ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Palmprint Template Protection Using Watermarking

S.Sandhya, R.Shankari, A.Dhivyamalini

Assistant Professor, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India

Assistant Professor, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India

Assistant Professor, Dept. of ECE, Velammal Engineering College, Chennai, Tamilnadu, India

ABSTRACT: Security is an important aspect in the biometric system. Template is a very important part of biometric systems and attacker mostly attack on template, so securing them is a very crucial issue these days. In this thesis, our focus is on template security in biometrics. For our work we have chosen palm print image as the trait.

Initially, the pre-processing steps are applied to the palm print image for enhancement, then features are extracted. The concepts of texture feature and shape feature are considered for feature extraction. From the extracted features the template is created. Many Techniques like Cryptography, Steganography, Watermarking etc., are available to secure the biometric template. For our work, we have considered Watermarking using Least Significant Bit (LSB) algorithm for embedding the message/logo into the image. This work has been implemented through MATLAB

I. INTRODUCTION

A template is essentially a compact representation (a set of invariant features) of the biometric sample that is stored in system database. If the security of stored templates is compromised, the attacker can fabricate physical spoof samples to gain unauthorized access. Such efforts have been detailed in [1],[2],[3]. The stolen templates can also be abused for other unintended purposes, e.g. performing unauthorized credit-card transactions or accessing health related records.

Template security is of vital significance in the biometric systems because unlike passwords, stolen biometric templates cannot be revoked. Personal identity refers to a group of attributes that are linked with an individual such as name, social security number etc. Trustworthy identity management machinery is at once required to battle scourge expansion in identity theft and to have the improved security need in a diversity of utilizations varying from international border crossing to having personal information. Substitute representations of identity such as passwords and ID cards can be effortlessly mislaid, shared or stolen.Passwords can also be simply guessed using social engineering and dictionary attacks and gives very little security.

Biometric authentication, or rather biometrics, gives a likely and consistent answer to the quandary of identity revelation by making use of the identity of a person. Biometric systems by design find out or confirm a person's identity based on his anatomical and behavioral features such as fingerprint, face, iris, voice and gait and these traits cannot be easily lost or forgotten or shared or forged. Since biometric systems need the user to be in attendance at the time of authentication, it can also daunt users from making false denial claims.One of the most vital harmful attacks on a biometric system happens when it is against thebiometric templates. Attacks on the templates can direct to grave vulnerabilities where a template can be replaced by an impostor’s template to achieve unlawful access, or a physical spoof can be fashioned from the template [4],[5],[6] to achieve unauthorized access to the system, or the stolen template can be replayed to the matcher to have unauthorized access. Hence, biometric templates should not be stored in plaintext form and fool-proof methodologies are essentially needed to securely store the templates such that both the safety of the application and the users' solitude are not compromised by adversary attacks

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

II. RELATED WORK

The previous work in the security of biometric templates (ENCRYPTION BASED) tend to model the problem as that of building a classification system that separates the genuine and impostor samples in the encrypted domain [7] [8] [9]. Howevera strong encryption mechanism destroys any pattern in thedata, which adversely affects the accuracy of verification.Hence, any such matching mechanism necessarily makes a compromise between template security (strong encryption) and accuracy (retaining patterns in the data). The primary difference in our approach is that we are able to design the classifier in the plain feature space, which allows us to maintain the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security/privacy [10].Over the years a number of attempts have been made to address the problem of template protection and privacy concerns and despite all efforts, as A.K. Jain *et al.* puts it, *a template protection scheme with provable security andacceptable recognition performance has thus far remainedelusive*. [9]. Detailed reviews of the work on template protection can be found in Jain *et al.* [9], Uludag*et al.* [11], and Ratha*et al.* [12].

2.1 BIOMETRICS

The process by which a person's unique physical and other traits are detected and recorded by an electronic device or system as a mean of confirming identity is called biometrics. Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits.

2.1.1 TRAITS EMPLOYED IN BIOMETRICS

The traits employed in biometrics are physical traits and behaviouraltraits.Physical traits employed in biometrics are features of eye i.e.,Retina,Iris., Finger print, Palm print.Behavioural traits employed are Hand written signature, Key strokes or typing, Voice print, Gait, Gestures etc.

2.1.2CONDITIONS TO BE SATISFIED BY TRAITS

` The Conditions to be satisfied by the Traits are Uniqueness, Universality, Permanence, Collectability, Acceptability.Uniqueness indicates that any two person should be different enough to distinguish each other based on the adopted characteristics. Universality indicates that every person should have the characteristics. Permanence indicates that the characteristics should be stable enough and should not change within environment or time. Acceptability indicates to what extent people are willing to accept the biometric system. Collectability indicates characteristics can be measured quantitatively.

2.2 WHY BIOMETRICS

Biometrics provides a strong link between an individual and a claimed identity. Fraudulent multiple identities or identity fraud can be avoided. Representations of identities such as Passwords and ID Cards can be effortlessly mislaid, shared or stolen.Biometric traits cant be easily lost or forgotten or shared or forged, also requires user's presence at the time of authentication. Desirable factors of a good biometric system are accurate discrimination between individuals, ease of use, social acceptability, secure and robust against potential attackers.

2.2.1WHY PALM PRINT

The image of a human palm consists of palmar friction ridges and flexion creases.Latentpalmprint identification is of increasing importance in forensic applications since around 30% of the latent prints lifted from crime scenes (from knifes, guns, steering wheels) are of palms rather than of fingers. Similar to fingerprints, latent palm print systems utilize minutiae and creases for matching. While law enforcement and forensics agencies have always collected fingerprints, it is only in recent years that large palm print databases are becoming available.

Based on the success of fingerprints in civilian applications, some attempts have been made to utilize low resolution palm print images (about 75 dpi) for access control applications. These systems utilize texture features which

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

are quite similar to those employed for iris recognition. Palm print recognition systems have not yet been deployed for civilian applications (e.g., access control), mainly due to their large size.

Palm print provides greater level of security to personal authentication when compared to other traits like finger prints etc.Forensic departments prefer palm biometrics than finger prints because prints lifted from crime scenes are of palms rather than fingers. In palm print, system uses low resolution images but provides high accuracy. It needs very less co-operation from users for data acquisition. Compared to finger prints palm print provides large surface area, so more features can be extracted. It is a reliable human identifier because the print patterns are not found to be duplicated even in mono-zygotic twins.

III. PALM PRINT TEMPLATE CREATION

A typical biometric system comprises of several stages. The preprocessing stage acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. The feature extraction stage operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template. The template protection stage is used to enhance the protection of template.

Palm print recognition is one of the important biometric traits used among the people. Any palm print recognition process has the following major steps

- Image Preprocessing .
- Feature extraction .

3.1 PREPROCESSING

Preprocessing involves removal of noise from the image, extracting the shape and texture features.

Before extracting the central palm area, palm image can be filtered by using wiener filter. Wiener filter is used to remove noise. An image of the palm is shown in the figure 1

Figure 1 Palm Print Image

WIENER FILTER

Noises are classified into many types. These noises affect digital images by various methods. Noise is the result of errors in the image acquisition process that change value in pixels so we cant get the true intensities of the real scene.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

There are several ways that an image affected by noise depending on how the image is created.

If the image is scanned from a photograph made on film, here noise is introduced by film grain . Noise can also be the result of damage to the film,it can be introduced by the scanner in many digital devices. The mechanism for gathering the data in digital format (such as a CCD detector) can introduce noise. Transmission of image data by electronic mean scan introduce noise.

The main goal of the Wiener filter is to remove noises from a original signal, in our case image taken into consideration. Here weiner2 low pass filter is used.

This approach is used to better results than linear filtering. The adaptive filter is more selective than a linear filter because it preserves edges and other high-frequency parts of an image in accurate format. The wiener2 function carries all primary computations and implements the filter for an input image ,when compare to various filter. when compared to linear filtering wiener filter needs more time for computation.Wiener2 works best when the noise is constant-power ("white"), such as Gaussian noise. The noise free image obtained by using wiener filter is shown in figure 2

Figure 2 Noise free image

CENTRAL PALM AREA EXTRACTION

The noise-free image's pixels form a 2D vector P.After enhancing the palm print image. In many biometric systems preprocessing is the first block and , it is one of the most critical parts of the developed palm print recognition algorithm. Initially all images are obtained from the database should be preprocessed and the central area of a palm should be obtained. Preprocessing algorithm that will be used for this purpose should be selected such that the algorithm should be applicable to all images in the database and the desired area of the palm should be obtained with great accuracy. Otherwise, extracted features will not belong to the desired part of the palm; therefore accuracy of the developed palm print recognition algorithm would significantly decrease. In brief, accuracy of the preprocessing algorithm is very important, since possible errors in this block will affect subsequent blocks.

Before extracting the features from the palm image, we must extract the central palm area of the image I in the database D. Knowing the orientation of the hand is important for detecting the location of key points on the hand. There are several ways to find out the orientation of the hand. The orientation of the palm image varies based on the database. To fix a co-ordinate system ,the finger valleys (depression points present between fingers)are chosen with respect to which the palm image can be extracted.The line joining Y-axis and the X-axis in the lines are perpendicular to each other then only we can choose the finger points. Hence, to match two given palm images finger valley points are very important. This can be based on key point findings method. Once the co-ordinate axes are fixed, extracting the palm is relatively straight forward. One of the best approach is to extract a square region of fixed size from a palm. One of the ways to extract a palm is to taken at a fixed distance from the axis of a square sub-image of fixed size .

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

After reference points are located on rotated palm images, the next step is to extract the central palm area, which is the rectangular region. After rotation, the slope angle of the Yaxis is 90° therefore; the slope angle of the rectangular region's vertical sides is also 90°. This results in that the extracted rectangular region fits on the rectangular grid.

FEATURE EXTRACTION

For image identification and verification Feature extraction plays an important role . There are many features exhibited in a palm. By flexing hand and wrist in the palm, three principal lines caused ,which are named as heart line, head line and life line, respectively. A palm is normally divided into three regions, namely finger-root region I, inside region II and outside region III. The three marked curves, in the palm represents the three principal lines (heart line, head line and life line), respectively. The two endpoints,are often determined by the intersections of life line and heart line on both sides of a palm.

The locations of endpoints and their midpoint o in a palm remain unchanged with respect to rotation of the hand and the change of time because of the stability of the principal lines. Finally, these feature lines are regarded as reliable and stable features to distinguish a person from others. In our proposed method we extract 2 types of features such as 1) Shape feature and 2) texture feature.

DISCRETE WAVELET TRANFORM

One of the common wavelet transform is Discrete wavelet transform. A DWT is used to transform a images in discretely sampled wavelets

.The DWT consists of series of low and high pass filter.A signal is calculated by passing it through a series of low and high pass filters to obtain four sub bands. The output of DWT consists of one approximation band and three detailed bands belonging to low frequency and high frequency components respectively. The four sub bands of DWT are often called as approximation band, horizontal band, vertical band and diagonal bands are shown in Fig 3

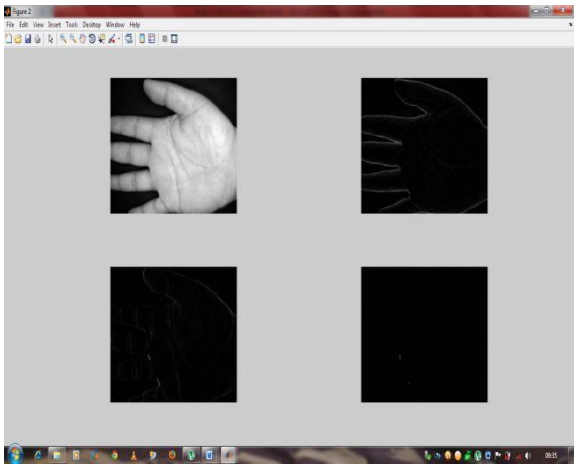

Figure 3.FOUR SUB-BANDS OF DWT

The significant information of palm print is present in the approximation band compared to other three high frequency component. In this discrete wavelet transform debauchies filter is used.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

SHAPE FEATURE

It is essential to locate the endpoints of each principal line for some palm print identification and verification systems.lots of ridges and fine wrinkles with various directions, lengths and thicknesses are present in human palm image.so that we can easily get the corresponding geometry features, such as width, length and area.LetIcp be the central palm image, and then apply morphological operations. Skeletonizing the central palm area, then perform thinning operation on the skeletonized image. After that, extract the patterns of each thinned palm images. The shape features $\hat{G}f$ is further used for palm matching. The length and thickness varies for each image in the database.

SOBEL FILTER

The problem in image processing is that the edge characterize boundaries. Edges in images are areas with strong intensity contrasts – a jump in the intensity from one pixel to the next.The useless information are filtered in edge detection ,while preserving the important properties in an image. though there are many ways to perform edge detection the various methods may be grouped into two categories, gradient and Laplacian.

The peak and less point in the first derivative of the image are used to detect the edges in gradient method .Zero crossings are used by laplacian method in the second derivative of the image to find edges. An edge has the one-dimensional shape of the ramp and calculating the derivative of the image can highlight its location.

Clearly, the derivative shows a peak located at the center of the edge in the original signal. This method of fixing an edge is one of the characteristic of the "gradient filter" family of edge detection filters and includes the Sobel method.

The pixel location are declared as an edge location if the gradient value exceeds some threshold. As mentioned edges might have higher pixel intensity values than those surrounding it. So once a threshold is set, you can compare the gradient value and the threshold value and detect an edge whenever the threshold is exceeded. Furthermore, when the first derivative is to a peak, the second derivative is zero. As a result, another alternative to finding the location of an edge is to fix the zeros in the second derivative.

Based on the mentioned one-dimensional analysis, the theory can be carried over to two-dimensions as long as there is an perfect approximation to calculate the derivative of a two-dimensional image. The Sobel operator performs a 2-D spatial gradient measurement on the image. Typically they are used to find the approximate absolute gradient magnitude at each point in an input grayscale image. It will use a pair of 3x3 convolution masks, one estimating the gradient in the x-direction (columns) and the other in the y-direction (rows). The convolution mask is usually much smaller than the actual image. As a result, the mask is creeped over the image, manipulating a square of pixels at a time. Figure 4 shows the shape feature of the image.

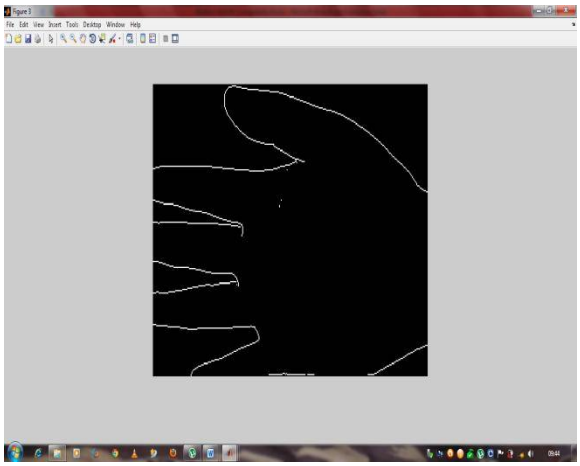

Figure 4 shape feature

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

TEXTURE FEATURE

High-order description of the local image content is provided by the texture. The analysis of texture requires the identification of those texture attributes which could be used in segmentation, discrimination, recognition or shape computation. Historically, the structural and statistical approaches have been adopted for texture feature extraction. The structural approach assumes that these texture is characterized by some primitives following a placement rule.

one has to describe both the primitives and the placement rule of a texture. The description should be sufficiently flexible so that the class of equivalent textures can be generated by using similar primitives in similar relationships. Although there are reported progress in this area, the approach is restricted by the complications encountered in determining the primitives and the placement rules those operate on these primitives. Therefore, textures suitable for structural analysis are confined to quite regular textures rather than more natural textures in practice.

IMAGE SEGMENTATION

The way of partitioning a digital image into multiple segments (sets of pixels, also known as superpixels) is known as Image Segmentation. The main goal of segmentation is to simplify and/or change the representation of an image into something that will be more meaningful and easier to analyze. Image segmentation is typically used to locate the objects , lines, curves, etc. in an images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that these pixels with the same label share certain visual characteristics.

The outcome of image segmentation are a set of segments that collectively cover the entire image, or a set of contours being extracted from the image. Each of the pixels in a region are similar with respect to the characteristic or computed property as color, intensity, or texture. Adjacent regions are significantly different with respect to the same characteristics. Entropy filter is used in image segmentation. Entropy is a statistical measure of randomness.

ENTROPY FILTER:

J = entropyfilt(I) gives the array J, where each output pixel contains the entropy value of the 9-by-9 neighborhood around the corresponding pixel in the given input image I.I can have any dimension. If I has more than two dimensions, entropyfiltertreats it as a multidimensional grayscale image and not as a true color (RGB) image. The output image J is the same size as the input image I.

For the pixels on the borders of I, entropyfilt uses symmetric padding. In symmetric padding, the values of padding pixels are a mirror reflection of the border pixels in I. Figure 5 shows the texture feature of the image.

Figure 5 Texture feature

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

TEMPLATE PROTECTION-WATERMARKING

Digital watermarking is defined as one of the process of embedding data (watermark) into a multimedia object to help to protect the owner's right to the object. The embedded data (watermark) may be either visible or invisible. n the visible watermarking of images, the secondary image (the watermark) is embedded in a primary image such that the watermark is intentionally perceptible to the human observer whereas in the case of invisible watermarking the embedded data is not perceptible, but can be extracted by a computer program. Some of the expected characteristics of watermark are listed in [13],[14],[15].Figure6 shows the watermarked image.

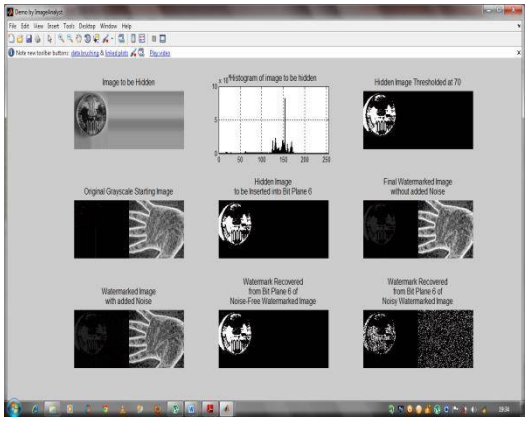

Figure6 watermarked image

IV. CONCLUSION

This paper accord with the watermarking strategy of extracting video frame and it is tested by assorted intrusion. Embedding process on the authentic video frame and watermarked video is extracted without affecting image quality. A watermark is extracted and its robustness are verified by using normalized correlation. The proposed scheme is based on two level discrete wavelet transform in affiliation with independent component analysis. From the Experimental results we conclude that our technique is robust against attacks, thus providing better results in case of Copyright Protection and Ownership Identification

REFERENCES

[1] Adler A (2004) "*Images can be reconstructed from quantized biometric match score data*". Proc. Canadian Conf Electrical Computer Eng, Niagara Falls: 469-472
[2] Ross A, Shah J, and Jain AK (2007) "*From templates to Images: Reconstructing fingerprints from minutiae points*". IEEE Trans Pattern Anal Mach Intell, vol. 29, no. 4: 544-560
[3] Feng J and Jain AK (2009) "*FM Model Based Fingerprint Reconstruction from Minutiae Template*". Proc. ICB 2009, Alghero, Italy: 544-553
[4] Andy Adler, "*Images can be Regenerated from Quantized Biometric Match Score Data*", InProceedings Canadian Conference on Electrical and Computer Engineering, pp. 469-472, 2004.
[5] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, " *Fingerprint Image Reconstruction From Standard Templates*", IEEE Transactions on Pattern Analysis and Machine Intelligence,Vol.29, No.9, pp.1489-1503, 2007
[6] Kumar A (2008) Incorporating cohort information for reliablepalmprint authentication. ProcICVGIP 2008: 583-590.
[7] F. Farooq, R. M. Bolle, T.-Y.Jea, and N. Ratha, "Anonymous andrevocable fingerprint recognition," in *CVPR Biometrics Worshop*, Jun.2007, pp. 1–7.
[8] A. Teoh, D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *PatternRecognition*, vol. 37, no. 11, pp. 2245–2255, November 2004.
[10] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP*, vol. 8, no. 2, pp. 1–17, 2008.
[11] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Efficient biometric verification in the encrypted domain," in *Third International Conference on Biometrics*, Jun. 2009, pp. 906–915.
[12] U. Uludag, S. Pankanti, S. Prabhakar, and A. K.
Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92,no. 6, pp. 948–960, Jun. 2004.
[13] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis*

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

&Machine Intelligence (PAMI), vol. 29, no. 4, pp. 561–572, Apr. 20

[l3] M.M. Yeung, et al., "Digital Watermarking for High-Quality Imaging", Proc. IEEE First Workshop on Multimedia Signal Processing, June 1997, Princeton,New Jersey, pp- 357-362.

[14] F.Mintzer, et al., "Effective and Ineffective Digital Watermarks", IEEE International Conference on Image Processing, ICIP-97, 1997, Vol.3, pp. 9-12.

[15] I.J.Cox, et al., "Secure Spread Spectrum Watermarking of Images, Audio and Video", Proc. IEEE International Conference on Image Processing, ICIP-96, 1996,Vol.3, pp.243-246.