Digital Watermarking using Biometric Features

P.Vignitha[1] Ch. Sai Theja Swaroopa[2] TVL. Kalyani[3]
[1,2,3]Student
[1,2,3]SCSVMV University

Abstract— A digital watermark is digital data that can be embedded into all forms of media content, including digital images, audio, video and even certain objects. Special software is available for embedding imperceptible information via subtle changes to the data of the original digital content. Digital watermarks can be easily detected and read by computers, networks and a variety of digital devices, validating the original content and or initiating actions. Digital watermarking relates to a technology known as steganography, which literally means "covered writing." It is a technique designed to secure a message by hiding that message within another object so that it can be kept secret from everyone except the intended recipient. This is quite different from cryptography that renders the message) unintelligible to unauthorized viewers to prevent access. Steganographic messages may or may not be encrypted. Through many advances in the technology, steganography is now successfully used across a variety of industries. Digital watermarks provide the means of hiding steganographic messages for many different purposes.

Key words: Multimodal biometric, Unibiometric Watermarking, Security.

I. INTRODUCTION

We are living in the era of information where billions of bits of data is created in every fraction of a second and with the advent of internet, creation and delivery of digital data (images, video and audio files, digital sources and collections, web publishing) has developed many fold. Meanwhile reproduction a digital data is very easy and loose besides so, issues like, protection of moralities of the content and verifying ownership, arises. Digital watermarking is a technique and a tool to copyright laws for digital data. The field of watermark is that it remains complete to the refuge work even if it is copied. So to prove possession or copyrights of data watermark is extracted and verified. It is very difficult for criminals to eliminate or change watermark. As such the real holder can always have his data safe and secure. Biometric identification systems have recently gained considerable attention from the research community, since these systems have been used in various commercial applications such as surveillance and access control against potential imposters. Now a day, multimodality is a new and rapidly developing subject of research in the field of biometrics. Multimodal biometric systems are a type of pattern recognition systems, which identifies an individual on the basis of physiological or behavioral characteristics, like that fingerprint, face, iris, retina, palm, voice, and vein. In order to recognize individuals, multi-biometric systems use more than one biometric trait. These systems provide higher recognition

rate as compared to Unibiometric systems that relay on only one biometric trait. The main aim of this paper to study different watermarking techniques.

II. EXISTING SYSTEM

The duplicate copy of a digital media is as good as the original and hence the issue of Piracy and copyright protection is alarming. Illegal production and unauthorized distribution of digital media has become a high alarming problem in protecting the copyright of digital media. Digital watermarking has been proposed as one of the solution for the copyright protection and digital right management. A watermark is designed for residing permanently in the original digital data even after repeated reproduction and circulation. An optimized watermarking embedding and extraction method is supposed to meet necessities of perceptual transparency, robustness to sustain signal processing attacks and also needs to be secure. Perceptual transparency means that the insertion of the digital watermark in the host image does not change the visibility of image. Robustness means that the embedded watermark survives even if the watermarked image is subjected to signal processing operations like filtering, histogram equalization etc. Security of a watermarking algorithm means that the watermark should be detected by authorized person only. All these issues are mutually conflicting and a proper algorithm has to be designed for optimizing these parameters. Some advanced methods have been proposed below.

III. PROPOSED SYSTEM

The two major ways of doing watermark are spatial domain and the robust transform domain. In this study, method for watermarking of digital images, with biometric data is presented. The usage of biometric instead of the traditional watermark increases the security of the image data. The biometric used here is iris. This paper proposes a method to establish joint ownership of digital images by embedding imperceptible digital pattern in the image. This digital pattern is generated from biometric features of more than one subject in a strategic matter so that the identification of individual subject can be done and the multiple ownership of the digital images can be established. This digital pattern was embedded and extracted from the image and the experiments were also carried out when the image was subjected to signal processing attacks. Coefficients of mid frequency band discrete cosine transform was used for embedding as these coefficients do not adversely affect the perceptual transparency and is also significantly robust to normal signal processing attacks. Experimental results indicate that the insertion of this digital pattern does not change the perceptual properties of the image and the pattern survives signal processing attacks which can be extracted for unique identification.

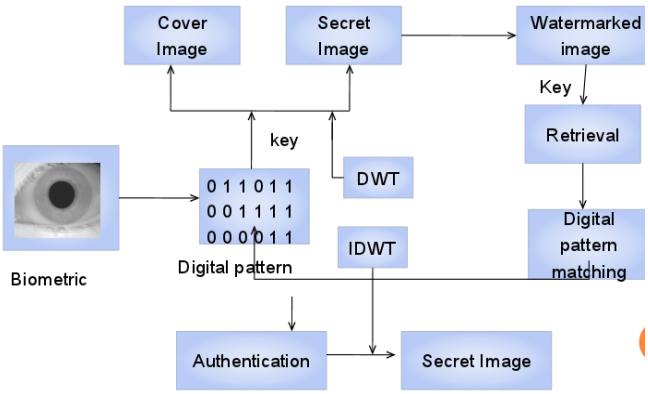

Fig. 1: Block diagram

IV. CLASSIFICATION OF WATERMARKING SYSTEMS

This section will discuss about the some of the popular watermarking algorithm that are used for multimodal biometric watermarking systems.

A. Modified Correlation based system:

This watermarking system uses modified correlation watermarking algorithm. The iris code is watermarked into face image using secret key. Before watermarking the cover image is pre-processed by using pre filtering techniques, the pre-processing increases the high result correlation. The face image act as cover image then iris is a watermark image. The additive pseudo random noise is applied to the biometric templates for watermark embedding. During watermark extraction the iris code extract from watermarked face image using same secret key and then calculate the correlation between noise pattern and watermarked image. If the correlation is greater than a certain threshold value, the watermark is decoded and a single bit is set. The entire image is divided into various blocks and performing the above procedure separately on each blocks even the attacks are present in this systems it gives high probability correct decision for decoding.

B. Modified 2D discrete cosine transform based system:

In this system the image is divided into 8×8 blocks and discrete cosine transform of the image is calculated on each blocks of image then find the lowest and highest frequency coefficient components of the image. so the DCT approaches for watermarking systems do not give some forms of attacks.

C. Redundant Discrete Wavelet Transform (RDWT) based watermarking system:

Mostly the discrete wavelet transform is used in image watermarking because discrete wavelet transform gives frequency information in stable form and it allow good localization both in time and frequency domain. Conversely The DCT having one of the main demerits is that the transformation does not provide shift invariance because of the down sampling of its band. The shift variance of the DWT leads incorrect extraction of watermarking systems so we need to know the precise locations of where the watermark information is embedded so the small shift variance cause the wavelet coefficient of the input image but The RDWT overcomes the shift variance problem.

D. Wavelet based watermarking system:

In this uses wavelet based watermarking techniques and it is based on the human visible system. The human visible system having the one essential characteristics that is Just Noticeable Profile (JND) which is used for watermark embedding to improve the imperceptibility of the system. First estimate the allowable visibility ranges of the JND threshold for all coefficient of the wavelet transformed image. The system deeds the range to calculate the adaptive strength to be covered in the wavelet coefficient while embedding watermark. Then the system exploits the artificial neural network which is used for remember the relationship between the original wavelet coefficients and its watermark version. During the extraction the trained artificial neural network used to calculate the watermark coefficient without use of the original image. It gives better performance compared to other watermarking systems.

E. Singular value Decomposition based watermarking system:

The SVD based algorithms mostly used in image processing and visualization it operates only on a positive matrix. The cover image considered as a matrix then the cover image matrix divided into three sub matrix with singular value decomposition and watermark image added with cover image matrix it having the singular values and it will generate watermarked image. The decomposition technique is applied to the watermarked image. Finally the watermark image decoded from cover image using decomposition method. This system gives the very good image stability and intrinsic algebraic image properties.

F. Particle Swarm Optimization based watermarking system:

In particle swarm optimization methods, the cover image divided into different blocks and calculates the best DCT coefficients for watermark embedding. A PSO algorithm maintains a swarm of particles where each particle indicates the optimal solution .This method does not required original image for watermark extraction. The main function of PSO is to reduce the robustness and improves the imperceptibility of the systems. After extraction the extracted image is good quality even if the attacks are present in the systems.

G. Compressive sensing theory based watermarking system

This system generate the measurement vector about the watermark templates by using the image transformation and measurement matrix and the measurement vectors embedded into the cover image. so the security is very difficult because it is very difficult to recover the secure biometric templates from measurement vector without Knowledge of original measurement matrix and image transformation.

V. METHODOLOGY

A. Host image:

In this module, we load the images from the local directory. Here the images refer to the carrier or host images. The images are read using Matlab commands like imread & resized as per the requirement. It is then converted to gray for further processing.

B. Biometric Key:

In this module, the Iris Biometric images from datasets are used for feature extraction. It involves below stages for feature extraction

- Segmentation
- Canny edge detection
- Circular Hough transform
- Normalization
- Trapezium normalization
- Feature Encoding

C. Logo image:

In this module, we load the secret images from the local directory. The images are read using Matlab commands like imread & resized as per the requirement. It is then converted to gray for further processing.

D. Watermarking:

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

VI. PSNR CALCULATIONS

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation. Image enhancement or improving the visual quality of a digital image can be subjective. Saying that one method provides a better quality image could vary from person to person. For this reason, it is necessary to establish quantitative/empirical measures to compare the effects of image enhancement algorithms on image quality. psnr & mse are calculated for watermarked Image & these values are compared for robust and are further processed

VII. CONCLUSION

The proposed method address joint ownership of digital water The method propose to generate watermark from the features multiple subjects. The choice of and the experimental results in satisfies the requirements of robustness. The PSNR watermarked image has been invisibility of the watermarking uses an important restriction in watermarks for unique recognition. A digital pattern to be used as extracted from the iris images of of watermarking was DCT based indicate that the proposed method of perceptual transparency and between the original and more than 30dB indicating effect.

REFERENCES

[1] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain" IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777–790, Jun. 2008.

[2] P. L. Lin, C.-K. Hsieh, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," Pattern Recognition, vol. 38, no. 12, pp. 2519–2529, 2005.

[3] Xinpeng Zhang, Zhenxing Qian, Yanli Ren, and Guorui Feng , "Watermarking With Flexible Self-Recovery Quality Based on Compressive Sensing and Compositive Reconstruction", IEEE Transactions On Information Forensics And Security, VOL. 6, NO.4, pp. 1223-1232, December 2011.

[4] Chih-Chin Lai and Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transactions On Instrumentation And Measurement, VOL. 59, NO. 11, pp. 3060-3063, Nov.2010

[5] Malay Kishore Dutta, Phalguni Gupta and Vinay K. Pathak "Blind Watermarking in Audio Signals using Biometric Features in Wavelet Domain", International Conference of IEEE Region 10,TENCON 2009, 2009, pp-1-5.

[6] Malay Kishore Dutta, Phalguni Gupta and Vinay K. Pathak "Biometric Based Unique Key Generation for Audio Watermarking"- International Conference on Pattern Recognition and Machine Intelligence, LNCS, Vol. 5909, 2009, pp- 458-463.

[7] Malay Kishore Dutta, Anushikha Singh, K.M.Soni, Radim Burget& Kamil Riha "Watermark Generation from Fingerprint Features for Digital Right Management Control", 36th IEEE

