Secure Biometrics and Biometric Types

Punitha M, 2nd sem, MTech, SJBIT, Bangalore,
Mr.Shanthakumar H C, Asst.Prof,
Dept of Computer Science and Engineering,
SJBIT, Bangalore-60
Punithamahadevappa92@gmail.com

***Abstract*: Biometrics are an important and widely used class of methods for identity verification and access control. Biometrics are attractive because they are inherent Properties of an individual. They need not be remembered like passwords and are not easily lost or forged like identifying documents. At the same time, biometrics are fundamentally noisy and irreplaceable. The two types of biometric modals are : (1) Unimodal Biometrics, (2) Multimodal Biometrics. The example discussed in this report is for Unimodal and multimodal biometrics are (a) Iris recognition is a popular technique for recognizing humans (b) Multimodal sparse representation method. When this two methods fails to identify and verify the biometric feature. A new technique finger-vein recognition system is being proposed to identify and verify a human being.**

Keywords: Secure biometrics, Types of biometrics, Unimodal biometrics, Multimodal biometrics, Finger-vein recognition system.

I. INTRODUCTION

Biometrics are an important and widely used class of methods for identity verification and access control. They need not be remembered like passwords and are not easily lost or forged like identifying documents. At the same time, biometrics are fundamentally noisy and irreplaceable. There are always slight variations among the measurements of a given biometric,and, unlike passwords or identification numbers, biometrics are derived from physical characteristics that cannot easily be changed. The proliferation of biometric usage raises critical privacy and security concerns that, due to the noisy nature of biometrics, cannot be addressed using standard cryptographic methods. In this article, we present an overview of secure biometrics, also referred to as biometric template protection, an emerging class of methods that address these concerns.

The traditional method of accommodating measurement variation among biometric samples is to store the enrollment sample on the device and to match it against a probe provided by the individual being authenticated. Consequently, much effort has been invested in the development of pattern recognition algorithms for biometric matching that can accommodate these variations. Unfortunately, this approach has a serious flaw: an attacker who steals or hacks into the device gains access to the enrollment biometric. In conventional password-based systems, this type of problem can be mitigated by storing a noninvertible cryptographic hash of the password rather than the password itself. However, cryptographic hashes are extremely sensitive to noise and thus incompatible with the inherent variability of biometric measurements. Therefore, the above approach used for securing passwords is ill suited to biometric security.

The loss of an enrollment biometric to an attacker is a security hazard because it may allow the attacker to gain unauthorized access to facilities, sensitive documents, or the finances of the victim. Further, since a biometric signal is tied to the unique physical characteristics and identity of an individual, a leaked biometric can result in a significant loss of privacy. The article, refers to a security breach as an event wherein an attacker successfully accesses a device. It refers to a privacy breach as an event wherein an attacker partially, or completely, determines the victim's biometric. Security and privacy breaches represent distinct kinds of attacks.

Addressing these challenges demands new approaches to the design and deployment of biometric systems. Research into secure biometrics has drawn on advances in the fields of signal processing, error correction coding, information theory, and cryptography. Four main architectures dominate: fuzzy commitment, secure sketch, secure multiparty computation, and cancelable biometrics. The first two architectures, fuzzy commitment and secure sketch, provide information-theoretic guarantees for security and privacy, using error correcting codes (ECCs) or signal embedding's. The third architecture attempts to determine the distance between enrollment and probe biometrics using computationally secure cryptographic tools such as garbled circuits and homomorphic encryption.

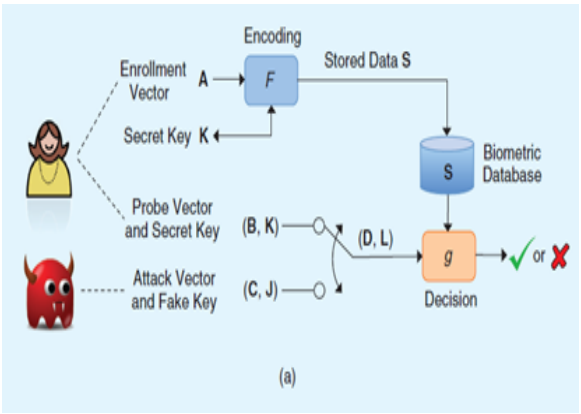


Fig 1: Secure biometrics framework.

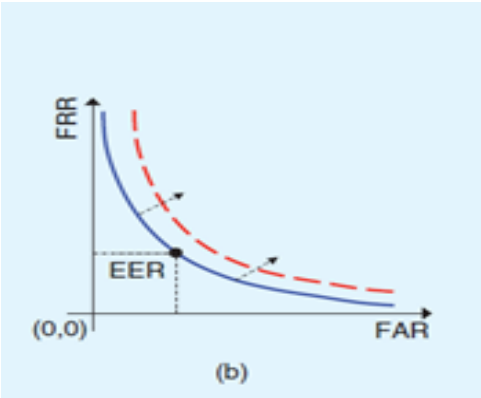
The final architecture, cancelable biometrics, involves distorting the biometric signal at enrollment with a secret user-specific transformation, and storing the distorted biometric on the access control device.

Unimodal biometric systems rely on a single source of information such as a single iris or fingerprint or face for authentication. Unfortunately these systems have to deal with some of the following inevitable problems: (a) Noisy data. (b) Non-universality. (c) Intra-class variations. (d) Spoof attack.

Classification in multibiometric systems is done by fusing information from different biometric modalities. Information fusion can be done at different levels, broadly divided into feature-level, score-level and rank/decision-level fusion. Due to preservation of raw information, feature-level fusion can be more discriminative than score or decision-level fusion. But, feature-level fusion methods are being explored in the biometric community only recently. This is because of the differences in features extracted from different sensors in terms of type and dimensions. Often features have large dimensions, and fusion becomes difficult at the feature level. The prevalent method is feature concatenation, which has been used for different multibiometric settings.

II. SYSTEM ARCHITECTURE

Secure biometrics may be viewed as a problem of designing a suitable encoding procedure for transforming an enrollment biometric signal into data to be stored on the authentication device, and of designing a matching decoding procedure for combining the probe biometric signal with the stored data to generate an authentication decision.



The system is depicted in Figure 1. Any analysis of the privacy and security tradeoffs in secure biometrics must take into account not only authentication accuracy but also the information leakage and the possibility of attacking the system when the stored data and/or keys are compromised. At the outset, note that in authentication, a probe biometric is matched against a particular enrollment of one claimed user. This differs from identification, in which a probe biometric is matched against each enrollment in the database to discover the identity associated with the probe. These are distinct but closely related tasks. For clarity, our development focuses only on authentication.

III. SECUREBIOMETRICS ARCHITECTURE

The following are methods for converting biometrics features into "secure" signals that can be stored in the biometrics database, to be used for authentication.

A. Secure Sketches

A secure sketch-based system derives information—called a sketch or helper data S—from Alice's enrollment biometric A and stores it in the access control database, as shown in Figure 2. The decision function tests whether the probe biometric D is consistent with the sketch and grants access when it is. The sketch S should be constructed so that it reveals little or no information about A.

Secure sketches can be generated in several ways, for example, by computing a small number of quantized random projections of a biometric feature vector. A particularly instructive method—one that shows the connections between secure sketches and the fuzzy commitment architecture—employs ECCs. The secure sketch is constructed as a syndrome of an ECC with parity check matrix H, given by S =HA. The idea is that a legitimate probe biometric D =B would be a slightly error-prone version of A. Therefore, authentication can be accomplished by attempting to decode A given D and S. Secure sketches constructed in this way provide information theoretic security and privacy guarantees that are functions of the dimension of the ECC.

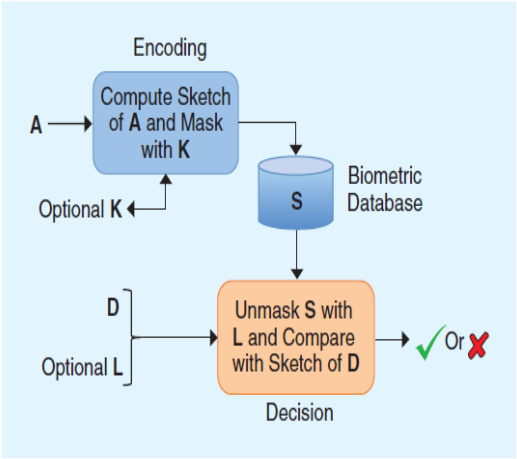


Fig 2. Secure sketch system.

B. Fuzzy Commitment

Fuzzy commitment involves binding a secret message to the enrollment biometric which can later be recovered with a legitimate probe biometric to perform authentication. As depicted in Figure 3, Alice binds her biometric feature vector A to a randomly generated vector Z, producing the data S that is stored in a database as the secure biometric. Again, the encoding function should ensure that S leaks little or no information about A or Z. To perform authentication, a user claiming to be Alice provides a probe biometric feature vector D and the device attempts to recover Z. Access is granted only when there is exact recovery of the message Z, which would happen only if D is sufficiently similar to A.

There are several ways to bind a secret message to the enrollment biometric. One such method uses quantization index modulation (QIM), in which the biometric features are quantized in such a way that the choice of the quantizer is driven by the secret message.

C. Secure multiparty computation

This architecture involves finding the distance between enrollment and probe biometric features in the encrypted domain. There has been intense research activity recently on accomplishing this using public-key homomorphic cryptosystems. These allow an operation on the underlying plaintexts such as addition or multiplication to be carried out by performing a suitable operation on the ciphertexts. To fix ideas, consider the following simple example.

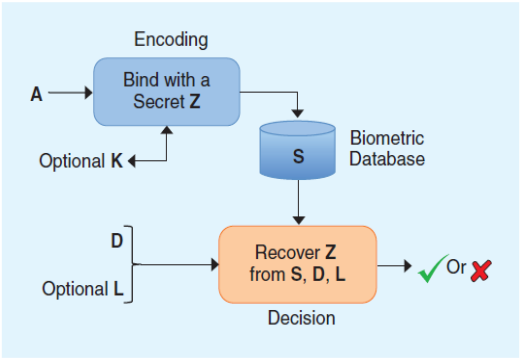


Fig 3. Fuzzy Commitment system.

Suppose the length-n enrollment feature vector A is encrypted elementwise using an additively homomorphic cryptosystem and the resulting ciphertext S is stored in the database of the access control system, as shown in Figure 4. An additively homomorphic cryptosystem, e.g., the Paillier cryptosystem, satisfies E(a)E(b) =E(a +b) for integers a, b and encryption function E($).

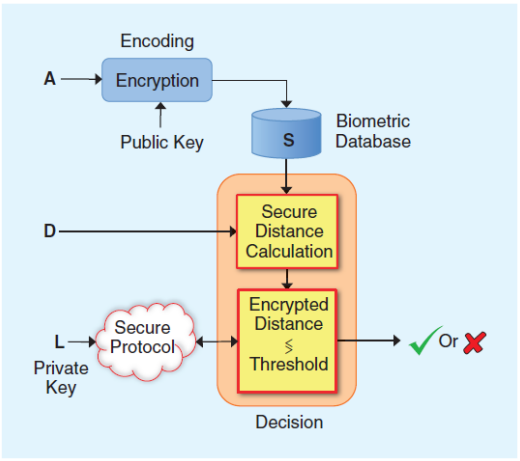


Fig 4. Secure multiparty computation

A realistic assumption in our simple example is that the encryption key is public, while the decryption key L is available only to the individual attempting to authenticate. Thus, by construction, this secure biometrics architecture results in two-factor systems, in which the first factor is a biometric token and the second factor is a privately held decryption key for a homomorphic cryptosystem.

D. Cancelable Biometrics

Cancelable biometrics refers to a class of techniques in which the enrollment biometric signal is intentionally distorted before it is stored in the biometric database. This architecture is depicted in Figure 5. The distorting function is repeatable, so that it can be applied again to the probe biometric, facilitating comparison with the distorted enrollment biometric. Further, the distorting function is intended to be a noninvertible and "revocable" mapping. This means that, if Alice's stored distorted biometric is known to have been compromised, a system administrator can cancel her enrollment data, apply a fresh distorting function to Alice's biometric, and store the result as her new enrollment.

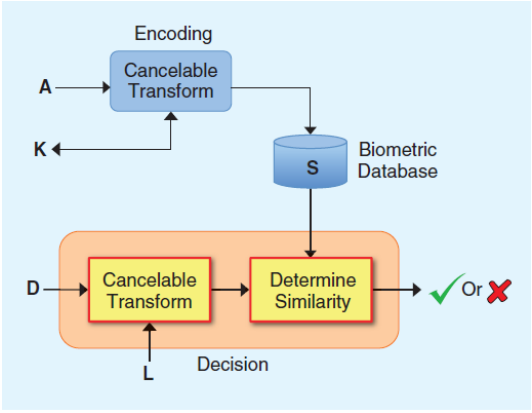


Fig 5. Cancelable Biometrics system.

Thus, by construction, these are two factor systems in which the second factor K is a secret value held by the user which indexes the user-specific deformation, or salting key, or the realization of a random matrix. The secret value can be in the form of a memorized personal identification number or a longer key held on a smart card.

IV. TYPES OF BIOMETRICS MODALS

The types can be classified based on the number of biometric features used for authentication. Basically there are two types of biometric modals they are: (a) Unimodal biometric system (b) Multimodal biometric system.

Traditional biometric recognition systems rely on a single biometric signature for authentication. Unimodal biometric systems rely on a single source of information such as a single iris or fingerprint or face for authentication.

Iris recognition is a popular technique for recognizing humans. For years, bodily features such as the face, fingerprint, and iris have been used for the purpose of recognition. Since the mid-nineteenth century, when Alphonse Bertillon proposed using body measurements to identify criminals, biometrics has been extensively used in law enforcement to identify criminals and to establish identity in a broad range of applications (e.g., refugee control and computer logins). Various traits have been considered to have potential for biometric recognition because they satisfy four requirements: (1) Universality: - Means that each person should possess the characteristic; (2) Distinctiveness: - Means that any two persons should be sufficiently differentiable by the selected characteristic; (3) Permanence: - Means that the characteristic should be invariant over a period of time; (4) Collectability: - Means that the characteristic can be measured quantitatively.

Disadvantages of Unimodal biometrics system are:- (a) Noisy data: poor lighting on a user's face or occlusion are examples of noisy data. (b) Non-universality: the biometric system based on a single source of evidence may not be able

to capture meaningful data from some users. For instance, an iris biometric system may extract incorrect texture patterns from the iris of certain users due to the presence of contact lenses. (c) Intra-class variations: in the case of fingerprint recognition, the presence of wrinkles due to wetness can cause these variations. These types of variations often occur when a user incorrectly interacts with the sensor.(d) Spoof attack: hand signature forgery is an example of this type of attack.

The limitations of unimodal biometric systems can be addressed by deploying multimodal biometric systems that essentially integrate the evidence presented by multiple sources of information such as iris, fingerprints and face. Such systems are less vulnerable to spoof attacks as it would be difficult for an imposter to simultaneously spoof multiple biometric traits of a genuine user. Due to sufficient population coverage, these systems are able to address the problem of non-universality. Joint Sparse Representation for Robust Multimodal Biometrics Recognition : In recent years, theories of Sparse Representation (SR) and Compressed Sensing (CS) have emerged as powerful tools for efficient processing of data in non-traditional ways .This has led to a resurgence in interest in the principles of SR and CS for biometrics recognition. Wrightetal. proposed the seminal sparse representation-based classification (SRC) algorithm for face recognition.

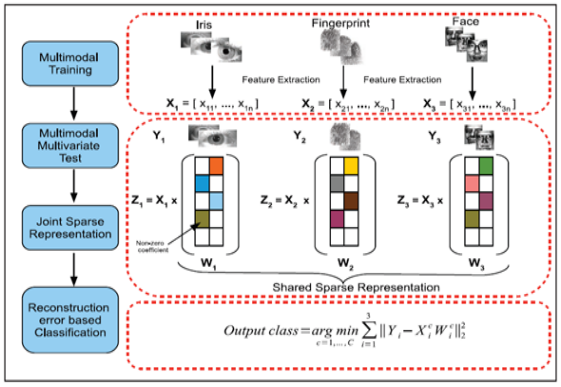


Fig 6. Overview of Joint spare algorithm.

It was shown that by exploiting the inherent sparsity of data, one can obtain improved recognition performance over traditional methods especially when data is contaminated by various artifacts such as illumination variations, disguise, occlusion and random pixel corruption. Pillai et al. extended this work for robust cancelable iris recognition in. Nagesh and Li presented an expression-invariant face recognition method using distributed CS and joint sparsity models. Patel et al. proposed a dictionary-based method for face recognition under varying pose and illumination. A discriminative dictionary learning method for face recognition was also proposed by Zhang and Li . For a survey of applications of SR and CS algorithms to biometric recognition.

Motivated by the success of SR in unimodal biometric recognition, we propose a joint sparsity-based algorithm for multimodal biometrics recognition. Figure 6 presents an overview of our framework. It is based on the well known regularized regression method, multi-task multi-variate Lasso. The proposed method imposes common sparsities both within each biometric modality and across different modalities. The idea of joint sparsity has been explored recently for image classification and segmentaion. However our method is different from these previously proposed algorithms based on joint sparse representation for classification. For example, Yuan and Yan proposed a multi-task sparse linear regression model for image classification. This method uses group sparsity to combine different features of an object for classification. Zhang et al. proposed a joint dynamic sparse representation model for object recognition. Their essential goal was to recognize the same object viewed from multiple observations i.e., different poses. Our method is more general in that it can deal with both multi-modal as well as multi-variate sparse representations.

The proposed algorithm represents the test data by a sparse linear combination of training data, while constraining the observations from different modalities of the test subject to share their sparse representations. Finally, classification is done by assigning the test data to the class with the lowest reconstruction error.

The finger-vein is a promising biometric pattern for personal identification in terms of its security and convenience. Compared with other biometric traits, the finger-vein has the following advantages: (1) The vein is hidden inside the body and is mostly invisible to human eyes, so it is difficult to forge or steal.(2) The non-invasive and contactless capture of finger-veins ensures both convenience and hygiene for the user, and is thus more acceptable.(3) The finger-vein pattern can only be taken from a live body. Therefore, it is a natural and convincing proof that the subject whose finger-vein is successfully captured is alive.

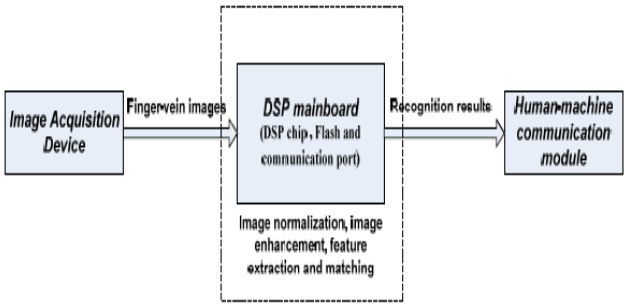


Fig 7. Hardware diagram of the proposed system

The proposed system consists of three hardware modules: image acquisition module, DSP mainboard, and human machine communication module. The structure diagram of the system is shown in Fig.7. The image acquisition module is used to collect finger-vein images. The DSP mainboard including the DSP chip, memory (flash), and communication port is used to execute the finger-vein recognition algorithm and communicate with the peripheral device. The human machine communication module (LED or keyboard) is used to display recognition results and receive inputs from users.The proposed finger-vein recognition algorithm contains two stages: the enrollment stage and the verification stage. Both stages start with finger-vein image pre-processing, which includes detection of the region of interest (ROI), image segmentation, alignment, and

enhancement. For the enrollment stage, after the pre-processing and the feature extraction step, the finger-vein template database is built. For the verification stage, the input finger-vein image is matched with the corresponding template after its features are extracted. Fig. 8 shows the flow chart of the proposed algorithm. Some different methods may have been proposed for finger-vein matching.

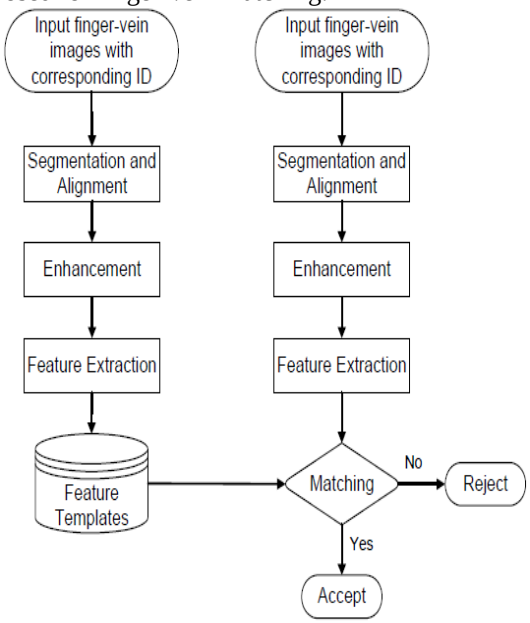


Fig 8. The flowchart of the finger vein recognition algorithm.

To obtain high quality near-infrared (NIR) images, a special device was developed for acquiring the images of the finger vein without being affected by ambient temperature. Generally, finger-vein patterns can be imaged based on the principles of light reflection or light transmission. The developer a finger-vein imaging device based on light transmission for more distinct imaging. Our device mainly includes the following modules: a monochromatic camera of resolution 580 × 600 pixels, daylight cut-off filters (lights with the wavelength less than 800 nm are cut off), transparent acryl (thickness is 10 mm), and the NIR light source. The structure of this device is illustrated in Fig. 9. The transparent acryl serves as the platform for locating the finger and removing uneven illumination. The NIR light irradiates the backside of the finger. In a light-emitting diode (LED) was used as the illumination source for NIR light. With the LED illumination source, however, the shadow of the finger-vein obviously appears in the captured images. To address this problem, an NIR laser diode (LD) was used in our system. Compared with LED, LD has stronger permeability and higher power. In our device, the wavelength of LD is 808nm. Fig. 10 shows an example raw finger-vein image captured by using our device.

Algorithm:

Image Segmentation and Alignment:- Because the position of fingers usually varies across different finger-vein images, it is necessary to normalize the images before feature extraction and matching. The bone in the finger joint is articular cartilage.

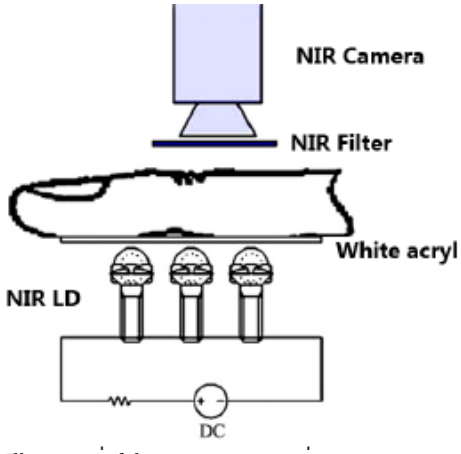


Fig 9. Illustration of the imaging device.

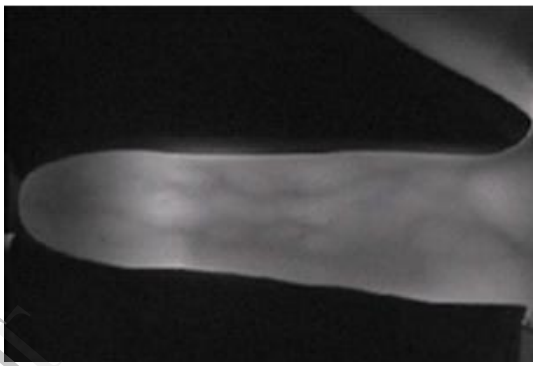


Fig 10. example raw finger-vein captured by our system.

Unlike other bones, it can be easily penetrated by NIR light. When a finger is irradiated by the uniform NIR light, the image of the joint is brighter than that of other parts. Therefore, in the horizontal projection of a finger-vein image, the peaks of the projection curve correspond to the approximate position of the joints. Since the second joint of the finger is thicker than the first joint, the peak value at the second joint is less prominent. Hence, the position of the first joint is used for determining the position of the finger. icon, a nurse can recognize the points in the environment that can be touched with the mobile terminal and actions that the system performs when those points are touched.

Because the position of fingers usually varies across different finger-vein images, it is necessary to normalize the images before feature extraction and matching. The bone in the finger joint is articular cartilage. Unlike other bones, it can be easily penetrated by NIR light. When a finger is irradiated by the uniform NIR light, the image of the joint is brighter than that of other parts. Therefore, in the horizontal projection of a finger-vein image, the peaks of the projection curve correspond to the approximate position of the joints . Since the second joint of the finger is thicker than the first joint, the

peak value at the second joint is less prominent.

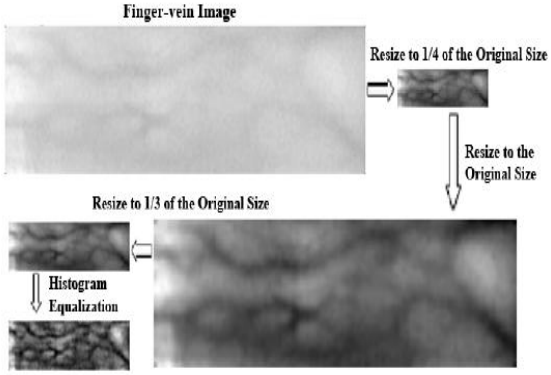


Fig 11. Procedure of our method for image enhancement

Hence, the position of the first joint is used for determining the position of the finger. (a) Image Enhancement:- The segmented finger-vein image is then enhanced to improve its contrast as shown in Fig. 11. The image is resized to 1/4 of the original size, and enlarged back to its original size. Next, the image is resized to 1/3 of the original size for recognition. Bicubic interpolation is used in this resizing procedure. Finally, histogram equalization is used for enhancing the gray level contrast of the image. (b) Feature Extraction:- The fractal model developed by Mandelbrot provides an excellent method for representing the ruggedness of natural surfaces and it has served as a successful image analysis tool for image compression and classification. Since different fractal sets with obviously different textures may share the same fractal dimension, the concept of lacunarity is used to discriminate among textures. The basic idea of lacunarity in many definitions is to quantify the "gaps or lacunae" presented in a given surface, which is used to quantify the denseness of a surface image. In this study, we focus on combining fractal and lacunarity measures for improving finger-vein recognition. (c) Lacunarity Based on Blanket Technique:- Lacunarity is another concept introduced by Mandelbrot to quantify the gaps in texture images. It is a measure for spatial heterogeneity. Visually different images sometimes may have similar values for their fractal dimensions. Lacunarity estimation can help distinguish such images. Lacunarity can be defined quantitatively as the mean-square deviation of the fluctuations of mass distribution function divided by its square mean. It is also defined as the width of the mass distribution function of a set of points, given the ''box size''.

Thus, a higher value of lacunarity implies more heterogeneity, as it means a wider mass distribution function, or a larger number of different mass values, of the set of points. A lacunarity value is assigned for the center pixel of the image window, and the lacunarity value of each pixel in an image can be obtained by moving the W*W window throughout the whole image.

V. CONCLUSION

Biometric technology adds a new layer of security by ensuring secure identification and authentication. But biometric authentication systems like any other technology are also vulnerable to attacks such as transmission, replay and spoofing. There are many proposed methodologies that are used to defeat them. Multimodal biometric system is a major approach to defeat spoofing attacks..

An end-to-end finger-vein recognition system based on the blanket dimension and lacunarity implemented on a DSP platform. The proposed system includes a device for capturing finger-vein images, a method for ROI segmentation, and a novel method combining blanket dimension features and lacunarity features for recognition. The images from 600 fingers in the dataset were taken over long time interval (i.e., from summer to winter) by a prototype device we built. The experimental results showed that the EER of our method was 0.07%, significantly lower than those of other existing methods. Our system is suitable for application in mobile devices because of its relatively low computational complexity and low power consumption.

VI. REFERENCES

[1] Shantanu Rane, Ye Wang, Stark C. Draper, and Prakash Ishwar, "Secure Biometrics Concepts, authentication architectures, and challenges" IEEE SIGNAL PROCESSING MAGAZINE Spet 2013.

[2] Luís Cardoso, André Barbosa, Frutuoso Silva, António M. G. Pinheiro, Member, IEEE, and Hugo Proença, "Iris Biometrics: Synthesis of Degraded Ocular Images", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013.

[3] Sumit Shekhar, Student Member, IEEE, Vishal M. Patel, Member, IEEE, Nasser M. Nasrabadi, Fellow, IEEE, and Rama Chellappa, Fellow, IEEE, "Joint Sparse Representation for Robust Multimodal Biometrics Recognition" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 14.

[4] Zhi Liu and Shangling Song, "An Embedded Real-Time Finger-Vein Recognition System for Mobile Devices", IEEE Transactions on Consumer Electronics, Vol. 58, No. 2, May 2012.