MMBAS-NS: Multimodal Biometric Authentication System and Key Generation Algorithm for Network Security on Mobile Phones

Saritha Reddy Venna, Ramesh Babu Inampudi

Abstract: Nowadays mobile devices are an important part of our everyday lives since they enable us to access a large variety of ubiquitous services. In recent years, the availability of these ubiquitous and mobile services has significantly increased due to the different form of connectivity provided by mobile devices. In the same trend, the number and typologies of vulnerabilities exploiting these services and communication channels have increased as well. As the number of vulnerabilities and, hence, of attacks increase, there has been a corresponding rise of security solutions proposed by researchers. To overcome these issues in security solutions, we introduce a new method based on cryptographic generation system. We proposed a new multimodal biometric authentication system, here key values are created via the use of multiple biometrics instead of a single biometric, in an effort to generate strong and repeatable cryptographic keys. In this work, a multimodal biometric authentication system (MMBAS) is developed using face, fingerprint and retina images and key generation is also done using these images. Initially images are pre-processed using adaptive median filtering and Otsu's segmentation algorithm for background subtraction. Then minutiae feature of these images are extracted with the use of Local Binary Pattern (LBP) algorithm and then the feature vectors of face, fingerprint and retina are fused using XOR operation. Later the fused feature vector is used for cryptographic key generation. The evaluation is performed on network security for showing the reliability of the newly introduced approach in terms of Precision, Recall, Accuracy and false rejection rate.

Keywords: Biometrics, Authentication System, Key Generation, Network Security, Face, Fingerprint, Retina.

I. INTRODUCTION

Nowadays, mobile devices are an important part of the everyday lives since they enable us to access a large variety of services [1]. The ubiquitous use of mobile phones has caused an emergence of applications targeted to mobile platforms. Since mobile devices become the major mobile platforms for users to transfer and exchange diverse mobile data over the wireless networks or wireless internet, mobile security for mobile accesses becomes very important and critical to assure secured mobile transactions, mobile data integrity and confidentiality. Mobile security also is critical to protect mobile users and mobile-based application systems from unauthorized accesses and diverse attacks [2].

The strong demand of mobile applications and services raised increasing concerns on the security for mobile accesses, user privacy, and mobile applications. This leads an increasing demand on emerging mobile security technologies and solutions for mobile accesses. Hence, security becomes very important for mobile users and mobile accesses, and it is becoming a vital research topic [3]. When discussing mobile security, must understand mobile security threats to mobile phones and mobile accesses. Mobile phones have certain specific features (such as mobility) which make these devices more vulnerable to security attacks such as 1) Mobility 2) Strong Personalization 3) Strong Connectivity 4) Technology Convergence 5) Limited Resources and Reduced Capabilities [4].

Although the fundamental concepts of security remain the same while considering mobile security relating to mobile accesses, some new needs and requirements must be considered to cope with the above threats in mobile accesses. They are summarized below. 1) Mobile access confidentiality 2) Mobile data integrity 3) Mobile service availability and 4) Disrupted mobile service charging. These mobile security threats bring new requirements and needs for more effective mobile security solutions and technologies to ensure mobile access security on mobile devices so that the end-to-end protection between mobile devices can be assured [5].

Biometric Authentication is a security mechanism or technology, provided in a given application environment (or systems), identifies the individuals and their accesses of the systems by measuring their physical or behavioral attributes. Because of the uniqueness exhibited by these attributes of mobile users, it is possible to uniquely identify them and their accesses on the mobile devices. Physiological attributes of mobile users are related to the shape of their body [6]. The biometric based security solutions for mobile user accesses, inclusion of biometric data in communication is very successful today, basically for its enormity. Inclusion of biometric technologies for security includes recognition of faces, fingerprints, iris, retina, voice, signature strokes etc. [7].

Cryptography, on the other hand, is a widely used technique for secure transmission or storage of sensitive data. Hence, the secure communication is the basic requirement of every transaction over networks. Cryptography is an important security feature of mobile network and using cryptography, further strengthens the **mobile communication security [8].**

Manuscript received January 25, 2019.

Saritha Reddy Venna, Research Scholar, Department of CSE, Acharya Nagarjuna University. Guntur, AP

Ramesh Babu Inampudi, Professor, Department of CSE, Acharya Nagarjuna University,Guntur, AP

It is an essential component for secure transmission of information through security services like confidentiality, data integrity, access control, authentication and non-repudiation. It provides a way to protect sensitive information by transferring it into unintelligible and only the authorized receiver can be able to access this information by converting it into the original text. The process of converting the plaintext into cipher text using a key is termed as encryption and the reverse process of encryption is called decryption [9].

Bio-cryptography is a new and embryonic field that combines the strengths from both cryptography and biometrics. Though cryptography provides high and adjustable security levels, biometrics bring in non-repudiation and eliminates the need to remember passwords or carrying tokens etc. whereas biometrics provide non-repudiation and expediency, standard cryptography provide flexible level of security and it not able to just for authentication but also for encryption [10]. Biometric-based key release refers to authentication required to release a cryptographic key. Biometric-based key generation refer to extract/generate a cryptographic key from biometric template. The secret key be bounded to the biometric information also the biometric template is not stored in plain form. The similar biometric signal by a device or an environment [11]. Whereas it should be very convenient to use biometric traits for encryption, for instance someone using his fingerprint are handwritten signature to encrypt a document and securely send it over public network, this is very difficult due to variability of the biometric signal and the fact that encryption and decryption operation cannot tolerate the perturbation of even a single bit.

Biometric systems based solely on unimodal biometrics are often not able to meet the desired performance requirements for large user population applications, due to problems such as noisy data, intra-class variations, restricted degrees of freedom, non-university, spoof attacks, and unacceptable error rates [12]. In order to overcome the disadvantages of unimodal biometrics, for biometrics to be ultra-secure and to provide more-than-average accuracy, more than one form of biometrics is required, and hence, the need arises for the use of multimodal biometrics [13]. Instead of using single biometrics, a combination of different biometric (like a combination of face, finger print, iris, ears, etc.), can be used for recognizing a human being. Multimodal biometric system is mortal increasingly deployed in many large-scale biometric applications because they have several rewards such as lower error rates and large population coverage compare to unimodal biometric systems [14].

In order to guarantee better user-friendliness and higher accuracy, beyond the existing traditional single-factor biometric systems, the multimodal ones appear to be more promising. Two or more bio-metric measurements for the same identity are extracted, stored and compared during the enrollment, authentication and identification processes. Deployed multimodal biometric systems also referred to as multi-biometrics or even as multimodalities are commonly found and used in many high security applications in mobile environments [15].

In this work develop the secure cryptographic key generation approach. Initially, the minutiae points are extracted from the fingerprint, face and retina image. The extraction process utilized the subsequent steps such as noise removal using adaptive median filtering and background subtraction using Otsu's process. On the other hand, the texture features are extracted from the face, fingerprint and retina images utilizing local binary pattern (LBP). Then, the extracted features are used to perform the fusion process, using of feature level fusion technique. The merged multimodal biometric template is obtained from the fusion process and thereby, a user-specific secure cryptographic key is generated.

The overall organization of the research paper is given as follows: In this section, introduction about the mobile network security and the biometric authentication is discussed. In section 2, various related research techniques has been discussed in detail with their working procedure. In section 3, discussion about the proposed research methodology has been given with suitable examples and explanation. In section 4, performance evaluation of the proposed research methodology is given based on simulation outcome. Finally, in section 5, final conclusion of the research method is given based on outcome obtained.

II. LITERATURE REVIEW

Feng et al [16] proposed a new biometrics-based authentication scheme with key distribution for the mobile multi-server environment. This proposed scheme is based on smart card and elliptic curve cryptosystem. Informal and formal security analyses demonstrate that our scheme can satisfy the security and functional requirements in the mobile multi-server environment. Moreover, performance results such as computation and communication cost obtained with the proposed scheme demonstrates the significant improvements in the level of security. The performance analysis of the proposed scheme in terms of its computational and communication overhead to show that, improved the level of security with minimal performance costs.

Naidu et al [17] proposed fingerprint and palm print multi-modal biometric security system. At first, the preprocessing steps are completed on chosen images which include binarization, thinning and minute extraction. Using minute extraction different angles are formed for the thinned images for choosing the specific area of the images. In the next step for identifying the specific area in the finger print images region of interest is carried out. After the initial stage (preprocessing) features are extracted by using Feature Extraction method from both the finger print and palm print images and all the extracted features are combined to form a feature vector element. Secrete key is generated using the fuzzy extractor from the biometric features and stored in the fuzzy vault. In final stage authentication methods are carried out for the test images.

Jagadiswary et al [18] proposed enhanced multimodal authentication system is based on feature extraction (using fingerprint, retina and finger vein) and key generation (asymmetric cryptographic algorithm) RSA. The feature level fusion technique is used for the design of multimodal biometric traits such as fingerprint, retina and finger vein, which protects the multiple templates using RSA. A realistic security analysis of the multimodal biometric cryptosystem has also been conducted using fingerprint, finger-vein and retina, which provide a remarkable improvement performance in a multimodal biometric cryptosystem using RSA. The overall performance of multimodal system has increased, which is compared to unimodal biometric using RSA.

Lalithamani et al [19] presented a technique to generate face and palm vein-based fuzzy vault for multi-biometric cryptosystem. Here, initially the input images are pre-processed using various processes to make images fit for further processing. In this proposed method, the features are extracted from the processed face and palm vein images by finding out unique common points. The secret key points which are generated based on the user key input are added to the combined feature vector to have the fuzzy vault. For decoding, the multi-modal biometric template from palm vein and face image is constructed and is combined with the stored fuzzy vault to generate the final key. Hence, template security is even more critical in multi-biometric systems where it is essential to secure multiple templates of a user.

Kanade et al [20] proposed a multi-biometric based cryptographic key regeneration scheme. Since left and right irises of a person are uncorrelated, treat them as two independent biometrics and combine in the system. A shuffling key which is protected by a password is used to shuffle the error correcting codes data. The feature level fusion is combined with weightederror correction algorithm which allows the fusion of different biometric modalities having variation in performances (e.g., face and iris). The difficulty is to find appropriate Elliptic Curve Cryptography (ECC) for that modality and the binarization of the feature vector.

Sanjay Kumar et al [21] proposed biometric-based multi-modal authentication system with four levels of securities. Level 1 uses username and password only; Level 2 uses fingerprint with user name and password; Level 3 uses fingerprint and face with user name and password; Level 4 uses fingerprint, face and iris with user name and password. In the proposed architecture, web applications hosted in the server or servers in a wireless Local Area Network (LAN) can be accessed through wireless client after its authentication by Advance Authentication Server (AAS). The proposed system can be developed as firmware in router to implement device level security.

Sarier et al [22] described the first generic construction for multimodal biometric Identity Based Encryption considering two distance measures at the same time. The similarity measures for biometric templates can be quite different from those considered in theoretical works. For instance, a fingerprint template usually consists of a set of minutiae, and two templates are considered as similar if more than a certain number of minutiae in one template are near distinct minutiae in the other. In this case, the similarity measure has to consider both Euclidean distance and set difference at the same time. Similarly, multimodal systems that are designed to address the limitations of unimodal systems may involve two different traits requiring different distance measures for each modality. The author combines a fuzzy IBE-type scheme and the recently introduced Distance Based Encryption (DBE) scheme with minimum overhead in terms of public parameters, ciphertext and private key size.

Ali et al [23] proposed a secured multimodal biometric authentication system using encrypted templates. In the proposed system, the edges transmit the encrypted speech and face for processing in the cloud. The cloud then decrypts the biometrics and performs authentication to confirm the identity of an individual. The model for speech authentication is based on two types of features, namely, Mel-frequency cepstral coefficients and perceptual linear prediction coefficients. The model for face authentication is implemented by determining the eigenfaces. The final decision about the identity of a user is based on majority voting. Experimental results show that the new encryption method can reliably hide the identity of an individual and accurately decrypt the biometrics, which is vital for errorless authentication.

Saevanee et al [24] described a novel text-based multimodal biometric approach utilizing linguistic analysis, keystroke dynamics and behavioural profiling. Experimental investigations show that users can be discriminated via their text-based entry, with an average Equal Error Rate (EER) of 3.3%. Based on these findings, a framework that is able to provide robust, continuous and transparent authentication is proposed. The framework is evaluated to examine the effectiveness of providing security and user convenience. The result showed that the framework is able to provide a 91% reduction in the number of intrusive authentication requests required for high security applications.

Gomez-Barrero et al [25] present the first software attack against multimodal biometric systems. Its performance is tested against a multimodal system based on face and iris, showing the vulnerabilities of the system to this new type of threat. Score quantization is afterwards studied as a possible countermeasure, managing to cancel the effects of the proposed attacking methodology under certain scenarios. Research works such as the one presented in this work pretend to bring some insight into the difficult problem of biometric security evaluation through the systematic study of biometric systems vulnerabilities and the analysis of effective countermeasures that can minimize the effects of the detected threats, in order to increase the confidence of the final users in this rapidly emerging technology.

Vazquez-Fernandez et al [26] discussed the use of face biometric technology and share the thoughts on key related issues and concerns: usability, security, robustness against spoofing attacks, and user privacy among others.

In the proposed work, the implementation of the recent Deep Neural Network paradigms for face recognition into mobile devices, taking advantage of the embedded GPU and exploiting its capabilities for energy optimized real-time processing. Unfortunately, the operation of a face recognition system usually varies due to the use of different camera and optics (capture device). This points out a question very related to the above point: the analysis of cross-device performance and how the performance can be affected if different devices are used for enrolment and for authentication. More research on multimodal cross device authentication needs to be done for a better mobile biometric authentication experience.

Galdi et al [27] presented a novel system that combines the recognition of user’s iris and user’s device, i.e. something the user is plus something the user has. To do so, the author adopted an iris recognition algorithm, namely Cumulative SUMs, and a well-known technique in the image forensic field for camera source identification based on the extraction of the Sensor Pattern Noise. The two identification processes are performed on the same picture leading to a system with a good trade-off between ease of use and accuracy. The approach is tested on Mobile Iris Challenge Evaluation (MICHE), a database composed by iris images captured with different mobile devices in unconstrained acquisition conditions.

III. PROPOSED METHODOLOGY

In this paper mobile verification-based network security is performed by using multi-biometric authentication. In this work, finger print, face and retina images are taken as input from a benchmark database. The finger print, face and retina images are subjected to pre-processing using adaptive median filtering and Otsu’s segmentation is applied to remove background pixels to enhance the image quality. Then the features of the pre-processed images are extracted by using Local Binary Pattern (LBP) and fused at the feature level by Binary NOR operation to create a merged template. And finally, the cryptographic key is generated for security using mobile verification.

Data

Although common sense would suggest that biometrics provides a very high degree of security, there are actually several means for attackers to compromise a biometric system. Data acquired from biometric sensors during the authentication of a legitimate user can be logged and later reused by the attacker, in a similar way as logging keystrokes allows obtaining passwords typed at a terminal. Another option is to create an artificial biometric sample, which is actually feasible with common materials even for those considered strong biometric traits, like finger print [28].

The purpose of the system is to provide an authentication service, which operates as a bridge between users that need to access to a given application, and applications that require secure access control. The core elements of the multimodal biometric authentication architecture are the authentication server and the template database, in which samples of biometric data (“templates”) are stored. The multimodal biometric authentication service supports very different kind of applications, including those with high security constraints, but also entertainment and informational applications. The main assumption on client devices is that they have the only role of acquiring biometric data, while all the processing and comparison tasks are performed server-side [29].

In the following list some of the vulnerabilities that have been identified for the authentication service, briefly discussing how they could be exploited by an attacker and which are the possible countermeasures. Such list has been used as a basis in the construction of the analysis model.

Denial of service (DoS) attacks are designed to corrupt or incapacitate the biometric sensors, and can consist in physical damage, power loss, or introducing adverse environmental conditions to degrade the quality of the acquired data. Using *fake physical biometric*, also known as *sensor spoofing*, consists in using counterfeit physical biometrics to circumvent the biometric system.

Reuse of residuals exploits the fact that some biometric devices may hold the last few acquired samples in some kind of local memory. If an attacker gains access to this data, he may be able to reuse it to provide a valid biometric sample. Countermeasures to this attack include clearing memory and forbidding perfectly identical biometric samples.

Replay attacks involve the communication between the sensor and the processing resource that performs the comparison. A replay attack is composed of at least two stages: first an authentic communication is intercepted (*eavesdropping*), then it is replayed when needed, possibly modifying its content in accordance with the objectives of the attacker. Data encryption and digital signatures offer significant protection against this kind of attack.

Template modification consists in directly altering the template database, and it is one of the most serious threats to biometric systems: it potentially allows an attacker to obtain unauthorized access by simply presenting its real biometrics, and substituting to any of the legitimate users of the system. Countermeasures to this kind of attack include strict access policies to the template database, as well as encryption and digital signature for database content [30].

To overcome the above-mentioned issues, in this work multimodal biometric authentication is proposed in multimodal biometric authentication System for mobile security verification.

Supporting three biometric traits: fingerprint face, and retina. The authentication server and the template database reside on a private network, protected from the Internet by a firewall. Communication between the client and the authentication server uses an encrypted logical channel.

Biometric systems require a transformation of biometric template to ensure privacy, security, and revocability of biometric data. The technique which can meet this requirement is called cancellable or revocable biometric. This privacy enhancement problem is identified, and conceptual frameworks of biometric templates are presented in formally defined the problem of cancellable biometric.

Recently, proposed three practical solutions to cancellable multi-biometrics and generate cancellable fingerprint templates. These three template transformation approaches are Cartesian, polar, and functional transformations on feature domain. In Cartesian transformation approach, the minutiae space is divided into rectangular cells which are numbered with sequence. A user-specific transformation key (i.e., matrix) is used to shift the cells to a new location, and the points are relocated to the new cells. In polar transformation, coordinate space is divided into polar sectors that are numbered in sequence. In functional transformation, model the translation using a feature vector-valued function (F (x, y)) which is an electric potential field parameterized by a random distribution of charges. The phase angle of the resulting vector decides the direction of translation and the magnitude |→F | of this vector function parameterizes the extent of movement. In an alternate formulation, use the gradient of a mixture of Gaussian kernels to determine the direction of movement and the extent of movement is determined by the scaled value of the mixture. Some researchers proposed shuffling-based transformation to generate cancellable templates using a user-specified random key [31-32].

No assumptions are made on the kind of application(s) to which the authentication service provides access. Consequences of unauthorized access depend on the actual application, and potentially include catastrophic events in case of critical infrastructures control systems [33]. Therefore, focus on security attributes of the authentication service, and consider the time that it takes for an attacker to obtain unauthorized access as the main indicator of system security. In particular, evaluate: $p_E\ (t)$: Probability that, at time t, the attacker has been successfully authenticated, and T_e: Mean time required to the attacker to obtain authentication

In this analysis will compare two different system configurations, which have been identified as representative alternatives within the project:

1. User authentication requires only two of the three supported biometric traits. This configuration allows to trade security for broader client support: the absence of one sensor (e.g., fingerprint reader on mobile phones) or bad environment conditions (e.g., low light or noise) will still allow authentication by using the remaining sensors. The acquired biometric data is transmitted using a single encryption key.

2. User authentication requires all the supported biometric traits, and the biometric data is transmitted using three separate encryption keys.

The three above configuration variants are intended for systems having different security requirements, and aim to provide an increasing level of security, with #1being the least secure configuration, and #3 being the most secure. It is assumed that the system is subject to different kind of attackers, distinguished by the knowledge they have of the system, the elements they can access, and their skills. Objective is to assess the ability of above configuration to contrast the different attackers.

A realistic characterization of attackers is a challenging task for system-level security analysis; a common technique for network-based systems is the use of "honeypots", i.e. intentionally low protected machines exposed on public networks to attract attackers and analyse their actions. This approach is however less practical when non-network-based attacks are considered. In this analysis consider a representative set of attackers, covering different abilities, knowledge, and accesses [34].

In this section, discuss the proposed approach in details. An overview of the approach is shown in Figure 1. In this approach, the fingerprint, face and retina images are taken as input from a benchmark database. The fingerprint, face and retina images are subjected to pre-processing using adaptive median filtering and Otsu's algorithm to enhance the image quality. The features are then extracted using LBP and fused at the feature level to create a merged template. And finally, the cryptographic key is generated from this merged template for security purpose.

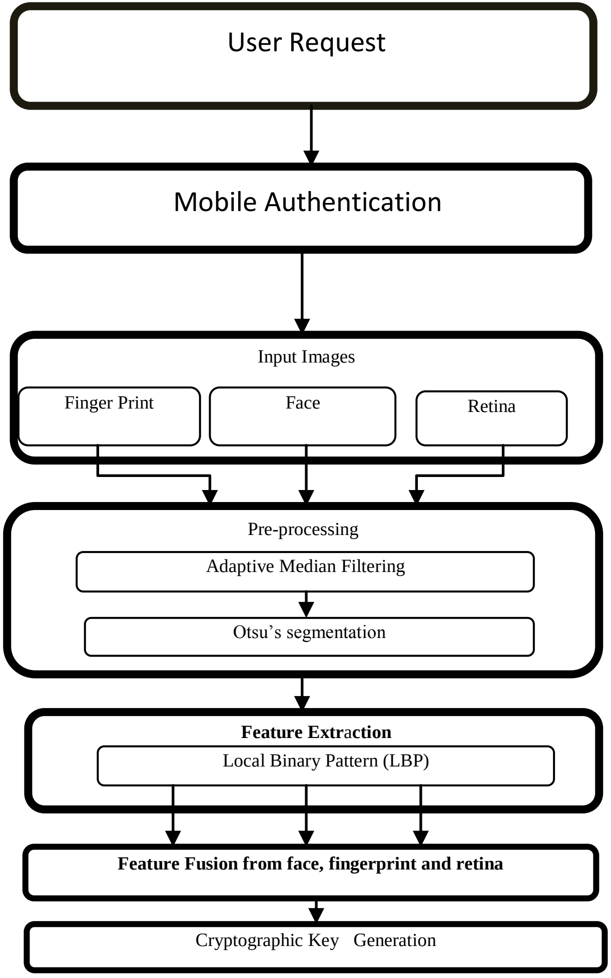

User Request
Mobile Authentication
Input Images
Finger Print
Face
Retina
Pre-processing
Adaptive Median Filtering
Otsu's segmentation
Feature Extraction
Local Binary Pattern (LBP)
Feature Fusion from face, fingerprint and retina
Cryptographic Key Generation

Figure 1: Overview of the proposed approach

3.1. Preprocessing

Pre-processing of includes various steps such as region of interest (ROI) extraction, normalizing it in terms of size and intensity, noise removal and image contrast enhancement. The pre-processing phase plays an essential role in the subsequent extraction of the multiple patterns from the fingerprint, face and retina images.

1) Region of Interest extraction: Firstly, the face, fingerprint and retina input images are converted to gray-scale images. Then the required region of the finger, face and retina is extracted from the image eliminating the unwanted regions. ROI image is then resized so that the computational time decreases for subsequent processing.

2) Denoising and Background removal: using adaptive median filtering algorithm to remove unwanted noise from the input image.

De-noising algorithms might be better if they involve not only the noise, but also the image spatial characteristics. Adaptive Median Filter is a non-linear smoothing method that reduces the blurring of edges, in which the idea is to replace the current point in the image by the median of the brightness in its neighbourhood. Individual noise spikes do not affect the median of the brightness in the neighbourhood and so median smoothing eliminates impulse noise quite well. In this experiment, the median filter was applied and got the median filtered fingerprint, face and retina image as a good quality image for the further enhancement.

3.1.1. Pre-processing using Adaptive median filter

The input fingerprint, face and retina image are initially changed into grey level format. After that using Adaptive median filter, the grey level finger print, face and retina image is pre-processed to take away salt and pepper noise. The input image may have noises which destroy the good pixels in the image. The noise must be eradicated from the input image in order to attain good precision. The images are applying adaptive median filter to salt and pepper noise in suggested work. It identifies the impulse by calculating the difference between the standard deviation of the pixels inside the filter window and the concerned current pixel. Let the database contains many eye images and let x $_{i,j}$ be one of the grey level images taken from the database. The lower and upper bounds x are min max s $_{min}$ s_{max} correspondingly. The grey level of image 'x' is specified by probability

$$y_{i,j}=\begin{cases} s_{\min}\ , probabilityp \\ s_{max}, probabilityq \\ x_{i,j}, 1-a-b \end{cases} \quad (1)$$

The noise level is described as ns=a+b. The functioning procedure of Adaptive median filtering is explained below,

- Initialize the window size ws = 3.
- Work out maximum ($s_{i,j}^{min,wz}$) minimum ($s_{i,j}^{\max wz}$), and median ($s_{i,j}^{\mathrm{med}\, wz}$)of the pixel values in $s_{i,j}^{wz}$
- If $s_{i,j}^{\min ws}$<$s_{i,j}^{\mathrm{med}\, ws}$<$s_{i,j}^{\max ws}$, then go to step 5. Else increase the window size ws by 2.
- If ws ≤ ws $_{max}$ go to 2. Else substitute y $_{i,j}$ by $s_{i,j}^{\mathrm{med}\, ws \quad max}$.
- If $s_{i,j}^{\min ws}$<$y_{i,j}$<$s_{i,j}^{\max ws}$<, then $y_{i,j}$, is not a noise candidate or else substitute , $y_{i,j}$ by $s_{i,j}^{\mathrm{med}\, ws}$

$$s_{i,j}^{w} = \{(k,l): |k-i| \leq \text{ws and } |j-1| \leq \text{ws} \quad (2)$$

At this point $s_{i,j}$ is window of size ws x ws centered at (i, j). ws_{max} be the maximum window size.

s_{min} s_{max}, are computed as follow:

$$su(i,j) = \sum_{m=i-k}^{i+k} \sum_{n=i-k}^{j+k} S_{\ m,n} \quad (3)$$

$$\text{ws(i,j)=(2l+1)2} \quad (4)$$

Using equ(4) and (5), Local mean value μ(i,j) and local standard deviation σ (i,j) ,are computed as below.

$$\mu(i,j) = \frac{su(i,j)}{ws(i,j)} \quad (5)$$

$$\sigma(i,j) = \sqrt{\frac{\sum_{m=i=k}^{i+k} \sum_{n=i=k}^{i+k} \left(s_{i,j-}\mu(i,j))\right)}{ws(i,j)}} \quad (6)$$

Next by means of these local mean, standard deviation and as well a user defined multiplier upper and lower bounds are computed. Lower bound (s_{min}) and upper bound (s_{max}) are computed as

$$s_{min} = \mu 1(i,j) - m \times \sigma(i,j \quad (7)$$

$$s_{\max} = \mu 1(i,j) + m \times \sigma(i,j) \quad (8)$$

The noise candidates only substituted by the median $s_{i,j}^{\mathrm{med}\, ws}$, in the above adaptive median filter algorithm, while staying behind are unaltered. By means of the above adaptive median filter algorithm the salt and pepper noise is eliminated from the specified input face, finger print, retina images and the pre-processed face, fingerprint, retina image is indicated as x'. This pre-processed face, fingerprint, retina image (x') is subsequently subjected to localization face, fingerprint, retina process [36].

The background of the images is removed using Otsu's segmentation algorithm. In order to classify the pixels into two classes: C1, the image pixels and C2, the background pixels, the Gaussian filtered image has to be thresholded. Let $F_R(x,y)$ denote the Gaussian filtered image with background pixels removed, can express the segmentation as

$$F_R\text{(x,y)=}\begin{cases} F_G(x,y), if\, F_G(x,y) \geq u; \\ 0, \qquad otherwise \end{cases} \quad (9)$$

where *u* = [0,255]] e threshold value that maximizes the Otsu's cost function for the separation of foreground and removal of background pixels.

3) Image Contrast enhancement: The images have to be enhanced in order to extract the unique patterns efficiently. A guided filter [37] is an edge preserving smoothing operator which is used to enhance the extracted patterns. Gabor filter [38] is an excellent band pass filter to remove noise along with preservation of ridges. After applying pre-processing for the input images here extracting the features from the pre-processed images using the local binary pattern (LBP) operator.

3.2. Feature Extraction

The local binary pattern (LBP) operator is defined as a gray-scale invariant texture measure, derived from a general definition of texture in a local neighbourhood. Through its recent extensions, the LBP operator has been made into a really powerful measure of image texture, showing excellent results in many empirical studies. The LBP operator can be seen as a unifying approach to the traditionally divergent statistical and structural models of texture analysis.

Perhaps the most important property of the LBP operator in real-world applications is its invariance against monotonic gray level changes. Another equally important is its computational simplicity, which makes it possible to analyze images in challenging real-time settings. The LBP method and its variants have already been used in a large number of applications all over the world. The LBP feature vector, in its simplest form, is created in the following manner:

i. Divide the examined window to cells

ii. For each pixel in a cell, compare the pixel to each of its 8 neighbours (on its left-top, left-middle, left-bottom, right-top, etc). Follow the pixels along a circle, i.e. clockwise or counter- lock wise.

iii. Where the centre pixel's value is greater than the neighbour, write "1". Otherwise, write "0" The feature vector now can be processed using machine learning algorithm, to produce a classifier [39].

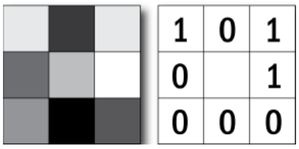


Figure 2: The brighter neighbours around the centre pixel are given value 1 and 0 otherwise.

The 8-bit representation for the central pixel would be 10000110 and 134 in decimal. The basic idea of this approach is demonstrated in Fig. 2. consider a 3×3 neighborhood around each pixel. All neighbors that have values higher than the value of the central pixel are given value 1 and 0 otherwise. The 8binary numbers associate with the 8 neighbours are then read sequentially in the clockwise or counter clockwise direction to form an 8-bit binary number. The equivalent of this binary number (usually converted to decimal) may be assigned to the central pixel and it may be used to characterize the local texture. LBP texture for centre point (x_c; y_c) can be represented as

$$LBP(x_c, y_c) \sum_{n=0}^{N-1} S(i_n - i_c)2^{\,n} \qquad (10)$$

where i_n denotes the intensity of the n^{th} surrounding pixel, i_c denotes the intensity of the center pixel, N is the length of the sequence, and

$$s = \begin{cases} 1 \;\; if\, i_n \geq i_c \\ 0 \;\; if\, i_{n<i_c} \end{cases} \qquad (11)$$

can extend the methodology to circular neighbourhoods of increasing radii. This leads to a multi-resolution representation of the local texture pattern. As the radius of the neighbourhood increases, the number of neighbours increases and this may lead to large value of the local binary pattern. This may be avoided by selecting only neighbours which are at the chosen radius and at a certain angular distance from each other. This is demonstrated in Fig.3.

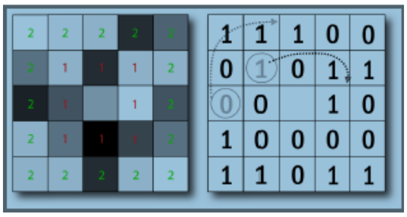


Figure 3: Two circular neighbourhoods with radii 1 (marked with 1's) and radii 2 (marked with 2's) are considered around the central pixel.

Here, features of face, finger print and retina textures are extracted using Local Binary Patterns (LBP). LBP operator forms labels for the image pixels by thresholding the neighbourhood of each pixel and considering the result as a binary number. Combining the features of face, finger print and retina using fusion method after extracted the features from face, finger print and retina images [40].

3.3. Fusion of Multimodal Biometric Image Features

The feature level to obtain a multimodal biometric template that can perform biometric authentication.

Fingerprint - Each minutiae point extracted from a fingerprint image is represented as (x, *y)* coordinates. Here, store those extracted minutiae points in two different vectors: Vector F_1 contains all the *x* co-ordinate values and Vector F_2 contains all the *y* co-ordinate values

$$F_1 = [x_1 x_2 x_3 \ldots x_n]; |F_1| = n \qquad (12)$$

$$F_2 = [y_1 y_2 y_3 \ldots y_n]; |F_2| = n \qquad (13)$$

Eye Retina - The texture properties obtained from the Gaussian filter are substitute complex numbers $r = \sqrt{x^2 + y^2}$. Similar to fingerprintrepresentation, store the retina texture features in two different vectors: Vector I_1 contains the real part of the complex numbers and Vector I_2 contains the imaginary part of the complex numbers.

$$I_1 = [a_1 a_2 a_3 \ldots a_n]; |I_1| = m (14)$$

$$I_2 = [b_1 b_2 b_3 \ldots b_n]; |I_2| = m \qquad (15)$$

Face – Similar to fingerprint and eye retina, also store the face pixel extracted minutiae points in two different vectors: A_1 contains the real part of the p co-ordinate values and vector A_2 contains the imaginary part of the q co-ordinate value.

$$A_1 = [p_1 p_2 p_3 \ldots p_n]; |A_1| = t \qquad (16)$$

$$A_2 = [q_1 q_2 q_3 \ldots q_n]; |A_2| = t (17)$$

Thereby, the input to the fusion process (multimodal biometric generation) will be six vectors F_1, F_2, I_1, I_2, A_1 and A_2. The fusion process results with the multimodal biometric template. The steps involved in fusion of biometric feature vectors are as follows.

1) *Shuffling of individual feature vectors:* The first step in the fusion process is the shuffling of each of the individual feature vectors F_1, F_2, I_1, I_2, A_1 and A_2. The steps involved in the shuffling of vector F_1 are,
   i. A random vector *R* of size $F_1$is generated. The random vector *R* is controlled by the seed value.
   ii. For shuffling the i^{th} component of fingerprint feature vector F_1.

a) The ith component of the random vector *R* is multiplied with a large integer value.

b) The product value obtained is modulo operated with the size of the fingerprint feature vector F_1.

c) The resultant value is the index say '*j*' to be interchanged with. The components in the ith and jth indexes are interchanged.

iii. Step (ii) is repeated for every component of F_1. The shuffled vector $F_1$is represented as S_1. The above process is repeated for every other vectors F_2, I_1, I_2, $A_1$and $A_2$with S_1, $S_2$and S_3as random vectors respectively, where $S_2$is shuffled $F_2$and $S_3$is shuffled I_1. The shuffling process results with six vectors S_1, S_2, S_3, S_4,S_5, and S_6.

2) *Concatenation of shuffled feature vectors:* The next step is to concatenate the shuffled vectors process S_1, S_2, S_3, S_4, S_5, and S_6. Here, concatenate the shuffled fingerprints S_1 and S_2 with the shuffled eye retina features S_3 and S_4 and face features S_5, and S_6 respectively. The concatenation of the vectors S_1S_3 and S_5 is carried out as follows:

i. A vector M_1 of size $|S_1|+|S_3|+|S_5|$ is created and its first $|S_3|$values are filled with S_1 and $|S_5|$ values are filled with S_3.

ii. For every component S_1,

a) The corresponding indexed component of M_1 say 't' is chosen.

b) Logical right shift operation is carried in M_1 from index 't'.

c) The component of $S_1$is inserted into the emptied tth index of M_1.

The aforesaid process is carried out between shuffled vectors $S_2$and $S_4$to form vector M_2 and shuffled vectors S_4 and S_6 to form vector M_3. Hereby, the concatenation process results with three vectors M_1, M_2 and M_3.

3) *Merging of the concatenated feature vectors:* The last step in generating the multimodal biometric template B_T is the merging of three vectors M_1, M_2 and M_3. The steps involved in the merging process are as follows.

i. For every component of M_1, M_2 and M_3,

a) The components M_{11}, M_{21}, and M_{31} are converted into their binary form.

b) Binary NOR operation is performed between the components M_{11}, M_{21} and M_{31}.

c) The resultant binary value is then converted back into decimal form.

ii. These decimal values are stored in the vector B_T, which serves as multimodal biometric template.

After fused those features, generating cryptographic key using feature level fusion [42].

3.4. Cryptographic Key Generation Using Feature Level Fusion

The feature vectors generated from the fingerprint, retina and face images are fused at the feature level to generate a new merged feature vector. Then the cryptographic key is generated from the merged feature vector. The strength of cryptography can be measured based on the stability of cryptographic keys generated from uncertain biometrics. The matrix Fused DM is used for generating cryptographic key which can be used to transfer information in a more secure manner.

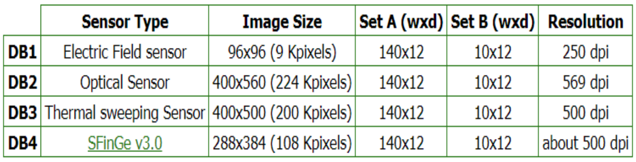
The key generated can be used to encrypt the data by the sender before transmission. The key used to encrypt the message should be sent to the receiver in order to decrypt the encrypted message [41].

IV. EXPERIMENTAL RESULTS

The experimental results of the proposed approach have been presented in this section. The proposed approach is implemented in MATLAB (Matlab7.4) and tested with different sets of fingerprints, eye retina, and face images of the corresponding individuals. Fingerprint verification competition 2006 (FVC2006) is used in this work for biometric authentication. Four different databases (DB1, DB2, DB3 and DB4) were collected by using the following sensors/technologies: Each database is 150 fingers wide and 12 samples per finger in depth (i.e., it consists of 1800 fingerprint images). Each database will be partitioned in two disjoint subsets A and B:

1. Subsets DB1-A, DB2-A, DB3-A and DB4-A, which contain the first 140 fingers (1680 images) of DB1, DB2, DB3 and DB4, respectively, will be used for the algorithm performance evaluation.
2. Subsets DB1-B, DB2-B, DB3-B and DB4-B, containing the last 10 fingers (120 images) of DB1, DB2, DB3 and DB4, respectively, will be made available to the participants as a development set to allow parameter tuning before the submission.

Table 1: Sensor Types and Dataset Information



	Sensor Type	Image Size	Set A (wxd)	Set B (wxd)	Resolution
DB1	Electric Field sensor	96x96 (9 Kpixels)	140x12	10x12	250 dpi
DB2	Optical Sensor	400x560 (224 Kpixels)	140x12	10x12	569 dpi
DB3	Thermal sweeping Sensor	400x500 (200 Kpixels)	140x12	10x12	500 dpi
DB4	SFinGe v3.0	288x384 (108 Kpixels)	140x12	10x12	about 500 dpi

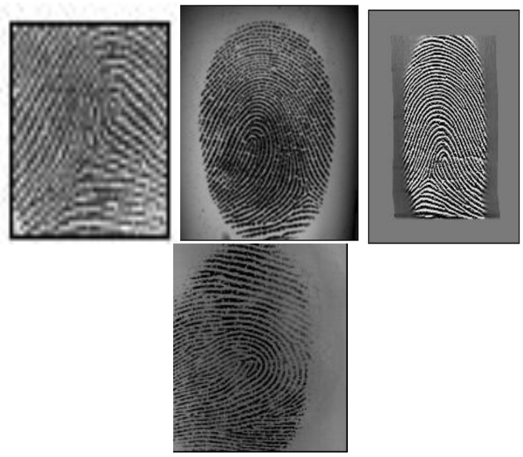


Figure 4: Fingerprint Verification Competition 2006 (FVC2006) Images

Digital Retinal Images for Vessel Extraction (DRIVE) database has been established to enable comparative studies on segmentation of blood vessels in retinal images. The research community is invited to test their algorithms on this database and share the results with other researchers through this web site are shown in figure 5.

Figure 5: DRIVE Image Sample

The Specs on Faces (SoF) dataset, a collection of 42,592 (2,662×16) images for 112 persons (66 males and 46 females) who wear glasses under different illumination conditions. The dataset presents a new challenge regarding face detection and recognition. It is focused on two challenges: harsh illumination environments and face occlusions, which highly affect face detection, recognition, and classification. The glasses are the common natural occlusion in all images of the dataset. However, there are two more synthetic occlusions (nose and mouth) added to each image. Moreover, three image filters, that may evade face detectors and facial recognition systems, were applied to each image. All generated images are categorized into three levels of difficulty (easy, medium, and hard). That enlarges the number of images to be 42,592 images (26,112 male images and 16,480 female images). There is metadata for each image that contains much information such as: the subject ID, facial landmarks, face and glasses rectangles, gender and age labels, year the photo was taken, facial emotion, glasses type etc.

Figure 6: Sample of SoF Dataset

Evaluation of the Multimodal Biometrics

The evaluation of the proposed multimodal biometric was done against the Binary Key Generation (BKG) and the fingerprint and voiceprint developed using Soft Computing Method (SCM). The voiceprint and fingerprint were also evaluated against each other to establish which performs better than the other.

Recall

Recall evaluates the percentage of actual positive which classifies actual image as actual. The sensitivity is defined as below:

$$Recall = \qquad (23)$$

$\frac{T_p}{T_p+F_n}$allT_p/T_p+F_n

Where $T_p$defines the face image correctly as face image. F_p defines the non-face image incorrectly as the non-face image.$F_n$defines the non-face image incorrectly as the face. $T_n$defines the non-face correctly as non-face.

Precision

Precision is defined as the proportion of the true positives against both true positives and false positives results for multimodal biometric images. It is defined as follows.

$$Precision = \qquad (24)$$

$\frac{T_p}{T_p+F_p}$cisionT_p/T_p+F_p

Accuracy

Accuracy is defined as the overall correctness of the model and is calculated as the sum of actual classification parameters $(T_p + T_n)$ separated by the total number of classification parameters $(T_p + T_n + F_p + F_n)$.

$$\text{Accuracy} = \qquad (25)$$

$\frac{T_p+T_n}{T_p+T_n+F_p+F_n}$uracy=T_p+T_n/T_p+T_n+F_p+F_n

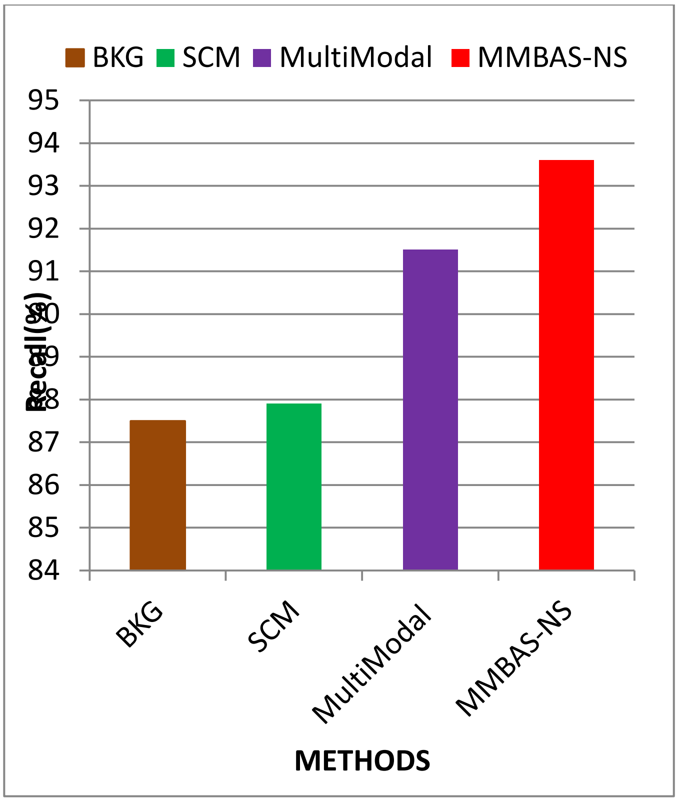


Figure 7: Recall comparison with Different Methods

Figure 7 shows that the recall evaluation of the proposed MMBAS-NS method is better than the existing methods. The proposed MMBAS-NS produces higher recall results of 93.6%, whereas BKG method metric is 87.5 %, SCM method metric is 87.9% and the multimodal method metric is 91.5%. Figure 7 shows better recall result in comparison to other methods.

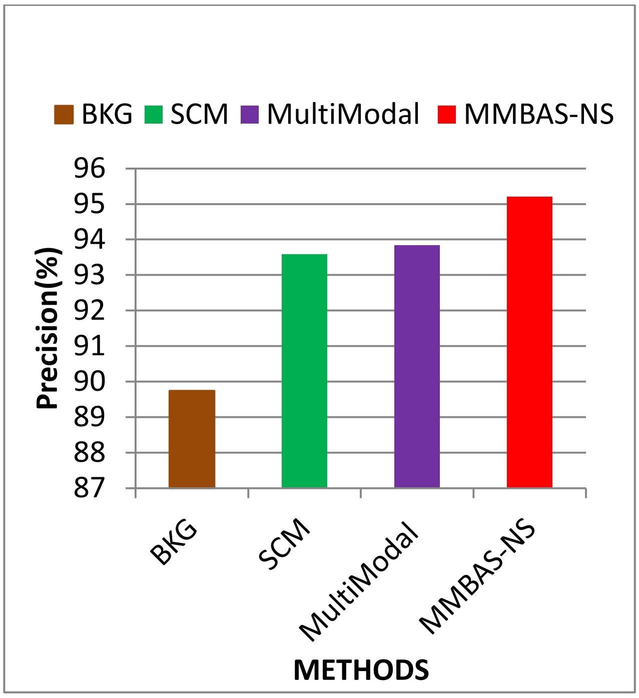


Figure 8: Precision comparison with Different Methods

Precision comparison of the proposed MMBAS-NS method is better than the existing methods. The proposed MMBAS-NS produces higher Precision results of 95.2%, whereas BKG method metric is 89.7 %, SCM method metric is 93.5% and the multimodal method metric is 93.83%. As shown above, figure 8 shows better Precision in comparison to other methods.

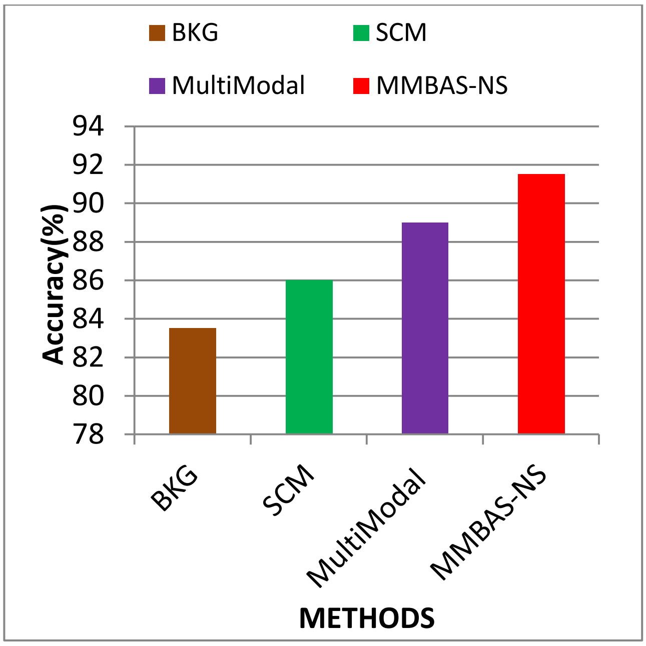


Figure 9: Accuracy comparison with Different Methods

Accuracy comparison of the proposed MMBAS-NS method is better than the existing methods. The proposed MMBAS-NS produces higher Accuracy results of 91.52%, whereas The BKG method metric is 83.5 %, SCM method metric is 86.00% and the multimodal method metric is 89.00%. Figure 9 shows better accuracy results in comparison to other methods.

The performance evaluation is done using the FAR (false acceptance rate) and FRR (false rejection rate).

$$FAR = \frac{N_a}{N} \qquad (26)$$

$$FRR = \frac{N_r}{N} \qquad (27)$$

Where $N_a$is the number of imposters which were falsely accepted i.e. scores of imposters match are more than T. N_r is the number of genuine samples which were false rejected i.e. score of genuine match T; N is total number of matches; T is the threshold.

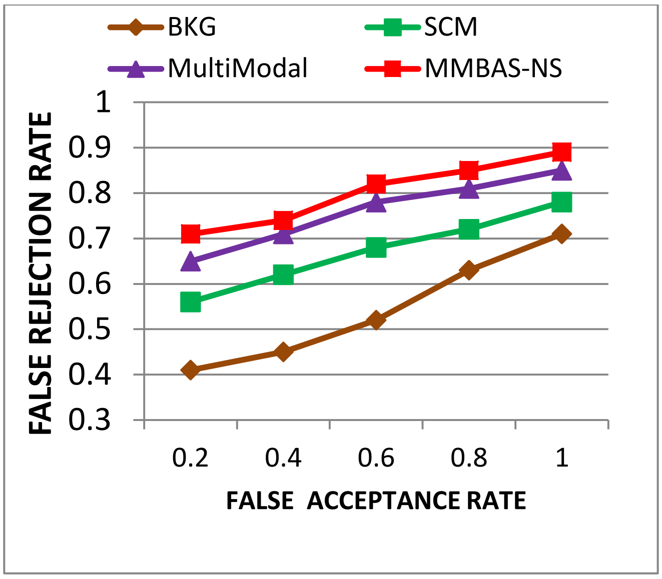


Figure 10: FAR Versus FRJ (authentication methods)

The above figure 10 shows that the Evaluation of the proposed MMBAS-NS system. It can be seen that the MMBAS-NS system has a better performance and also reduces the error rates (FAR and FRR) of the individual other model systems.

V. CONCLUSION AND FUTURE WORK

In this paper, mobile verification-based network security is performed using multi-modal biometric authentication. In this work, fingerprint, face and retina images are taken as input from benchmark database. The fingerprint, face and retina images are subjected to pre-processing using adaptive median filtering and Otsu's segmentation is applied to remove background pixels to enhance the image quality. Then the minutiae feature of the pre-processed images are extracted using Local Binary Pattern (LBP) and fused at the feature level by Binary NOR operation to create a merged template. And finally, the cryptographic key is generated for security using mobile verification. The main advantage of utilizing biometric for key generation is its high availability and adjustable security levels; on the other hand, biometrics brings in non-repudiation and eradicates the necessity to memorize passwords or to carry tokens. In future, we will explore subspace analysis and sum, multiplication based fusion methods for feature fusion and multi-modal biometric authentication can also be applied to MANETS (Mobile Adhoc Networks).

REFERENCES

1. La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE communications surveys & tutorials, 15(1), 446-471.
2. Jobanputra, N., Kulkarni, V., Rao, D., & Gao, J. (2008). Emerging security technologies for mobile user accesses. The electronic Journal on E-Commerce Tools and Applications.
3. Dedo, D. (2004). Windows mobile-based devices and security: Protecting sensitive business information. Microsoft Corporation Apr.
4. Schneider, K. N. (2013). Improving data security in small businesses. Journal of Technology Research, 4, 1.
5. Mahmood, S., Amen, B., & Nabi, R. M. (2016). Mobile Application Security Platforms Survey. International Journal of Computer Applications, 133(2), 40-46.
6. Sabhanayagam, T., Venkatesan, V. P., & Senthamaraikannan, K. (2018). A Comprehensive Survey on Various Biometric Systems. International Journal of Applied Engineering Research, 13(5), 2276-2297.

A. K. Jain, A. Ross and S. Pankanti, "Biometrics, A Tool for Information Security", IEEE Transactions on Information Forensics And Security, 2006, vol.1, no.2, pp. 125 – 144.

7. Kataria, A. N., Adhyaru, D. M., Sharma, A. K., & Zaveri, T. H. (2013, November). A survey of automated biometric authentication techniques. In Engineering (NUiCONE), 2013 Nirma University International Conference on (pp. 1-6). IEEE
8. Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Ahmad, N. S., & Shakir, M. M. D. (2017). A Survey on the Cryptographic Encryption Algorithms. Proceeding of (IJACSA) International Journal of Advanced Computer Science and Applications, 8(11).
9. James Wayman, Anil Jain, Davide Maltoni and Dario Maio, "An Introduction to Biometric Authentication Systems". In Biometrics:Technology, Design and performance evaluation. Springer Publications. ISBN 978-0-7923-8345-1.
10. Kapoor, V., & Verma, S. "A survey of various Cryptographic techniques and their Issues" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 12, December 2014.
11. Parvathi Ambalakat, "Security of Biometric Authentication Systems", in proceedings of 21st Computer Science Seminar, 2005.
12. AlMahafzah, H., & AlRwashdeh, M. Z. (2012). A survey of multibiometric systems. arXiv preprint arXiv:1210.0829.
13. EL-SAYED, A. Y. M. A. N. (2015). Multi-biometric systems: a state of the art survey and research directions. IJACSA) International Journal of Advanced Computer Science and Applications, 6.
14. Jagadeesan, A., Thillaikkarasi, T., & Duraiswamy, K. (2010). Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. Int. J. Comput. Appl, 2(6), 16-26.
15. Feng, Q., He, D., Zeadally, S., & Wang, H. (2018). Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. Future Generation Computer Systems, 84, 239-251.
16. Naidu, P. A., Prasad, C. H. G. V. N., Prasad, B., & Bodla, B. "Fingerprint and Palmprint Multi-Modal Biometric Security System". International Journal of Engineering and Applied Computer Science Volume: 02, Issue: 05, May 2017.
17. Jagadiswary, D., & Saraswady, D. (2016). Biometric authentication using fused multimodal biometric. Procedia Computer Science, 85, 109-116.
18. Lalithamani, N., & Sabrigiriraj, D. M. (2014). Technique to generate a face and palm vein-based fuzzy vault for a multi-biometric cryptosystem. Machine Graphics and Vision, 23(1/2), 97-114.
19. Kanade, S., Petrovska-Delacrétaz, D., & Dorizzi, B. (2009, September). Multi-biometrics based cryptographic key regeneration scheme. In Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on (pp. 1-7). IEEE.
20. Sanjay Kumar, Surjit Paul, Dilip Kumar Shaw "Real-Time Multimodal Biometric User Authentication for Web Application Access in Wireless LAN" Journal of Computer Science 2017, 13 (12): 680.693
21. Sarier, N. D. (2018). Multimodal biometric identity based encryption. Future Generation Computer Systems, 80, 112-125.
22. Ali, Z., Hossain, M. S., Muhammad, G., Ullah, I., Abachi, H., & Alamri, A. (2018). Edge-centric multimodal authentication system using encrypted biometric templates. Future Generation Computer Systems, 85, 76-87.
23. Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2015). Continuous user authentication using multi-modal biometrics. Computers & Security, 53, 234-246.
24. Gomez-Barrero, M., Galbally, J., & Fierrez, J. (2014). Efficient software attack to multimodal biometric systems and its application to face and iris fusion. Pattern Recognition Letters, 36, 243-253.
25. Vazquez-Fernandez, E., & Gonzalez-Jimenez, D. (2016). Face recognition for authentication on mobile devices. Image and Vision Computing, 55, 31-33.
26. Galdi, C., Nappi, M., & Dugelay, J. L. (2016). Multimodal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity. Pattern Recognition Letters, 82, 144-153.
27. Snelick, R., Uludag, U., Mink, A., Indovina, M. and Jain, A., 2005. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. IEEE transactions on pattern analysis and machine intelligence, 27(3), pp.450-455.
28. Li, S.Z. (ed.): Encyclopedia of Biometrics (First Edition), Springer Reference (2009).
29. Henniger, O., Scheuermann, D. and Kniess, T., 2010, March. On security evaluation of fingerprint recognition systems. In Internation Biometric Performance Testing Conference (IBPC), pp. 1-10.
30. Kanade, S., Camara, D., Krichen, E., Petrovska-Delacrétaz, D. and Dorizzi, B., 2008, Three factor scheme for biometric-based cryptographic key regeneration using iris. In Biometrics Symposium, pp. 59-64.
31. Kanade, S., Petrovska-Delacrétaz, D. and Dorizzi, B., 2010, Generating and sharing biometrics based session keys for secure cryptographic applications. Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1-7.
32. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol – Version 1.2",RFC 5246, IETF Network Working Group, August (2008).
33. Salles-Loustau, G., Berthier, R., Collange, E., Sobesto, B., Cukier, M.: Characterizing Attackers and Attacks: An Empirical Study. IEEE 17th Pacific Rim International Symposium on Dependable Computing (PRDC), pp.174-183, 2011.
34. Krishna, N.M. and Reddy, P.C.S., 2014. A Dimensionality Reduced Iris Recognition System with Aid of AI Techniques. Global Journal of Research in Engineering, pp.1-17.
35. He K., J. Sun, and X. Tang, "Guided image filtering," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35,no. 6, pp. 1397–1409, 2013.
36. Yang J., J. Yang, and Y. Shi, "Finger-vein segmentation based on multichannel even-symmetric gabor filters," IEEE International Conference on Intelligent Computing and Intelligent Systems, Vol. 4. 2009, pp. 500–503.
37. Abhilash Sharma1, and Ms. Rajani Gupta, 2015. Iris recognition based learning `vector quantization and local binary patterns on iris matching. International Journal of Technical Research and Applications, vol.3, no. 5 , pp. 7-14.
38. Xu, J., Cha, M., Heyman, J.L., Venugopalan, S., Abiantun, R. and Savvides, M., 2010, September. Robust local binary pattern feature sets for periocular biometric identification. Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1-8.
39. Sahu, D.K. and Parsai, M.P., 2012. Different image fusion techniques–a critical review. International Journal of Modern Engineering Research (IJMER), 2(5), pp.4298-4301.
40. Chang, Y.J., Zhang, W. and Chen, T., 2004, Biometrics-based cryptographic key generation. IEEE International Conference on Multimedia and Expo, 2004. pp. 2203-2206.
41. Nandakumar, K., Jain, A.K. and Pankanti, S., 2007. Fingerprint-based fuzzy vault: Implementation and performance. IEEE transactions on information forensics and security, 2(4), pp.744-757.