Multilayer Secure Data Protection using Steganography

A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt

Email: cheddad-a@email.ulster.ac.uk
URL: http://www.infm.ulst.ac.uk/~abbasc/

University of ULSTER
Faculty of Computing and Engineering

INTELLIGENT SYSTEMS RESEARCH CENTRE

I. 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.

The concept behind the proposed systems stems from advanced research into the strengthening of digital steganography in digital imaging. Steganography is defined as the science of hiding or embedding "data" in a transmission medium. This poster unveils two novel systems one to combat digital document forgery and the other entails a massive secure storage system for confidential data.

II. The Problem

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.

- Forged Documents

In July 2005 it was discovered that a number of Second 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.

- Loss of Confidential Data

During 2008 there have been large scale losses of personal sensitive data in the UK, e.g. the loss of 25 million child benefit records after HMRC sent two unregistered/unencrypted discs to National Audit Office and the theft of a laptop from a Navy officer which held the personal details of 600,000 people.

III. The Proposed Solutions

+ Combating Forgery using Self-Embedding

We propose an approach to scanned document forgery detection and correction which uses an information hiding technique that is secure, efficient and robust to various image attacks, see Figs 1-2. It is a novel method 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 as shown in Fig 3.

+ Securing Confidential Data

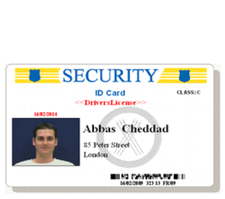
Using the aforementioned method we can embed unrelated data in the cover, i.e., confidential data, for the sake to hide its very existence. This goes under the note that if the feature is visible the point of attack is evident. To cope with the limited space, frames in a video can be targeted for embedding as sketched in Fig 4.

V. Conclusions

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. The poster highlights a cost effective yet highly secure systems in which individuals' details or other sensitive data are embedded into images/frames using a multi layer security channel reliant on steganography.

Future Work

A grant has been secured to produce a workable prototype for secure ID cards. The aim is to increase the security level for data authentication with the least possible cost. This means that the produced smart ID card will be able to attract various organisations, companies and societies which cannot afford investing into high cost systems such as RFID based tecknologies.



IV. Results

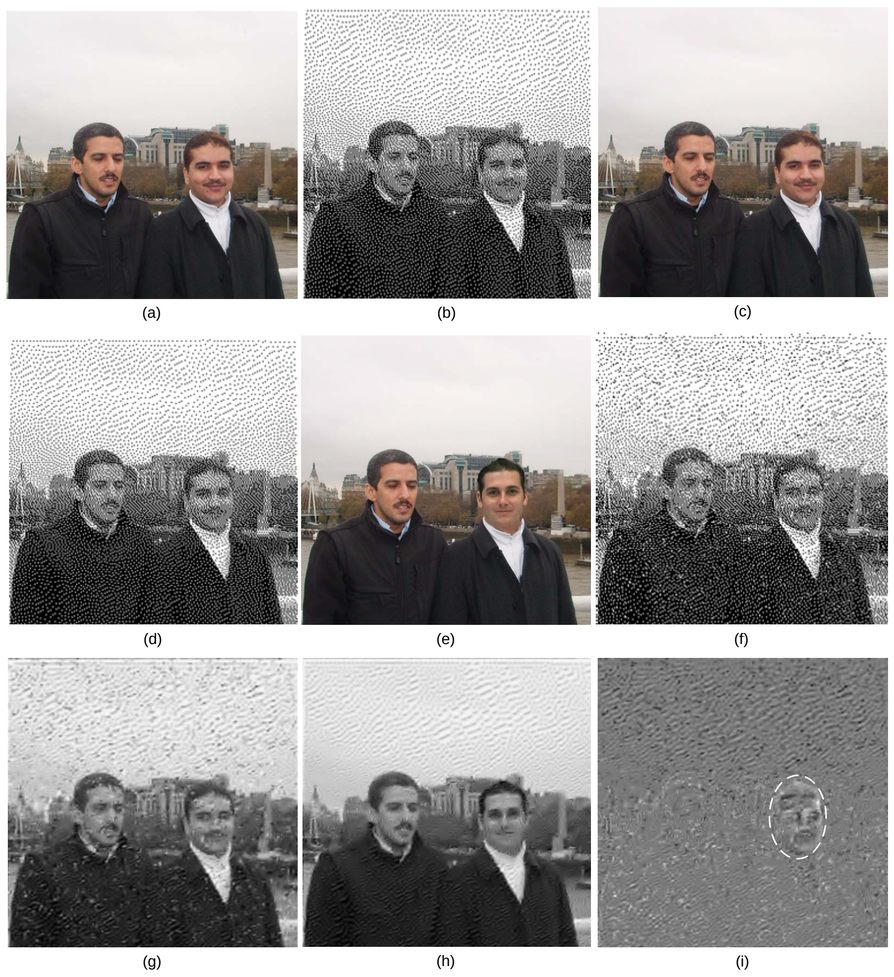


Fig 1. Performance of proposed algorithm on digital images: the original image (a), dithered version of original used as a payload (b), Stego image after embedding (c), extracted payload without attacks (d), attacked Stego, i.e., face tampered with (e), reconstructed hidden data from the attacked version (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)*.

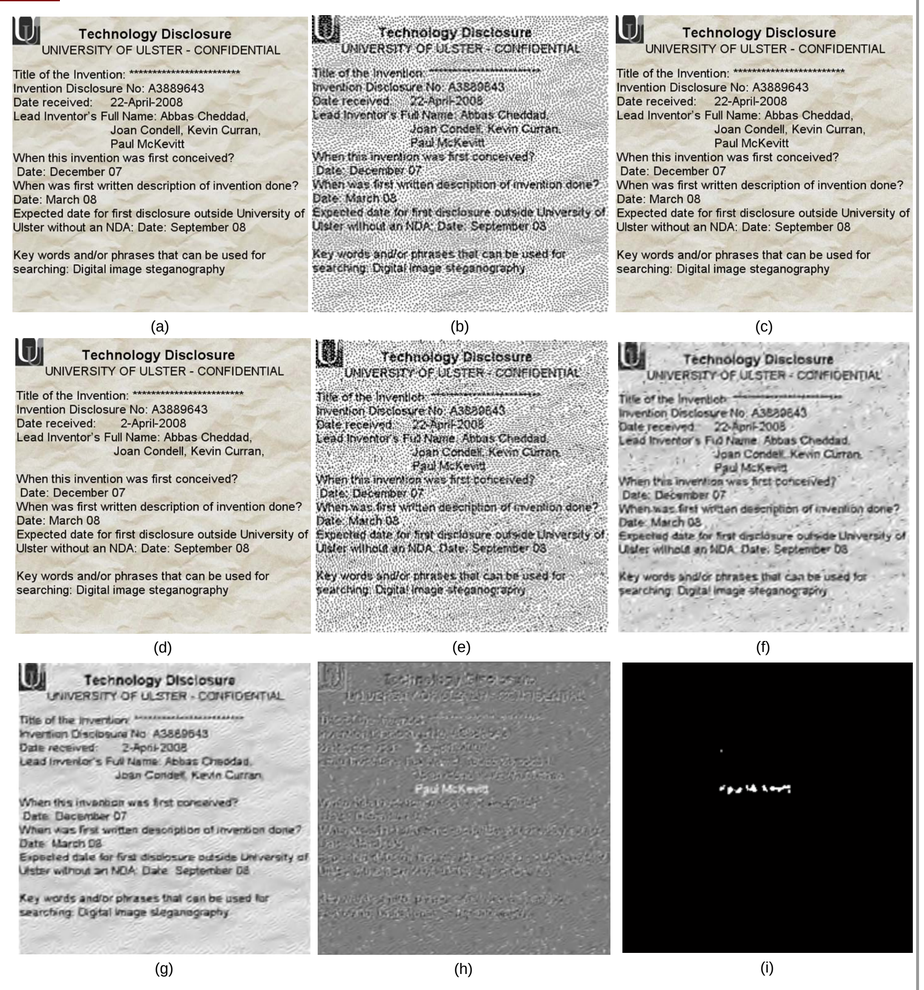


Fig 2. Performance of proposed algorithm on digital document: the original document (a), dithered version of original used as a payload (b), Stego image after embedding (c), attacked Stego, i.e., date received has changed and the 4th lead inventor's name has been removed (d), reconstructed hidden data 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).

Fig 3. (top) Block diagram of the steps used in the proposed algorithm for image encryption and (bottom) histogram analysis: (left) plain image and its histogram, (right) encrypted image and its histogram.

Fig 4. A generic graphical scheme showing the advantage of adopting the algorithm for securing confidential data in Video files.

VI. Recent Publications & Awards

- **United Kingdom Patent** Application No. 0819976.2 "An Encryption Method" University of Ulster.
- **United Kingdom Patent** Application No. 0819982.0 "Method for Skin Tone Detection" University of Ulster.
- **Research Grant:** "Identity Cards Employing Steganography" £7,430. The Faculty of Computing and Engineering.
- **Best Literature Review prize** (2007).
- **Best paper award** at the 8th International Conference on Information Technology and Telecommunication (2008).
- **Book Chapter:** "Advances in Digital Image Steganography: State of the Art, Counterattacks and Security Applications". Accepted, Handbook of Research on Threat Management and Information Security: Models for Countering Attacks, Breaches and Intrusions. Publishers: IGI Global Hershey, USA.
- 2009. "A New Skin Tone Detection Algorithm Illustrated Through the Application of Steganography". Accepted, **Signal Processing Journal**, Elsevier.
- 2009. " A Secure and Improved Self-Embedding Algorithm To Combat Digital Document Forgery". **Signal Processing Journal**, Elsevier. doi:10.1016/j.sigpro.2009.02.001.
- 2008. "Skin Tone Based Steganography in Video Files Exploiting the YCbCr Colour Space". Proc of **IEEE International Conference** on Multimedia and Expo, Hannover, Germany. pp. 905-909. June 23-26, 2008.
- 2008. "Securing Information Content using New Encryption Method and Steganography". Proc of **IEEE International Conference** on Digital Information Management, University of East London. UK. pp: 563-568.

VII. Acknowledgments

This work is fully supported by a VCRS (Vice Chancellor Research Studentship) from the University of Ulster in the UK and the first author gratefully acknowledges it.

The Steganoflage Project:

School of Computing and Intelligent Systems
Faculty of Computing and Engineering
University of Ulster, Magee College, Northland Road, Londonderry. BT48 7JL.

Office: 02871375156 (MS 125)
Fax: 02871375470 (General Office)
URL: http://www.infm.ulst.ac.uk/~abbasc/