Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(5): 665-668

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Digital wartermarking based in normalized feature area

Zhongjie Xiao

School of mathematics and computers, Wuyi University,FuJian,China

---

ABSTRACT

With the rapid development of internet and digital technology,digital products become more and more popular,especially due to they can be transmitted conveniently, but the Problem of copyright Protection is also more and more serious.The inapplicability of traditional information security technology for copyrights problem promotes the development of digital watermark. From MIBIN theory, some solutions to these problems are given in this paper.

Keywords:digital; copyright;watermark technology

INTRODUCTION

In order to solve the problem of information security and copyright protection effectively, in recent years,a variety of technologies of the encryption, digital signature, digital fingerprints, water printing are proposed[1].Digital watermarking is a new technology in the 1990s, it determine the ownership of the digital products or testing numbers primitiveness through embedding the watermark information to in the digital products.It makes up deficiency that the encryption technology cannot be used to get further protection to decrypted data,also makes up weaknesses that digital signature can't be used to embed a large number of information in original data,and the limitation rights destroyer information offered by the digital fingerprint.This paper classifies its application research status and the existing problems, by analyzing the characteristics of digital watermarking, puts forward the possible research direction in the future.

THE CHARACTERISTICS, CLASSIFICATION AND APPLICATION OF DIGITAL WATERMARK

Digital watermarking technology which embed specific digital information (such as identity information, serial number, text or image symbols, etc to a variety of digital products such as image audio, video or software etc in order to achieve information security and copyright protection.Digital watermarking is digital signal embedded in the digital works, the existence of the waterprint obey the principle which does not destroy the original works appreciation and the usage value.

FUNDAMENTAL FEATURE GENERAL FEATURES

(1)Invisibility

Digital watermarking embedding should not make perceivable changing in the original data,also can't feel the protected data distortion occurring on the quality.

(2) Robustness

Digital watermarking embedding should not make perceivable changing in the original data,also can't feel the protected data distortion occurring on the quality, or immunity,robustness.Refers to the embedding watermark ability which can detect the watermark after various processing intentionally or unintentionally.Possible actions include processing geometric distortion, lossy compression, information processing, etc. Possible attacks include forgery attack and collusion attack.

(3)Security safety
Digital watermarking should be hard to forge or process,and individuals without authorized may not read and modify the watermark.the ideal situation is that customer without authorized will not be able to detect the watermark whether existing in the product.

(4)certainty
The watermark should provide reliable, unique and definite evidence for the authenticity of a digital works,and it is evidence with legal force.which actually is the basic force to develop watermarking technology[2].

THE CLASSIFICATION OF DIGITAL WATERMARKING

Digital watermarking technology has the following methods from different angles:

(1)According to the application of media,it can be divided into text watermark, image watermark, audio watermarking and video watermark.(2)According to the watermark characteristics, it can be divided into visible watermarking and invisible water print.Invisible watermarking is the most commonly used watermarking technology, it takes advantage of the characteristics of the people visual system and makes the watermark hidden in the data which cannot be to be distinguished by the naked eye.It can be divided into fragile watermarking, and fragile watermark and robust watermark.(3)Generally speaking, the plaintext watermarking robustness is strong, but its application is confined by the cost of storing restrictions. Most digital watermarks in academic research are blind watermarks[3].

THE APPLICATION AREAS OF DIGITAL WATERMARK

Digital watermarking is mainly used in the following respects:

(1) Copyright protection
The owners of the digital works produced watermarks using available key, and embed them in the original data, and then release the watermark version .When the works are piracy or copyright disputing,the owners can obtain watermark signal from pirated works so as to protect the rights and interests.

(2) Digital fingerprinting
To prevent unauthorized copying and distribution, digital work copyright owners can identify user information in the way of embedding different watermark to different user works.The watermark can be generated according to the user's serial number and relevant information, if unauthorized copy is founded,you can determine its source according to the fingerprints from the recovering copy。

(3) The authentication and integrity check
Usually fragile watermark is adopted,when the digital content inserted by watermark is tested,you must use a unique key associated with the data content to extract the watermark, then take a test to extract the watermark integrity to verify the integrity of digital content.Its advantage is that the certification integrated with the contents,Thus the process is simple.

DIGITAL WATERMARKING SCHEME

Digital watermark embedding
W denotes the digital watermarking, X and -X represents point coordinates in a centrosymmetric way,Wx is watermark in point x. by adopting the method of superposition,the formula of digital watermark embedding is：

$$A_X^{'} = A_X + K(w_X)L_X$$

Where,Ax is composed of four points in host image,corresponding to the embedding neighborhood matrix of digital watermark pixel X.Neighborhood embedding strength is $L_X = \sigma\overline{\theta_X}$, among which constant is embedded intensity adjustment reason, $\overline{\theta_x} = (\theta_x + \theta_{-x})/2$ is intensity mask, through the brightness $I = mean(A_x)$ $Tex = \mathrm{var}(A_x)$, $Ctr = \max(A_x) - \min(A_x)$, determine $\theta_x = f(I, Ctr, Tex)$, $K(w_x)$ as the template mapping function.

Am and Am take as the embedding and extracting template at the same time which is used to embed and extract 1 and 0 respectively.With the adjacent four points embedding a watermark, visible embedded information meet the requirements of the theorem.The embedding steps are as follows:

(1)In order to enhance the stability of the normalized image to noise attacks, first of all,preprocessing to make smooth image.

(2)In order to improve the stability of the normalized image, grayscale histogram equalization after smoothing pretreatment.Smoothing and gray histogram equalization are intermediate processing steps,the purpose is to eliminate noise and disorder of gray histogram adjustment to point extraction, and acquire more stable normalized image ,so it does not affect the result of the embedded watermark image finally[4].

(3)The feature points are extracted after preprocessing,and determine feature area according to feature points.

(4)Normalized matrix An is obtained by normalizing the area ,normalized feature is obtained by the An.

(5)Embedding digital watermark in the region of the normalized features.

(6)To get anti-normalized matrix an by normalized matrix An,normalization of embedding digital watermark areas are normalized to get the original size and shape features area;

(7)The original image embedded watermark image is obtained by using the characteristics area to cover the relevant area of original image.

AP stands for smooth processing,GLHE is image gray histogram equalization,MIBIN is image normalization based on invariant moments,IMIBIN represents the anti-normalization,FPE expresses feature point extraction,FAE is feature area extraction,FPE expresses feature point extraction,FAE is feature area extraction,Io is the original image,Iw denotes digital watermark image[5].

The function diagram of embedding the digital watermark is as shown in fig.1

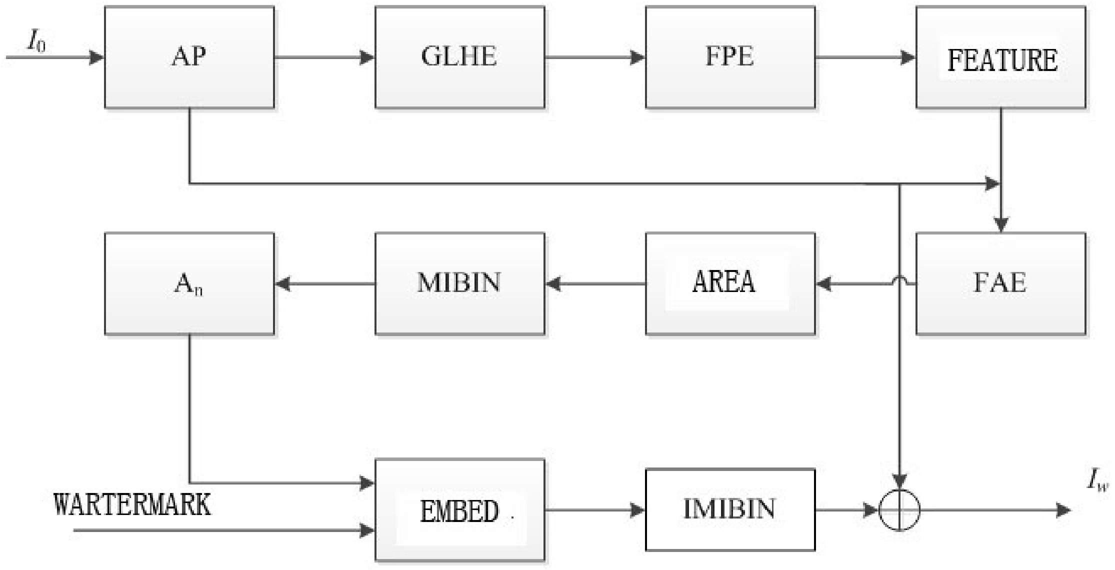

Fig .1 digital watermark

THE INITIAL AND BOUNDARY VALUE PROBLEMS

For non-degenerate semiconductors, equilibrium carrier density p_0 、 n_0 meet $p_0 n_0 = n_i^2$. For the N type semiconductor

$$\begin{cases} p_0 = \frac{1}{2}\left(-N_D + \sqrt{N_D^2 + 4n_i^2}\right) \\ n_0 = \frac{1}{2}\left(N_D + \sqrt{N_D^2 + 4n_i^2}\right) \end{cases} \quad (2)$$

For the P type semiconductor

$$\begin{cases} p_0 = \frac{1}{2}\left(N_A + \sqrt{N_A^2 + 4n_i^2}\right) \\ n_0 = \frac{1}{2}\left(-N_A + \sqrt{N_A^2 + 4n_i^2}\right) \end{cases} \quad (3)$$

Suppose Initial detectors working temperature value is T_0 ,the initial value of the heat balance carrier density is p_0 、n_0 . the initial value of electric field intensity is the electric field produced by the bias circuit in the detector, tat is $\frac{E_c \cdot R_D^0}{(R_D^0 + R_L)d}$. E_c is the electromotive force in the external circuit, R_L is the external resistor, R_D^0 is the initial value of the detector dark resistance, d is the detector thickness.

Photoconductive detectors have a semiconductor material, therefore, p 、n 、E only have two boundary, in the light of surface（$x = 0$）, $\partial p / \partial x\big|_{x=0} = 0$， $\partial n / \partial x\big|_{x=o} = 0$， there is no drop in the boundary surface, so $E\big|_{x=0} = 0$, the boundary on the back has the same boundary conditions. For temperature T, the boundary conditions are formulated according to the detector structure.

CONCLUSIONS

Although all kinds of watermarking algorithms such as bamboo shoots, but the research field of digital watermarking technology is still not mature, there are many problems need to be solved.Due to current digital watermarking technology is difficult to solve the problem of collusion attack, opportunity attack and interpretation attack,which makes the digital watermarking is limited in copyright protection, access and copy control, digital fingerprint application, many researchers are working to solve the above problem.In addition, the reliability and performance evaluation of digital watermarking algorithm requires more standard method, the watermark theory also needs to be more perfect, can foresee will likely become a multimedia digital watermark technology In the field of security technology base[6].

REFERENCES

[1] LiuYong Liang, Wen Gao. **2004** *IEEE International Conference on Multimedia and ExPo*(ICME),923-926.
[2] NaorM.Bit commitment using Pseudo-randomness, Proceedings of CryPto89,Springer.
[3]Modern CryptograPhy-Theory&Practice,Prentice Hall PTR,Prentice-Hall,Inc.Upper Sad dlerRiver,New Jersey 07458, **2003**.
[4]S.Craver. Zero-knowledge Watermark Detection[J].Information Hiding:Third International Workshop,LNCS1768,Springer-Verlag,**2000**,PP.101-116.
[5] YangWX,ZhaoY. *Signal Processing*,**2004**,20(3):245-250.
[6]QiSong,ZhuGuangxi,LuoHangjian. *IEEE International Symposium on Communications and Information Technology*,**2005**,vol.2:151 -154.