OpenAIR @RGU ROBERT GORDON UNIVERSITY ABERDEEN

This publication is made freely available under GREEN open access.

AUTHOR(S): AMBADIYIL, S., JAYAN, K.G., PRABHU, R., PILLAI, V.P.M

TITLE: Microstructure encryption and decryption techniques in optical variable and invariable devices in printed documents for security and forensic applications.

YEAR: 2015

Publisher citation: AMBADIYIL, S., JAYAN, K.G., PRABHU, R. and PILLAI, V.P.M. 2015. Microstructure encryption and decryption techniques in optical variable and invariable devices in printed documents for security and forensic applications. In Baldini, F., Homala, J. and Lieberman, R.A. (eds.) Proceedings of the SPIE optical sensors 2015 conference, 9506, 13-16 April 2016, Prague, Czech Republic. Bellingham, WA: SPIE [online]. Available from: https://doi.org/10.1117/12.2179635

OpenAIR citation: AMBADIYIL, S., JAYAN, K.G., PRABHU, R. and PILLAI, V.P.M. 2015. Microstructure encryption and decryption techniques in optical variable and invariable devices in printed documents for security and forensic applications. In Baldini, F., Homala, J. and Lieberman, R.A. (eds.) Proceedings of the SPIE optical sensors 2015 conference, 9506, 13-16 April 2016, Prague, Czech Republic. Bellingham, WA: SPIE. Held on OpenAIR [online]. Available from: https://openair.rgu.ac.uk

Publisher copyright statement:

This is the AUTHOR ACCEPTED version of proceedings originally published by SPIE and presented at Proceedings of the SPIE optical sensors 2015 conference, 9506, 13-16 April 2016, Prague, Czech Republic. (ISBN _____; eISBN _____; ISSN 0277-786X).

© 2015 Society of Photo-Optical Instrumentation Engineers. One print or electronic copy may be made for personal use only. Systematic reproduction and distribution, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper are prohibited.

OpenAIR takedown statement:

Section 6 of the "Repository policy for OpenAIR @ RGU" (available from http://www.rgu.ac.uk/staff-and-current-students/library/library-policies/repository-policies) provides guidance on the criteria under which RGU will consider withdrawing material from OpenAIR. If you believe that this item is subject to any of these criteria, or for any other reason should not be held on OpenAIR, then please contact openair-help@rgu.ac.uk with the details of the item and the nature of your complaint.

This publication is distributed under a CC BY-NC-ND 4.0 license.

https://creativecommons.org/licenses/by-nc-nd/4.0

OpenAIR at RGU Digitally signed by OpenAIR at RGU DN: cn=OpenAIR at RGU, o=Robert Gordon University, ou=Library, email=publications@rgu.ac.uk, c=GB Date: 2016.12.19 16:49:15 Z

Microstructure encryption and decryption techniques in optical variable and invariable devices in printed documents for security and forensic applications

Sajan Ambadiyil[a], K.G. Jayan[a], Radhakrishna Prabhu[b] and V.P. Mahadevan Pillai*[c]
[a]Center for Development of Imaging Technology, Thiruvanthapuram-695027, Kerala, India; [b]School of Engineering, Robert Gordon University, Aberdeen, UK; [c]Department of Optoelectronics, University of Kerala, Thiruvanthapuram-695581, Kerala, India

ABSTRACT

Today, document counterfeiting is a global menace because of the advanced technologies available at ever decreasing prices. Instead of eschew the paper documents; applying efficient cost effective security methodologies are the feasible solutions. This paper reports a novel cost effective and simple optical technique using micro text encrypted optical variable device (OVD) threads, ultra-violet (UV) based optical invariable device (OID) patterns and artistic fonts for secure preparation of the documents and its forensic application. Applying any one of the above technique or together can effectively enhance the level of security of the most valuable document. The genuineness of the documents can be verified using simple decryption techniques.

Keywords: Anti-counterfeiting, Security printing, Forensic applications

1. INTRODUCTION

All the existing governance procedures are based on paper documents. People do not want, or cannot afford, to change their existing business procedures. Paper document is tangible and gives immediate feel of trust. These documents are mobile, can be presented to anybody, at any time, and at any place. With the revolutionary advancement in the field of digital technologies, it has become easier to fabricate forgeries of any document very easily. The history of document security is one of a continuous struggle to stay one step ahead of the fraud[1]. An array of high technology features comprising traditional protection methods such as special inks, security threads and new generated overt and covert characteristics are continuously being developed to defend documents against forgery and counterfeiting[2]. But most of these techniques require either special equipment to embed the security features or too expensive for an average consumer. Hence the search for novel cost effective techniques which can provide enhanced security and easy verification is of great importance in a scientific/commercial point of view[3]. In this investigation the design, development and implementation of a simple cost effective secure methodology is discussed. This involve the features like i) the development of micro text encrypted OVD threads instead of security window thread (ii) the development of microstructure embedded UV based OID patterns as an alternative to the security fibres (iii) encryption of micro letters in the core heading made up of artistic fonts.

1.1 Window thread and Security fibers – an overview

Window thread as shown in Fig.1 (a) and Fig.1 (b) is one of the methods for paper security which is partially embedded within the paper mass and partially appears at the paper surface as a metallic feature[4]. The major problem of this technology is its cost prohibitive nature and the invariable data content encrypted in the thread which is visible to everybody using a minor magnifier. In the commercial point of view, it is not viable to produce the same for fewer requirements.

Another popular method for paper security is embedding security fibers in various colours in to the paper mass. These fibres can be made either visible or invisible. The colour makes the visible fibres stand out clearly against the paper and can easily be seen with the naked eye. Invisible security fibers as in Fig.1(c) and Fig 1(d) with fluorescent properties are visible only under ultraviolet radiation. Security fibres are embedded in the paper in random places at varying depths. This technology is also cost prohibitive and no data content are encrypted in the fiber. Since the fibres are embedded in the paper in random manner it is not possible to verify the orientation of the same. Here also in the commercial point of

*vpmpillai9@gmail.com; phone 0091 471 2308167

view it is not viable to produce the same for fewer requirements. In a similar approach, fluorescent micro glass beads have been proposed to enhance the security of optical documents[5].

Fig. 1.(a) Window thread embedded within the paper mass (b) Patterns in window thread (Magnified view) (c) Security fibers embedded within the paper mass under UV light (d) Magnified view of a security fiber under UV light.

2. PRESENT APPROACH

The goal of our work is to provide security and verify the documents using micro-text/structure/letters encrypted optical variable devices (OVDs), UV based optical invariable devices (UV-OIDs) and artistic font on cost effective basis. This also enables the customisation of the OVDs/UV-OIDs/Font encryptions by incorporating the client's desired microstructures like letters/patterns/text etc.

2.1 Micro text encryption and decryption in OVD Threads

Optical variable device (OVD) is an iridescent image that exhibits various optical effects such as movement or colour changes[6,7]. The main charm of OVDs lies in the fact that the most modern digital imaging and image processing tools fail to duplicate it. OVDs can neither be photocopied/scanned, nor be accurately replicated/reproduced. OVDs are based on diffractive optical structures which give the appearance of having different patterns, colours, and designs depending on the amount of light striking on them and the viewing angle. The development of OVDs can be divided in to the following three steps; Master Fabrication, Replication and Mass production. The most prevalent methods of master fabrication are either by the use of a high-resolution dot matrix OVD origination, or by interference of two or more laser beams. The recording of the microstructure OVDs requires a photosensitive material, typically photo resist material coated on glass substrate. This will record the microstructure as a surface relief after exposure.

In the present case, the master OVD has been developed by encrypting the micro texts 'CDIT' and 'GOK' in Arial type font(height <100 µ), in consecutive layers using Kinemax dot matrix OVD origination machine having 6000dpi resolution. Since the master developed in the glass substrate is too fragile to be used in mass production, it is necessary to make a metallic replica of the same. Electroforming is the method used for the fabrication of the metallic replica. In this process a thin metal layer is pasted on the photoresist glass master to make it electrically conductive. The glass master is placed in a Ni-sulphamate bath as a cathode together with a Ni anode. By passing a current through the bath, Ni is electrolytically deposited on the cathode in a layer with a thickness of a few 100 microns. After the process this Ni-replica is removed from the glass master. The Ni-replica of the said OVD is then mass fabricated using embossing technique. A locally designed embossing machine with a metal roller is used. The nickel replica is fixed round the roller of the machine. The roller can be heated to a desired temperature. The information in the nickel replica is transferred in to an aluminium metalized Polyethylene terephthalate (PET) film of thickness 23µm by hot pressing (temperature - 100°C & pressure-3.5kg/cm^2) method. This metalized OVD patterns are finally transferred to the document using a hot stamping machine (desk top type). The dye required for the hot stamping machine is designed in a dash type pattern as in the Fig. 2a and fig 2b with 5 mm height and 2mm width. The gap between the patterns is 5mm. Encryptions in the OVD,

shape and dimension of the dye can be varied in the desired manner. This flexibility of the said technology will add up the security and uniqueness of the documents. In order to verify the security features we have to decrypt the information encrypted in the OVD pattern. For this the image was first captured microscopically and then digitally zoomed. The decrypted image after image processing using MATLAB is shown in Fig. 2c.

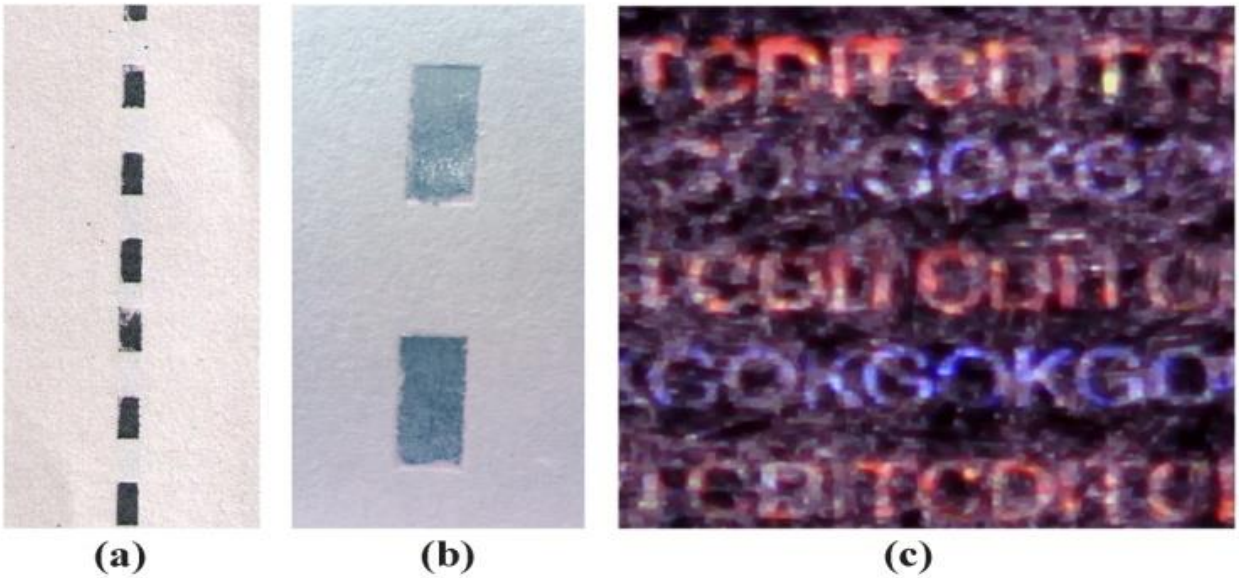

Fig. 2 (a) Micro text encrypted OVD Thread embedded on the paper document (b) Magnified view of the OVD thread (c) decrypted information embedded within the OVD Thread (CDIT-GOK)

2.2 Microstructure encryption and decryption in UV-OID patterns

Ultra violet (UV) based optically invariable devices (OIDs) are more or less diffusely reflecting devices, under ultraviolet illumination and are independent of the angle of illumination and observation[6]. The idea of embedding an authenticating fluorescent pattern on document security is not new. But incorporating microstructure/text to the authenticated fluorescent pattern in a specific manner in the whole area as an alternative to the security fibre is a new idea.The detail of the encryption will be visible to the naked eye only if it is exposes to ultra violet black light along with a microscope and the processing software. In this method it is possible to embed any text in any shape and dimension and in any orientation along with any available colours to the paper documents. Here a text "CDIT" is encrypted as a sin wave pattern of axis length 10.25 mm (font type Arial) with a font size of 500 µm. This is embedded on the document using the conventional offset printing technology with at most care taken in the cleaning procedure. The Fig.3 shows the embedded UV-OID pattern in the paper document under 366 nm UV light and its processed microscopic image in gray scale and inverted mode

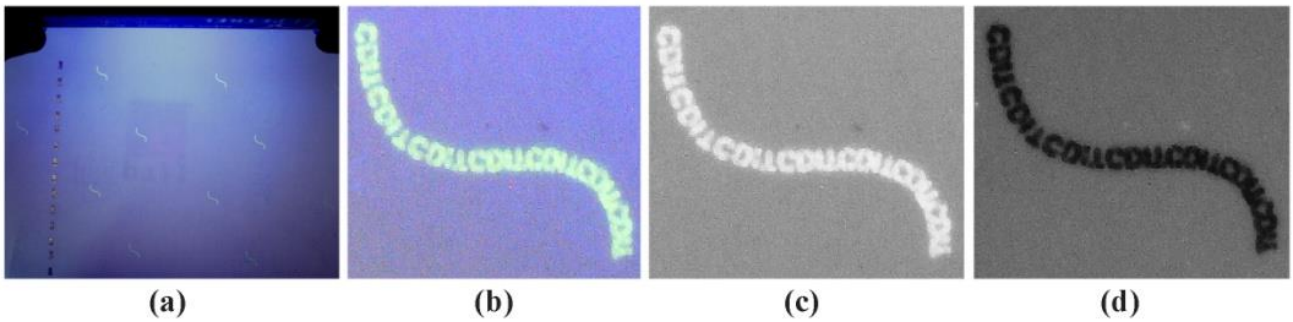

Fig. 3 (a) Microstructure encrypted UV-OID Pattern (b) Microscopic view of UV-OID Pattern (c) Gray scale image of UV-OID Pattern after image processing (d) Inverted image after image processing

Generally security fibers are embedded in the paper in random places at varying depths as shown in Fig. 1c. These security fibres do not contain any particular orientation. In the present technique a specific orientation is introduced in the distribution of UV-OID patterns in to the paper. This will add up the security and uniqueness of the documents. Fig. 4 shows the method of measurement of orientation of the image along with its scaling. This is realised by connecting the horizontal/vertical/slanted coordinates of the UV-OID patterns using MATLAB software. From this, it is possible to identify the pattern structure, measurement of distance in between of the UV-OID patterns and number of the pattern structure with in the unit area. The horizontal distance between the patterns assigned here is 76mm. The shape, orientation, in-between distance and no. of pattern in the UV-OIDs can be varied as per the desired manner.

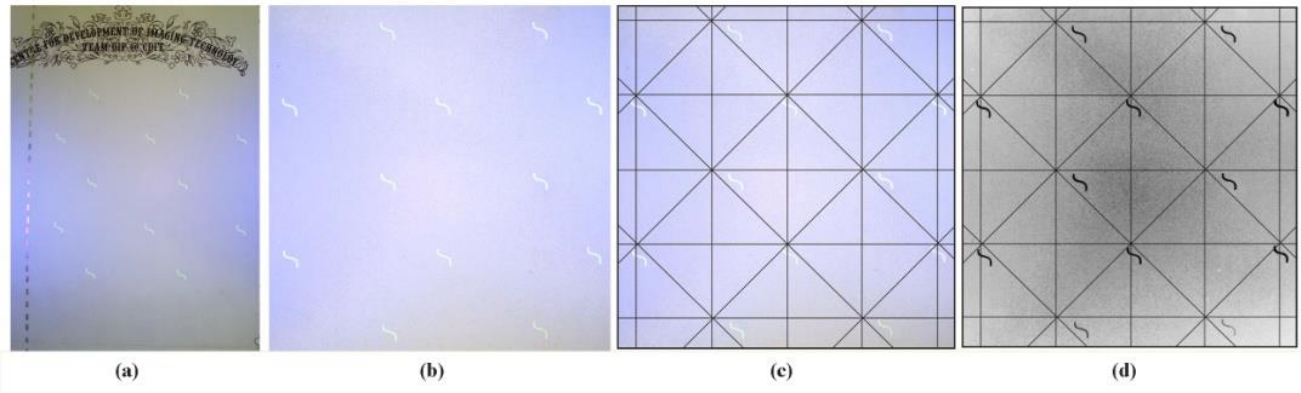

Fig.4 (a) Orientation of UV-OID Pattern embedded in the paper document (b) Orientation –after processing (c) Scaling of the orientation (d) Scaling in Black and white mode (processed)

2.3 Micro letters encryption and decryption in the Artistic fond

Embedding micro letter into the core heading font of the documents is another method for enhancing the security of the document in a cost effective manner. Legible artistic font is the best option for the encryption of the micro letters in the same. Stylistic effect of the artistic font makes the encryption unnoticed and the legible nature makes quick reading of the core heading. While selecting the artistic fonts care has to be taken to avoid confusions and close eye to the letters that is being displayed. The balance between legibility and style is one of the important factors to be considered when choosing a font for the micro letter encryption.

The font selected for the artistic core heading “CENTER FOR DEVELOPMENT OF IMAGING TECHNOLOGY” is URWWOOD (font size 7 mm). Arial font of height 400µm is selected for the microscopic encryption (micro text - CDIT). The letters of the artistic core heading contains micro letters C, D, I, T encrypted in a sequential manner using Corel draw software. The colour of the Artistic font selected is Black (C=0, Y=0, M=0 and K=100). Also to hide the encryption from the normal view, a complex pattern with the colour combination of (C=0, Y=0, M=0 and K=60) is made around the artistic font.

To decrypt the information from the Artistic font, the image obtained from the microscopic camera is first zoomed using digital method using MATLAB. Edge detection[8] is an important pre-processing step and successful results of image analysis extremely depend on edge detection. After the edge detection and noise removal of the above image edge enhancement operation was made to make edges in an image slightly sharper and crisper. To improve the readability further thresholding followed by sharpening using high pass filter is performed to obtain the clear image and to identify the characters encrypted in the same.

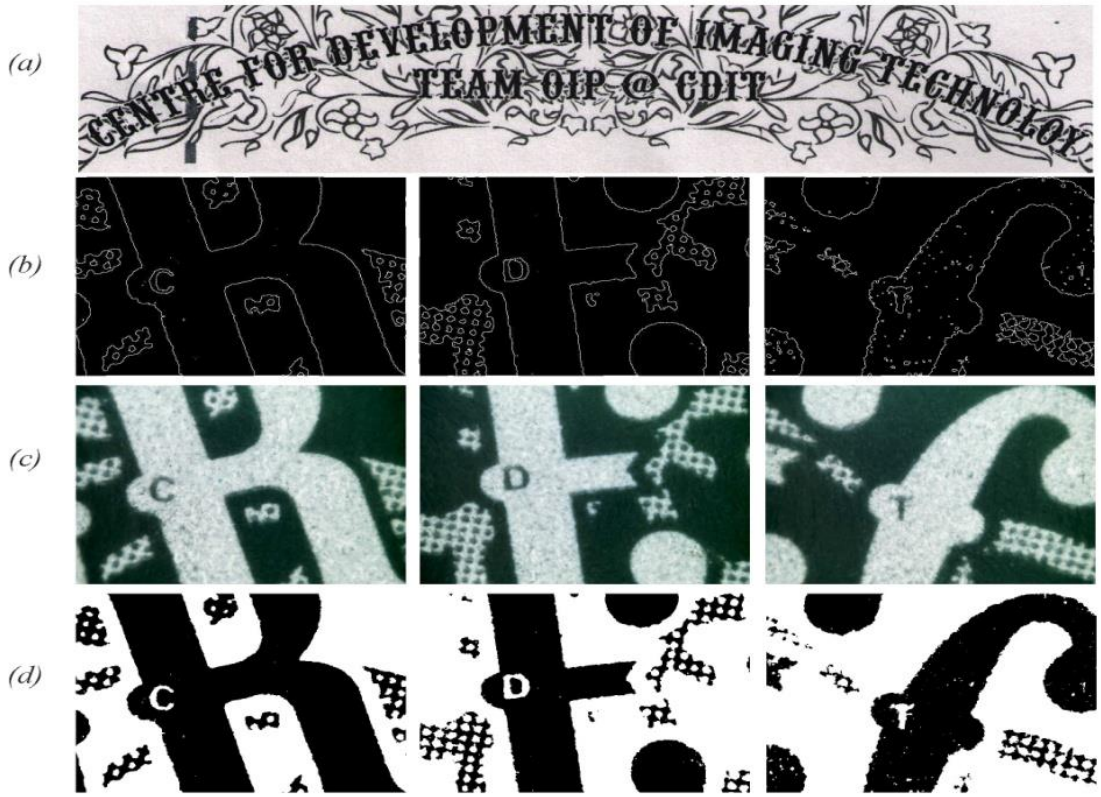

Fig. 5 (a) Micro letter embedded Artistic font (b) Decryption technique of the microscopically captured image using Edge detection(c) Inverse version (processed image). (d) Corrected BW image

The present investigation points towards the cost effective, efficient and simple optical technique to enhance the security level of the valuable documents from counterfeiting and forgery. Applying any one of the above technique can effectively enhance the level of security. By introducing the combination of these techniques can enhance the degree of security of the most valuable document without incurring high cost. The genuineness of the documents can be verified by using simple decryption techniques explained above. We believe the present approach is a technological advancement towards the production of secured documents, stamp papers and currencies to avoid counterfeiting and forgery.

3. CONCLUSION

The ultimate goal of the security printer is to produce items in a way that deters counterfeiters, forgers, fraudsters, and terrorists from unauthorized copying or alterations of authentic items in a cost effective manner. This paper reports the microstructure encryption and decryption techniques in optical variable and invariable devices in printed documents for security and forensic applications. In this work we have developed micro text embedded OVD threads as an alternative to the security window thread, microstructure embedded UV based OID patterns as an alternative to the security fibres and micro letter embedded core heading in Artistic fonts for safe and secure preparation of the documents in a cost effective manner. All the encryption was also decrypted using image capturing tools and processing software for the forensic level operation.

REFERENCES

[1] K.J. Schell, "Security printing, a part of optical security systems or vice versa?" Symposium Optical Security Systems, Proc. SPIE 0900, (1987); doi: 10.1117/12.944688

[2] R. L. Van Renesse, "Paper based document security - a review," IEE European Conference on Security and Detection, no. 437, pp. 75-80 (1997).

[3] Aravind K. Mikkilineni, Gazi N. Ali, Pei-Ju Chiang, George T. C. Chiu, Jan P. Allebach and Edward J. Delp, "Signature-embedding in printed documents for security and forensic applications", Proc. SPIE 5306, 455 (2004)

[4] R. L. Renesse, Optical Document Security – a review, ECOS 97, European Conference on Security and Detection, 437, 75-80 (1997).

[5] S. Officer, R.G. Prabhu, P. Pollard, C. Hunter and G. Ross, "Novel online optical security system based on rare earth doped micro glass beads" Proceedings of Optical Security and Counterfeit Deterrence Techniques V, edited by R. L. van Renesse, Proceedings of SPIE-IS&T Electronic Imaging, SPIE 5310, 387-395 (2004).

[6] E. J. Delp, "Is your document safe: An overview of document and print security," Proceedings of the IS&T International Conference on Non-Impact Printing, International Conference on Digital Printing Technologies (Hardcopy), San Diego, California, 18, (2002), ISBN / ISSN: 0-89208-240-2

[7] Rudolf. L. Van Renesse "Ordering the Order - A survey of optical document security features", Proc. SPIE 2406, 268-275 (1995); doi: 10.1117/12.206227

[8] T. Geback, P. Koumoutsakos, "Edge detection in microscopy images using curvelets", BMC Bioinformatics 10, 75 (2009)