THOMSON REUTERS
ENDNOTE

[Kumar, 4(2): February 2017]
DOI- 10.5281/zenodo.1405756

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

STUDY THE LIST OF SECURITY FEATURES FOR PASSPORT AND VISA

Pankaj Kumar*[1] & Manjeet Kumari[2]

*[1]Assistant Professor, Department of Printing Technology, GJUS&T, Hisar

[2] Scholar, M. Tech., Department of Printing Technology, GJUS&T, Hisar

ABSTRACT

Passport and visa are used as a travelled document and are the most important documents used by the travellers all over the world for the security enhancements and for the identification. It is the responsibility of the particular country to make the document secured enough so that it can't be easily counterfeit. Such type of the documents requires higher degree of security, so that they can't be duplicated. Document security can be measured either by covert, overt, semi-covert, forensic, and digital in nature.It is the world- wide- issue to protect these documents from duplicity and forgery.

Objective of this research paper is to find out various security features used for passport and visabeing used across globe. Security printing is not a special printing process but it is the combination of various processes with security/special features, to protect passport and visa from counterfeiting and forgery.

Keywords*: Security Features, Covert, Overt, Semi-covert, Forensic, Passport, Visa, FIT(Fine Intaglio Technology), INFACIO.*

I. INTRODUCTION

Security features are intended to adders an existing or potential risk of counterfeiting or fraud in a product or document. All effective security features, broadly speaking, deepen the divide between genuine product and their counterfeits by making a genuine product distinguishable in some manner that is difficult to replicate using commercially available manufacturing processes. It is always recommended that a layered approach be used in curtailing the various forms of attack on an item of value. This approach entails the use of various technologies that work in conjunction with each other to deter the anticipate threat. Various trade-offs are necessary between security and usability. It is possible to secure a document or product almost absolutely by applying layer after layer of complex security features, but to fully authenticate would require more equipment's and resources than it really practicable or necessary.

Security printing is the field of the printing industry that deals with the printing of items such as bank notes, cheques, passport, visa etc. The main goal of security printing is to prevent forgery, tampering, or counterfeiting. More recently many of the techniques used to protect these high –value documents have become more available to commercial printers whether they are using the more traditional offset and flexographic presses or the newer digital platforms. A number of technical methods are used in the security printing industry to protect the documents from forgery and delicacy. The most effective security printing techniques for passport and visa requires a combination of printing processes. For instance, a document could include a micro-printing as well as security binding. It is logical to infer that the more features that are used on a passport or visa increase the security of the document, thus making it harder to easily counterfeit. However, a deeper look into the counterfeit problem will illustrate that the difference between a successful counterfeiter and an unsuccessful counterfeiter is perception. If a counterfeiter can produce a document that is perceived to be real by the recipient, the counterfeiter has succeeded. The problem is that no matter how stringent or effective a security printing technique is, it will unfortunately be only one strategy to combat counterfeiters. The lawfulness ofthe passport and visa, and also narrowing the perception of what is considered authentic. Nonetheless making improvements in security printing is a crucial element in the battle against counterfeiters.

The purpose of this study is to evaluate different methods of security printing in developed countries and to determine what methods are the most effective in eliminating counterfeit production. The most effective security printing technique is the one that is the hardest to counterfeit while simultaneously acting as an effective means of

ISSN 2348 – 8034
Impact Factor- 4.022

graphic communication through passport. There will be an emphasis on the printing of passport and visa, domestic and foreign. Due to its extreme versatility and value, passport requires complex security printing practices. Thus, there is a great amount that can be evaluated by understanding the security printing practices of producing passport and visa.

II. SECURITY FEATURES FOR PASSPORT & VISA PROTECTION

Special Paper

In most of the countries special paper is used for passport and visa manufacturing. Most of the passport and visa are made-up of heavy paper, which contains most of cotton fibres due to their strength and durability, in most of cases linen or speciality coloured or forensic fibres are added to give the paper added security features and protect from counterfeiting.

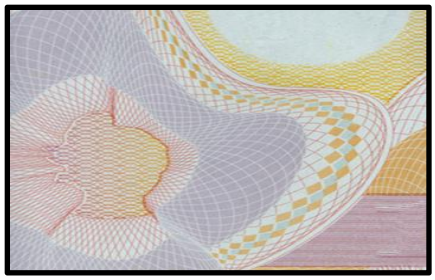
Anti–Scan /Anti-Copy Pattern

Anti-scan / anti-copy patterns are printed security features integrated in the background/ security printing to protect against simulation through coping. The printed images and patterns contain hidden information (usually constructed of fine lines) that is invisible to the naked eye under normal inspection conditions but becomes visible or legible or causes mistakes to appear after coping or reproduction with a scanner

Anti-Scan/Anti-Copy Pattern

Background / Security Printing

Background / Security printing serves as a protection against counter fitting and manipulation of data. Background / Security printing consists of print designs and security elements like e.g. Guilloches / fine line patterns, micro print, rainbow colouring, see – through register, latent image. For background printing, traditional Offset printing is used as a background to others security printing techniques and security elements like e.g. Intaglio printing, pre- printed text and bio graphical data in security documents.

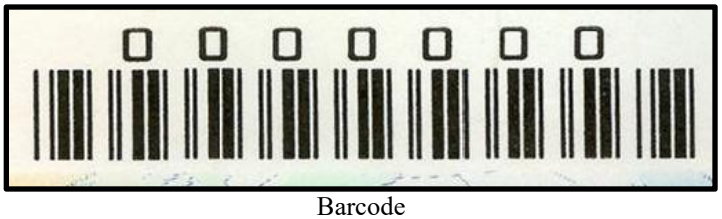


Background/Security printing

[Kumar, 4(2): February 2017] ISSN 2348 – 8034
DOI- 10.5281/zenodo.1405756 Impact Factor- 4.022

Barcode and Data Matrix

Barcode is made up of bars and spaces.Every set of bar will represent one digit. Barcodes are linear one dimensional code and can only hold up to twenty numerical digits.It can be read by the machine and safe from alteration and duplication. It is verified by scanning through barcode readers



Barcode

Bio-data / Photo / Signature Integration

Itrefers to an operation where by a printing, engraving or photographic technology is used to incorporate an image, a signature or bio-data text directly into a substrate or laminate during the personalisation process.

Bio-data/Photo/Signature Integration

Biometric Identifier (Biometric Data)

A biometric identifier is a personal biological (anatomical and physiological) or behavioural characteristic which can be used to establish a person's identity by comparing it with stored reference data. Traditionally, the most popular biometric identifiers are fingerprints and the facial image. Other frequently used biometric identifiers include the iris image and hand geometry.Biometric identifiers can be used for biometric recognition processes such as facial and iris recognition. The method of measuring biometric identifiers is known as biometrics. But biometric passports are not available in India

Biometric Identifier (Biometric data)

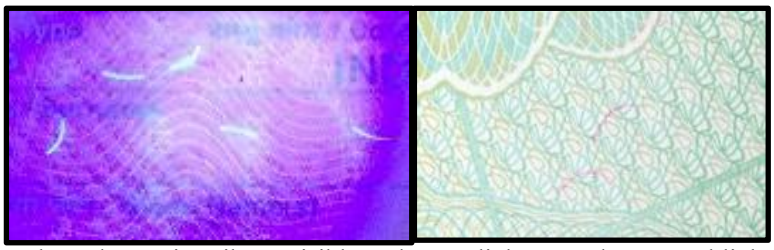
Bleeding (Penetrating) Ink

Bleeding ink is a security ink containing dyes which, together with solvent used, penetrate ("beed out or through") the paper substrate so that any attempt at mechanical ensure will cause visible damage to the document.

[Kumar, 4(2): February 2017]
DOI- 10.5281/zenodo.1405756
ISSN 2348 – 8034
Impact Factor- 4.022

Bleeding (Penetrating) Ink

Coloured Security Fibres
Coloured security fibres are fibres in various color which are mixed into the paper pulp during the paper manufacturing process, so that they are embedded in the paper in random places at varying depths also different on each page.


Coloured Security Fibres Visible under UV light & Under Normal light

Document Code
The document code is used in this database for authentic documents are made up of the following components
For example: - "IND-P-010001" this code consists of:-

- IND for India the document country = 3 letters country code
- P for Passport (National Passport) = document category
- 010001 (6 digits) of which the first two ("01") = Document number
  The last three("0001") = Version number

Embossing Stamp
Embossing is an impression in relief made by means of a seal or stamp e.g; to authenticate a document, or a conventionally fixed(e.g. glued)image of the holder in the document. The impression appears with a partly raised / lowered surface booth on the front and reverses side.

Endless Text
Endless text denotes repeated, sometimes un-spaced, line of a text in the background/ security printing on a security thread.


Endless Text

Fluorescent Serial Number

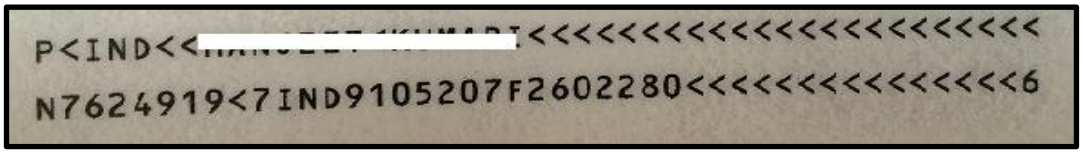
[Kumar, 4(2): February 2017] ISSN 2348 – 8034
DOI- 10.5281/zenodo.1405756 Impact Factor- 4.022

A unique document number is printed on a document and assigned as an additional safe guard for identification a fluorescent serial number fluoresces when exposed to UV light.

Fluorescent Serial Number

Machine Readable Zone (MRZ)

In a machine readable travel document (MRTD), the machine readable zone (MRZ) contains some of the information from the visual inspection zone in the form of a sequence of alpha numeric characters and the symbol "<", forming two or three lines. This sequenceof characters can be read by document readers in order to facilitate inspections of travel documents (OCR–Optical Character Recognition – fonts).

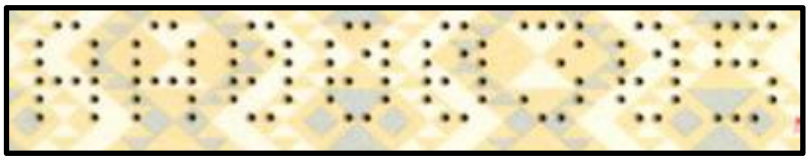


Machine Readable Zone(MRZ)

Laser–Perforated Serial Number

By using Laser technology, perforations of different types and sizes can be produces.The ID document serial number is perforated through the substrate with a laser. Typical distinguishing marks are produced:

- Traces of burning round the edges of the holes
- No raised edges round the holes in the substrate on the back of the perforations
- Conical decrease in size of the perforated holes in the booklet document when viewed from front to back.

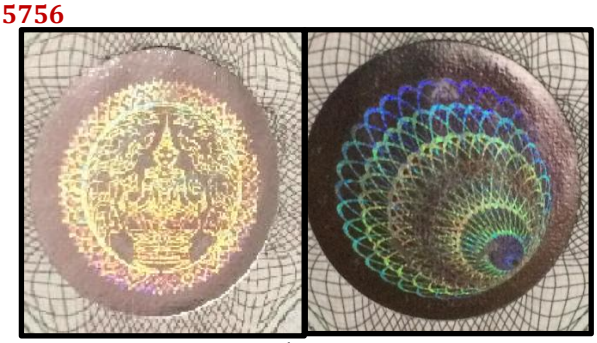


Perforated Serial Numbering

Hologram

The hologram is the most popular traditional type of Diffractive Optically Variable Image Device (DOVID) that is used as a security element. A number of effects are possible, e.g. 2D holograms with structural and color changes, 3D holograms with images, holograms with kinematic effects, etc.

ISSN 2348 – 8034
Impact Factor- 4.022



Hologram

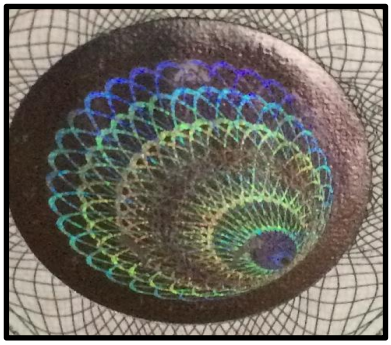
Ink Stamp

Liquid ink is transferred to the substrate by means of a stamp, e.g. for the authentication of a document or of a conventionally fixed(e.g. glued) image of the holder.

Ink stamp

Kinegram

The kinegramis a computer generated hologram capable of producing multiple high-resolution images. It contains special types of computer-generated diffractive optical elements. These can be designed in different ways to exhibit kinematic, color changing, contrast reversal and other special effects.

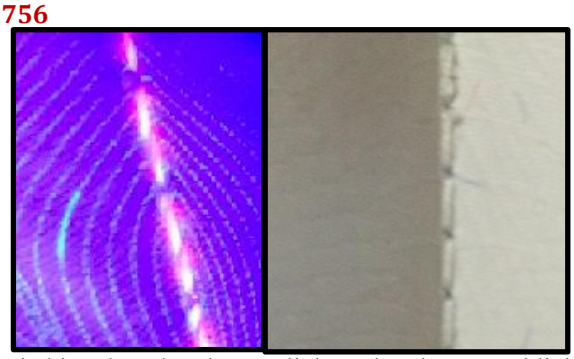


Kinegram

Fluorescent Stitching Thread

A fluorescent stitching thread is a thread(it can also consist of several individual, interlaced, threads) that is used for holding together the pages of a booklet, which fluoresces in one or several colors when exposed to UV light. Fluorescent stitching thread is also used in Indian passport for stitching.

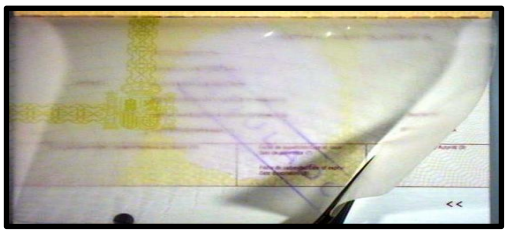
[Kumar, 4(2): February 2017]
DOI- 10.5281/zenodo.1405756
ISSN 2348 – 8034
Impact Factor- 4.022



Stitching thread under UV light and under normal light

Laminate Integrated by Binding

In many passports with traditional bio-data pages thee holder's image andthe bio-data are safeguarded with a transparent laminate. In order to complicate manipulation, the laminate can be integrated in the passport booklet by binding



Laminate Integrated by binding

Chemical Sensitizing

The paper contains an invisible colorant. Any attempt to remove or alter data using bleaching agents or solvents activates the colorant and is thus immediately obvious.

Country Code Security Thread

This security is incorporated vertically intothe security paper and is readable on both side of the page. The thread shows rainbow effects under both white and UV light (fluorescence).

Embossed Surface Structures

Tactile security features prevent falsified information from being pasted over plastic data pages. The feature can be combined with micro lettering just 100um in size.

FIT (Fine Intaglio Technology)

The first-ever intaglioprinting method that can produce ultra-fine lines. This high-resolution technology enables the creation of innovative security features that are unparalleled in terms of design and quality.For example guilloches/ fine-line patterns.

FIT Latent Image

Fine intaglio printing with a latent image, providing an excellent anti-copying and anti-scanning feature to enhance passport security.

Infacio

This is a copy of the data page using UV-reactive inks. Depending on the UV wavelength, the data become visible in monochromatic blue or in color shadings from blue to red and green.

Prismatic Colouration

[Kumar, 4(2): February 2017] ISSN 2348 – 8034
DOI- 10.5281/zenodo.1405756 Impact Factor- 4.022

The use of color can greatly assist the prevention of forgeries. By including a color on a document a color photocopier must be used in the attempt to make a copy however the use of these machines also tends to enhance the effectiveness of other technologies such as void pantographs and verification grids.

By using two or more colors in the background and blending them together a prismatic effect can be created. This can be done on either a traditional or a digital press.A frequent example of prismatic colouring is on visa, passport and checks.

III. CONCLUSION

In this era of globalisation people from across the world are meeting together, the current scenario for secured travel documents and other sectors where authorization of documents is of utmost importance, it is vital to secure the documents by adding enhanced and developed features on constant basis. The newer features state with replacement of conventional paper with non-tear able paper, along with drastic improvement in printing ink and design need for printing the same.

In this modern world printers are more concise about security of documents printed by the combination of conventional, non-conventional and digital printing processes, by doing this they produce excellent prints/products difficult to counterfeit but due to this cost of the printed product may get increased. It is the need of the era to secure the documents by adding or enhancing developed security features on constant basis. The newer features state with replacement of conventional paper with non-tear able paper, along with drastic improvement in printing ink from Micro to Nano-particles and intricate printing design in excellent registration makes prints difficult to imitate design. These features are not only increasing the security of the document but also enhancing the brand value of that document up to certain level. As newer printing technologies, newer types of substrates, complex design of the graphics and special inks are being used to increase the security of the secured documents. So, during this study we suggested a comprehensive list of security features used for travel documents, out of which in some of the products we use fewer number of security features and in some other products we use large number of security features i.e. In passport and VISA we use large amount of the security features. While in other personal documents less number of security feature are used. Security features are used according to the type of the document or according to end user requirement

IV. ACKNOWLEDGEMENT

Authors are thankful to all the researcher, writers, managements and various professionals for their contribution and for their publication already exist on the same topic. Our purpose was to take this technical issue more general for easy understanding and promote the knowledge and contribution of various authors on this topic. However all credit goes to original researchers and if any copyright issue, please let us know, we will humbly acknowledge the same and we take corrective action as suggested by them.

REFERENCES

1. ***Printing techniques used to secure border crossing documents***
Cristina Marcela Borota, International Journal of Criminal Investigation, Volume 2 Issue 1 31-40.
2. ***Overt Security Features through Digital Printing***
Mark-Hampden-Smith, Scott Haubrich, Ralph Kornbrekke, Jainisha Shah, RimpleBhatia, Ned Hardman and Rich Einhorn Cabot Corporation- Albuquerque, New Mexico USA 2006-02-09T15:07:20.
3. ***Hologram Counterfeiting: Problems and Solutions***
Stephen P. McGrew President New Light Industries, Ltd. 9715 W. Sunset Highway, Spokane, WA 99224 USA Published in Proc. SPIE Vol. 1210, pp. 66-76, Optical Security and Anti-counterfeiting Systems, William F. Fagan; Ed. April 1990.
4. ***The Securities Technology Institute for Counterfeit Deterrence***
John C. Murphy, chairman of the APL Graduate Fellowship Committee, and is a member of the Executive Committee of the Johns Hopkins Center for Nondestructive Evaluation.

Daniel C. Dubbel, Mr. Dubbel is a Principal Professional Staff member of the Submarine Technology Department and currently manages the STI at APL.
Richard C. Benson he is a member of the IEEE, American Physical Society, American Vacuum Society, and Materials Research Society. Johnshopkinsapl technical digest, volume18, no. 2 (1997).

5. ***Intrinsic and Extrinsic Signatures for Information Hiding and Secure Printing with Electro photo graphic Devices***
   Gazi N. Aliy, Aravind K. Mikkilineniy, Pei-JuChiangz, Jan P. Allebachy, George T. Chiuz, and Edward J. Delpyschool of Electrical and Computer Engineering School of Mechanical Engineering Purdue University West Lafayette, Indiana. , In proceeding, International Conference on Digital Printing Technologies, 2003, page: 511-515.
6. ***New Digital Anti-Copy/Scan and Verification Technologies***
   George K. Phillips Verify First Technologies, P.O. Box 7001, Paso Robles, CA 93447 USA., Optical Security and Counterfeit Deterrence Technique V June 3, 2004, Volume 5310, No. 5310 ISBN/ISSN: 0-8194-5213-0, 450 pages.
7. ***Biometric Security Using Finger Print Recognition***
   SubhraMazumdar, VenkataDhulipalaUniversity of California, San Diego., Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.
8. ***Security Printing: Innovative Technologies with Comprehensive Approach as an Anti-Counterfeiting Tool***
   VikasJangra Department of Printing Technology, Guru Jambheshwar University of Science & Technology, Hisar - 125001 (Haryana) India, IJSRD - International Journal for Scientific Research & Development, Vol. 4, Issue 05, 2016 , ISSN (online): 2321-0613.
9. ***Variable Data Security Printing and the "Layered" Deterrent***
   Steven Simske and Roberto Falcon, Hewlett-Packard Company, USA Digital Fabrication 2005 Final Program and Proceedings, pp. 124-127(4).
10. ***Print signatures for document authentication***
    Mohan S. Kankanhalli, National University of Singapore, New York, NY, USA 2003.
11. ***QR Codes and Security Solutions***
    Sankara Narayanan, Department of Information Technology, Salalah College of Technology, Sultanate of Oman, International Journal of Computer Science and Telecommunications Volume 3, Issue 7, July 2012.
12. ***Security Printing Deterrents: A Comparison of Thermal Ink Jet, Dry Electrophotographic, and Liquid Electrophotographic Printing.***
    Steven J. Simske, Jason S. Aronoff and Margaret M. Sturgill Hewlett-Packard Laboratories, 3404 E. Harmony Rd., Mailstop 36, Fort Collins, Colorado 80528 September 2008.
13. ***On Secure Digital Image Watermarking Techniques***
    ManjitThapa, Sandeep Kumar Sood, Journal of Information Security, 2011, 2, 169-184.

WEB SUPPORT

1. *https://en.wikipedia.org/wiki/Securityprinting on 20-12-2015.*
2. *http://en.wikipedia.org/wiki/cover security features on 20-12-2015.*
3. *http://www.consilium.europe.eu on 22-12-2015*