Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080358

Study on The Digital Encryption Algorithm of the Papermaking Process

Zhijian Li[1,*] *and Kaisheng Zhang*[2,*]

[1] College of Light Industry and Energy of Shaanxi, University of Science and Technology, Xi'an, 710021, P. R China
[2] College of Electrical and Information Engineering of Shanxi, University of Science and Technology, Xi'an, 710021, P. R China

Received: 29 Jun. 2013, Revised: 3 Nov. 2013, Accepted: 4 Nov. 2013
Published online: 1 May. 2014

Abstract: It summarizes the necessity and significance on fiber digital technology of paper forming process, utilizes QR code principle to embed the code into non-weaving process and make digital processing for embedded code. In implementing, it mixes magnetic fiber into pulp in advance and uses magnetic controller which lies above the wet end to make control. The code is embedded invisibly into paper fiber in this method, it overcomes drawbacks in numerous anti-counterfeiting paper, create a new kind of specialty paper and solves authentication problem thoroughly. So it has important consequences for improving theoretical research level and engineering level of papermaking industry.

Keywords: Paper Forming Process; Digitization; Encryption Algorithm; QR code; Paper identity

1 Introduction

In recent years, with the development of modern science and technology, paper product is no longer limited to its original purpose and become more widely used in every field such as industry, architecture, pharmaceutical and living field. Specialty paper is a new type of paper which is manufactured by special processing, it is developed on the basis of converted paper. It may change people's traditional view of paper. It has close ties to physical process (such as thermology, electricity, optics and magnetics), chemistry principles and biomechanism. The leading characteristic of specialty paper is its differences on paper quality, performance and application with ordinary paper, specifically the following aspects: Firstly, diversified raw material ratio, ordinary paper tend to utilize plant fibers, such as wood, grass-like plants, while specialty paper can equip other non-plant fiber, chemical fiber, carbon fiber and metal fiber. Secondly, specialized capability changes, specialty paper possess some kind of outstanding performance by means of different processing method and material adding. Thirdly, wide practical application, because of the progressive kinds of specialty paper, according to the statistics, it accounts of more than 80% of total paper production. So it owns numerous uses in cultural education, industrial production, military technology and daily life.

Magnetic paper is a kind of specialty paper with great development potential. In 1969s, it is firstly applied to automatic ticket checker of railway system in industry-developed country. Magnetic material has been developed since ancient times. It relies on its unique performance in chemistry and physical structure, such as flexibility and folding resistance. The development of magnetic paper solves many problems well. The product which is made of magnetic paper is widely used in many ways such as agriculture, industry, magnetic recording, security, electromagnetic transducer, screening, medical treatment and biotechnology.

Research on magnetic paper in our country is comparatively late, properties of products are relatively poor, and application fields are relatively narrow. But with the rapid development of economy and cultural life, it will surely impel applications in more new fields. Our country must accelerate the development and technological innovation in face of foreign competition.

At present, in order to solve identification problem of paper, several kinds of security paper are invented. Security paper can be divided into two categories: one is to security paper itself, it uses security method in papermaking process; another type applies printing

* Corresponding author e-mail: lizj@sust.edu.cn, zhangkaisheng@sust.edu.cn

method and computer laser information icon to paper carrier. According to security effect and representation, it is divided into watermark security paper, safety line security paper, cellosilk security paper, color-change security paper, biotechnology security paper, nuclear technology security paper, chemical protected security paper and comprehensive security paper. According to application objects, it is divided into product security, packaging security, brand security, lottery and securities anti-counterfeiting, certificate security and banknote security. According to subjects, it is divided into physical security, chemistry security, biology security and multidisciplinary security.

Security paper combined anti-counterfeiting technology in every field with paper, it is a product of multi-subject cross-technology. It has identifiability and confidentiality, and occupies a quite important role in research and application. It is a subject which receives worldwide publicity. It is of important meaning to take protective measures for local currencies, bills, valid documentation and has specific influences on national economy and security.

There are many types of magnetic paper at present, such as nanometer ferromagnetic paper, it can manufacture micro-robot. Researchers at Purdue University have developed ferromagnetic paper, a kind of nanometer grade material. This kind of special material utilizes mineral oil and iron oxide ”magnetic nanometer particles” to make permeation in ordinary paper or newspaper and form magnetic paper. Now it has 4 kinds of processing methods:

(1)Coating method, it uses reversed roller or gravure cylinder to coat magnetic coatings directly on body paper, then coat a layer of protective film. This processing method is simple and practicable, and has a lower cost, so it owns a wide application range, such as the recording layer of magnetic ticket, phone card and food card.

(2) Printing method, in order to enhance liquidity of magnetic ink, it also needs to add plasticizer such as castor oil. Then uses screening printing to print the magnetic stripe in proper position of body paper. Many credit cards use this method. (3) Attaching method, it attaches polyester film, magnetic adhesive and slitting magnetic stripe to body paper or cards. (4)Transfer printing method, it applies silicone compounds as peel ply on film-polyester, then coats protective film, magnetic film and thermal-resistance layer, uses heating method to put them to based paper by transfer printing, stripes film-polyester after cooling. Magnetic plane tickets, cash cards commonly use this method.

Identification problem of paper is more complex, although magnetic paper above can effectively resist imitations in some respects, most parts are manufactured by later printing technique. The characteristics of paper presents on the surface, it can’t guarantee uniqueness of paper identity, so it can’t solve identification problem of paper fundamentally. In order to enhance reliability and uniqueness of paper identification, it needs a kind of fiber digitization technology of paper forming process urgently.

This subject tends to applies inherent advantages and characteristics of cellulose fiber, utilizes digitization technology to embed the composite fiber which contains magnetic fiber into non-weaving process with the aid of advanced papermaking method and control theory, solves identification problem of paper and enhances reliability and uniqueness of paper identification. Research of this subject has great significance on developing cellulose application area, increasing new kinds of specialty paper, solving identification problem of paper thoroughly and improving theoretical research level and engineering level of papermaking industry in our country.

2 Topic Basis

2.1 Theoretical Basis

According to national standard GB/T18284-2000¡¡Quick Respond Code¿¿ encode the statistics input by user and output the result in form of matrix. It adopts QR code, character set is divided into numeric data (number 0-9), alphanumeric data (number 0-9; capital number A-Z; 9 other characters: space,$, %, *, + -/,:), 8 bytes data (ASCII character set), Chinese character code. Different character sets will have different QR code mode to encode, and different methods will put to use. When encoding, it can make transition between each mode, so that it can transform the data into binary bit-stream efficiently. The bit-stream after encoding is composed of one or more sections with different modes, each section is composed of mode indicator (4 bytes), character counter indicator and data bit-stream. Because of every mode of character set has overlaps, it makes the bit-stream’s length short by means of mode swapping to generate efficient codes. Theoretically speaking, it is the most efficient way to encode by using the least bytes mode which every data code needs, but it all needs additional spending such as related mode indicator and character counter indicator when makes every time of mode swapping. So it may not make the least bit-stream amounts for fewer characters by using mode swapping. There are 40 kinds of versions in QR code marks, version1, version2 version40, separately. Dimension of version1 is 21 modules x 21 modules, dimension of version2 is 25 modules x 25 modules, and so on, each version is 4 modules more than the prior one, until version 40. Dimension of version 40 is 177 modules x 177 modules (module refers to every piece of black or white little square).

2.2 Reading Principle

The reading process of QR code is divided into 3 parts: QR code image pre-processing, QR code recognition and

QR code decoding. The main task of QR code image pre-processing is to location QR code in the images which have collected; QR code recognition mainly utilizes image recognition to get bar code mark matrix of each modular unit, then transform the mark matrix into one-dimensional bye stream; QR code decoding get the information data which stores in QR code mark matrix by means of error correction.

Because of uneven brightness, non-standard operation and complex environment, original two-dimension code image exists problems like unbalanced brightness and different kinds of noise pollution, these are all not benefit to bar code image recognition. At present, a desirable way is to make image binarization and only retains useful information. The ultimate purpose of image pre-processing is to transform the original image into binary image, binarization process can remove many irrelevant information. In order to avoid redundant operation, ignore image filtering dispose when in image pre-processing phase. So the main task of image pre-processing phase is image binarization.

Image binarization is a transition process from original gray level image to binary image, binary image is a kind of image whose whole pixels are only have black and white condition. In digital image, for a 8-bit pixel depth image, its grey level range is 0255, its color makes transition from black to white. Compared with colored image and grey level image, it only needs 1 bit memory space in every pixel bit of binary image. So it has small memory spaces, fast processing speed, and makes Boolean operation conveniently. Owing to easy and highlighted information in image, it can be easier to obtain geometrical characteristic and other characteristic of target area, such as describing boundary of target area, obtaining location and size of given target area. These characteristics are all benefit to bar code recognition, so image binarization is very important to bar code recognition.

Image binarization has been widely used in image segmentation technology, it has K-means method, thresholding method and so on. At present, it mainly applies thresholding method. Image thresholding segmentation applies the gray property differences between image objectives and backgrounds, by means of choosing a proper threshold value to determine every pixel should belongs to objective area or background area, and give gray value ”0” or ”255”, transform original gray level image into binary image. There are three steps in thresholding segmentation: determine threshold, compare with threshold value, pixel classification. Suppose a input gray level image , and output a binary image , if the image segmentation threshold value is T, then

$$g(x,y)) = \begin{cases} 0 & \text{if } f(x,y) < T \\ 1 & \text{if } f(x,y) \geq T \end{cases} \quad (1)$$

Otsu method is a kind of global threshold segmentation method presented for Otsu in 1979. This method applies threshold of one-dimensional gradation histogram to make image segmentation, it is automatic, nonparametric and unsupervised. Because of its easy calculation and impregnability, it is regarded as the best method of automatic threshold selection. The core idea of this calculation is that the best segmentation threshold should make the weighted sum between variance of the two groups which are separated from threshold, and weighting coefficient of each group is probability. In other words, obtaining threshold can make the class maximum variance between objective area and background area.

Suppose that the image has L-level gray scale in total, probability of every level (p_i) is as follow:

$$p_i = n_i/N, p_i \geq 0, \sum_{i=1}^{L} = 1 \quad (2)$$

Among them, n_i is pixel amount of this level,N is pixel amount of image. If the gray level value of segmentation threshold is k, gray level probability of objective and background, and expectation of both are as follows:

$$\omega_0 = \sum_{i=1}^{k} p_i = \omega(k) \quad (3)$$

$$\omega_1 = \sum_{i=k+1}^{k} p_i = 1 - \omega(k) \quad (4)$$

$$\mu_0 = \sum_{i=1}^{k} ip_i/\omega_0 = \mu(k)/\omega(k) \quad (5)$$

$$\mu_1 = \sum_{i=k+1}^{k} ip_i/\omega_1 = \mu_T - \mu(k)/1 - \omega(k) \quad (6)$$

So inter class variance between objective and background (${\sigma_B}^2$) can be expressed as follows:

$${\sigma_B}^2 = \omega_0(\mu_0 - \mu_T)^2 + \omega_1(\mu_1 - \mu_T)^2 = \omega_0\omega_1(\mu_1 - \mu_0)^2 \quad (7)$$

$${\sigma_B}^2(k) = \frac{[\mu_T\omega(k) - \mu(k)]^2}{\omega(k)[1 - \omega(k)]} \quad (8)$$

When ${\sigma_B}^2(k)$ gets the maximum, the gray level value k is threshold value T. That is as follow:

$${\sigma_B}^2(T) = max{\sigma_B}^2(k), 1 \leq k \leq L \quad (9)$$

2.3 QR code encryption techniques

In order to overcome decoding and reproduction when QR code transfers in physical space, it utilizes cryptographic technique to encrypt QR code and improve security. Original QR code encryption techniques are only easy bitwise XOR, it is not encryption strictly. Therefore,

it is a must to provide deep encryption to QR code when in specific area, it means adopt password anti-counterfeiting technology to improve QR code security and confidential procedures.

A group of disguise rules (or mathematical translation) of realizing information encryption are called encryption algorithm, and a group of recovering disguise rules (or mathematical inverse translation) of decryption are called decryption algorithm, encryption algorithm and decryption algorithm usually under the control of a y group of secret key, they are called encryption key (record k_e) and decryption key (record k_d). Refers plaintext to m, cipher text to c, encryption algorithm to D, decryption algorithm to then encryption also records as follow:

$$c = Ek_e(m) \tag{10}$$

According to whether people utilize between encryption and decryption they encountered the same pair, it can be divided into two kinds of cryptography: symmetric cryptography and asymmetric cryptography. In order to overcome For applications to QR code general area, it can utilize RSA public key cryptosystem, and according to information safety procedure requirements to select encryption key. At present, it can reach 2048 bytes internationally; domestic application systems mostly use 512 bytes. If applies 1024 bytes, for the present computing facilities, it needs 20 years above to decode. If requires higher encryption, it can select ECC, new results suggest that ECC can handle 1000 times per second and more complicated. Take safety into consideration, it can select safe elliptic curve optionally, such as elliptic curve based on $K = GF(p), p = 2^n$, $y^2 = x^3 + ax^2 + b$.

It can select a and b randomly on $K = GF(p)$, applying elliptic curve based on finite field can realize data encryption, key exchange, digital signature, and so on.

For encryption and decryption of QR code, it must according to specific design requirement to add decryption scheme.

3 Main content and scheme of research

Main research of this subject is digitization technology of paper forming process. In the process of paper forming, it is about to control magnetic fiber in pulp.

In the process of pulping, add magnetic fiber and mix it up; in pulp flowing process, use magnetic code controller to control magnetic fiber which has impact on pulp, magnetic code controller is located on the wet end, it includes input module, transition module memory module and processing module. Input module connects with transition module, it is used for inputting decimal number; transition module connects with memory module, it is used for transforming input number into 8421 code; processing module connects with memory module, it is used for controlling code magnetism of magnetic encoder; the encoding region of this magnetic encoder is a rectangle, the width is width of paper web, magnetic stripes are distributed at regular intervals in encoding region. Magnetic encoder utilizes electricity to control magnetism of each magnetic stripe. When the pulp flows through encoding control region, the magnetic fiber in pulp will gather under the partition that corresponds to the magnetic controller in the action of magnetic field, thus it will from magnetic bar code inside of the paper as shown in Fig. 1, Fig. 2 and Fig. 3.

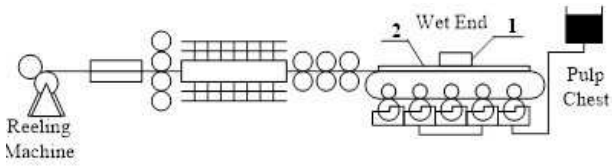

Fig. 1: Sketch map of papermaking process.

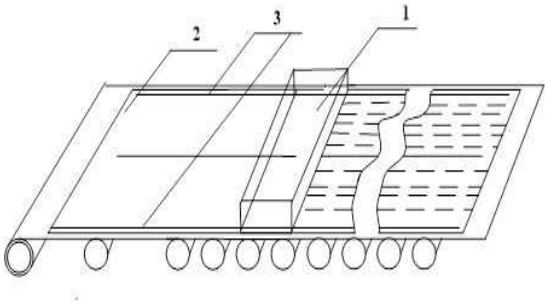

Fig. 2: Sketch map of wet end reconstruction.

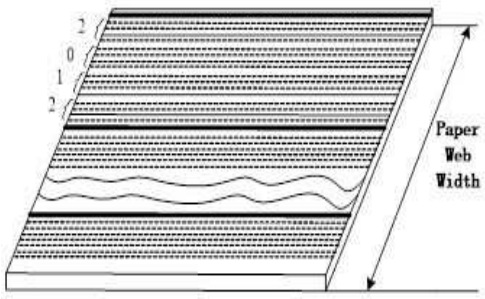

Fig. 3: Sketch map of fiber embedded characters.

4 Technological difficulties and intended solution

When researching fiber digitization technology of paper forming process, it may face some technical problem such as proportion of magnetic fiber, flocculation problems of magnetic fiber, encryption and decryption of one dimensional code and QR code, and so on.

For proportion of magnetic fiber, it can not influence the deflection and toughness after adding magnetic fiber by trial and error.

For flocculation problems of magnetic fiber, it will adopt ”partition” which is under the magnetic controller.

For encryption and decryption of one dimensional code and QR code, it will adopt programs like encryption before coding, coding before encryption, double-encryption, manual encryption and combined encryption, and so on. The specific research method and technology roadmap are as follows:

(1) Do trial test, ensure the proportion of magnetic fiber by repeated adjustment to make the deflection and toughness will not change after adding magnetic fibers.

(2) Adopt ”partition” which is under the magnetic controller to solve the flocculation problems.

(3) Adopt one dimensional code and QR code to embed the pattern into pulp fibers.

(4) For patterns, it will adopt programs like encryption before coding, coding before encryption, double-encryption, manual encryption and combined encryption, and so on.

(5) Other problems

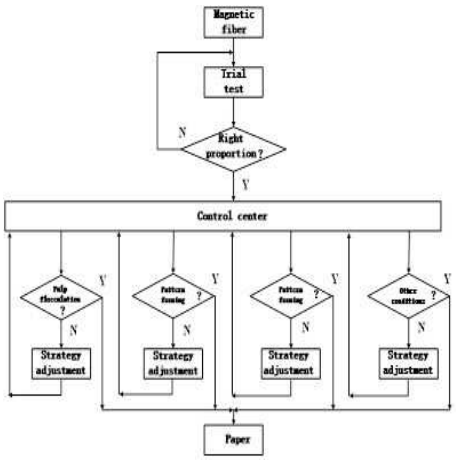

Fig. 4: Technology roadmap.

5 Expected result

With the help of advanced papermaking method and control theory, solves identification problem of paper and enhances reliability and uniqueness of paper identification, by means of digital technology to make paper identity uniquely, finally makes research program practicable. It will provide theoretical direction for uniqueness and reliability of specialty paper identification.

6 Acknowledgments

This research is supported by Grants from the National Natural Foundation of China and Graduate Innovation Fund of Shaanxi University of Science and Technology. The National Natural Foundation of China: ”Study on Chemical Mechanisms of Cellulose Fibrillation and Its Correlation with Properties of Fluff Pulp”, No: 1170559.

References

[1] Qi Lu, Ye Jianzhong, Zou Jianzhu. Study on properties of magnetic fiber materials [J]. JOURNAL OF TIANJIN POLYTECHNIC UNIVERSITY, **23**, 22-25 (2004).

[2] Tang Aimin, Zhang Hongwei, Chen Gang,etc. Preparation of Cellulose/Magnetic Nano-Composites by in-Situ Compounding[J]. TRANSACTIONS OF CHINA PULP AND PAPER, **21**, 66-70 (2006).

[3] Zhou Junfeng Magnetic Fiber and Paper for Information Storage. WORLD PULP AND PAPER, **25**, 30-35 (2006).

[4] Nanometer Ferromagnetic Paper-a kind of paper which can manufacture micro-robot. Nanotechnology, **17**, 59 (2010).

[5] Liu Renqing, Huang Yanyi. Electromagnetic Specialty Paper. HUBEI PULP AND PAPER, 43-44 (2006).

[6] Liu Yue, Liu Mingye. Research on Data Encoding of Two-Dimensional QR Code Barcode[J]. TRANSACTIONS OF BEIJING INSTITUTE OF TECHNOLOGY, **25**, 352-355 (2005).

[7] Niu Xiamu, Huang Wenjun, Wu Di, Zhang Hui. Information Hiding Technique Based on 2D Barcode[J] ACTA SCIENTIARUM NATURALIUM UNIVERSITATIS SUNYATSENI, **43**, 21-25 (2004).

[8] Otsu. A thleshold seleetion method from gray-level histograms[J]. IEEE Transaetions on Systems Man and Cybernetics, **9**, 62-66 (1979).

[9] Shi Shulan, He Fuwang. Analysis and Detection of Pulp and Paper [M]. Beijing: China Light Industry Press, (2006).

[10] GLong Yanquan. Paper Principle and Engineering [M]. Beijing: China Light Industry Press, (1994).

Zhijian Li was born in September 1964, native of Shaanxi. He began working in July 1987. Now he is a Professor and PhD supervisor. In July 2010, he was appointed the Dean of the College of Paper Making Engineering of SUST. He served as the Director of Paper Making Department (2002.9-2003.4), the Deputy Director of the Office of Educational Administration (2003.5-2008.6), and the Director (2008.7-2010.6). He is the Vice President of Shaanxi Paper Industry Technical Association, member of Management Branch of China Society for Higher Education, and one of the experts in Shaanxi Environmental Protection Agency. He is also an advanced research scholar in Australian National University.

Kaisheng Zhang was born in 1963. He is a professor in SUST and in-service studying for his doctorate. He was engaged in teaching and research for over 20 years, published over 40 articles at home and abroad, 21of them are indexed by ISTP and EI. His three items obtained patent. He charged several teaching and researching programs, one of the programs- quantitative control of paper waterpassed the test of Light Industrial Products Department, won the Silver Medals in trade fair for Light Industrial Products and was listed into the key popularization plan.