VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSE-2008-NETWORK SECURITY

WINTER SEMESTER 2019-2020

TOPIC: APPLICATION OF DIGITAL WATERMARKING IN PRINTING

BY

G.ROHITH (18BCI0226)

G.VINEETH (18BCI0227)

N.SRAVANA KUMAR (18BCI0232)

ANIRUDH REDDY (18BCI0218)

FACULTY: KATHIRAVAN S

Abstract:

In this project we are going to discuss about the program of applying digital watermarking technology for printing, and find a kind of printing anti-counterfeiting technology which is difficult to copy, easy to identify, bottom cost and pollution-free. We summarized the research program of three stages that included generating and embedding watermarks, printing and scanning, extracting and detecting watermarks, was defined that divided from the process of digital watermarking technology. The results shown that, further studies could focus on the research on effects of the printing and scanning attacks on watermarks, so the relationship of invisibility and robustness to resist printing-scanning attacks could be balanced. Due to digital watermarking technology that was applied to digital images, it was necessary to research the fragile ability that prevents the secondary printing to establish the relationship between watermarking algorithm, printing process and parameters.

Introduction:

As the medium of carrying and transfer product information, printing direct contacted with consumers and became numerous anti-counterfeiting means, such as packaging, book, receipt newspapers and magazines. Existing anti-counterfeiting technology for printing always using a special printing process, some special materials or the combination of a variety of ways, such as hand-engraved plate, light sensitive inks. However, special printing process or materials tend to face the difficult of automatic identification, rising cost, environmental pollution problems. In order to solve these problems and exploited printing anti-counterfeiting technology, which is difficult to copy, easy to identify, low cost, pollution-free, scholars tried to apply digital watermarking technique on printing.

The watermarks that used in digital watermarking technology is invisible for human, but computer could read it. Embedded the watermark into the printing

design, and the location was determined by key, so there is no chance for counterfeiters to access it. Applying the technology in digital field is valid, such as broadcast monitoring, identification, prove ownership, transaction tracking, content authentication, copy control, device control and digital copyright protection. In recent years, scholars try to transfer the technique from the field of digital copyright protection to the field of anti-counterfeiting printing, research was achievements, but there also were issues that obstruct the application.

Literature survey:

Reference Number	Name of the Algorithm/ Model/System	Dataset Used	Brief Description about the model/system	Parameters influencing the performance of the model	Advantages of the model/system	Limitations of the model/system
[1]	digital watermarking algorithm		Digital watermarking is a technique used for protecting the intellectual property rights of digital media.	To increase the security of the watermark, Arnold transform is used to shuffle the original binary watermarking image. After k times Arnold transform, the watermark WI ‘ is obtained.	Applying dual watermarking technology in DMR system can provide complete protection of the digital media	Watermarking doesn't prevent image copying but we can track down and detect ownership of copied images

[2]	Extraction algorithm embedding algorithm		We have described recent developments in the digital watermarking of images in which the watermarking technique is invisible and designed to exploit some aspects of the human visual system. Many of these techniques rely either on transparency (low-amplitude) or frequency sensitivity to ensure the mark's invisibility	An algorithm based on DCT domain has been proposed to make the watermark more robust. At the first step, the requirements, techniques and applications of digital watermarking for high-quality images are addressed. Second, is to implement the algorithm using the tool (i.e. Mat Lab) for embedding the watermark into original image in DCT domain.	more robust to many attacks based on linear and nonlinear signal processing operations. The protection of intellectual property rights is perhaps one of the last major barriers to the "digital world."	Resizing, compressing images from one file type to another may diminish the **watermark** and it becomes unreadable.
[3]	Multilevel security feature for online transaction using QR code & digital watermarking		proposed a new authentication system for online banking which ensures better security and convenience. The experimental results prove that the digital watermark method is feasible and effective. It is complex to counterfeit the QR code when digital watermarking technology is used with the QR code.	**OTP** An OTP (One Time Password) is a generated password that is legitimate for a short interval of time. On the server side, the OTP is generated using an algorithm which either generates a numeric, alphabetic or alphanumeric string and is provided to the customer through SMS mail. **SMS Banking** SMS Banking is a facility which present users to gain access to their account information by means of mobile. Biometric: Biometric is particularly	proposed a new authentication system for online banking which ensures better security and convenience. The experimental results prove that the digital watermark method is feasible and effective. It is complex to counterfeit the QR code when digital watermarking technology is used with the QR code.	It is only good forgood pixel images.

				utilized for safe online transaction. In this, it makes use of a biometric mechanism like scan of iris/retinal or the fingerprint scan can.		
[4]	A Novel Text Watermarking Algorithm Based on Graphic Watermarking Framework		presents a new algorithm based on similarity of line, etymon and character, describes the implementation and points out the effectiveness theoretically. However, it needs a lot work to implement, verify and try to apply it in practical environment.	watermark information embedding and watermark information extracting.	full use of the self-characteristics, similarity and structural feature of line, etymon and character. Therefore, the correctness, security, and robustness will be better indirectly.	It is only good forgood pixel images
[5]	Watermarking of digital media with encrypted biometric features for digital ownership		presents a method of secure watermarking by using encrypted fingerprint images as digital watermarks. The use of such digital watermark ensures the ownership of the watermark and the encryption ensures that the biometric data is not exposed to any threat or vulnerability.	Encryption Using Arnold Cat Map Arnold Cat Map employs shearing and wrapping operation to completely scramble a matrix after several iterations. Arnold cat map is one to one mapping.	ownership of the watermark and the encryption ensures that the biometric data is not exposed to any threat or vulnerability. This clearly indicates a significant development in identification and proof of ownership for digital media.	Biometric authentication details cannot be invalidated remotely if something goes wrong.

Proposed model:

Generating and Embedding Watermarks

Operated the secret and hidden information with the key that we had chosen to generate the watermark w.
In the system of digital watermarking technology, watermark w was embedded in the host image o *to* obtain the watermarked image m, and the embedding formula could be numbered as formula.

$$m=e(w,o)$$

Where e is the algorithm of embedding watermark. The algorithm of extracting watermark was the reverse algorithm of embedding watermark, so the watermark could be extracted.
The quality of watermarked image m should be evaluated by the requirements, such as fidelity. If the quality of watermark image m did not meet the requirements, the embedding algorithm should be optimized until it meets the requirements; If the quality watermarked image m met the requirements, print the watermarked image.

Printing and Scanning

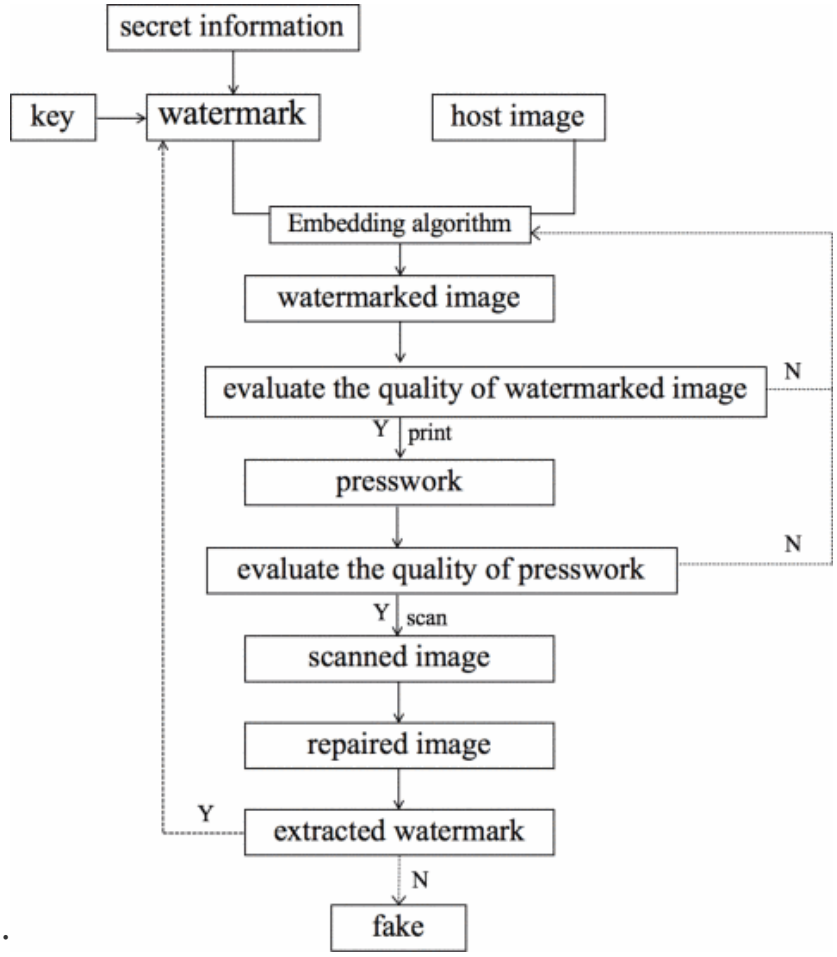
Applied a series of printing parameters that suit the embedding algorithm which we designed in sept 2) to obtain presswork. The quality of the presswork should be evaluated by the national standard and the needs of customers.
If the quality of presswork did not meet the requirements, the embedding algorithm should be optimized until it meets the requirements; If the quality presswork met the requirements, scan the presswork.
Scanning the presswork which contained the watermark, so converted the presswork into digital image to obtain the scanning image.

Extracting and Detecting Watermark

The different between scanned image and watermarked image included the geometric distortion and pixel values distortion, so it is inevitable to repair the scanning watermarked image to obtain the repaired image.

Extract the watermark from the repaired image, and compared it with watermark which generated in sept 1) to obtain the similarity. If the similarity within the

permitted threshold, then determine the print for real, if not within the permitted threshold, which this print for forgery



.

The different between applying digital watermarking technology in the field of digital image and presswork focus on the process of printing and scanning, so the robustness of watermark to printing and scanning challenging problem. Therefore, watermark, which contained a lot of information, has the ability to be robust to printing and scanning, ensures the quality of printing, and has high fidelity.

It is worth noting that even if the requirements of robustness and high fidelity was satisfied and the watermark could be extracted, does not mean that after the first printing problems have been settled satisfactorily. If forgers used high-fidelity devices scanned the presswork, print it again, and the watermark also could be extract from the secondary presswork, it is unable to meet the anti-counterfeiting requirements.

Therefore, the performance of the watermark that prevent secondary printing is also important. In this paper, the digital watermarking technology is applied to the main process is divided into three parts of generating and embedding watermarks, printing and scanning, extracting and detecting watermarks to discuss the key problems needed to solve and its research progress.

Characteristics of Watermark

Robustness

Robustness is the ability of watermark that can resist various attacks. Common attacks include compression attack when the watermarked image suffered compression storage, attack of printing and scanning. The printing process would transfer digital image into analog image, the scanning process would transfer the analog image into a digital image, and the distortion of these two kinds of attack is multiple. First of all, common geometric distortion cannot be ignored, such as rotation, cutting, and scaling. In addition, there are pixel values of the nonlinear distortion, which due to the change of brightness and contrast, such as gamma correction, halftone processing or noise.

The robustness of the watermark determines whether the watermark that suffered attacks can be extracted successfully. If the watermark was robust to the attack of progress of printing and scanning, extracting the watermark would be easy, so watermark needs to have the ability of robustness. However, if scanned the presswork by high-fidelity devices and printed it again, still could extract the watermark from the secondary presswork, it is unable to meet the anti-counterfeiting requirements. Therefore, watermark needs the fragility to secondary printing and scanning attack to prevent secondary printing.

Invisibility

The algorithm of generating and embedding the watermark needs watermark have the nature of robustness, invisibility, capacity, safety and efficiency.

Without high invisibility, the different between host image and watermarked image could be noticed by human eyes, so the host image fidelity is low. Otherwise, the

host image fidelity is higher, the watermark is perceptual. Applied to packaging printing, for example, if the host image used for the carrying product information or promoting the sales of packaging decoration, the watermark should not affect the visual effect of packaging decoration. Therefore, the problem of how to keep the high invisibility should be considered when designing algorithm of embedding watermark.

Capacity

Capacity is the amount of data that could be embedded in the host image. With widely used, the number of embedded watermark must ascend, so the capacity for the promotion of this technology is particularly important.

Efficiency

Especially, the efficiency of the extracted watermark is related to whether the application of this technology can adapt to modern fast rhythm, and directly affects the practicability of digital watermarking.

For the majority algorithm of digital watermarking, printing and scanning attack is a challenging problem. For carrying large amounts of information in the watermark, watermark needs invisibility and robustness to resist the attack of printing and scanning process. As shown in figure 1, the algorithm of embedding watermark not only needs to ensure that information with enough capacity can be embed and extract, also constraints by the quality evaluation of watermarked image and presswork. As a result, three properties that includes capacity, robustness and invisibility are important.

Three properties that include capacity, robustness and invisibility mutual restrict between each other. On the one hand, as shown in references , in order to achieve enough robustness of watermark, watermark was placed in the position of the perception is important; On the other hand, for the sake of high fidelity, the watermark was placed in a part of the not easily perceived. Therefore, the robustness and invisibility are the performance of the mutual restriction. In the same way, there is not an algorithm of watermarking can resist a wide range of attack and has a high capacity, not reducing fidelity cannot improve the capacity.

Characteristics of Attack

Transplanting the digital watermarking technology in the field of anti-counterfeiting printing, the attack of printing and scanning process was the serious challenge, and its characteristics can be summed up in the following three points.

Randomness. Depending on the different of mode and process parameters, there was a different between scanned image and watermarked image. For example, different mode of printing, such as offset lithography, intaglio printing or letterpress printing, provided different color. As shown in references, ZHANG pointed out that different features of host image, screen Ruling, dot shape and printing stock affect the quality of the extracted watermark, and it is vain to recover color for presswork, which cause unnecessary increasing cost. Therefore, instead of increasing the quality of recovering color for presswork, scientifically establish the relationship between host image, watermarking algorithm and printing process parameters, the proper watermarking algorithm and corresponding process parameters was prepared for host image with distinguishing feature.

Artificially. In the process of printing or scanning images, the operator adjusts some parameters according to the specific requirements, such as contrast change, gamma correction, rotation, scaling or certain artistic processing. Mutual dependence. Without scanning, presswork cannot be detected to extract watermark and analysis. Therefore, the process of printing and scanning are mutual dependence, and the two process also would cause image distortion and distortion.

Extracting and Decting Watermarks

In progress of extracting watermark, the different between scanned image and watermarked image could not be ignored. In order to improve the quality of extracted watermark and ensure accuracy of watermark detection, it is inevitable to repair the scanning watermarked image before extracting watermark. Focus on the geometric distortion in the process of printing and scanning, Sun[2] designed the positioning-correction program to repair the geometric distortion, realized blind extraction, and the watermarking algorithm is practical.

In the process of detecting watermark, compared to extracted watermark and the original watermark to obtain the similarity using Normalized Correlation coefficient.

Recently, the research and development of QR code technology provided a method to extract and detect watermark. Applying QR code as watermark or host image to digital watermarking, using its ability of correction and the advantage of fast recognition to enhance robustness of the watermark, improve the detection efficiency of the watermark.

Conclusions:

In recent years, there also were issues that obstruct the applying digital watermarking technology to the field of anti-counterfeiting printing. In the progress of generating and embedding watermark, existing algorithm mainly focus on the tradeoff between robustness and invisibility, but research on secondary prevention printing was dissatisfied. In the progress of printing and scanning, existing research was involved the image color space transformation. However, without definite conclusion, the effects of the process of watermark has not been sufficient research.

References:

[1] Y. Geng Wang, Z. Ming Lu, L. Fan, "Robust dual watermarking algorithm for AVS video", *Signal Processing: Image Communication*, vol. 24, no. 4, pp. 333-344, Apirl 2009.

[2] S.P. Mohanty et al., "A Dual Watennarking Technique for Images", *Proc. 7th ACM International Multimedia Conference ACM-MM'99 Part 2*, pp. 49-51, Oct. 1999.

[3] Samir Pakojwar, N. J. Uke, "Security in Online Banking Services - A Comparative Study", *International Journal of Innovative Research in Science Engineering and Technology*, vol. 3, no. 10, October 2014.

[4] Brassil, J. T., S. Low, and Maxemchuk,N. F., "Copyright Protection for the Electronic Distribution of Text Document," Proceedings of the IEEE, vol. 87, Jul. 1999, pp. 1181-1196.

[5] AsYu-Hsun Lin and Ja-Ling Wu, "A Digital Blind Watermarking for Depth-Image-Based Rendering 3D Images"IEEE Transactions on Broadcasting, VOL. 57, no. 2, 2011, pp-602-611.

[6] Yong Xie, Juan Li and Juan-juan Wang, "A Kind of Printing and Scanning Tilt Distortion Resistant Digital Watermarking Algorithm[J]", *Packaging Engineering*, vol. 34, no. 15, pp. 104-108, 2013.

[7] Yun-feng Sun, Hong-chen Zhai, Xiao-ping Yang et al., "Application of Fourier CGH Digital Watermarking Technique in Color Image Forgery-Prevention Printing[J]", *Journal of Optoelectronics· Laser*, vol. 19, no. 7, pp. 952-955, 2008.

[8] Yong Xie, Qi-qin Feng, Wu-yang Shan et al., "Application of Digital Hologram Watermark in Printing Halftone Image[J]", *Packaging Engineering*, vol. 34, no. 1, pp. 101-105, 2013.

[9] Meng-tao Li, Liu-jie Sun, Chen-lu Li et al., "Research on Fourier Encryption Printing Watermarking Algorithm Based on Wavelet Transform [J]", *Packaging Engineering*, vol. 33, no. 1, pp. 108-112, 2012.

[10] Liu-jie Sun and Song-lin Zhuang, "Forgery Prevention Based on In-Line Fourier Holographic Watermark with Double Random Phase Encryption[J]", *Optica Sinica*, vol. 27, no. 4, pp. 621-624, 2007.