Verification of document with social values using watermark exclusion

Mukesh Kumar

Abstract— Cryptography ensure the authenticity and integrity of a document but after encryption it is helpless but watermark prove all such aspects with legitimacy and ownership of document at all levels. Digital watermarking is a technique for inserting information (the watermark) into an image, which can be later extracted or detected for variety of purposes including identification and authentication purposes A watermark is a pattern made in high-quality papers by means of an improved or worst design that comes in contact with the paper; it is approximately 90% water and 10% fibers. The watermark designs are spaced at specific intervals (depending on the frequency of appearance required in the finished sheet) along the surface of a skillfully crafted wire roll called a “Groovy roll”. As the revolving groovy roll comes in contact with the fibers, the designs displace with the fibers and produce the pattern visible in the finished sheet known as a watermark. Most people are familiar with two types of document watermarks which can be found in banknotes or on cheques. In banknotes, these are recognizable designs that are put into the paper on which the documents are printed, while in cheques they tend to be specific patterns. These watermarks are normally used to prevent people from being able to make fake copies, and, therefore, to be confident that the banknote or document is authentic. Our aim to remove all the vulnerability by checking the genuineness of documents with social values through such methods that verify the legitimacy of documents.To deter copying using water marks:- The numbers of specialized techniques make it possible to detect the fakeness of a document with printed watermarks whether it is appear or vanish and a protected document is photocopied or scanned and it relay work upon high quality printing processes and created successfully. The printing techniques that produce 'raised' printing, use magnetic inks or inks that will change color if they get wet (either with water or other liquids), but they are very specialized and are used together with watermarks to provide higher levels of document protection and copy prevention.

Index Terms— check the ownership of legal document, Check ligtimacy of document, currency verification, check the genuineness of documents, detect fackeness of document, document authenthicatin using watermark exclusion, To deter copying using watermark

1 Introduction

Higher decreasing cost of computing equipments and high quality peripherals devices are driving electronic publishing in the current era. Furthermore, availability of low cost, high speed and very high quality scanner and printers, made it possible for every one to make clone of the original documents with perfect ness. The scanning of documents with high resolution scanner makes the copy of the real one. The prepared copy is so perfect that we couldn’t differentiate between the original and the duplicate. There are lots of symbols are present on the document with social values for their authenticity but in this paper watermark has been chosen for the verification. Almost every legal document contains watermark, we can divide watermark into two categories visible and invisible. Visible watermark can be easily identified by the naked eye but hidden watermark is verified by the experts or by the technology. There are lots of algorithms implemented on the currency paper, legal documents recognition.

To achieve such a goal it should be ensured that "widespread illegal document distribution " should be ideally at least as costly or difficult as obtaining the document legitimately. "Illicit distribution" is defined as the distribution of document by any possible means, both electronic and otherwise, without the knowledge and payment to the publisher of the document. A way to discourage illicit reproduction of copyrighted and sensitive documents is to watermark the document before distribution. A unique mark is permanently embedded in the document, called watermark. Such a mark must be hardly noticeable. Yet it must survive common processes a document must be subjected to, such as printing, photocopying, scanning and facsimile transmission, so that it can be detected from noisy illicit copy to verify the document. One such system has been implemented in this paper

The documents with social value should be embedded with watermark according to their value and usage, methods / techniques are able to verify the document legitimacy.

2 Method of verification

Basically legal documents can be verified by two methods: first-line inspection methods and second-line inspection methods.

2.1 First-Line Inspection Methods

- Watermarks
- Ultraviolet Fluorescence
- Intaglio Printing
- Micro text
- Hologramsand Kinegrams

First-line inspection methods are used on-the-spot by vendors and retailers to determine, at best guess, the authenticity of currency being exchanged. The disadvantages of these methods are that they are generally easier to counterfeit than second-line inspection characteristics, since they are just as visible to the counterfeiter as to the verifier, and the methods used to apply them are usually inexpensive. However, the visibility of these features means that the general population is aware of the security measures and can spot many fraudulent notes quickly.

2.1.1 Watermark

By varying the density of the paper in a banknote a watermarks can be applied. These are visible when a bright light shines onto the rear of banknote, and the varied paper density causes varying intensities of light to pass through, causing the watermarked image to appear on the other side of the note.

2.1.2 Ultraviolet Fluorescence

Embedding fluorescent fibers into the paper, or printing ultraviolet ink onto the paper, creates a form of optical verification easily used at counters, checkouts, etc. By exposing the note to ultra-violet light, the ink or fibers fluoresce, revealing a colored pattern not visible under natural light.

2.1.3 Intaglio Printing

This gives a more complex and reliable first-line inspection method, since it is the printing process itself that serves to vouch for the authenticity of the document. The note is subjected to a high-pressure printing process that strengthens and slightly raises the paper's surface structure. Using different alignments of lines printed in this manner, a latent image can be produced which changes appearance depending on the angle at which the note is viewed. This method can also be used with optically-variable ink to produce interference which shows different spectral colors when viewed from different angles.

2.1.4 Microtext

It is very common for banknotes to have extremely small text printed at much higher resolutions than most commercial copiers, scanners or printers are capable of it. When a copying or scanning attempt is made, the insufficient resolution causes the text to become illegibly blurred, announcing the illegitimacy of the note. This method requires specialized printing equipment but ultimately adds very little cost to the manufacture of the currency.

2.1.5 Hologram and Kinegrams

These techniques are becoming more and more regularly used in modern anti-counterfeiting measures, once used mostly on credit / debit cards but now progressively more using on new bank notes and cheques. In producing diffractive optically variable image devices, shining foils are added to the printed currency usually after printing. The hologram itself is applied using the obstacle of light from different sources in a specific pattern, and kinegrams are produced with achromatic and polarization effects. The result is seems actually 3D full-color image when illuminated from different angles. ISIS uses stacked quantities of thin films to create a similar effect, with each layer having different refractive properties. The refraction of light when viewed is such that a spectral pattern has been extracted and a full-color image is produced which varies under different viewing angles.

2.2 Second-Line Inspection Methods

A second-line inspection method is one that cannot be verified by the naked eye alone, and requires an extra device to perform a verification function. These are more secure and harder to counterfeit than visual methods, but the extra security adds extra cost at both the manufacturing and verification ends.

2.2.1 Isocheck / Isogram

Related to intaglio printing (described above), these methods rely on a specific pattern of dots and/or lines to cause a moiré pattern when printed or scanned. Hidden watermarks can also be applied in these patterns such that when a special filter is placed between the viewer and the note, the hidden verification is revealed and verifies the note as genuine.

3 PROBLEMN DESCRIPTION

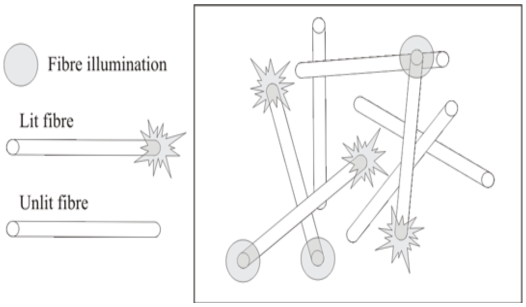
With the advent of technique and technologies, it is easier for a person to create a fake copy of the legal document very easily. High resolution scanner and printer made people capable of preparing almost perfect copy of the document. So, we need a technique by which we can verify the truth ness of the document. To propose a technique, this can verify the truth ness of legal document. To verify the document, technique should be capable of extracting watermark from the document and verify on the basis of accuracy of the watermark.

Hand written signature is the most widely form of personal identification as well as for document verification, especially for cashing cheques, deeds etc However, for several reasons the task of verifying human signature can't be considered for pattern recognition because signature samples from the same person may be similar but not identical. A person's signature often changes radically during their life. We can see much variability in signature according to country, age, time, and psychological or mental state. So to remove all such vulnerabilities form the system to check the genuineness of the documents, we can use such methods that verify the legitimacy of the document that we use for social value purpose.

4 Future aspects

Current proposed method is based on the link mapping and neural network. However this technique is better than other technique on the basis of speed and cost. Combination of link mapping and neural network gave the better solution to this problem. However following are some issues to be work on in future.

4.1.1 Fibre-Based Certificates of Authenticity



Based on the characteristics of fiber-optic light transmission, this method makes use of unique configurations of fibers embedded in the paper.

Using a scanner to illuminate one end of an embedded fiber, the other corresponding end of that fiber will become illuminated. By using the position of both illuminated ends, the certifier has a “fiber signature”. This can be converted into a bit pattern with a private key, the corresponding public key made available. The final result of these steps can then be encoded onto the banknote (this method is suitable for certifying a wide range of other documents too) in the form of a barcode or verification number of some kind.

4.1.2 Instead of Sign use Watermark for Verification

Instead of verification of signature on a document (Signature of individuals changes according to age, memory and physical conditions), we also required the verification of the document whether it is real or fake. To verify the legitimacy of documents with social values, a new technique with low cost and high reliability is capable to detect the watermark exclusion on the document easily and verify the legitimacy of the document on the basis of the watermark exclusion. This technique works on high resolution scanner; if high resolution scanner is not available this technique will not work efficiently.

We can make such method on which, we are able to check the truth ness of document whether it is clone copy or true copy by high resolution printing or scanning technique. So improvement can be made by making it resolution independent.

4 References

[1] Anderson, R., Cox, I., Low, S., Maxemchuk, N., & Tranter, W. Guest Editorial Copyright and Privacy Protection. IEEE Journal on Selected Areas of Communications. Vol 16, No 4. May 1998.

[2] Anderson, R., Fabien, A., Peticolas, P. On the Limits of Steganography. IEEE Journal on Selected Areas in Communications. Vol 16, NO 4. May 1998.

[3] Hardin, R. W., “Optical Tricks Designed to Foil Counterfeiters”. OE Reports Number 191, International Society for Optical Engineering, November 1999

[4] Benedens, O. Geometry-Based Watermarking of 3D Models. IEEE Computer Graphics and Applications. Vol 19, No 1. Jan/Feb 1999.

[5] Kundur D., Hatzinakos D., “A robust digital image watermarking method using wavelet-based fusion,” Int. Conf. on Image Processing, Vol. 1, Oct 1997, pp. 544-547.

[6] Cox I. J., Kilian J., Leighton F. T., & Shamoon T., “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing,Vol. 6, No: 12, Dec 1997, pp. 1673-1687.

[7] Tirkel A.Z.., Rankin G. A., Schyndel R.G. van, Ho W.J., Mee N.R.A., and Osborne C.F., “Electronic Watermark,” In Dicta-93, Dec 1993, pp. 666-672.

[8] Bender W., Gruhl D., and Morimoto N., “Method and apparatus for data hiding in images,” U.S. Patent # 5689587, 1996.

[9] Goffin F., Delaigle J.F., De Vleeschouwer C., Marc B., and Quisquater J.J., “A low cost perceptive digital picture watermarking method,” Storage and Retrieval for Image and Video Database, Vol. 3022, Feb 1997, pp. 264-277.

[10] Kutter M., Jordan F., & Bossen F., “Digital signature of color images using amplitude modulation,” Proc. of SPIE-EI 97, Feb 1997, pp. 518-526.

[11] Cox I. J., Miller M. L., and McKellips A. L., “Watermarking as Communications with Side Information,” Proc. of IEEE, Vol. 87, No: 7, July 1999, pp. 1127-1141.

[12] Ho A.T.S., Jun S., Soon H. T., & Kot A.C., “Digital image-in-image watermarking for copyright protection of satellite images using the fast Hadamard transform,” IEEE International Geoscience and Remote Sensing Symposium (IGARSS '02), 24-28 June 2002, Vol. 6, pp. 3311-3313.

[13] Hsu C. T., and Wu J.L., “Hidden digital watermarks in images,” IEEE Transactions on Image Processing, Vol. 8, No: 1, Jan 1999, pp. 58-68.