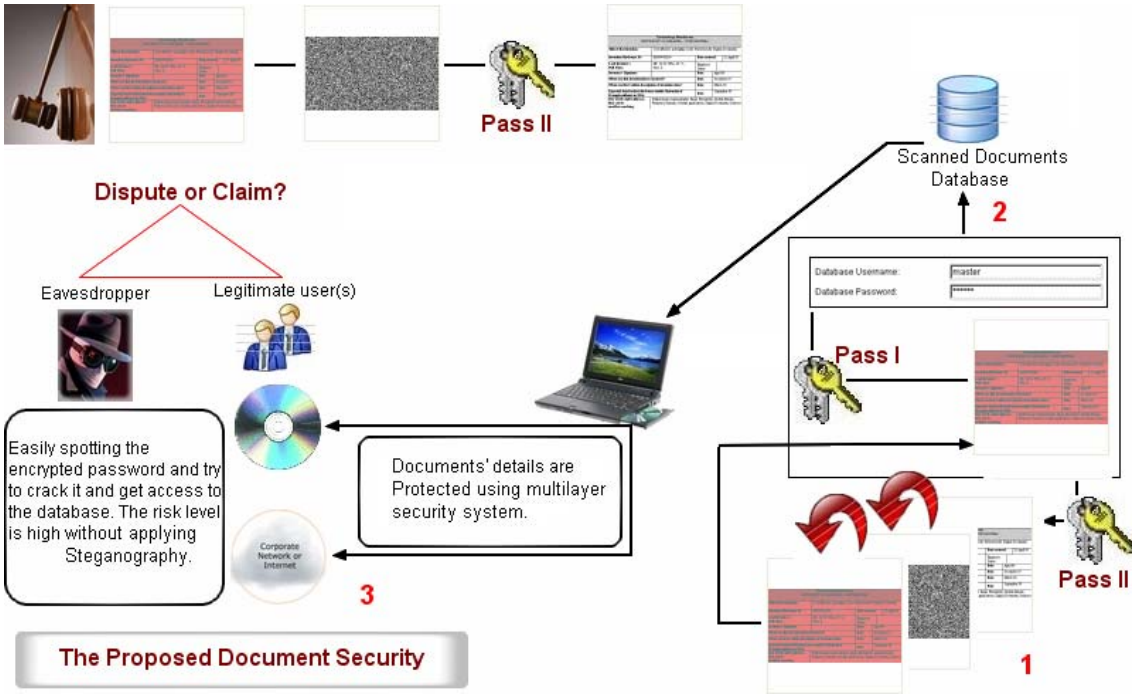

Figure 4. A general graphical scheme showing the advantage of adopting our algorithm for securing scanned document archives.

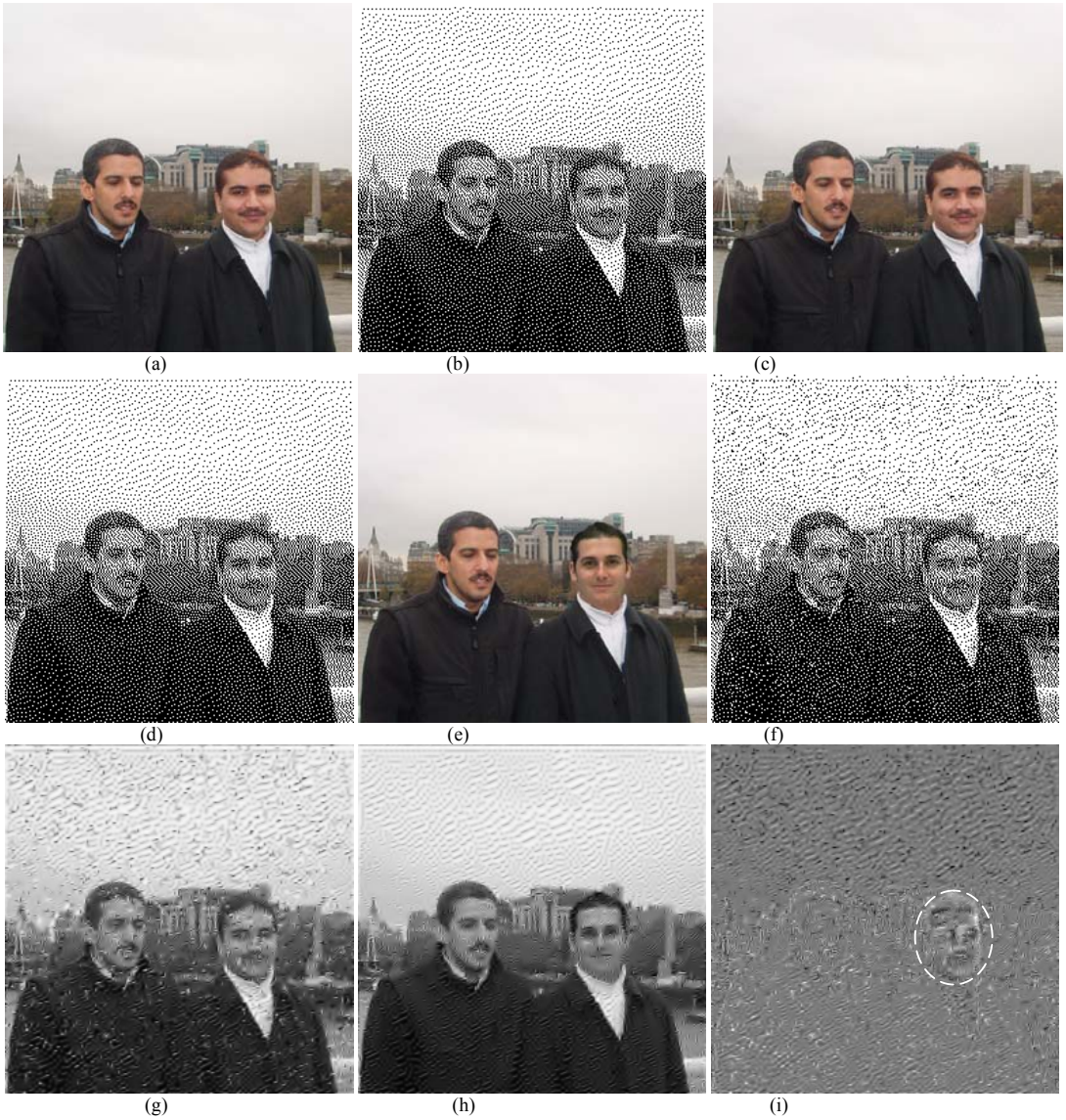

Figure 5. Example 1, performance of proposed algorithm on digital images: the original image (a), dithered version of original used as a payload (b), Stego image after embedding (c), extracted payload without attacks (d), attacked Stego, i.e., face tampered with (e), reconstructed hidden data from the attacked version (f), inverse halftoning of *(f)* shown in (g), inverse halftoning of *(e)* shown in (h), and error signal of *(g)* and *(h)* with contrast being enhanced for display shown in (i). Notice that only the tampered region, herein shown within a superimposed circle, demonstrates a coherent object in *(i)*.

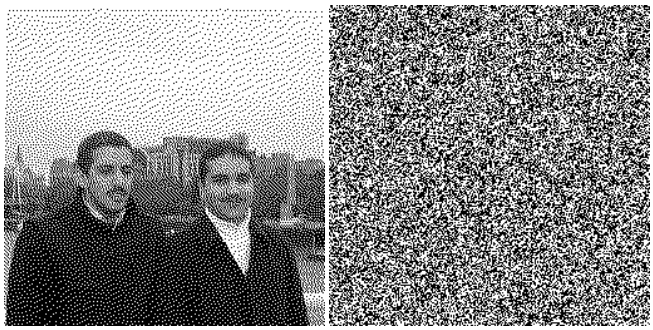

Figure 6. Our encryption algorithm: payload as appears in figure 5 (b) shown on the left hand side and its encrypted version on the right hand side. Note that both images are binary.

Figure 7. Example 2, performance of proposed algorithm on digital document: the original document (a), dithered version of original used as a payload (b), Stego image after embedding (c), attacked Stego, i.e., date received has changed and the 4th lead inventor's name has been removed (d), reconstructed hidden data from the attacked version (e), inverse halftoning of *(e)* shown in (f), inverse halftoning of *(d)* shown in (g), error signal of *(f)* and *(g)* shown in (h), and *(h)* after undergoing binary thresholding shown in (i).