Signal Processing 89 (2009) 2324–2332

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

A secure and improved self-embedding algorithm to combat digital document forgery

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, UK

ARTICLE INFO

Article history:
Received 31 October 2008
Received in revised form
30 January 2009
Accepted 2 February 2009
Available online 12 February 2009

Keywords:
Image processing
Steganography
Information hiding
Self-embedding
Encryption
Document forgery
Security

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 Deconvolution (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 organizations, 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

* Corresponding author.
E-mail addresses: cheddad@gmail.com, cheddad-a@email.ulster.ac.uk (A. Cheddad), j.condell@ulster.ac.uk (J. Condell), kj.curran@ulster.ac.uk (K. Curran), p.mckevitt@ulster.ac.uk (P. Mc Kevitt).

0165-1684/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2009.02.001

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 [2–6]. 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 organized 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 discrete cosine transform (DCT) and discrete wavelet transform (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 generalized.

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 8×8 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

[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〉.