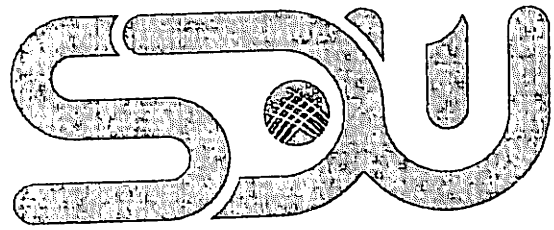
Ministry of Education and Science of the Republic of Kazakhstan
Suleyman Demirel University

UDC 50.13



Dadakhanov Sher

Analyze and Development System with Multiple Biometric Identification

THESIS

Presented in Partial Fulfillment for the
Degree of Master of Science in Computing Systems and Software
(degree code: 6M070400)
Department of Computer Sciences
Faculty of Engineering and Natural Sciences

Supervisor: **Ph.D., Assist. Prof. Baimuratov O**

Kaskelen, 2020

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Sher Dadakhanov

Abstract

In the case of quick progress in technological improvement, growing shopper cheating, fraud, the threat to private knowledge is additionally increasing daily. ways developed earlier to confirm personal info from the crimes weren't effective and safe. statistics were introduced once it had been needed technology for more practical security of personal info. recent ancient procedures like Personal identification number(PIN), keys, passwords, login ID may be forgotten, stolen, or lost. during a biometric identification system, the user might not get any keys or transfer any keys. As individuals they acknowledge one another by the physical look and behavioral characteristics that biometric systems use natural characteristics, like fingerprints, face recognition to differentiate between the particular user and cheater. To progress safety in 2005, identification ways were developed government and business sectors, however, currently it's reached nearly all non-public areas like Banking, Finance, home security and residential protection, healthcare, business security, and safety, etc. Since biometric examples and templates of a biometric system having one biometric characteristic to acknowledge and therefore the user may be replaced and increased, the new plan of merging multiple identification technologies has referred to as multimodal biometric recognition systems are introduced that use two or a lot of biometric knowledge characteristics of the person who may be known as a true user or not.

Аңдатпа

Технологияның қарқынды дамуы, тұтынушылардың алаяқтықтары, алаяқтықтың өсуі жағдайында жеке ақпаратқ деген қауіп күн сайын артып келеді. Бұрын қолданыста болған әдістерді зерттеу арқылы қылмыстар туралы жеке ақпаратты растау әдістері тиімді және қауіпсіз болған жоқ. Статистикалық деректер жеке ақпаратты практикалық қорғау үшін технология қажет болған соң енгізілді. Жеке сәйкестендіру нөмірі (PIN), кілттер, пароль-дер, логин сияқты соңғы ежелгі процедуралар ұмытылуы, ұрлануы немесе жоғалуы мүмкін. Биометриялық сәйкестендіру жүйесі кезінде пайдаланушы ешқандай кілттерді ала алмайды немесе оларды жібере алмайды. Адамдар сияқты, олар бір-бірін сыртқы келбеті мен мінез-құлық ерекшеліктерімен таниды, олар биометриялық жүйелер белгілі бір қолданушы мен алаяқтың арасын ажырату үшін саусақ іздері, бетті тану сияқты табиғи сипаттамаларды пайдаланады. 2005 жылы қауіпсіздікті қамтамасыз ету үшін үкімет пен бизнес секторында сәйкестендіру әдістері әзірленді, бірақ қазіргі кезде ол банк, қаржы, үй қауіпсіздігі және үйді қорғау, денсаулық сақтау, бизнес қауіпсіздігі және т.б. сияқты барлық қоғамдық емес салаларды қамтыды. Растау үшін бір биометриялық сипаттамаға ие биометриялық жүйенің биометриялық мысалдары мен шаблондарынан кейін, оны ауыстыруға және көбейтуге болады, адамның биометриялық білімінің екі немесе одан да көп сипаттамаларын қолданатын мультимодальды биометриялық тану жүйелері деп аталатын бірнеше сәйкестендіру технологияларын біріктірудің жаңа жоспары енгізілді. Бұл технологияны қолдану арқылы біз нақты қолданушы немесе болмауы мүмкіндігін біле аламыз.

Аннотация

В случае быстрого прогресса в технологическом совершенствовании, растущего обмана покупателей, мошенничества, угроза частным знаниям дополнительно увеличивается с каждым днем. Ранее разработанные способы подтверждения личной информации о преступлениях не были эффективными и безопасными. Статистические данные были введены, как только понадобилась технология для более практичной защиты личной информации. Последние древние процедуры, такие как персональный идентификационный номер (ПИН), ключи, пароли, логин, могут быть забыты, украдены или утеряны. Во время системы биометрической идентификации пользователь может не получить какие-либо ключи или передать их. Как люди, они признают друг друга по внешнему виду и поведенческим характеристикам, которые биометрические системы используют естественные характеристики, такие как отпечатки пальцев, распознавание лица, чтобы различать конкретного пользователя и мошенника. Чтобы обеспечить безопасность в 2005 году, были разработаны способы идентификации в правительственном и бизнес-секторах, однако в настоящее время он охватил практически все непубличные области, такие как банковское дело, финансы, домашняя безопасность и защита жилья, здравоохранение, безопасность бизнеса и т.д. После биометрических примеров и шаблоны биометрической системы, имеющие одну биометрическую характеристику для подтверждения, и, следовательно, пользователь может быть заменен и увеличен, введен новый план объединения технологий множественной идентификации, названный мультимодальными системами биометрического распознавания, которые используют две или несколько характеристик биометрических знаний человека, который может быть известен как истинный пользователь или нет.

Acknowledgements

First of all I would like to thank my thesis supervisor Olimzhon Baimuratov, for constant support and helpful discussion and for giving motivation. due to the external reviewer for terribly helpful feedback that helped to considerably improve the present work. due to my groupmates for all types of support. To conclude, I cannot forget to impart my family and friends for all the unconditional support during this intense year.

To my family

Contents

1. Introduction

In today's, security is the main downside, and everyone is searching for reliable ways to make sure safety. Previous ways that of securing our homes and things used key and lock systems, that is kind of inefficient keys will be duplicated. Later, the ensuring level of protection was provided by fashionable technologies with PIN and password. Fashionable systems area unit quite effective, however, they will even be hacked and gain access. To attain high accuracy and dependableness, identity verification technology has been introduced that uses physical or behavioral characteristics to verify the individual. The most reason for selecting identity verification The technology on top of ancient identification methodology is that traditional identification techniques area unit vulnerable security, unreliable and unsure. Most developed biometric systems use one biometric technology for biometric identification and verification. These unimodal systems area unit unable to satisfy a number of the challenges like enrollment massive population, high performance, etc. Later advanced identity verification technology with higher performance and a high degree of accuracy, referred to as a multimodal biometric recognition system, area unit introduced. Multimodal systems area unit capable of victimization two or a lot of physical or behavioral characteristics of an individual to put in writing, verify, and supply a call. Multimodal biometric systems conjointly mix two or a lot of identification technologies, like fingerprint systems, and face recognition, with a lot of sensors and supply choices by combining results from every system. Once victimization multimodal biometric systems, if one detector or the system fails to hold out identification, different systems will be accustomed to build choices. Multimodal systems are employed in varied areas, for instance in homes for the biometric door locks to avoid stealing, hospitals to register details of patient in code companies and educational institutions, to form positive participation at intervals the banks for safe and secure payment method,

biometric alarm systems simply just in case of data security in various sectors. Multimodal systems area unit a lot of convenience and overcome all limitations of unimodal systems with exaggerated security, high accuracy, and liveliness.[1].

1.1 Aims and Objectives

A growing range of huge companies' entry and exit systems area unit currently supported biometric. As there area unit numerous ways that of conducting biometric verification - together with biometric authentication, fingerprints, RFID card identification - bioscience may be an advanced issue.

Using passwords and codes for security access is pretty easy however generic. Biometric verification systems not solely enhance security, however, create it's easier and additional economical to manage key functions like attending trailing for payroll.

There's simply no have to be compelled to reset the passwords. Once the biometric take a look at is activated, all fingerprints, facial recognition, and biometric authentication area unit done - and staff area unit sensible to travel. It's even convenient to log the information and audit it consequently. As corporations evolve, security needs to grow at the side of it. One major advantage of biometric verification is that the ability to scale. These systems area unit extremely versatile, and may simply settle for extra employee's knowledge. Managing, fitting, and even analyzing biometric verification is incredibly easy – providing technological and correct results with marginal want for intervention.

The objectives of this research are:

- Survey varied authentication models;
- Analyze the present systems and develop own authentication system that uses multiple biometric identification.

1.2 The feature of the work

The feature of this project is to make secure the information by using multiple biometric identification: face recognition, fingerprint identification, and RFID card reader with the Arduino hardware control system. It will be low cost. Why

multiple because if there will some problems with one of the sensors to identify the user we can use another one, also if we will use only one it is more easier to hack it, and it will be more efficient.[2]

2. Literature Review

2.1 General statement of the multimodal authentication problem

The multimodal authentication task consists of several steps:

1. Get the results of the individual systems.

2. To normalize these results.

3. Perform the merger of the normalized components.

Thus, the result is obtained, which has the same form as if a unimodal authentication was performed. Moreover, it contains information from all the components of a multimodal model.[3]

The first stage is not difficult to implement, since authentication on individual systems can be performed simultaneously. For example, you can ask the user to simultaneously fix a finger on a fingerprint scanner and scan the retina. Further steps are performed within the overall system.

This approach can significantly increase the security level of authentication systems. It uses not just one characteristic of a person, but several, which complicates the task of faking biometric data. It is also significant that such systems not only identify attackers with greater accuracy, but also have fewer failures for registered users (that is, a higher True Positive Rate). This quality can significantly improve the quality of authentication solutions.

2.2 Normalization Methods

The need for this part is due to the fact that when merging, usually the summation (often with weights) of the results of unimodal authentication methods occurs. They are numbers that, when normalized to the **[0, 1]** scale, are interpreted as the probability that the user has the requested access. Thus, it is necessary to standardize them before the merger in order to effectively carry out the merger procedure.[4]

2.2.1 Min-Max

This method allows you to display raw estimates on the segment **[0, 1]**. In this case, the transformation preserves the shape of the initial distribution. **Min (S)** and **max (S)** are the boundary values for the model S; they must be supplied by the supplier of the corresponding unimodal system.[5] The formula is:

$$n = \frac{s - min(S)}{max(S) - min(S)}, n \in [0, 1].$$

2.2.2 Z-Score

This method results in a distribution with a mean of zero and a standard deviation of unity. If the values of the initial distribution are known, then this method can be used without any problems. However, if this information is not available, then we can calculate them using the training sample, which we use to train our model. This solution may not be optimal if outliers are present in the sample, since a biased estimate is obtained.[6] The method is described by the following expression:

$$n = \frac{s - mean(S)}{std(S)}, \text{ where } mean(n) = 0, std(n) = 1.$$

2.2.3 Tanh

This method is referred to as the so-called reliable statistical methods. In contrast to the approach described above, it is resistant to outliers and large distribution tails, which makes it a stronger and more reliable normalization tool.[6]

The formula is:

$$n = \frac{1}{2} * (tanh(0.01 * \frac{s - mean(S)}{std(S)}) + 1)$$

2.2.4 Adaptive normalization

Authentication errors are caused by the fact that the true distributions and distributions of the impostor overlap. This overlap region is described by two characteristics: the center c and the width w. The main idea of this normalization approach is to increase the differences between these two distributions by reducing this overlap, which will reduce the likelihood of errors.[6]

General view of all adaptive normalization methods:

$n_{AD} = f(n_{MM})$, where n_{MM} - Min-Max normalization result, and f display function. There are several types of display functions for adaptive normalization, which will be described below.

2.2.5 Two-Quadrics

It is a function whose second derivative changes sign at the point c.

$$n_{AD} = \begin{cases} \frac{1}{c} * n_{MM}^2, & n_{MM} < c \\ c + \sqrt{(1-c)(n_{MM} - c)}, & n_{MM} > c \end{cases}$$

2.2.6 Logistic

The shape of the function graph is similar to the graph of the Two-Quadrics function.

$$n_{AD} = \frac{1}{1 + A * e^{-B * n_{MM}}}, \text{ where } A = \frac{1}{d} - 1, B = \frac{ln(A)}{c} - 1.$$

In the expressions for A and B, the symbol dd denotes a constant, which is most often chosen by a small number (often the value 0.01). It's easy to see that $f(0) = d$.

2.2.7 Quadric-Line-Quadric

In this case, the overlap zone remains unchanged (on the graph this can be seen in the linear section in the center). Outside, the Two-Quadrics display function is used.[7]

$$n_{AD} = \begin{cases} \frac{1}{c - \frac{w}{2}} * n_{MM}^2, & n_{MM} < (c - \frac{w}{2}) \\ n_{MM}, & (c - \frac{w}{2}) < n_{MM} < (c + \frac{w}{2}) \\ (c + \frac{w}{2}) + \sqrt{(1 - c - \frac{w}{2})(n_{MM} - c - \frac{w}{2})}, & n_{MM} > (c + \frac{w}{2}) \end{cases}$$

2.3 Merge Methods

After the results of the work of individual authentication algorithms went through the normalization process, it is necessary to combine them. There are a number of ways to merge. The first three of the following are classic. The latter two are more complicated due to the fact that they use the logic that some authentication methods are more important and some less important.

We introduce the notation for further definitions. Let n_i^m - be the normalized output of the method $m(m = 1, 2, ..., M)$ for user $i(i = 1, 2, ..., I)$. In this case, M is the number of unimodal methods used in multi-modal, and I is the number of users in the database.[8]

2.3.1 Simple Sum

Simple summation for the user of the normalized results of all authenticators.

$$f_i = \sum_{m=1}^{M} n_i^m$$

2.3.2 Min Score

Selects the minimum among all normalized authenticator results for this user.

$$f_i = min(n_i^1, n_i^2, ..., n_i^M)$$

2.3.3 Max Score

Selects the maximum among all normalized authenticator results for this user.

$$f_i = max(n_i^1, n_i^2, ..., n_i^M)$$

2.3.4 Matcher Weighting

This merge method is based on the use of Equal Error Rate (EER). This error function makes an estimate of the ROC curve. We denote the EER for the m method as $e^m (m = 1, 2, ..., M)$. Then the weight for the m method is w^m.

$$w_m = \frac{1}{\sum_{m=1}^{M} \frac{1}{e^m}} * \frac{1}{e^m}$$

Moreover, it is clear from the formula that for all m the $0 \leq w^m \leq 1$ is true, and also that $\sum_{m=1}^{M} w^m = 1$. An important point is that the higher the error value e^m, the lower the corresponding weight coefficient w^m. Thus, more accurate methods will contribute more to the final assessment.

The final formula is:

$$f_i = \sum_{m=1}^{M} w^m * n_i^m$$

2.3.5 User Weighting

This method differs from the previous one in that we weigh the methods for each user individually. Initially, this method of merging was more complicated from the point of view of calculations. Later, on its basis, a scheme was proposed that reduces the number of operations, which will be described in this section.

We denote the weight for the method m for user i as w_i^m.

Consider in more detail how to calculate the required weight w_i^m. This method of merging takes as a basis the concept of a wolf-sheep. We designate sheep for users whose data can be easily faked. On the other hand, wolves denote users who easily mimic other customers. Both wolves and sheep reduce the efficiency

of the authentication process, since both of these groups lead to false positives.

In order to use this approach for the multimodal case, it is necessary to introduce the lambness metric for each pair (i, m). It shows how much the user i is a sheep in the framework of the m method. When calculated, it is assumed that the mean and standard deviation parameters for the true distribution and distribution of impostors are known. To obtain lambness, the d-prime metric is calculated, which shows how distinguishable are the two distributions (in our case, true and fake). We denote for the user-method pair (i, m) the mean and standard deviations of the true distribution as $\mu^m_{i,gen}, \sigma^m_{i,gen}$, for fake $\mu^m_{i,n}, \sigma^m_{i,n}$ respectively. In this case, the indices gen and imp denote genuine and impostor, respectively.

$$d^m_i = \frac{\mu^m_{i,p} - \mu^m_{i,n}}{\sqrt{\sigma^m_{i,p} - \sigma^m_{i,n}}}.$$

It is easy to see that the smaller the value of d^m_i, the more the user is a sheep for some wolves. This is due to the fact that in this case a strong overlap of the distributions is observed.[8]

And finally, everything is ready to calculate the weights for the user i:

$$w^m_i = \frac{1}{\sum_{m=1}^{M} d^m_i} * d^m_i.$$

The formula for merging with the resulting weights is:

$$f_i = \sum_{m=1}^{M} w^m_i * n^m_i$$

2.4 Combination of methods

In the course of studies of multimodal authentication systems, it was shown that the use of a combination of several methods is superior in quality of work to unimodal systems. Moreover, the increase is achieved even when combined with top unimodal systems. In some cases, this can help reduce the cost of the final architecture by using simple methods.

It was also shown that in applications where there is a constant influx of new people (for example, airports), the most suitable combination is Min-Max normalization and Simple Sum merging. If the work is carried out with a limited circle of people (for example, a laboratory or office), then the best combination

is adaptive normalization of Quadric-Line-Quadric and merging User Weighting. The main reason for the difference in results for the two cases is that when working with the same users, biometric data are constantly repeated, which allows them to be collected and accumulated into algorithms. Similar results were also obtained in other studies. The cases described are comprehensive and describe all possible examples of the use of authentication systems.

When solving applied problems, it is worth trying various combinations of methods for creating multimodal systems. This is due to the fact that due to differences in which unimodal methods are used, what equipment performs authentication and how the data were collected for training a multimodal system, the results can differ greatly from those presented in various studies. However, as a basic solution, it is worth trying first of all the ones described above.[6]

2.5 Facial Recognition

Facial Recognition - a practical application of the theory of pattern recognition, the task of which is to automatically localize the face in the photograph and, if necessary, identify the person by face. The function of identifying people in photographs is already actively used in photo album management software.[9]

The task of identifying and recognizing faces is one of the first practical tasks that stimulated the formation and development of the theory of recognition and identification of objects. There are nine categories of objects that correspond to gnostic areas and evoke visual images:

The interest in the procedures that underlie the process of recognizing and recognizing faces has always been significant, especially in connection with increasing practical needs: security systems, verification, forensic examination, teleconferences, etc. Despite the clarity of the everyday fact that a person identifies well faces of people, it's not at all obvious how to teach computers to carry out this procedure, including how to decode and store digital images of faces. Even less clear are assessments of the similarity of individuals, including their integrated processing. There are several areas of research on the problem of face recognition:

- neuropsychological models;
- neurophysiological models;

- informational and procedural models;
- computer recognition models.

The problem of face recognition was considered in the early stages of computer vision. For over 40 years, a number of companies have been actively developing automated, and now automatic, facial recognition systems: Smith and Wesson (ASID - Automated Suspect Identification System); ImageWare (FaceID system); Imagis, Epic Solutions, Spillman, Miros (Trueface system); Vissage Technology (Vissage Gallery system); Visionics (FaceIt system).[10]

Face recognition technologies allow automatic search and recognition of faces in graphic files and video stream. We have two categories to recognize human by face:

1. Facial Verification
2. Facial Identification

2.5.1 Facial Verification

This method works by checking with other candidates whether they are same or not. It is one-to-one mapping: you need to check whether this person is correct or not.[11]

2.5.2 Facial Identification

This method also working like previous one but not 1 to 1 it's 1 to many. It will compare against all image templates which stored in database to identify it.

2.5.3 Facial Recognition Methods

Presently, there are four main signs of face recognition:

1. Method of Eigenfaices;
2. Distinctive Features analysis ;
3. method of "automatic processing of facial images";

4. analysis based on Neural Networks.

All these methods are characterized by the complexity of implementation also the scope of the application.

Eigenfaces Method

It is often translated as "own face." This technology uses two-dimensional grayscale pictures that represent the distinctive options of a face image. The eigenface technique is usually used because of the basis for different face recognition strategies.

Combining the characteristics of one hundred-a a hundred and twenty "eigenface" will restore an outsized range of faces. At the time of registration, the "eigenface" of every person is bestowed as a series of coefficients. For the authentication mode, during which the image is employed for identification, the live example is compared with Associate in Nursing already registered example to work out the distinction constant. The degree of distinction between the patterns determines the very fact of identification. The eigenface technology is perfect once employed in well-lit rooms, once it's attainable to scan the face ahead.[12]

Distinctive

The "distinctive features" analysis technique is that the most generally used identification technology. This technology is analogous to the Eigenface technique, however is additional custom-made to dynamic the looks or facial expressions of an individual (smiling or displeased face). The technology of "distinctive options" uses dozens of characteristic features of assorted areas of the face, and taking under consideration their relative location. a personal combination of those parameters determines the characteristics of every individual person. The person's face is exclusive, however dynamic enough, as a result of an individual will smile, jilting of his beard and hair, placed on glasses - all this will increase the complexness of the identification procedure. Thus, as an example, once you smile, there's some displacement of the components of the face settled close to the mouth, that successively can cause an analogous movement of the adjacent components. Given such displacements, it's potential to unambiguously determine an individual with numerous facial expressions. Since this analysis considers native areas of the

face, the tolerances may be up to 25° within the horizontal plane, and up to concerning 15°within the vertical plane and need quite powerful and big-ticket instrumentation, that consequently reduces the unfold of this technique.

Neural Network

In the methodology supported the neural network, the characteristic options of each persons - registered and verified, square measure compared for coincidence. Neural networks use Associate in Nursing formula that establishes the correspondence between the distinctive face parameters of the person being checked and therefore the parameters of the model placed within the info, and therefore the most potential variety of parameters is applied. because the comparison is formed, discrepancies between the person of the person being verified and therefore the model from the info square measure determined, then a mechanism is launched that, exploitation acceptable weight factors, determines the degree to that the person being checked matches the model from the info. This methodology will increase the standard of face identification in tough conditions.

Automatic Face Image Processing

The "automatic face image processing" technique is that the simplest technology that uses the distances and also the magnitude relation of the distances between simply acknowledgeable points on the face, like the eyes, the top of the nose, and also the corners of the mouth. though this technique isn't as powerful as "eigenfaces" or "neural network", it is used quite effectively in low lightweight conditions.[11]

2.5.4 Comparative Analysis Face Recognition Algorithms

Now I'll show modern methods of face recognition.

Principal Component Analysis

The idea of the strategy is to represent facial pictures within the variety of a collection (vector) of the most elements of the image, known as "own faces" (Eigenfaces). They, persons, have a helpful property: that the image appreciate

every such vector incorporates a face-like form. The calculation of the most elements is reduced to the calculation of the eigenvectors and eigenvalues of the variance matrix, that is calculated from the image. The add of the principal elements times corresponding eigenvectors is image reconstruction. for every face image, its main elements area unit calculated. typically from five to two hundred main elements area unit taken. Recognition method may be a comparison main elements of associate unknown image with elements of all glorious pictures. It is assumed that pictures of faces appreciate one person, grouped in clusters in their own house. Candidates with the tiniest image area unit designated from the information. Distance from the input (unknown) image. the strategy of own persons needs idealised conditions for its application like uniform lighting paramcters, neutral face expression, lack of interference like glasses and beards. just in case of non-compliance of those conditions, the most elements won't mirror interclass variations. for example, under varied lighting conditions own persons is much not applicable, since the primary main elements principally mirror changes in lighting, and therefore the comparison produces pictures having the same level of illumination. underneath idealised conditions, accuracy recognition victimization this methodology will reach values over 90%, that may be a excellent result. The calculation of a collection of eigenvectors is very labor intensive. a method is to twist pictures row and column during this kind, the image illustration is associate order of magnitude smaller size, computation and recognition is quicker, however it's now not potential to revive the first image.

Viola Jones Method

This technique is extremely effective for search objects in pictures and video sequences in real time. This detector has extraordinarily low the chance of false detection of the face. the tactic works well associated detects countenance even once observant an object underneath a slight angle, up to concerning 30°. Accuracy recognition mistreatment this technique will reach values over 90%, that may bc a superb result. At angle of inclination larger than 30°, thc chance of detective work someone drops sharply. The indicated feature of the tactic doesn't allow a regular implementation to observe a person's face, turned at associate discretionary angle, that greatly complicates or makes it not possible to use the algorithmic rule in trendy production systems, taking into consideration their

growing wants.

Comparison of templates (Template Matching)

The basis of this methodology is to spotlight areas of the face within the image, so compare these areas for 2 completely different pictures. every the matching space will increase the live of image similarity. to match areas victimisation straightforward algorithms like component by component comparison. The disadvantage of this methodology is therein it needs a great deal of resources for each storage sites, and for comparison. in sight of the actual fact that the best comparison algorithmic rule, pictures ought to be shot beneath strictly established conditions: not noticeable changes in angle, lighting, emotional expression, etc. Recognition accuracy victimisation this methodology is concerning 80%, that could be a sensible result.

Hopfield Neural Network

Algorithm Hopfield network learning is considerably totally different from classic learning algorithms perceptrons therein rather than in turn approaching the required state with error calculation, all coefficients of the burden matrix ar calculated one at a time formula, in one cycle, once that the network in real time able to go. Method Limitations:

- - memorized pictures mustn't be very similar;
- - the image mustn't be shifted or revolved relative to its original condition.

To address these shortcomings, varied modifications of the classical Hopfield neural network ar thought-about. The Hopfield network with orthogonal transformation permits you to revive extremely correlative pictures by changing them the initial set to the twin set vectors. Thus, a neural network is obtained, which might store an explicit range of vectors, and once applied to the input of any vector, will confirm that Of the memorized ones, he's most similar. Recognition accuracy victimisation this methodology is over 90%, and in some cases - even on the point of 100%, that is AN nearly wonderful result. For most fashionable systems automatic face recognition main task is that the task of examination a given face image with a collection of pictures persons from the information. System options

automatic face recognition during this case ar evaluated by deciding the possibilities of AN inaccurate failure in recognition (errors of the primary kind) and inaccurate recognition (errors of the second kind). additionally to error possibilities for evaluating AN automatic face recognition system often accustomed live resistance to disturbance of pictures caused by a mixture with advanced backgrounds, lighting variability, dynamical hairstyles, etc. Considering the on top of, it appears that the creation of hybrid ways victimisation benefits and leveling disadvantages various non-public approaches mentioned on top of.

2.5.5 Face recognition systems on the market

To date, variety of business product designed for face recognition are developed. The algorithms employed in these product square measure completely different and it's still tough to judge that technology has blessings. the present leaders square measure the subsequent systems: Visionic, Viisage and Miros.

- Visionic's FaceIt application is predicated on an area feature analysis algorithmic program developed at altruist University. One United Kingdom of Great Britain and Northern Ireland business company integrated FaceIt into a tv anti-crime system known as Mandrake. this method searches for criminals by video knowledge that come back from a hundred and forty four cameras connected in a very closed network. once associate degree identity is established, the system reports this to the safety officer. In Russia, the representative of Visionic is DanCom.

- Another leader during this space, Viisage, uses associate degree algorithmic program developed at the Massachusetts Institute of Technology. business firms and government agencies in several North American nation states and variety of different countries use the Viisage system with identification cards, like a driver's license.

- metal Vision Technologies silver (Germany) offers variety of merchandise on the market that use face recognition technology. These systems area unit bestowed on the Russian market by Soling.

- Miros TrueFace biometric identification system uses neural network technology, and therefore the system itself is employed in adult male. Payroll

Corporation's money withdrawal advanced and is put in in casinos and different recreation venues in several North American nation states.

In follow, once victimisation face recognition systems as a part of customary electronic security systems, it's assumed that the person to be known is wanting directly at the camera. Thus, the system works with a comparatively straightforward two-dimensional image, that considerably simplifies the algorithms and reduces the intensity of the calculations. however even during this case, the popularity task continues to be not trivial, since the algorithms should take under consideration the likelihood of fixing the amount of lighting, dynamic the expression, the presence or absence of makeup or glasses.

The responsibleness of the face recognition system abundantly depends on many factors:

- Image quality. The likelihood of error-free operation of the system isn'ticeably reduced if the person we have a tendency to try to spot is not wanting directly at the camera or taken in poor lighting conditions.
- The connexion of the photograph recorded within the info.
- the scale of the info.

Face recognition technologies work well with customary video cameras that transmit knowledge and area unit controlled by a private laptop, and need a resolution of 320x240 pixels per in. with a video stream speed of a minimum of 3-5 frames per second. For comparison - acceptable quality for a video conference needs a video stream speed of fifteen frames per second already. the next video stream speed at the next resolution results in associate degree improvement within the quality of identification. once recognizing faces from an extended distance, there's a robust correlation between the standard of the camera and therefore the results of identification.

The volume of databases victimisation customary personal computers doesn't exceed 10,000 images.[13]

2.6 Fingerprint Verification

Fingerprints are embossed lines, the so-called papillary patterns, the structure of which is due to the rows scallop ridges of the skin, separated by grooves. These lines form complex skin patterns (arc, loop, curl), which have the following properties:

- individuality (various combination of papillary lines forming pattern drawing according to their location, configuration, relative position, unique in another pattern);
- relative stability (the invariance of the external structure of the pattern that occurs during the period of intrauterine development of a person and persists for his whole life);
- recoverability (with superficial violation of the skin papillary lines are restored as they were).

There are several fingerprint recognition algorithms. The most common is the algorithm based on the selection of parts. Typically 30 to 40 small details. Each of them is characterized by its position - coordinates, type (branching, ending or delta) and orientation.

The fingerprint standard is formed from the set of characteristics data. Physiologically, a fingerprint is embossed skin surface containing pores. Blood vessels are located directly under the epidermis. Morphology The fingerprint is closely associated with the electrical and temperature characteristics of the skin. This means that to obtain a fingerprint image you can use not only paint, but also electromagnetic energy in various its manifestations. Note that fingerprint scans with well distinguishable papillary lines is not easy challenge. Since the prints are too small, you have to use enough sophisticated methods. All existing electronic methods fingerprints, depending on the physical principles they use, are divided into the following types:

- optical;
- capacitive;
- radio frequency;

- pressure;
- ultrasound;
- temperature.

Next, we give an overview of each of these species and explain why Atmel was the temperature method is selected as the most promising for the product line FingerChip.

2.6.1 Optical method

There are currently several varieties of scanners designed for optical fingerprints:

1. FTIR scanners are devices that exploit the effect of disturbed total internal reflection (Frusted Total Internal Reflection). The effect is that when light falls on the interface between two media, light energy divided into two parts - one is reflected from border, another crosses the border in the second environment. The fraction of reflected energy depends on the angle falling light flux. Starting from a certain value of a given angle, all light energy is reflected from the interface. This phenomenon is called total internal reflection. In case of contact more dense optical medium (in our case finger surface) with less dense (for example, with a prism surface) at a point full internal reflection of a beam of light passes through this boundary. Thus, only beams of light reflected at certain points of total internal reflection, to which there was no papillary finger pattern applied. A special image sensor (CMOS or CCD, depending on the implementation of the scanner) is used to capture the light image of the surface of the finger. Leading manufacturers of such scanners are BioLink, Digital Persona, Identix.

2. Fiber Optic Scanners (Fiber Optic Scanners) are a fiber optic matrix in which all the waveguides at the output are connected to the photosensors. Sensitivity of each sensor allows you to fix the residual light, passing through the finger, at the point of contact of the finger with the surface of the matrix. The image of the entire fingerprint is formed according to the data read from each photosensor. The manufacturer of fiber optic scanners is the Elsys Consortium.

3. Electro-Optical Scanners (Electro-Optical Scanners) - the technology is based on the use of a special electro-optical polymer, which includes a light-emitting layer. When finger applied to the scanner, heterogeneity electric field at its surface (potential difference between the tubercles and hollows of the skin) is reflected in the glow of the layer. Thus formed fingerprint image. Subsequently, the image sensor converts the resulting image into a digital form. This type of scanner is manufactured by Security First Corp.

4. Optical broaching scanners (Sweep Optical Scanners) - almost everything is similar to FTIR devices, except the fact that to obtain the fingerprint image is not just applied to the scanner, but is carried out along a narrow strip - the reader. As you move your finger, a series of instant photos. In this case, neighboring frames removed with some overlap that allows you to significantly reduce the size of the used prism and the scanner itself. To obtain the resulting fingerprint image, apply specialized software. Leading scanner manufacturer this type is Cogent Systems

5. Roller Scanners (Roller Style Scanners) - These devices are the smallest scanners. The fingerprint is captured when a finger rolls a transparent thin-walled roller. Similar to a broach scanner, as you move fingers take snapshots of fragments of a papillary pattern with some image overlay. When scanning, the simplest optical technology is used: there is a static source inside the transparent cylinder light, lens and image sensor. After full scrolling of a finger programmatically going to the resulting image its imprint. Roller scanners are manufactured by Digital Persona, CASIO Computer, ALPS Electric.

6. Contactless scanners (Touchless Scanners) - in these devices the finger does not It contacts directly with the surface of the scanner. A finger is just applied to the scanner hole and is illuminated from below from different sides by several light sources. Center hole a lens is located with which the fingerprint image is projected onto the CMOS camera. Scanners of this type are manufactured by Touchless Sensor Technology. We note a number of drawbacks that are inherent in optical scanners and indicate which of they have already been fixed:

- Inability to make them compact. This problem was until recently, but, as can be seen from the above figures, this drawback is a thing of the past.
- Optical modules are quite expensive due to the large number of components and complex optical system. This flaw Today it is also leveled due to a significant reduction in the cost of image sensors.
- There is no effective protection against dummies.

The last drawback is the most significant, despite the fact that many manufacturers have announced the implementation of protection mechanisms at one or another stage of processing the scanned image.

2.6.2 Capacitive Scanners

Capacitive Scanners are today the most common semiconductor devices to obtain a fingerprint image finger. Their work is based on the effect of changing the capacitance of the pn junction of a semiconductor in contact with the papillary crest pattern with an element of a semiconductor matrix. There are modifications of capacitive scanners in which each semiconductor element in the matrix acts in the role of one capacitor plate, and the finger in the role of another. By applying a finger to the sensor between each sensitive an element and a protrusion-depression of the papillary pattern forms a container, the value of which is determined by the distance between the embossed surface of the finger and the element. The matrix of these capacities is converted to a fingerprint image. The leading manufacturers of scanners of this type are Infineon, STMicroelectronics, Veridicom The disadvantage of the capacitive method is the same ineffective protection from dummies.

2.6.3 RF-Field Scanners

RF-Field Scanners - these scanners use a matrix of elements, each of which works as a miniature antenna. The radio frequency module generates a low-intensity signal and directs it on the scanned surface of the finger. Each of the sensitive elements of the matrix takes reflected from papillary signal pattern. The magnitude induced in each miniature antenna EMF depends on the presence or

absence of a ridge near it papillary pattern. The stress matrix obtained in this way is transformed into a digital image of a fingerprint. Since the method is based on the physiological properties of the skin, it is difficult to fool. Imitation of a finger. The disadvantages of the method include the need for high-quality contact between the finger and the transmitter, which can be quite hot. A well-known manufacturer of RF scanners is Authentec company.

2.6.4 Pressure Scanners

Pressure Scanners in their design use a matrix of piezoelectric elements that are sensitive to pressure. When applying a finger to the scanning surface, the crested protrusions of the papillary pattern exert pressure by a subset of the elements of the matrix. The hollows of the skin pattern do not exert any pressure. Thus, the totality of the voltages obtained from the piezoelectric elements is converted into a fingerprint image. This method has a number of disadvantages:

- low sensitivity;
- ineffective protection from dummies;
- susceptibility to damage due to excessive efforts.

Pressure sensitive scanners are manufactured by BMF.

2.6.5 Ultrasonic Scanners

Ultrasonic Scanners scan the surface of a finger with ultrasonic waves. Distances between wave source and scallop ridges and hollows of the papillary pattern are measured by the echo reflected from them. Received image quality tenfold better than any other method on the biometric market. In addition, this method is almost completely protected from dummies, because it allows in addition to the papillary print finger pattern to receive information about some other characteristics (for example, about the pulse).

The main disadvantage of ultrasound The method is the high price of scanners of this type in comparison with optical and semiconductor scanners. The leading manufacturer of this type of scanner is Ultra-Scan Corporation.

2.6.6 Thermal Scanners

Thermal Scanners - in such devices sensors are used, which consist of pyroelectric elements that allow you to record the temperature difference and convert it to voltage. When applying a finger to the scanner,temperature of papillary protrusions touching pyroelectric elements pattern and air temperature in depressions, a temperature map is built finger surface, which later converted to digital image. The temperature method has many advantages. These include:

- high resistance to electrostatic discharge;
- steady work in a wide temperature range;
- effective protection against dummies.

The disadvantages of this method include the fact that the image quickly disappears. When applying a finger at the first moment, the temperature difference is significant and the signal level, respectively, is high. After a short time (less than one tenth of a second), the image disappears because the finger and sensor come to temperature equilibrium. It is this the feature was used by Atmel in temperature scanning technology, which is reflected in FingerChip microchips. Today Atmel is a leading manufacturer of thermal scanners.

2.6.7 FingerChip Technology

FingerChip Technology Uses Temperature Imaging Method in combination with lingering scanning, which is used in optical lingering scanners discussed above. Lingering the method can significantly reduce size of the sensitive matrix and make it in width equal to the resulting print, and in length - only a few fractions of a millimeter. To get an image, you just need to drag your finger along a narrow strip of the reader. Note that in combination with the temperature method, this method of obtaining fingerprints leaves no residue after scanning due to the small image lifetime. Small size and low cost of the matrix, combined with effective protection against dummies, as well as reliable operation over a wide temperature range, are the hallmarks of Atmel's temperature scanning technology.

Atmel currently releases three Reader types:

- AT77C102B;
- AT77C104B;
- AT77C105A.

Their main technical characteristics are presented in the table. The FingerChip AT77C102B sensor is made using the 35 micron process technology and combines on a monolithic rectangular CMOS substrate with a size of 1.64 Q17.46 mm of a data reading and conversion circuit. Imprint finger is read in the vertical movement of the finger attached to the matrix.

Clock frequency can be set programmatically up to 2 MHz, providing receiving up to 1780 frames per second, which is sufficient even with fast finger movement along the sensor. Resultant the imprint is collected from a series of frames using software providing Atmel.

The work cycle for each frame is as follows:

1. A column of 280 + 1 pixels is selected in the matrix. Columns are selected sequentially from left to right with a cyclic return to the beginning. After a reset, the output starts from the leftmost column.

2. Each pixel in a column sends its own temperature value as analog signal to the line of amplifiers.

3. Two rows are selected at the same time. (even and odd). Amplified signals they are fed to 4-bit analog-to-digital converters (ADCs). The obtained analog values can also be used as output (not shown in the diagram).

4. Two 4-bit digital equivalents are stored in a shift register and sent in parallel with one byte through the parallel outputs De 0-3 (even line) and Do 0-3 (odd line).

In addition to the inherent reading function all three devices, model AT77S104V and AT77S105A have additional options navigation (similar to the touch screen) and emulation of a keystroke, which allows them to be controlled. The presence of various cases provides an opportunity to optimally choose the method of installing the sensor in the device under development.

2.7 Radio Frequency Identification

RFID is a method of automatically identifying objects in which data stored in so-called transponders or RFID tags are read or written by means of radio signals.

Any RFID system consists of a reader (reader, reader or interrogator) and a transponder (aka RFID tag, sometimes the term RFID tag is also used).

By reading range, RFID systems can be divided into systems:

- near identification (reading is carried out at a distance of up to 20 cm);
- medium range identification (from 20 cm to 5 m);
- distant identification (from 5 m to 300 m)

Most RFID tags have two parts. The first is an integrated circuit (IC) for storing and processing information, modulating and demodulating a radio frequency (RF) signal and some other functions. The second is an antenna for receiving and transmitting a signal.

With the introduction of RFID tags in everyday life, a number of problems are associated. For example, consumers who do not have readers may not always be able to detect tags that are attached to the product at the stage of production and packaging, and get rid of them. Although during the sale, as a rule, such tags are destroyed, the very fact of their presence causes concern among human rights and religious organizations.

Already known RFID applications (contactless cards in access control and management systems, long-distance identification systems and payment systems) are gaining additional popularity with the development of Internet services.

2.7.1 RFID tag classification

There are several ways to organize RFID tags and systems:

- By operating frequency
- By power source
- By memory type
- By execution

2.7.2 By power source

According to the type of power supply, RFID tags are divided into:

- Passive
- Active
- Semi-passive

2.7.3 By type of memory used

According to the type of memory used, RFID tags are divided into:

- RO (Read Only) - data is recorded only once, immediately at the time of manufacture. Such tags are for identification purposes only. No new information can be recorded in them, and it is almost impossible to fake.
- WORM (Write Once Read Many) - besides a unique identifier, such labels contain a block of write-once memory, which can be read many times in the future.
- RW (Eng. Read and Write) - such labels contain an identifier and a memory block for reading / writing information. The data in them can be overwritten many times.

2.7.4 Benefits of RFID

- Ability to rewrite. These RFID tags can be overwritten and supplemented many times, while the data on the barcode cannot be changed - they are written right away when printed.
- No need for line of sight. An RFID reader does not require the direct visibility of a tag to read its data. The relative orientation of the tag and the reader often does not play a role. Tags can be read through the packaging, which makes their hidden placement possible. To read the data, it is enough for the tag to get into the registration zone at least for a while, moving, including at a fairly high speed. In contrast, a barcode reader always needs the line of sight of a barcode to read it.

- Longer reading distance. An RFID tag can be read at a much greater distance than a barcode. Depending on the model of the tag and the reader, the reading radius can be up to several hundred meters. At the same time, such distances are not always required.

- More data storage. An RFID tag can store significantly more information than a barcode.

- Support for reading multiple tags. Industrial readers can simultaneously read multiple (over a thousand) RFID tags per second using the so-called anti-collision function. A barcode reader can only scan one barcode at a time.

- Reading tag data at any location. In order to ensure automatic reading of the barcode, the standards committees (including EAN International) have developed rules for placing bar codes on commodity and transport packaging. Radio frequency tags do not apply to these requirements. The only condition is the location of the tag in the reader's coverage area.

- Resistant to environmental influences. There are RFID tags with increased strength and resistance to harsh environments, and the barcode is easily damaged (for example, moisture or pollution). In those applications where the same object can be used an unlimited number of times (for example, in the identification of containers or returnable containers), the radio frequency tag is a more acceptable means of identification, since it does not need to be placed on the outside of the package. Passive RFID tags have an almost unlimited lifetime.

- Multipurpose use. An RFID tag can be used to perform other tasks than the data carrier function. The barcode is not programmable and is only a means of storing data.

- High security. The unique immutable identifier number assigned to the label during production guarantees a high degree of protection of labels against forgery. Also, the data on the tag can be encrypted. The RF tag has the ability to password protect data write and read operations, as well as

encrypt their transmission. In one tag, you can simultaneously store open and closed data.

2.7.5 Disadvantages of RFID

- The performance of the label is lost with partial mechanical damage.
- The cost of the system is higher than the cost of a barcode based accounting system.
- Ease of self-manufacturing. The barcode can be printed on any printer.
- Exposure to interference in the form of electromagnetic fields.
- Distrust of users, the possibility of using it to collect information about people.
- The established technical base for reading barcodes significantly exceeds the volume of RFID-based solutions.
- Insufficient openness of the developed standards.

3. Instruments and Technologies

The project is going to be done by using Arduino hardware and some sensors for recognizing the biometrics of humans.

3.1 Arduino Technologies

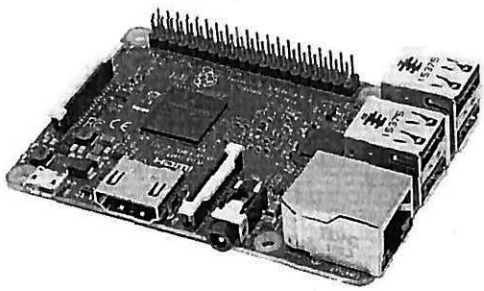


Figure 3.1: An Image of an Raspberry Pi 3B

Arduino is a brand of hardware and software for building automation and robotics systems aimed at non-professional users.

The software part will be done with the Python programming language for writing programs, compiling them, and programming hardware. The hardware is a set of mounted printed circuit boards. The completely open system architecture allows you to freely copy or complement the Arduino product line.

One of the platforms is a computer system for teaching computer science, but later it will gain wider application and fame. Developed by the British company Raspberry Pi Foundation, led by Eben Upton. To date, more than 30 million Raspberry Pi devices have been sold.

Most models of Raspberry Pi single-board computers are distributed fully assembled on a four-layer printed circuit board about the size of a bank card (models A and A +, Zero and Zero W are executed in different form factors). The standard package includes only the mini-computer itself. The housing, power supply and memory card must be ordered separately.

Technical details

The Raspberry Pi mini-computer was produced or is available in the following versions: "A", "A +", "B", "B +", "2B", "Zero", "Zero W", "3B", "3B +", " 3A + "and" 4B ". The first four models "A", "A +", "B" and "B +" are equipped with an ARM11 processor Broadcom BCM2835 with a clock frequency of 700 MHz and a 256 MB RAM module ("A", "A +") and 512 MB ("B", "B +") placed using the "package-on-packageruen" technology directly on the processor. The 2B model is equipped with a processor with 4 Cortex-A7 cores with a frequency of 900 MHz and a 1 GB RAM. The Zero and Zero W models were also released on the basis of ARM11, but with a frequency of 1 GHz, but the RAM was only 512 MB. Versions of the mini-computer "3B", "3B +" and "3A +" equipped, like the earlier model "2B", a 4-core Cortex-A53 processor (ARM v8), with a processor frequency of 1.2 GHz, "3B" and 1.4 GHz for "3B +" and "3A +", with 1 GB of RAM for "3B" and "3B +" and 512 MB for "3A +". Compared to previous versions, the 4B model has become more advanced, having received the new BCM2711 SoC with 4 cores, an ARM Cortex-A72 processor at a frequency of 1.5 GHz. The Raspberry Pi "4B" has become available in 3 versions with 1, 2 or 4 GB of RAM of your choice.

Model "A" is equipped with one USB 2.0 port, model "B" - two, and models "B +", "2B", "3B", "3B +", "4B" - four, while "4B" has four two USB ports are in USB 3.0 format. Also in the models "B", "B +", "2B", "3B", "3B +" and "4B" there is an Ethernet port. The Zero W, 3B, 3B +, and 4B models support Wi-Fi and Bluetooth. In addition to the main core, BCM2835 includes a graphics core with support for OpenGL ES 2.0, hardware acceleration and FullHD video, and a DSP core. One of the features is the lack of a real-time clock. For the "4B" model, VideoCore VI (OpenGL ES 3.x) is used on the graphics side and a hardware 4Kp60 decoder for HEVC video is added. For connecting monitors at "4B", 2 microHDMI ports (up to 4K) are available.

Video output is possible through a composite RCA connector or through a

digital HDMI interface. In the "B +", "2B" and "3B" versions, output is possible through an 3.5 mm audio jack. The root file system, kernel image and user files are located on the SD, MMC memory card (in models A and B), in new models, starting with "B +", microSD is used, in "3B", "3B +", "4B" exist the ability to boot from a USB stick or over a network, you can also use SDIOruen.

One of the most interesting features of the Raspberry Pi is the availability of GPIO (general purpose input / output) ports. Thanks to this, a "raspberry" computer can be used to control various devices. The model "B" has a 26-pin board, and the model "B +", "2B", "3B", "3B +", "3A +", "4B" have a 40-pin GPIO connector.

Software

Raspberry Pi works mainly on Linux-based operating systems. It is also possible to install Windows 10 IOT. Moreover, you can purchase Raspberry with a licensed Windows 10 IOT for $ 50. ARM11 is based on version 6 of ARM, which does not support all versions of Linux. To install operating systems, there is a NOOBS tool.

3.1.1 Raspbian OS

Raspberry Pi OS (formerly Raspbian) is a Debian-based operating system for Raspberry Pi. There are several versions of Raspbian, including Raspbian Stretch and Raspbian Jessie. Since 2015, Raspbian has been officially introduced by the Raspberry Pi Foundation as the main operating system for Raspberry Pi single-board computers. Raspbian was created by Mike Thompson and Peter Green as an independent project. The initial assembly was completed in June 2012. The operating system is under active development. Raspbian is optimized for the low-end ARM processors used in the Raspberry Pi line of computers.

PIXEL (Pi Improved Xwindows Environment, Lightweight) is used as the main desktop environment. It consists of a modified LXDE desktop environment and an Openbox window manager with a new theme and several other changes. The distribution comes with a copy of Mathematica's computer algebra program, a special version of Minecraft called Minecraft Pi, and a lightweight latest version of the Chrome browser.

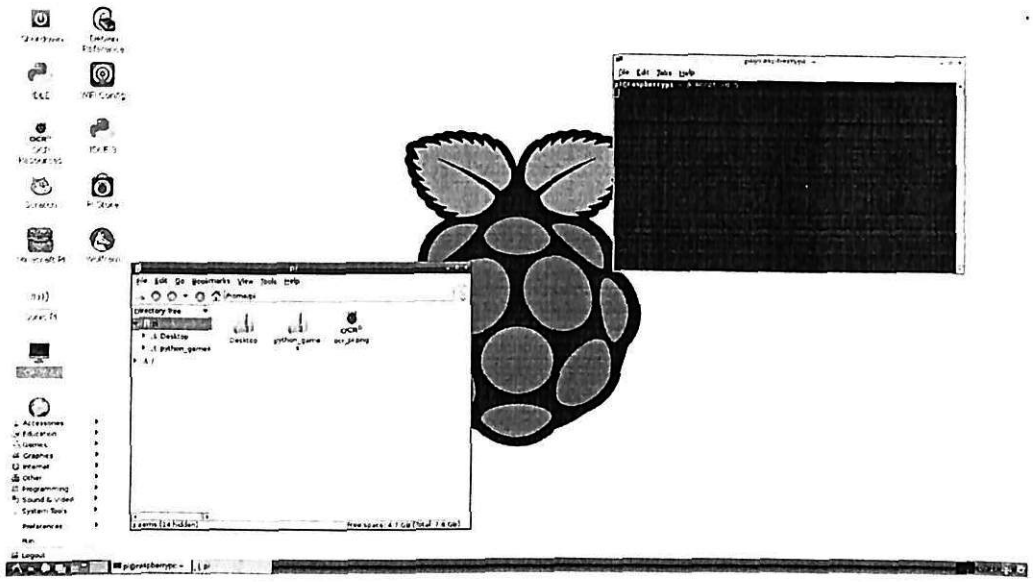


Figure 3.2: An Image of an Raspberry Pi Operating System

3.2 Fingerprint Sensor

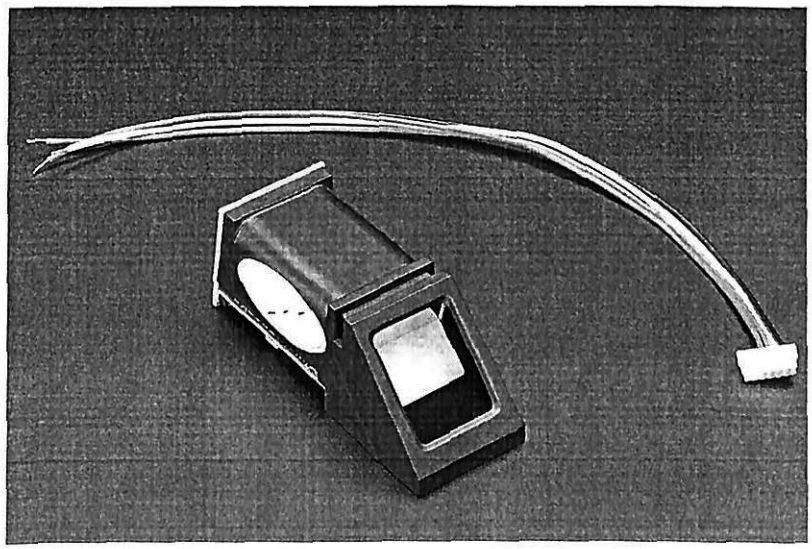


Figure 3.3: An Image of Fingerprint Sensor

Optical fingerprint sensors are commonly used in security systems.

These sensors include a DSP chip that processes the image, performs the necessary calculations to detect the correspondence between the recorded and current data. Inexpensive fingerprint sensors record up to 162 different fingerprints!

The sensor comes with software for Windows, which greatly facilitates its testing. Using native software, you can even display a photo of your fingerprint on the monitor! Well and the great thing is that there is a separate library for Arduino, using which you can configure the sensor in less than 10 minutes. But

I will control it using Python programming language.

3.2.1 Fingerprint Sensor Specifications

- Supply voltage: 3.6 - 6.0 V (direct current);
- Working current: 120 mA;
- Maximum current: 150 mA;
- Fingerprint image processing time: <1.0 second;
- Window Size: 14 mm x 18 mm;
- Number of simultaneously recorded files: 162 files;
- Security Level (from 1 to 5);
- Interface (connection): TTL serial;
- Baud rate: 9600, 19200, 28800, 38400, 57600 (default 57600);
- Operating temperature range: from -20 C to +50 C;
- Permissible humidity level: 40% - 85% RH;
- Overall dimensions: 56 x 20 x 21.5 mm;
- Weight: 20 grams.

3.2.2 Connection and use the fingerprint sensor with Raspberry Pi

Once connected, download the Adafruit-Fingerprint-Sensor-Library. For those who install additional libraries for the first time, there is a complete guide for installing libraries for Python.

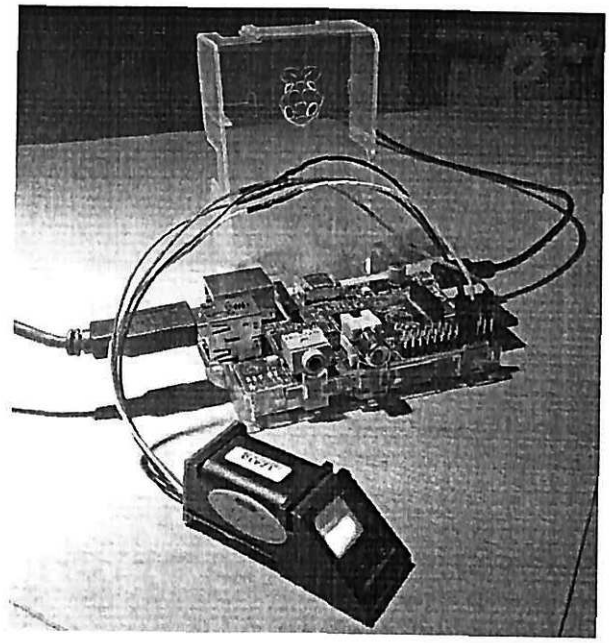


Figure 3.4: An Image of Connection Fingerprint Sensor with Raspberry Pi

3.3 PiCamera

The 5 MP camera sensor has a lens with a fixed focus and allows you to get pictures with a resolution of 2592x1944. Video support: 1080p 30 frames per second (fps), 720p at 60 fps and a resolution of 640x480 at speeds up to 90 fps. Full camera support has been added to the Raspbian OS, which needs to be updated.

Before moving on, you need an Internet connection. The camera module requires that the Raspian OS be updated to the latest version, because this way you can install the necessary drivers and tools.

You need to place the introduction tape from the edge of the connection near the Ethernet port and to the end of the Pi power connector. Hold the square of the tape in place and slide the tabs to lock the tape in position.

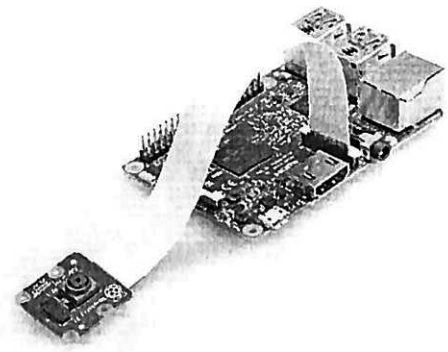


Figure 3.5: An Image of an Picamera

3.4 RFID Card Detector

Radio Frequency Identification (RFID) is a contactless technology for identifying objects using a radio frequency communication channel. Objects are identified by a unique identifier that each electronic tag has. The reader emits electromagnetic waves of a certain frequency. Tags send information in response - identification number, memory data, etc.[14]

Benefits of RFID Technology:

- contactless
- possibility of hidden marking
- high speed data reading
- possibility of installation in hazardous environments
- impossibility of falsification

There is a wide variety of RFID tags. Labels can be active and passive (without a built-in energy source, powered by the current induced in the antenna by a signal from the reader). Tags operate at different frequencies: LF (125 - 134 kHz), HF (13.56 MHz), UHF (860 - 960 MHz). Devices that read information from tags and write data to them are called readers (readers). In Arduino projects, the RFID-RC522 module is often used as a reader. The module is based on the NXP MFRC522 chip, which provides operation with HF tags (at a frequency of 13.56 MHz). Two tags are included with the RFID-RC522 module, one in the form of a card, the other in the form of a key fob.[15]

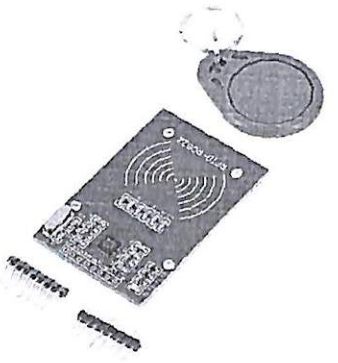


Figure 3.6: An Image of RFID Card Scanner

3.4.1 Technical Specifications of the RC522 RFID Module.

- Supply Voltage: 3.3V;
- Reading range: 0 - 60 mm;
- Transmission Rate: Maximum 10MBit / s;
- Interface: SPI;
- Operating frequency: 13.56MHz;
- Power Consumption: 13-26mA;
- Size: 40mm x 60mm;

3.4.2 Interfaces and pin assignment.

The MFRC522 chip supports SPI, UART, and I2C interfaces. The choice of interface is carried out by setting logical levels at specific pins of the microcircuit. The SPI interface is selected on this module.

SPI Pin Assignment:

- SCK — synchronization signal;
- SDA - slave selection;
- RST - output for reset;

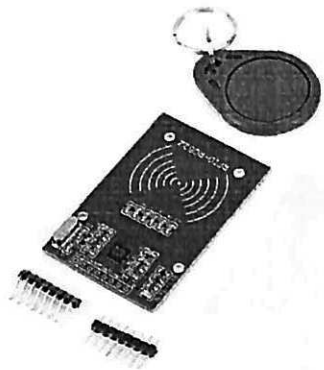


Figure 3.6: An Image of RFID Card Scanner

3.4.1 Technical Specifications of the RC522 RFID Module.

- Supply Voltage: 3.3V;
- Reading range: 0 - 60 mm;
- Transmission Rate: Maximum 10MBit / s;
- Interface: SPI;
- Operating frequency: 13.56MHz;
- Power Consumption: 13-26mA;
- Size: 40mm x 60mm;

3.4.2 Interfaces and pin assignment.

The MFRC522 chip supports SPI, UART, and I2C interfaces. The choice of interface is carried out by setting logical levels at specific pins of the microcircuit. The SPI interface is selected on this module.

SPI Pin Assignment:

- SCK — synchronization signal;
- SDA - slave selection;
- RST - output for reset;

- MISO - transmission from slave to master;
- MOSI - transfer from master to slave;
- Vcc - power supply 3.3 V;
- GND is the earth;
- IRQ - interrupt output.

The RST reset signal is the signal from the digital output of the controller. When the LOW signal arrives, the reader reboots. Also, by setting the RST to a low level, the reader reports that it is in sleep mode; to bring the module out of sleep mode, it is necessary to send a HIGH signal to this output.

3.4.3 Connecting the module to the Raspberry Pi board.

Consider connecting the module to the Raspberry Pi board. We will need the following details:

- Raspberry Pi Board
- prototyping board
- RFID-RC522 module
- 13.56 MHz RFID tags
- wires

We will connect the RFID-RC522 module to the Raspberry Pi board according to the connection diagram in Figure.[15]

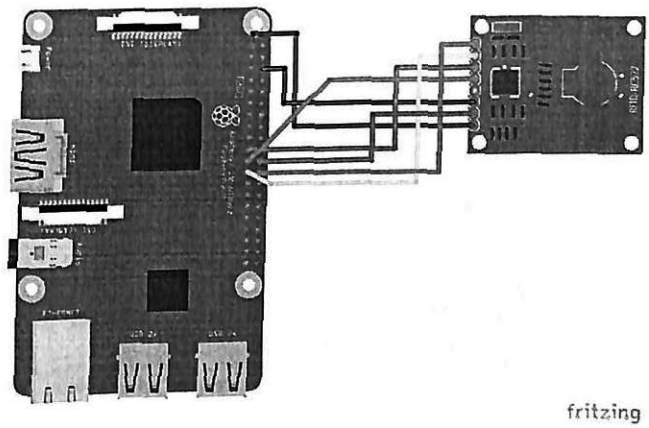


Figure 3.7: An Image of connection RFID Card Reader with Raspberry Pi

4. Implementation

4.1 Implementing Hardware and Software

4.1.1 Raspberry Pi

Raspberry pi is micro controller which can work instead of computer. It very useful to make projects like this. We can connect display, it has 4 usb input, ethernet, usb, aux, hdmi, display for camera. I'm using camera display, and gpio pins for lcd, buttons, leds, buzzer, fingerprint, rfid.

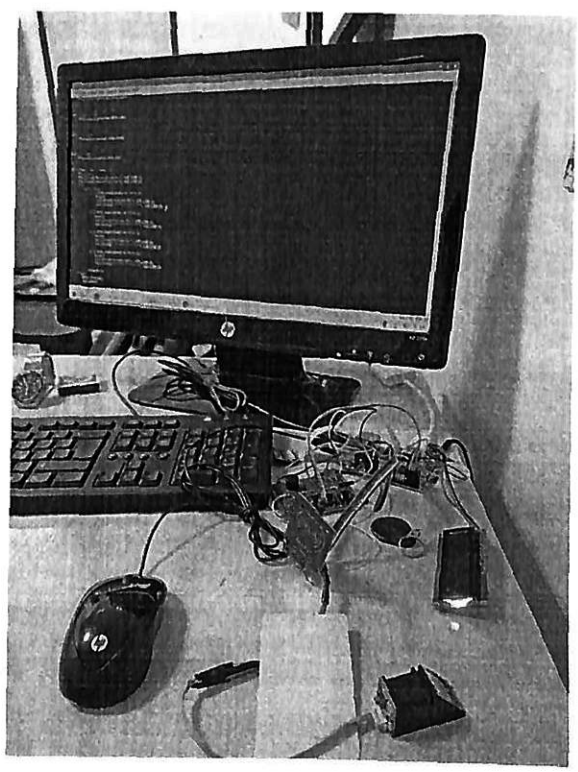


Figure 4.1: Connections

4.1.2 PiCamera

If you're exploitation the Raspbian distro, it's best to put in picamera exploitation the system's package manager: apt. this may make sure that picamera is straightforward to stay up up to now, and simple to get rid of must you would like to try to to therefore. it'll conjointly create picamera on the market for all users on the system. to put in picamera exploitation apt simply:

$ sudo apt-get update $ sudo apt-get install python-picamera python3-picamera To upgrade your installation once new releases square measure created you'll merely use apt's traditional upgrade procedure:

$ sudo apt-get update $ sudo apt-get upgrade If you ever got to take away your installation:

$ sudo apt-get take away python-picamera python3-picamera

4.1.3 MFRC522

A python library to read/write RFID tags via the budget MFRC522 RFID module.

This code was printed in regard to a web log post and you'll be able to conclude additional concerning a way to attach your MFRC reader to a Raspberry Pi there.

Installation Until the package is on PyPi, clone this repository and run python setup.py install within the high level directory.[16]

4.1.4 Adafruit Fingerprint

The library allows you to to speak with the r305 fingerprint module from higher laptop (your portable computer, a raspberry pi etc), instead of the arduino that it had been designed for by default. The module communicates via TTL, therefore, to speak you wish a USB - TTL device connected to the module.

It provides a category that exposes ways you'll decision to perform serial read/write actions with the module, these ways area unit enforced in keeping with the datasheet specification, that you'll transfer from the repo here.

Installation pip install adafruit-fingerprint

4.1.5 LCD 16x2 Screen with I2C

Connecting AN liquid crystal display to your Raspberry Pi can boost nearly any project, however what if your pins area unit occupied with connections to alternative modules? No downside, simply connect your liquid crystal display with I2C, it solely uses 2 pins (well, four if you count the bottom and power). There area unit one or two ways in which to use I2C to attach AN liquid crystal display to the Raspberry Pi. the best is to urge AN liquid crystal display with AN I2C backpack. The hardcore DIY approach is to use a typical HD44780 liquid crystal display and connect it to the Pi via a chip referred to as the PCF8574.

The PCF8574 converts the I2C signal sent from the Pi into a parallel signal that may be employed by the liquid crystal display. Most I2C LCDs use the PCF8574 anyway. I'll justify a way to connect it each ways in which during a minute.

I'll additionally show you the way to program the liquid crystal display mistreatment Python, and supply examples for a way to print and position the text, clear the screen, scroll text, print information from a sensing element, print the date and time, and print the information science address of your Pi. Connecting AN liquid crystal display with AN I2C backpack is pretty obvious. Connect the SDA pin on the Pi to the SDA pin on the liquid crystal display, and also the SCL pin on the Pi to the SCL pin on the liquid crystal display. the bottom and Vcc pins will have to be compelled to be connected. Most LCDs will operate with three.3V, however they're meant to be run on 5V, therefore connect it to the 5V pin of the Pi if attainable. Before we have a tendency to get into the programming, we'd like create|to form|to create certain the I2C module is enabled on the Pi and install one or two tools which will make it easier to use I2C. Now we'd like to put in a program referred to as I2C-tools, which is able to tell U.S.A. the I2C address of the liquid crystal display once it's connected to the Pi. therefore at the electronic communication, enter sudo apt-get install i2c-tools.

Next we'd like to put in SMBUS, which supplies the Python library we're getting to use access to the I2C bus on the Pi. At the electronic communication, enter sudo apt-get install python-smbus. We'll be mistreatment Python to program the liquid crystal display, therefore if this is often your 1st time writing/running a Python program, you will need to visualize out a way to Write and Run a Python Program on the Raspberry Pi before continuing. In photo below

the functions to get ready lcd screen to work.

```
def lcd_init():
    lcd_byte(0x33, LCD_CMD)
    lcd_byte(0x32, LCD_CMD)
    lcd_byte(0x06, LCD_CMD)
    lcd_byte(0x0C, LCD_CMD)
    lcd_byte(0x28, LCD_CMD)
    lcd_byte(0x01, LCD_CMD)
    sleep(E_DELAY)


def lcd_byte(bits, mode):
    bits_high = mode | (bits & 0xF0) | LCD_BACKLIGHT
    bits_low = mode | ((bits << 4) & 0xF0) | LCD_BACKLIGHT

    bus.write_byte(I2C_ADDR, bits_high)
    lcd_toggle_enable(bits_high)

    bus.write_byte(I2C_ADDR, bits_low)
    lcd_toggle_enable(bits_low)


def lcd_toggle_enable(bits):
    sleep(E_DELAY)
    bus.write_byte(I2C_ADDR, (bits | ENABLE))
    sleep(E_PULSE)
    bus.write_byte(I2C_ADDR, (bits & ~ENABLE))
    sleep(E_DELAY)


def lcd_string(message, line):
    message = message.ljust(LCD_WIDTH, " ")

    lcd_byte(line, LCD_CMD)

    for i in range(LCD_WIDTH):
        lcd_byte(ord(message[i]), LCD_CHR)
```

4.1.6 Button, LED, Buzzer

I used 4 buttons, 2 leds(one green which means user found, another red means no access), 1 buzzer. Buttons used for only admins to add new users. To cancel operations. Buzzer works when buttons pressed. LED for show is user has access or no.

```
def beep():
    GPIO.output(buzzer,GPIO.HIGH)
    sleep(0.05)
    GPIO.output(buzzer,GPIO.LOW)
#------------End of Buzzer----------------------

#------------On Green LED-----------------------
def green_on():
    GPIO.output(greenled,GPIO.HIGH)
#-----------------------------------------------

#------------Off Green LED----------------------
def green_off():
    GPIO.output(greenled,GPIO.LOW)
#-----------------------------------------------

#------------On Red LED-------------------------
def red_on():
    GPIO.output(redled,GPIO.HIGH)
#-----------------------------------------------

#------------Off Red LED------------------------
def red_off():
    GPIO.output(redled,GPIO.LOW)
#-----------------------------------------------
```

4.2 Software Tools

4.2.1 Python Programming Language

Python is a high-level general-purpose programming language aimed at increasing developer productivity and code readability. Python kernel syntax is minimal. At the same time, the standard library includes a large amount of useful functions.

Python supports structural, generalized, object-oriented, functional, and aspect-oriented programming. The main architectural features are dynamic typing, automatic memory management, full introspection, an exception handling mechanism, support for multi-threaded computing, and high-level data structures. The division of programs into modules is supported, which, in turn, can be combined into packages.

The reference Python implementation is the CPython interpreter, which supports most of the actively used platforms. It is distributed under the free Python Software Foundation License, which allows it to be used without restrictions in any applications, including proprietary ones [13]. There is an interpreter implementation for the JVM with the ability to compile, CLR, LLVM, and other independent implementations. The PyPy project uses JIT compilation, which greatly increases the speed of Python programs.

Python is an actively developing programming language; new versions with the addition / change of language properties are released approximately every two and a half years. The language has not been officially standardized; CPython, developed under the control of the author of the language, is the de facto standard. At the moment, Python is third in the TIOBE ranking with an indicator of 10.2%. Analysts note that this is the highest score of Python for all the time of his presence in the ranking.

4.2.2 Used Libraries

I used time, sleep, RPi.GPIO, smbus, picamera, cv2, numpy, os, serial, adafruit fingerprint, mfrc522 libraries to control sensors. Time for getting current time, sleep for add delay, gpio to connect raspberry pi pins, picamera ro control camera, cv2 for opencv, os for walking thorugh computer folder for saving images, getting them also, serial to use fingerprint serially connected, adafruit fingerprint to use fingerprint sensor, mfrc522 to use rfid sensor.

OpenCV

OpenCV - a library of computer vision algorithms, image processing and general-purpose open-source algorithms. Implemented in C/C++, it is also being developed for Python, Java, Ruby, Matlab, Lua and other languages. It can be freely used for academic and commercial purposes - it is distributed under the terms of the BSD license.

To approve a common standard computer vision interface for applications in this area. To help increase the number of such applications and create new patterns for using PCs.

Make Intel platforms attractive to developers of such applications by additionally accelerating OpenCV with Intel® Performance Libraries (Now includes IPP (low-level libraries for processing signals, images, as well as media codecs) and MKL (special version of LAPACK and FFTPack). OpenCV is able to automatically detect the presence of IPP and MKL and use them to speed up processing.

In version 2.2, the library was reorganized. Instead of the universal modules cxcore, cvaux, highGUI and others, several compact modules with a narrower specialization were created:

- opencv_core is the core functionality. Includes basic structures, calculations (mathematical functions, random number generators) and linear algebra, DFT, DCT, input / output for XML and YAML, etc.

- opencv_imgproc - image processing (filtering, geometric transformations, color space conversion, etc.).

- opencv_highgui - simple UI, input / output of images and videos. opencv_ml - machine learning models (SVM, decision trees, stimulated learning, etc.).

- opencv_features2d - recognition and description of flat primitives (SURF (Eng.) Russian, FAST and others, including a specialized framework).

- opencv_video - motion analysis and object tracking (optical flow, motion patterns, background removal).

- opencv_objdetect - detection of objects in the image (finding faces using the Viola-Jones algorithm, recognizing HOG people, etc.).

- opencv_calib3d - camera calibration, search for stereo matching and 3D data processing elements.

- opencv_flann - library for quick search of nearest neighbors (FLANN 1.5) and OpenCV wrapper.

- opencv_contrib - companion code not yet ready for use.

- opencv_legacy is legacy code stored for backward compatibility.

- opencv_gpu - acceleration of some OpenCV functions due to CUDA, created with the support of NVidia.

Here is the code for opencv: Firstly, to use opencv in Python we need to install it by using command "pip3 install opencv-python" at cmd. After in python we need to import it import "cv2 as cv".

Here in picture code of how I detected, and extracted images. We convert the image to gray after if it detects face by using detectMultiscale function it will crop it by using cv2.resize.

```
def face_extractor(img):

    gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)
    faces = face_classifier.detectMultiScale(gray,1.3,5)

    if faces is():
        return None

    for(x,y,w,h) in faces:
        cropped_face = img[y:y+h, x:x+w]

    return cropped_face

def face_detector(img, size = 0.5):
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
    faces = face_classifier.detectMultiScale(gray,1.3,5)

    if faces is():
        return img,[]

    for(x,y,w,h) in faces:
        cv2.rectangle(img, (x,y),(x+w,y+h),(0,255,255),2)
        roi = img[y:y+h, x:x+w]
        roi = cv2.resize(roi, (200,200))

    return img,roi
```

Here code for face detecting and saving to the folder faces. This function using when admin is going to add new user. When we are setting up the system to the company we need to add the admin to our system. By the same logic I will add one user by some priorities. Face, finger, and RFID card to the admin. After admin by using this functions he can add new user.

MFRC522

Here is code for using rfid sensor by using mfrc522.

```
def readCard():
    c = ""
    cardReader = SimpleMFRC522()
    lcd_string("Scanning for", LCD_LINE_1)
    lcd_string("card...", LCD_LINE_2)
    #print ("to cancel press ctrl+c")
    id1, text = cardReader.read()
    if(id1 == 787545154257):
        c = "admin"
    else:
        c = "user"
    return c

#writing data to the rfid tag

def writeCard():
    d = 1
    cardWrite = SimpleMFRC522()
    text = "MultipleBiometricSystem"
    lcd_string("place your tag", LCD_LINE_1)
    lcd_string("to write: ", LCD_LINE_2)
    cardWrite.write(text)
    lcd_string("Write Successful", LCD_LINE_1)
    lcd_string("ly", LCD_LINE_2)
    return d
```

Adafruit Fingerprint

In this section i have putted images for fingerprint recognition.

```
def fingerprint_check():

    while True:

        a = "0 0"
        if finger.read_templates() != adafruit_fingerprint.OK:
            raise RuntimeError("Failed to read templates")
        aaa = get_fingerprint()
        if (aaa==True):
            a = str(finger.finger_id)+" "+str(int(finger.confidence*(100/255)))
            break
        elif(int(aaa)==15):
            lcd_string("Time is up!", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
            sleep(0.2)
            a = "time"
            break
        else:
            lcd_string("Finger Not Found!", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
            sleep(0.2)
            a = "0 0"
    return a

def fingerprint_enroll(count):
    count = count/3 + 1
    if finger.read_templates() != adafruit_fingerprint.OK:
        raise RuntimeError("Failed to read templates")
    a = 1
    enroll_finger(int(count))
    return a
```

In first picture i will check existing fingerprints. From the template i will get the all data and then compare it with users fingerprint. After it gives the confidence. Percentage works like from 0-255. I will convert it to from 0 to 100

by formula. x*100/255 gives me percentage out 100.

Also I have here enroll function which used to add new fingerprint. By using enroll_fingerprint function we can add it to database of sensor.

```
def fingerprint_delete():
    while True:
        a = 0
        if finger.read_templates() != adafruit_fingerprint.OK:
            raise RuntimeError("Failed to read templates")
        if finger.delete_model(get_num()) == adafruit_fingerprint.OK:
            a = 1
            lcd_string("Deleted", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
            break
        else:
            a = 0
            lcd_string("Failed To Delete", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
    return a

def fingerprint_empty():

    if finger.read_templates() != adafruit_fingerprint.OK:
        raise RuntimeError("Failed to read templates")
    lcd_string("Deleting'", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    for i in range(128):
        if finger.delete_model(i) == adafruit_fingerprint.OK:
            a = 1
        else:
            a = 0
            lcd_string("Failed To Delete", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
```

Fingerprint delete functions deletes the users from database. Admin needs to give the location of the fingerprint which going to delete.

We can store 128 fingerprint in sensor. Fingerprint empty functions deletes all data from sensor database.

```
def get_fingerprint():
    timeout = time.time() + 10
    """Get a finger print image, template it, and see if it matches!"""
    lcd_string("Waiting for", LCD_LINE_1)
    lcd_string("finger image...", LCD_LINE_2)
    while finger.get_image() != adafruit_fingerprint.OK:
        end_time = time.time()
        if((end_time > timeout)):
            return 15
        pass
    lcd_string("Templating...", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    sleep(0.2)
    if finger.image_2_tz(1) != adafruit_fingerprint.OK:
        return False
    lcd_string("Searching...", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    if finger.finger_fast_search() != adafruit_fingerprint.OK:
        return False
    return True
```

Get Fingerprint Detail gets details about fingers from database.

```
def get_fingerprint_detail():
    """Get a finger print image, template it, and see if it matches!
    This time, print out each error instead of just returning on failure"""
    lcd_string("Getting Image...", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    i = finger.get_image()
    if i == adafruit_fingerprint.OK:
        lcd_string("Image Taken", LCD_LINE_1)
        lcd_string("", LCD_LINE_2)
    else:
        if i == adafruit_fingerprint.NOFINGER:
            lcd_string("No finger", LCD_LINE_1)
            lcd_string("detected", LCD_LINE_2)
        elif i == adafruit_fingerprint.IMAGEFAIL:
            lcd_string("Image Error", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        else:
            lcd_string("Other Error", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        return False

    lcd_string("Templating...", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    i = finger.image_2_tz(1)
    if i == adafruit_fingerprint.OK:
        lcd_string("Templated!", LCD_LINE_1)
        lcd_string("", LCD_LINE_2)
    else:
        if i == adafruit_fingerprint.IMAGEMESS:
            lcd_string("Image too", LCD_LINE_1)
            lcd_string("messy", LCD_LINE_2)
        elif i == adafruit_fingerprint.FEATUREFAIL:
            lcd_string("Couldn't identif", LCD_LINE_1)
            lcd_string("y features", LCD_LINE_2)
        elif i == adafruit_fingerprint.INVALIDIMAGE:
            lcd_string("Image invalid", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        else:
            lcd_string("Other Error", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        return False
```

Every time it will show the message in lcd screen about what happening. For example: Storing... message when it's storing data to database.

```
    lcd_string("Searching", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    i = finger.finger_fast_search()
    # pylint: disable=no-else-return
    # This block needs to be refactored when it can be tested.
    if i == adafruit_fingerprint.OK:
        lcd_string("Found Fingerprint", LCD_LINE_1)
        lcd_string("", LCD_LINE_2)
        return True
    else:
        if i == adafruit_fingerprint.NOTFOUND:
            lcd_string("No match found", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        else:
            lcd_string("Other Error", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        return False

# pylint: disable=too-many-statements
```

```
def enroll_finger(location):
    """Take a 2 finger images and template it, then store in 'location'"""
    for fingerimg in range(1, 3):
        if fingerimg == 1:
            lcd_string("Place Finger", LCD_LINE_1)
            lcd_string("on sensor...", LCD_LINE_2)
        else:
            lcd_string("Place same Finger", LCD_LINE_1)
            lcd_string("r again...", LCD_LINE_2)

        while True:
            i = finger.get_image()
            if i == adafruit_fingerprint.OK:
                lcd_string("Image Taken", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
                break
            if i == adafruit_fingerprint.NOFINGER:
                lcd_string("...", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
            elif i == adafruit_fingerprint.IMAGEFAIL:
                lcd_string("Image Error", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
                return False
            else:
                lcd_string("Other Error", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
                return False

        lcd_string("Templating...", LCD_LINE_1)
        lcd_string("", LCD_LINE_2)
        i = finger.image_2_tz(fingerimg)
```

In the pictures below and one is above code for enrolling the new fingerprint database.There square measure 2 separate stages concerned in employing a system like this. 1st you've got to travel through a method referred to as enrollment, wherever the system learns concerning all the individuals it'll have to be compelled to acknowledge every day. throughout enrollment, every person's fingerprints square measure scanned, analyzed, so keep during a coded kind on a secure info. usually it takes but a 0.5 second to store somebody's prints and also the system works for over ninety nine p.c of typical users (the failure rate is higher for manual staff than for workplace workers).

Once enrollment is complete, the system is prepared to use—and this can be the second stage, referred to as verification. Anyone WHO needs to achieve access should place their finger on a scanner. The scanner takes their fingerprint, checks it against all thc prints within the info keep throughout enrollmcnt, and dccidcs whether or not the person is entitled to achieve access or not. subtle fingerprint systems will verify and match up to forty,000 prints per second!

```
        if i == adafruit_fingerprint.OK:
            lcd_string("Templated", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        else:
            if i == adafruit_fingerprint.IMAGEMESS:
                lcd_string("Image too Messy", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
            elif i == adafruit_fingerprint.FEATUREFAIL:
                lcd_string("Couldn't identif", LCD_LINE_1)
                lcd_string("y features", LCD_LINE_2)
            elif i == adafruit_fingerprint.INVALIDIMAGE:
                lcd_string("Image invalid", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
            else:
                lcd_string("Other Error", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)
            return False

        if fingerimg == 1:
            lcd_string("Remove Finger", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
            sleep(1)
            while i != adafruit_fingerprint.NOFINGER:
                i = finger.get_image()

    lcd_string("Creating model...", LCD_LINE_1)
    lcd_string("", LCD_LINE_2)
    i = finger.create_model()
    if i == adafruit_fingerprint.OK:
        lcd_string("Created", LCD_LINE_1)
        lcd_string("", LCD_LINE_2)
    else:
        if i == adafruit_fingerprint.ENROLLMISMATCH:
            lcd_string("Prints did not ", LCD_LINE_1)
            lcd_string("match", LCD_LINE_2)
        else:
            lcd_string("Other Error", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        return False

    lcd_string("Storing model to", LCD_LINE_1)
    lcd_string(str(location)+"location", LCD_LINE_2)
```

```
    i = finger.store_model(location)
    if i == adafruit_fingerprint.OK:
        lcd_string("Stored", LCD_LINE_1)
        lcd_string("", LCD_LINE_2)
        return True
    else:
        if i == adafruit_fingerprint.BADLOCATION:
            lcd_string("Bad storage", LCD_LINE_1)
            lcd_string("location", LCD_LINE_2)
        elif i == adafruit_fingerprint.FLASHERR:
            lcd_string("Flash storage", LCD_LINE_1)
            lcd_string("error", LCD_LINE_2)
        else:
            lcd_string("Other Error", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)
        return False
```

SMBus

smbus2 is (yet another) pure Python implementation of the python-smbus package.

It was designed from the bottom up with 2 goals in mind:

It ought to be a drop-in replacement of smbus. The syntax shall be constant. Use the inherent i2c structs and unions to a bigger extent than alternative pure Python implementations like pysmbus will. By doing thus, it'll be a lot of feature complete and easier to increase. Currently supported options are:

Get i2c capabilities (I2C_FUNCS) read_byte

write_byte
read_byte_data
write_byte_data
read_word_data
write_word_data
read_i2c_block_data
write_i2c_block_data
write_quick
process_call
read_block_data
write_block_data
block_process_call
i2c_rdwr - combined write/read transactions with recurrent begin It is developed on Python a pair of.7 however works with none modifications in Python three.X too.

5. Future Work

Based on the above brief description of biometrics, multibiometric, biometric data templates and their protection, as well as the implementation of multibiometric. Remote authentication system it is advisable to realize that the need for development in the topics mentioned should cover a broad area.

The list below includes some areas to be developed:

Creating error-free algorithms, protocols, and databases.

Extraction Extracting functions, updating templates, recognizing, pre-processing data, and scheme exact match for multibiometric.

Perfect and stable cryptosystems for multi-biometric and multi-biometric remote authentication systems.

Cloud solutions are made widely available and include other biometrics templates.

The development of new technologies for data capture.

Unattainable the creation of publicly available databases for multibiometric.

Assessment of the effectiveness and reliability of multibiometric indicators in various fields everyday life.

6. Conclusion

In this digital era, most existing biometric systems use data from one biological operate verification and identification. The captured sample is because of the vulnerability of the biometric sensing element to noisy or unhealthy knowledge biometric functions may become pretend and it'll be potential to reject the Registered User incorrectly and incorrectly settle for the pretend user. within the case of a fingerprint recognition system, scanners might not acknowledge dirty or battle-scarred fingers conjointly underdeveloped fingerprint combos within the case of young kids and light fingerprint combos within the case of the older. Where, as within the case of a biometric authentication system, sensors might not be able to discover identical twins, whose look are nearly similar. Also, within the case of voice recognition systems, someone will imitate the voice of another person and gain access to their personal data. all told of the on top of cases because of associate incorrect call from the scanning devices offers unauthorized access and results in dishonorable activity. to beat these issues, a biometric system with a merger of 2 or additional biological characteristics and sensors referred to as multi-biometric systems are used. the most advantage of victimization multimodal biometric recognition there's associate enhanced accuracy of verification. Thus, North American nation|the utilization|the employment of multi-biometric recognition systems helps us in characteristic and additional exactly, as compared with the utilization of one biometric recognition system. I learned regarding totally different biometric recognition systems to use the mandatory multimodal methodology statistics for good homes to own safe and reliable access to our homes. I will do that multimodal statistics are additional reliable and correct compared to unimodal biometric recognition systems.

References

[1] G. Lawton, *Biometrics: A New Era in Security*, ser. An Industry Trends column that provides a brief survey of the field. BibRef, 1998.

[2] S. Ben-Yacoub, *Multi-Modal Data Fusion For Person Authentication Using SVM*, ser. Proc. 2nd Int. Conf. on Audio-and Video-based Biometric Person Authentication (AVBPA'99). Google Scholar, 1999.

[3] F. Wang and J. Han, "Robust multimodal biometric authentication integrating iris, face and palmprint", Information Technology and Control, vol.37, no.4, pp. 326-332, 2008.

[4] E. Bigün, *Expert Conciliation for Multi-Modal Person Authentication Systems by Bayesian Statistics.* Google Scholar, 1997.

[5] T. A. Kotropoulos C., "Frontal face authentication using discriminating grids with morphological feature vectors", 2000.

[6] K. N. A. Ross and A. Jain, "Handbook of multibiometrics 1st edition", 2006.

[7] V. K. A. Kumar and D. Zhang, "A new framework for adaptive multimodal biometrics management", IEEE Transactions on Information, 2010.

[8] M. S. S. Liu, "A practical guide to biometric security technology", IT Professional, 2001.

[9] F. D. Brunelli R., "Automatic person recognition by using acoustic and geometric features machine vision and applications", 1995.

[10] C. Chen and C. Huang, "Human face recognition from a single front view", 1992.

[11] J. Daugman, "Face and gesture recognition: Overview", 1997.

[12] F. Galton, "Personal identification and description - i", 1888.

[13] X. Jia and M. Nixon, "Extending the feature vector for automatic face recognition", 1995.

[14] "Data protection working party. working document on data protection issues related to rfid technology", 2005.

[15] T. Hjorth, "Supporting privacy in rfid systems (master thesis)", 2004.

[16] M. Aigner and M. Feldhofer, *Secure symmetric authentication for rfid tags.* Telecommunication and Mobile Computing, 2005.