Watermarking Digital Media with Encrypted Multi Modal Biometric

Mr B. Hariharan¹, S. Janani², P.M. BeemaParvin³ and C.B. Akshaya⁴
¹Professor, Department of Computer Science and Engineering, R.M.K College of Engineering and Technology
²,³,⁴UG Student, Department of Computer Science and Engineering, R.M.K College of Engineering and Technology

Abstract—A efficient digital watermarking algorithm is used from a encrypted biometric data. This biometric data is unique to everyone and can be logically owned to prove the ownership to digital media. So in that case we expose biometric as a watermark but it may not be secure hence in this paper proposes the method to encrypt the biometric data by using chaotic secret key to enhance the security. Thus this joint encryption and watermarking scheme helps us to address the ownership of digital media and keeps biometric secured. Arnold transformation is used for encryption and Discrete Wavelet Transform is used for watermarking in the image. Later the biometric extracted based on the watermark after decrypting the biometric was unique and was identified by feature matching algorithm and thus the ownership is proved.

Index Terms—Multimodel biometric fusion, Discrete Wavelet transform(DWT), Watermark, Arnold Transformation, Feature Matching.

I. INTRODUCTION

The multimedia data ownership problem has a solution. Embedding the watermark in audio signals or digital data is to be made in a way that it do not degrade the audibility or the originality of the signal. Applications of watermarking has many folds such that the copyright protection is to resolve the disputes on piracy, ownership proof, monitoring broadcast and secret communication. A watermark is designed for residing permanently in the original audio data even after repeated reproduction and distribution. A good watermarking algorithm should meet requirements of imperceptibility, robustness and security. Imperceptibility means that watermark is being embedded and it and it should be imperceptible that means the watermark should be embedded in a way that the watermark remains perceptually transparent. The watermark should be robust so that it can survive intentional and unintentional signal processing attacks. The watermarking algorithm is to be secure that means the watermark will only be detected by the person who is authorized. Thus these requirements are often contradictory with one other and there is a need to make a trade-off among themselves. There are some well known algorithms for watermarking in transform domain and in spatial domain. These methods have mainly focused in design of digital watermarking algorithms which maintains perceptual transparency of host signal and is robust in nature.

II. RELATED WORK

The processing of a two dimensional picture by a digital computer is termed as digital image. In this related work as considered in broader context, it implies digital processing of any two dimensional data. Thus a digital image is an array of complex numbers or real number represented by a number of bits that is finite. An image that is given in the form of a slide, transparency, X-ray or a photograph is first digitized and is stored in the computer memory as a matrix of binary digits. Then the digitized image is being processed and is displayed on a high-resolution television monitor. For displaying, the image is first stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second that produces a visually continuous display.

A digitizer converts an image into a numerical representation suitable for input into a digital computer. Thus the process is done using the digitizer. There are several digitizers they are Image dissector, Flying spot scanner, Micro - densitometer, Photo-sensitive solid- state arrays and Videocon camera.
III. OUTLINE OF IMAGE PROCESSING

Among many features, image processing is considered as the most discriminating feature of digitization. An image processor does the functions of storage, image acquisition, segmentation, preprocessing, representation, and recognition interpretation finally displays or records the resulting image.

The following is the block diagram that gives the fundamental sequence involved in an image processing system.

![Block Diagram of Fundamental Sequence Involved in an Image Processing System](image)

The first step in this process is the image acquisition by an imaging sensor in conjunction with a digitizer that digitize the image. The next step is the pre-process step where image is being improved being is been fed as the input to the next processes. Preprocessing means typically dealing with removing noise, enhancing, isolating regions etc. Thus Segmentation partitions the image into its constituent objects or parts. Segmentation is always produces the output raw pixel data, which consists of either the pixels in the region themselves or the boundary of the region. Then the process of transforming the raw pixel data into a form useful for subsequent processing by the computer is called represtation.

And description deals with extracting the features that they are basically in differentiating one class of objects from another. Recognition means that it assigns a label to an object based on the information that is provided by descriptors. Interpretation means assigning meaning to an ensemble of recognized objects. The knowledge about a problem domain is incorporated into the knowledge base. The knowledge base that guides the operation of each processing module and also it controls the interaction between the modules. Not all the modules need be present for a specific function. The composition of the image processing system depends on its own application. The frame rate of the image processor is normally around 25 frames per second.

Digital Computer: Processing mathematically the digitized image such as addition, averaging, subtraction, convolution, etc. and this is done by the computer.

Mass Storage: The secondary storage devices normally used in mass storage are CD ROMs, floppy disks etc.

Hard Copy Device: The device that is used to produce an image’s permanent copy and to the storage of the software that is involved.

Operator Console: It consists of equipment and the arrangements for verification of intermediate results and for alterations in the software as when required. Thus the operator is capable of checking for any errors that is produced and for the entry of requisite data.

IV. TECHNIQUES

We presented Digital image processing analysis that refers to processing the image in digital form. The digitalization process means quantization, sampling. Finally these images are processed by the five fundamental processes, or at least any one of them, but not necessarily all of them.

1) Image Enhancement improves the image’s quality like that it improve the image’s contrast and brightness characteristics.
2) Image restoration means that they are used to restore the images with some problems such as improper focus, geometric distortion, camera motion and repetitive noise.
3) Image analysis are the operations that produces graphical or numerical information based on original characteristics of the image.

4) Image compression and decompression that reduces the data content of the image that is to describe the image.

5) Image synthesis is the operation that creates images from other images or non-image data.

Approach and Description
Our Multimodel biometric framework is based on multimedia ownership problem. This is done by making several steps in which fusion, encryption, watermarking, feature extraction and feature matching. There are some well known algorithms to perform all these steps. Thus the algorithm for these modules have a major impact on each and every upcoming steps.

A. Multi Model Biometric Fusion:
1. Finger print:
   We enhance the quality of the image by cropping the fingerprint region in the given image and then performing the process called histogram which means equalize to increase the perception information.

2. Retinal:
   The input colour images are converted into corresponding gray images and then invert the gray image into inverted green channel in order to make the blood vessel to be more visible so that information can be clear.

3. Fingervein:
The finger images are noisy with rotational and translational variations resulting from unconstrained (peg-free) imaging. So segmentation of ROI, Translation and orientation alignment, Image enhancement to extract stable/reliable vascular patterns all these are performed to get a resultant image.

B. Chaotic Encryption:
   Arnold Cat Map is the algorithm that employs shearing and wrapping operation to completely scramble a matrix after several iterations. Arnold cat map is one to one mapping for encryption.

C. Feature Extraction:
   Haar wavelet technique is used to extract the features from the iris image. The inner iris boundary is localized on the iris image using circular Hough transformation. Once the inner iris boundary (which is also the boundary of the pupil) is obtained, outer iris is determined using intensity variation approach. The annular portion of iris after localization is transformed into rectangular block to take into consideration the possibility of pupil dilation. This
transformed block is used for feature extraction using Discrete Haar Wavelet Transform (DHWT).

D. Watermarking:
A discrete wavelet transforms (DWT) based algorithm is developed to use biometric based watermark for watermarking. The DWT is used to divide an image into different frequency bands, making it much easier to use middle frequency bands of an image for watermark embedding.

E. Feature Matching:
In mathematics, the Euclidean distance or Euclidean metric is the "ordinary" straight-line distance between two points in Euclidean space. With this distance, Euclidean space becomes metric space and it is associated with the norm is called the Euclidean norm. Older literature refers to the metric as Pythagorean metric. A generalized term for the Euclidean norm is the $L^2$ norm or $L^2$ distance.

$$d(p, q) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2}$$

$$= \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}.$$  

V. CONCLUSION
We present 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. The validation of such encrypted based biometric watermark has been done using a DCT based watermarking method. The method has PSNR above 25 dB and is robust to signal processing attacks. The feature points extracted from the recovered watermark have been uniquely mapped for identification. This clearly indicates a significant development in identification and proof of ownership for digital media. Future scope may deal to find other efficient ways of encryption and other biometric traits may be explored for generating digital watermark.

REFERENCES


