3WAY-ACCESS

by Three Way Authentication

Submission date: 23-Aug-2019 05:03PM (UTC+0530)
Submission ID: 1162674859
File name: ENCRYPT_ME-WITHOUT-REFERENCES.docx (968.75K)
Word count: 3933
Character count: 22982

3-WAY WEIGHT BASED AUTHENTICAION USING BIOMETRICS & DATA MINING

ABSTRACT:

In recent years, security and privacy are very important to keep our data safely. The normal cryptographic key generation for encryption and decryption is not highly secured in this modern world. This work introduced biometric concept for cryptography key generation for authentication process. Behavioral and physical characteristics are measured to identify individuals by biometrics. As every individual has a unique identity like IRIS, finger prints, palm prints, retinal, face, etc. It is difficult to strengthen the security process using single modality biometric system as it dealt with decision making. So, it is important to introduce multimodal biometric system which uses dual finger print, face and retina images for creating a multimodal template. This work also adopted SVM classifier for performing verification as well as validation. The given user biometric feature vector is verified using the existing binary digit of the individual personal key for acceptance or rejection. The multimodal template can be further used to generate the cryptography key. This proposed approach using weights can be helpful to simplify the key generation process but also increases the security of the data as well as privacy of users.

KEYWORDS:

Support Vector Machine, Multi-Modal Biometric

INTRODUCTION

Backbone of the modern security lies on Cryptography and cryptographic techniques for establishing security controls. The traditional and typical authentication which uses conventional cryptography purely depends on the secret codes such as passwords or token codes. These approaches may not be able to identify and validate the users in the real time effectively. Actual authentication of users could be carried out with the help of Biometrics like fingerprints, IRIS, retinal, and face recognitions. These techniques are more powerful compared to traditional authentication methods. Biometric data provides numerous preferences when compared with normal frameworks as these can't be speculated and overlooked [2].

Cryptography [4] signifies "secret writing". It is utilized for not only to provide exclusive privacy information in addition to that it is aimed to give answers for different issues like information honesty, confirmation, non-disavowal, Access control, and Availability of the pertinent security information. The plaintext is Original information, which is decipherable either by an individual or by a PC. While the ciphertext, which is muddled, without the best possible figure to unscramble it. The way toward encoding the plaintext into ciphertext is considered as encryption. Whereas inverting of unraveling ciphertext to plaintext is called Decryption. So the generation process

requires calculation and key for both encryption and decryption. Key assumes an imperative job in cryptography in light of the fact that the calculation legitimately relies upon it. The data encryption is classified into two unique classes namely symmetric and asymmetric encryption which is represented in Figure 1.1.

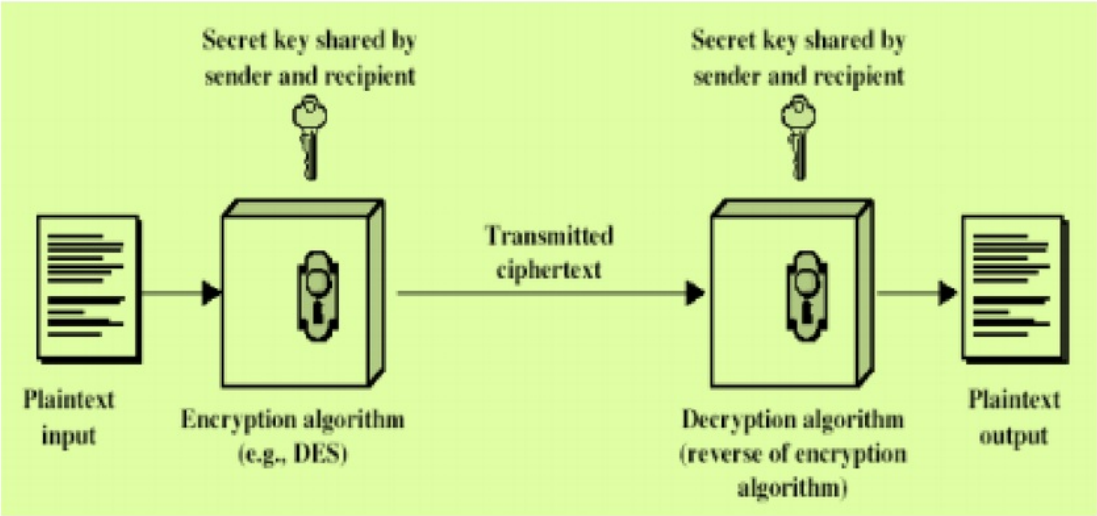


Figure 1.1: Symmetrical Encryption Model

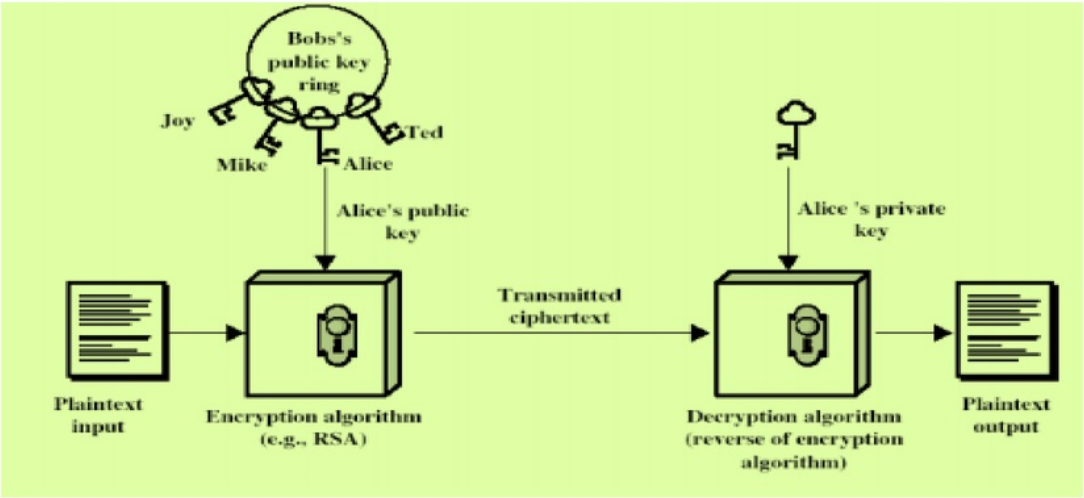


Figure 1.2: Asymmetric Encryption Model

The key used for encryption is once again used in decryption in symmetric encryption. This technique is also called as regular or mystery key encryption. One of the fundamental focal points of utilizing the symmetric key encryption is that the computational intensity of this encryption system is little. Figure 1.1 depicts to the model for ordinary encryption. In asymmetric encryption scheme, distinguishing keys are utilized for unscrambling and encryption. It is otherwise called open key or public encryption. Figure 1.2 represent the model for Asymmetric Encryption.

Biometric is the estimation of biological information [7] and it is usually personal attribute of individual which is robust, measurable and distinctive. Biometric indicates and provides the confirmation of qualities through fingerprint, marks and other human attributes. Biometric aims to provide validation when compared with other cards, keys, passwords and frameworks. The recognizable proof of an individual usually end up in using secret keys and PINs [5]. To avoid the theft of card ids and observations of things by others, biometrics would be ideal as they resolve this type of issues. Additional security protection can be provided using different type or modal of biometrics like hand geometry, face, IRIS, retinal, voice and fingerprint. The biometric system which is represented in Figure 1.3 contains four major components namely Input Interface, Output Interface, Processing unit and data store.

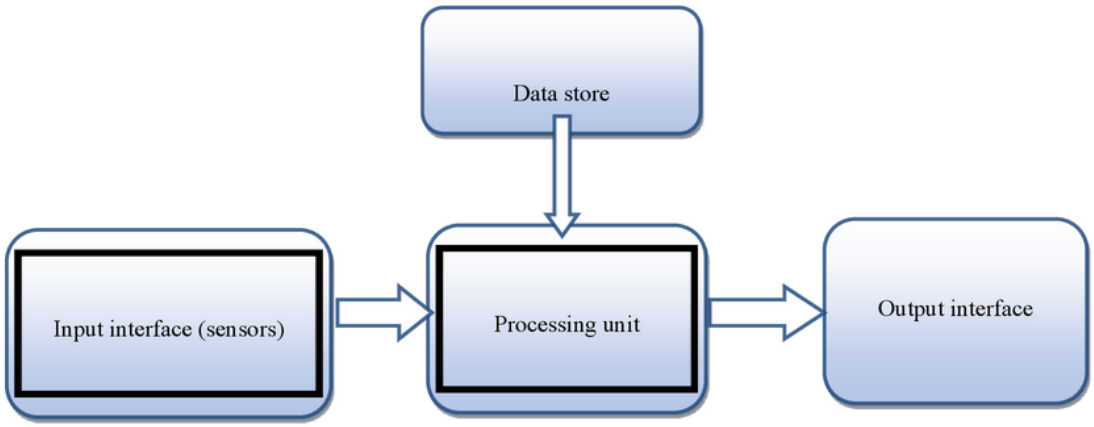


Figure 1.3: Components of Biometric System

The first component is Input Interface which includes set of sensors which translate biological data of human aspects into digital data. Input interface includes sensor component for converting human biological data into digital data. CMOS and/or CCD will be used for IRIS, Retinal, Fingerprint, and Face recognitions. For voice recognition microphone is used whereas for fingerprint optical sensors are used. In the processing unit of the biometric system either DSP or a capable small computer is used for data obtained from the input interfaces. The central part of the biometric system performs the processing of the images such as normalization, enhancements and feature extraction. Apart from that the processing component also performs the comparison of the samples in the database store. The storage component of database store is used for performing verification process. Either EPROM or RAM will be used for authentication proof and for a quick verification contactless or contact smart is utilized as a storage component. The output interface will enable access to the users through interfaces such as RS232 (Serial communication interface), USB, TCP/IP, Bluetooth or Wifi.

The Biometrics systems are broadly classified as physiological and behavioral to determine the identity of the individual. For proper estimation, distinctive qualities of both were used. Image Scan of Retina, Hand, Finger, Face and IRIS were treated as physiological biometrics as they were aiming of the portion of the body directly for scanning and estimation. Mark outputs and voice sweep can be viewed as social biometrics as they directly depend on the information for the estimation. The time of the activity is very important for social biometrics for example what time the word was spoken or marked arrangement of words from starting point to end point. This type of classifications is very much helpful for further innovations for supporting specific factors and further enhancing security improvements. The distinctions from physiological and behavioral could help to identify artificial similarity and fake identities. Social biometrics are treated as extents to physiology, for example, skill of hands and fingers in mark check and state of the vocal lines in voice. It is important to pay attention to the conduct of the users or clients during the biometric processing for example, how they show a finger or how they take a glance at the camera [13]. Figure 1.4 contains the information about the classification of biometric.

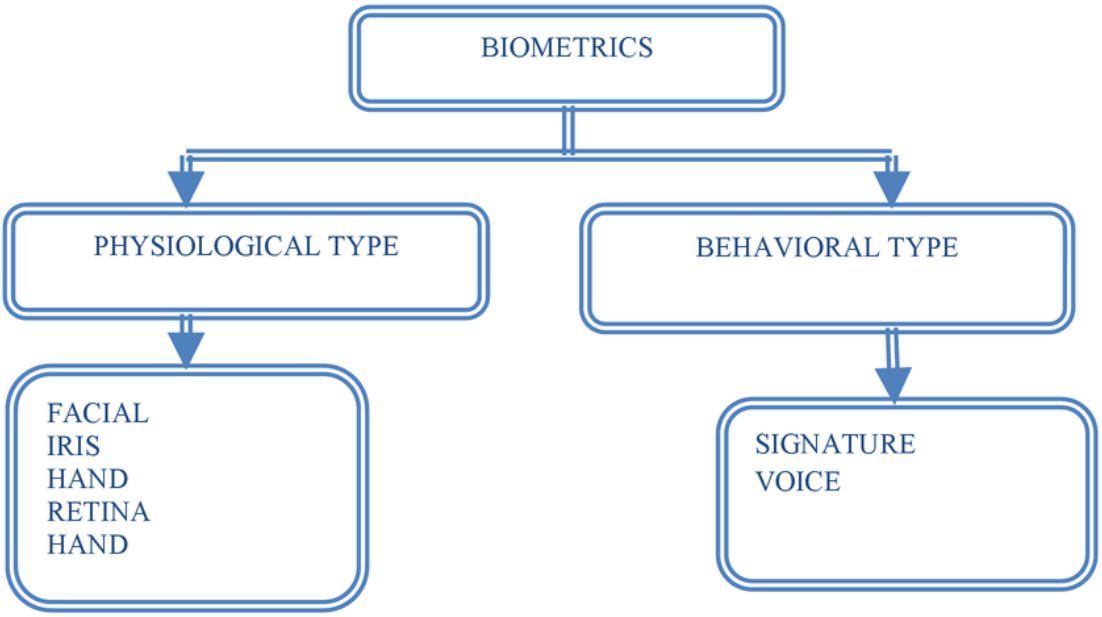


Figure 1.4: Classification of Biometrics

The following sections discusses about the basic requirements for biometric methods for collecting Physical and Behavioral characteristics. These requirements could be practical and theoretical might be theoretical or practical.

A Biometric modal can be basically classified into two categories. They are Unimodal and Multimodal. Prior to adopting the right biometric technique, it is imperative to ask whether to choose unimodal or multimodal. There exist many challenges when deploying single or unimodal biometric system for large population. Susceptibility towards noisy or bad data is an important feature to be looked at for the sensors. The captured biometric feature can be distorted due to bad acquisition and the quality of the images can also be affected due to the environment conditions especially illumination. Lack of power and issues with power in the sensor environment can affect the quality of image, so it is important to have multiple images apart from taking one single image sample. The features retrieved from the image samples can be used to develop a biometric key for encryption of text messages.

The passwords being weak or enabled as compromised are the primary reasons for the common security incidences and data breaches. The main door or entry point for hacker is the password

entry and even a strong password could not stop the attacks. Biometrics are less vulnerable compared to password based and other traditional mechanisms. Fingerprint Proper recognition of fingerprint checks for exclusive patterns of valleys and ridges in the user's fingerprint. Most of the times, these are unique for every person and therefore enable to identify the person from the large set of population. At the same time, single trait biometric does not provide better authentication and introduces many limitations and issues for attacks.

LITERATURE REVIEW:

Rane et al (2013) reviewed different biometrics and referred secure biometric and biometric template protection as a strategy for addressing different security issues. Biometrics assumes a significant job in personality confirmation and access control. Biometrics are appealing as individual characteristic or properties which always vary between person to person. Unlike passwords or tokens, these measures should not be recollected again and again and can't be lost. Biometrics are crucial and constantly shows slight varieties among the estimations [12].

Jadhav et al (2015) presented a computerized framework dependent on biometric unique finger impression verification. For this situation, fingerprints are valuable for the different administrations of government or association or business. Unique mark Matching calculations are utilized for correlation of recently put away formats of fingerprints with client fingerprints for the verification procedure. This work exhibited a sort of this sort of Fingerprint acknowledgment framework and this framework that can be effectively executed. In the meantime, the full execution of such a model will accomplish the goals like security, proficiency, dependability, and simple to-use by numerous individuals on the planet [6].

Kang and Park (2009) proposed a multi biometric framework dependent on unique mark and mark recognition. proposed another multimodal biometric acknowledgment dependent on the combination of finger vein and finger geometry. This examination demonstrates three curiosities contrasted with past works. In the first place, this is the principal way to deal with join the finger vein and finger geometry data in the meantime. Second, the proposed strategy incorporates another finger geometry acknowledgment dependent on the consecutive deviation estimations of finger thickness extricated from a solitary finger. Third, coordinate finger vein and finger geometry by a score-level combination strategy dependent on a help vector machine. Results demonstrate that acknowledgment exactness is essentially improved utilizing the proposed technique [8].

Tayal et al (2009) proposed a multimodal biometric framework that consolidates iris acknowledgment and speaker distinguishing proof framework utilizing the vitality compaction and

time-recurrence goals of wavelet examination. The uniqueness of the iris design and the strength of speaker recognizable proof dependent on pitch period estimation supplement each other in the proposed framework. This work likewise basically breaks down the execution of Daubechies wavelets (Db3 and Db4) in the investigation of iris and discourse tests with an undertaking to have a high achievement rate with ideal computational intricacy [14].

Kumar and Zhang (2009) presented exhibited another technique for individual verification utilizing face and palm print pictures. The facial and palm print pictures can be at the same time procured by utilizing a couple of computerized camera and incorporated to accomplish higher trust in close to home verification. This strategy utilizes the guaranteed personality of clients as an element for combination. Subsequently the required loads and predisposition on individual biometric coordinating scores are consequently processed to accomplish the most ideal presentation. The test results additionally show that additional computation principles for accomplishing improvements in execution. The technique proposed in this work can be stretched out for any multimodal validation framework to accomplish higher execution [9].

Kumar and Farik (2016) concentrated on multimodal biometric confirmation frameworks being used today. The point is to inspire the best blend of verification factors for multimodal use. They contemplate the qualities and shortcoming of chose biometric instruments and prescribe novel answers for incorporate into multimodal biometric frameworks to enhance the current biometric downsides. The creator trusted this work will furnish security specialists with some valuable knowledge while structuring better biometric frameworks. As confirmation is the way toward approving the personality of an individual dependent on certain info that the individual gives. Confirmation has turned into a noteworthy subject of research because of the expanding number of assaults on computer networks far and wide [10].

Parkavi et al (2017) provided staggered verification for the frameworks using multimodal biometrics for recognizing the people. Multimodal confirmation gives more dimensions or views for the purpose of verification when compared with single biometric like palm print or face or unique mark with a user. This work applied unique mark and IRIS of an individual for the programmed distinguishing proof of a person by consolidating unique mark and the IRIS of an individual. Edge discovery and minutiae coordination were applied and utilized. Both FRR and FAR were evaluated and shown ways to control precision by limiting FAR [11].

Asha and Chellappan (2008) proposed a validation framework with multi-biometrics to help different administrations in e-Learning where client confirmation is important. E-learning frameworks speak to another type of learning and are winding up increasingly well-known each

day. Security in e-Learning has turned into a major necessity. So to validate an e-student particularly if there should be an occurrence of e-tests is a noteworthy test in an e-learning condition. Client validation techniques can be arranged into three classifications: (1) strategies dependent on human memory, for example, passwords, (2) strategies dependent on physical gadgets, for example, attractive or Integrated Circuit (IC) cards, and (3) strategies dependent on biometrics, for example, unique mark, iris, and so on., Hence, Multi-modular biometric improves the unwavering quality of confirmation as single biometric verification innovation can't fulfill a required dependability level [3].

Besbes et al. [1] proposed a multi-modal biometric system which enhanced recognition accuracy and population coverage by using iris and fingerprint. Shahin et al. [2] proposed a high security system by fusing hand veins, hand geometry and fingerprint. Kumar and Ravikanth [3] proposed an approach for personal authentication using both finger geometry and dorsal finger knuckle surface features provides a high performance in person authentication. Chandra et al. [4] worked and proposed a method to improve the efficiency by integrating the features of iris and fingerprint. Chin et al. [5] suggested a proposal at which combines the features of palm print and fingerprint and a series of steps are applied on palm and finger print to increase performance and for feature extraction of 2D by implementing Gabor filter at feature level. Sheetal Chaudhary and Rajender Nath proposed a system by integrating palm print, fingerprint and face based on score level fusion [6]. Fan Yang and Baofeng Ma proposed a method to build an identity by combining different features like fingerprint, hand geometry, palm print comparison score fusion [7]. Muhammad Imran Razzak et. al. [8] proposed a multi-modal recognition system using the biometric traits like face and finger vein. This system effectively reducing the error rates like FAR (False Acceptance Rate) and thereby increases AAR (Authentic Acceptance Rate).

Gidudu Anthony, Hulley Greg and Marwala Tshilidzi (2007) proposed a simple image classification technique using Support Vector Machine (SVM). They compared the implementation of SVM using One-Against-One (1A1) and One-Against-All (1AA) techniques and evaluated their results in the field of remote sensing and land mapping.

Seyyed et al.[26] proposed Automatic MRI image threshold using Support Vector Machines. The number of thresholds in the segmented image determines the classification accuracy.

Vasta et al. [27] proposed an intelligent 2v-support vector machine-based match score fusion algorithm. The proposed method integrates the quality of images in order to improve the recognition performance of face and iris modalities. A face-iris multimodal biometric system based on matching score level fusion using support vector machine (SVM)

CRYPTOGRAPHIC KEY GENERATION PROCESS DESIGN:

There are many novice users doesn't even use the lock code or secured mechanism to either access or protect their confidential data. So, if the phones are stolen the saved account and password information can be used to mishandle the concerned bank accounts or their confidential data [3]. Many smartphone users store the email id and password and hence the access codes or messages retrieved in the emails can be easily used for accessing the bank and/or other web sites or applications. In this paper, to overcome these issues, cryptographic key generation using multimodal biometric authentication for the security of mobile phones is proposed. The following has the proposed algorithm using weight based authentication for three different images.

Step 1: The fingerprint database (fin_db1), face database (fac_db2) and retinal database (ret_db3) are the inputs to this algorithm.

Step 2: The weight for fingerprint ($w_{1)}$), face ($w_{2)}$), and retinal image ($w_{3)}$) is initialized to 33.33 i.e., $w_1 \leftarrow 33.33$, $w_2 \leftarrow 33.33$ and $w_3 \leftarrow 33.33$.

Step 3: The image match score threshold is set as 0.6(or 60%) i.e., match_threshold ← 0.6

Step 4: Capture the real-time fingerprint, face, and retina images of the user.

Step 5: Apply SVM classifier algorithm to classify the image type.

Step 6: Search the image type in the image type in the image stores fin_db1, fac_db2, and ret_db3 using binary search.

Step 7: If (match1 and match2 and match3) found then

Step 7.1: If (fin_img_match_score >= match_threshold and fac_img_match_score >= match_threshold and ret_img_match_score>= match_threshold) then

generate the fused key from the three image templates.

Step 7.2 else Calculate minimum match scores for finger, face, and retina images as

fin_min_match_score ← w_1 * fin_img_match_score,

fac_min_match_score ←w_2 * fac_img_match_score

and ret_min_match_score ←w_3*ret_ing_match_score.

Step 8: If (fin_min_match_score+fac_min_match_score+ret_min_match_score >= 0.45)

then the user is authenticated, and a unique key is created from 3 image templates.

else

user authentication fails and a user record is created in the failure database.

Step 9: Train the SVM model to give different weights based on failure count and the biometric modal probability.

The databases fin_db1, fac_db2, and ret_db3 are given as input to this algorithm. fin_db1 is the fingerprint template database, fac_db2 is the face template database, and ret_db3 is the retina template database. The initial weights for the fingerprint, face, and retina images is given as 33.33. The image match threshold for each of the three images is set as 0.6 i.e., img_match_threshold is equal to 0.6. This means that if the value of any image's image match score is equal to or greater than 0.6 then we consider it a match. This signifies that the real-time user template generated matches with the stored template in the database.

The real-time images of fingerprint, face, and retina of the user are captured using their respective sensors. The templates of these images are stored in the template databases for further processing. The Support Vector Machine (SVM) classification algorithm is applied to classify the type of the image. As SVM is a supervised machine learning algorithm, we train the machine beforehand about the input image types. Based on the previous knowledge, the machine reads the input data provided and classifies the input images into their corresponding type. Search for the matching templates of fingerprint, face, and retina images in the image template databases such as fin_db1, fac_db2, and ret_db3 using their respective matching algorithms. Here, we consider two cases. Both two cases are explained in the below sections.

Case I: If the template matches for the fingerprint, face, and retina are found, then we calculate the image match scores for all the three images as fin_img_match_score, fac_img_match_score, and ret_img_match_score. If the values of image match scores of all the fingerprint, face, and retina images is greater than the image match threshold value i.e., img_match_threshold, then we generate a merged template from the individual templates of fingerprint, face, and retina. A unique cryptographic key is also generated from the fused template that can be used to encrypt the information at the sender side and used at the receiver side to decrypt the information back to original form. This aids in secure transmission of information n in the context of network security.

Case II: If the template matches for all the three images are not found, then we calculate minimum match scores for fingerprint, face, and retina images as

fin_min_match_score as w_1 * fin_img_match_score,

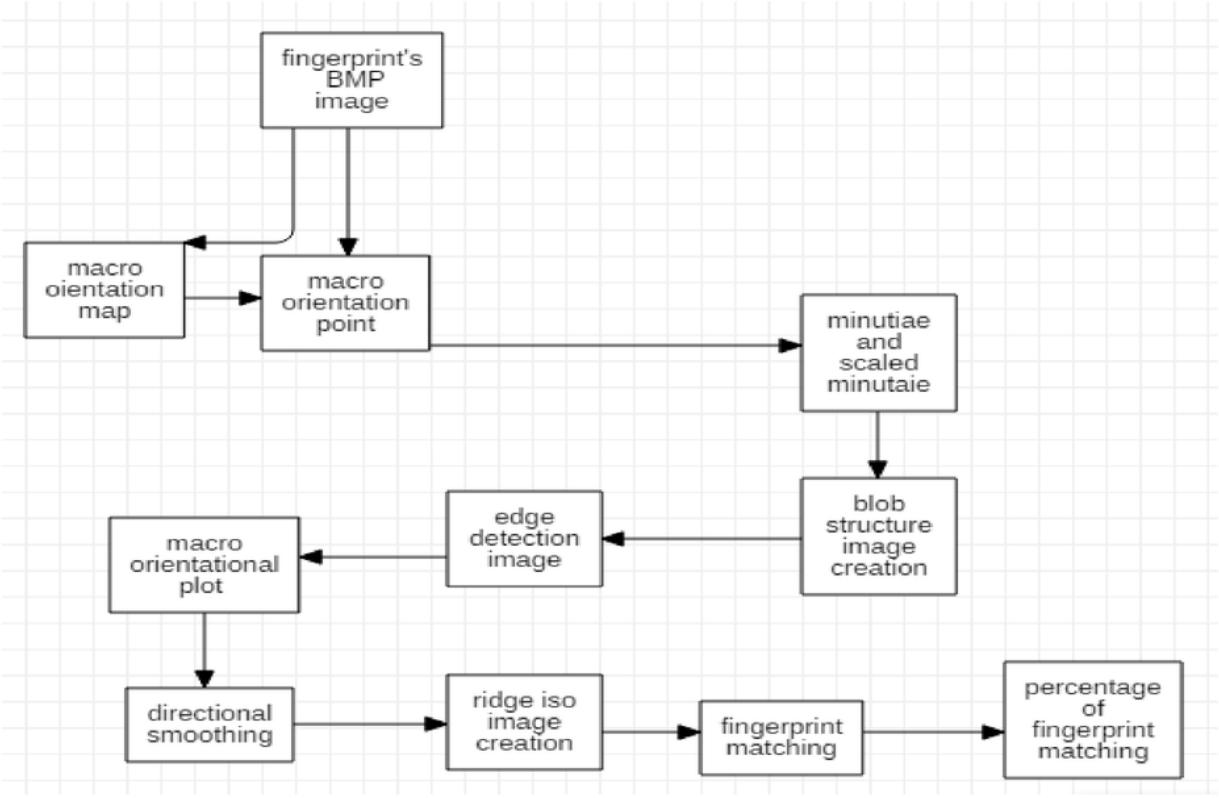
fac_min_match_score as w_2 * fac_img_match_score, and

ret_min_match_score as w_3 * ret_img_match_score.

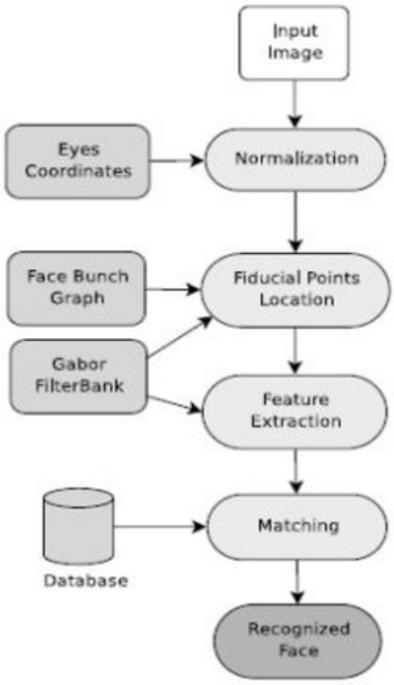
Then, we calculate the sum of minimum match scores of all the three images. If the sum of all min_match_scores of fingerprint, face, and retina images is greater than or equal to 0.45 then we authenticate the user and a unique key is generated from the fused image template. Otherwise the user is not authenticated, and the corresponding user record is stored into the failure or impostor database.

IMPLEMENTATION AND RESULTS ANALYSIS:

Feature extraction from fingerprint using minutiae detection



Feature extarction from face using extended bunch graph method (using gabor filters)



Feature extraction from iris using Gabor Filter method

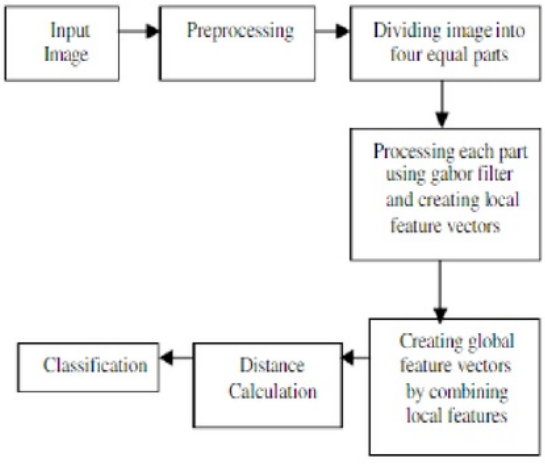


IMAGE TYPE CLASSIFICATION USING SVM:

```
from pathlib import Path
import matplotlib.pyplot as plt
import numpy as np

from sklearn import svm, metrics, datasets
from sklearn.utils import Bunch
from sklearn.model_selection import GridSearchCV, train_test_split

from skimage.io import imread
from skimage.transform import resize

def load_dir(container_path, dimension=(64, 64,3)):
    image_dir = Path(container_path)
    folders = [directory for directory in image_dir.iterdir() if directory.is_dir()]
    categories = [fo.name for fo in folders]

    descr = "A image classification dataset"
    images = []
    flat_data = []
    target = []
    for i, direc in enumerate(folders):
        for file in direc.iterdir():
            img = imread(file)
```

```
            img_resized = resize(img, dimension, anti_aliasing=True, mode='reflect')
            flat_data.append(img_resized.flatten())
            images.append(img_resized)
            target.append(i)
    flat_data = np.array(flat_data)
    target = np.array(target)
    images = np.array(images)

    return Bunch(data=flat_data,
                 target=target,
                 target_names=categories,
                 images=images,
                 DESCR=descr)
df = load_dir("imgs/")
X_train, X_test, y_train, y_test = train_test_split(
    df.data, df.target, test_size=0.8,random_state=None)

from sklearn.preprocessing import StandardScaler
sc = StandardScaler()
X_train = sc.fit_transform(X_train)
X_test = sc.transform(X_test)

param_grid = [
  {'C': [1, 10, 100, 1000], 'kernel': ['linear']},
  {'C': [1, 10, 100, 1000], 'gamma': [0.001, 0.0001], 'kernel': ['rbf']},
```

```
]
svc = svm.SVC()
clf = GridSearchCV(svc, param_grid)
clf.fit(X_train, y_train)
y_pred = clf.predict(X_test)


print("Classification report for - \n{}:\n{}\n".format(
    clf, metrics.classification_report(y_test, y_pred)))
out=[]
str1="face"
str2="finger"
str3="iris"
for i in y_pred:
    if i==0:
        out.append(str1)
    elif i==1:
        out.append(str2)
    else:
        out.append(str3)

from sklearn.metrics import accuracy_score
print(accuracy_score(y_pred,y_test))
```

```
Classification report for -
GridSearchCV(cv='warn', error_score='raise-deprecating',
       estimator=SVC(C=1.0, cache_size=200, class_weight=None, coef0=0.0,
  decision_function_shape='ovr', degree=3, gamma='auto_deprecated',
  kernel='rbf', max_iter=-1, probability=False, random_state=None,
  shrinking=True, tol=0.001, verbose=False),
       fit_params=None, iid='warn', n_jobs=None,
       param_grid=[{'C': [1, 10, 100, 1000], 'kernel': ['linear']}, {'C': [1, 10, 100, 1000], 'gamma': [0.001,
0.0001], 'kernel': ['rbf']}],
       pre_dispatch='2*n_jobs', refit=True, return_train_score='warn',
       scoring=None, verbose=0):
              precision    recall  f1-score   support

           0       1.00      0.96      0.98        90
           1       0.98      0.97      0.98        66
           2       0.94      1.00      0.97        78

   micro avg       0.97      0.97      0.97       234
   macro avg       0.97      0.98      0.97       234
weighted avg       0.98      0.97      0.97       234


accuracy_score is:
0.9743589743589743
```

CONCLUSION:

This work investigated the benefits as well as the security and privacy risks associated with the use of biometrics as an authentication mechanism for both smart phones and WSNs. In recent times the use of sensors has increased at an enormous rate in our day-to-day lives. An effective scheme is truly depending on multimodal biometrics for generating the cryptographic key in a secured manner. The proposed scheme followed in the work has three components namely extraction of features, biometric template generation using multimodal and key generation using the template. As the normal key used for encryption and decryption is not secure in this hackers' world, this work included multimodal biometric images. In the Multimodal biometric template generation consists of five major steps: pre-processing, feature extraction, feature fusion, biometric template creation. Based on the case studies and different evaluation exercises, this work shows that the proposed schema provides higher security.

FUTURE DIRECTIONS:

There is possibility to improve the existing system to identity the genuine users or intruders from the collections of multimodal biometric template existing in the database. The data mining and deep learning technique can be used to detect the structures and the failure patterns. The proposed model with real time sensors can be implemented to evaluate the performance and efficiency of the proposed methods. In order to improve the methods further, the WAM can be used to assign different weights for the biometric images generated from multimodal (fingerprints, retina and face) to classify effectively and process based on the quality preferences. The proposed system is

works very well under defined image capturing system and biometric capturing systems. The proposed modal and algorithm can be further enhanced automatically to handle the distorted, partial and less quality images. This research can be further extended to generate biometric template and keys using other types of biometrics such as smile, hair color, skin color, and eye. There are other possible research avenues to handle the different facial expressions such as anger, surprise, sadness and others.

3WAY-ACCESS

ORIGINALITY REPORT

11%	8%	8%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	esatjournals.org Internet Source	4%
2	www.mdpi.com Internet Source	1%
3	Submitted to Jawaharlal Nehru Technological University Student Paper	1%
4	qiita.com Internet Source	1%
5	file.allitebooks.com Internet Source	1%
6	Submitted to City University Student Paper	1%
7	Submitted to University of Bedfordshire Student Paper	<1%
8	"Biometric Recognition", Springer Nature, 2011 Publication	<1%
9	B. Santhosh, K. Viswanath. "A novel public key	

	cryptosystem for medical images", 2017 International Conference on Inventive Systems and Control (ICISC), 2017 Publication	<1%
10	Submitted to Bilkent University Student Paper	<1%
11	Submitted to Curtin University of Technology Student Paper	<1%
12	"Biometric System and Data Analysis", Springer Nature, 2009 Publication	<1%
13	Submitted to Sri Lanka Institute of Information Technology Student Paper	<1%
14	Submitted to Charotar University of Science And Technology Student Paper	<1%
15	Submitted to King's College Student Paper	<1%
16	Submitted to Universiti Tunku Abdul Rahman Student Paper	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		