DECLARATION OF ORIGINALITY

I declare that this final project report, entitled “Digital Lock System with Built In Camera” is my own original piece of work and, to the best of my knowledge and belief, has not been submitted, either in whole or in part, to another university to obtain a degree. All sources that are quoted or referred to are truly declared.

Cikarang, Indonesia, January 2013

Nicholas Joy
DIGITAL LOCK SYSTEM WITH BUILT IN CAMERA

By

Nicholas Joy

002201000014

Approved by

A. Suhartomo, Ph.D.
Final Project Supervisor

Dr-Ing. Erwin P. Sitompul, ST., M.Sc.
Head of Study Program
Electrical Engineering

Dr-Ing. Erwin P. Sitompul, ST., M.Sc
Dean of Faculty of Engineering
ACKNOWLEDGEMENT

I would like to take this opportunity to express my gratitude to all those who had given me the possibility to complete this project successfully, especially President University (PresUniv) for giving me the permission to commence this project in accordance upon submission of my proposal. I am bound to the President University (PresUniv) for their motivating support.

My deepest gratitude is to my advisor, Mr Suhartomo. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own and at the same time the guidance to recover when my steps faltered. Mr Suhartomo taught me how to question thoughts and express my ideas. His patience and support helped me to overcome many crisis situations and enable me to finish this project within the given timeframe. I am deeply grateful to him too for the long discussions that helped me sort out the technical details of my work.

I am also deeply indebted to my fellow course mates whose help, thought-provoking suggestions and encouragement helped me in all the time throughout the completion of this project.

Most importantly, none of this would have been possible without the love and patience of my family. My immediate family, to whom this exposition is dedicated to, has been a constant source of love, concern, support and strength all these years.

Lastly to God almighty for being a great source of strength, willpower and discipline, all of this which that aided me through the completion of this project in sound health.

I am incredibly lucky to be supported by only the good vibrations around me at all times.

Thank you, from the bottom of my heart

Nicholas Joy
DIGITAL LOCK SYSTEM WITH BUILT-IN CAMERA

ABSTRACT

To keep abreast with technological growth in the work front and business pots, security plays a huge significance in guarding physical and intellectual properties in most areas. The act of theft and its methods itself have advanced much in the modern times hence calling for development in the security field. This was what that initiated this study on a digital security system, only because the traditional security systems often catches the limelight for being obsolete. Recent study proved that many business owners prioritize security above other areas because all of the company in the world wanted their assets can be secure and safe through criminalization.

Thus, in order to design a fully functional digital lock system that is the core of this study; countful methods were analyzed and put into consideration. This has led to the interest in using face recognition as part of a multi-layered security system that could provide an enhanced defense mechanism. Face recognition using images is a very complex task and has been part of mush interest in recent years. This has led to the development of several recognition methods. A study of comparison between the methods was also done to differentiate and analyze the pros and cons of several possible methods. These methods were discussed as part of this study and taking into consideration the given timeframe, resources and practicality a particular method that is best suited is implemented.

As part of this study, a feasible security system which uses a digital locking mechanism and integrating the use of face recognition is designed and implemented. The workings, design development and the problems faced during the system development is discussed and shown in this report.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE PAGE</td>
<td>i</td>
</tr>
<tr>
<td>DECLARATION OF ORIGINALITY</td>
<td>ii</td>
</tr>
<tr>
<td>APPROVAL PAGE</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>vi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>ix</td>
</tr>
<tr>
<td>CHAPTER 1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1. Final Project Background</td>
<td>1</td>
</tr>
<tr>
<td>1.2. Problem Statement</td>
<td>5</td>
</tr>
<tr>
<td>1.3. Final Project Objectives</td>
<td>6</td>
</tr>
<tr>
<td>1.4. Final Project Scopes and Limitations</td>
<td>7</td>
</tr>
<tr>
<td>1.5. Final Project Outline</td>
<td>8</td>
</tr>
<tr>
<td>1.6. Conclusion</td>
<td>9</td>
</tr>
<tr>
<td>CHAPTER 2. LITERATURE REVIEW</td>
<td>10</td>
</tr>
<tr>
<td>2.1. Preliminary Remarks</td>
<td>10</td>
</tr>
<tr>
<td>2.2. Domain Research</td>
<td>11</td>
</tr>
</tbody>
</table>
2.3. Concept.................................................................................................................12

2.4. Approach ...............................................................................................................13

2.4.1. Holistic Approach .........................................................................................13

2.4.2. Feature – Based Approach .............................................................................13

2.4.3. Hybrid Approach .........................................................................................14

2.5. Face Recognition Techniques ...........................................................................14

2.5.1. Neural Networks ..........................................................................................14

2.5.2. Geometrical Feature Matching .................................................................15

2.5.3. Graph Matching ..........................................................................................15

2.5.4. Eigenfaces ..................................................................................................16

2.5.5. Fisherface ..................................................................................................19

CHAPTER 3. RESEARCH METHODOLOGY ...............................................................20

3.1. Preliminary Remarks .........................................................................................20

3.2. Research Approach .........................................................................................20

3.3. Primary Research ............................................................................................22

CHAPTER 4. METHODOLOGY AND SYSTEM EXPLANATION ..............................24

4.1. Preliminary Remarks .........................................................................................24

4.2. Reasoning on system development ................................................................24

4.3. Investigation on material/component selection .............................................26

4.4. Design and Simulation .....................................................................................30
4.5. Hardware Design .......................................................................................................................... 29

CHAPTER 5. SYSTEM IMPLEMENTATION & TESTING ................................................................. 35

5.1. Preliminary Remarks .................................................................................................................. 35

5.2. The Working Process of the System .......................................................................................... 35

5.2.1. Digital Lock ............................................................................................................................ 35

5.2.2. Face Recognition .................................................................................................................... 45

5.2.3. Testing and troubleshooting of the system ............................................................................ 51

5.3. Interpretation of Data ................................................................................................................ 52

CHAPTER 6. CONCLUSIONS AND RECOMMENDATIONS .................................................. 54

6.1. Preliminary Remarks .................................................................................................................. 54

6.2. Conclusions Relating to the Research objectives ....................................................................... 54

6.2.1. Recommendations and Suggestions ..................................................................................... 55

6.3. Limitations .................................................................................................................................. 56

6.3.1. Further Research .................................................................................................................... 58

6.3.2. Conclusion ............................................................................................................................ 59

REFERENCES ..................................................................................................................................... 60

APPENDICES ...................................................................................................................................... 62

Appendix A : Program Code

Appendix B : Final Project Consultation Records

Appendix C : Receipt
LIST OF FIGURES

Figure 1.1. Proposed System Design .......................................................... 8

Figure 2.1. Flow of typical face recognition systems ..................................... 12

Figure 3.1. Functional system overview ...................................................... 22

Figure 4.1. Digital lock system overview ..................................................... 26

Figure 4.2. PIC 16F877A microcontroller pin diagram ................................... 27

Figure 4.3. SK40C start-up kit by Cytron technologies .................................. 27

Figure 4.4. 4x4 Keypad Circuit ..................................................................... 28

Figure 4.5. 4x4 Keypad ................................................................................ 29

Figure 4.6. 16x2 LCD screen display ............................................................ 29

Figure 4.7. Program Flowchart ................................................................. 30

Figure 4.7. Hardware Design ....................................................................... 33

Figure 5.1. LCD Connections ....................................................................... 35

Figure 5.2. PIC 16F877A with SK40C startup kit ........................................ 36

Figure 5.3. Relay ......................................................................................... 36

Figure 5.4. LED ......................................................................................... 37

Figure 5.5. Buzzer ....................................................................................... 37

Figure 5.6. Complete Prototype .................................................................... 38

Figure 5.7. Program Flowchart ..................................................................... 39
CHAPTER 1

INTRODUCTION

1.1 Final Project Background

Technology can be defined as “the practical application of knowledge especially in a particular area” and “a capability given by the practical application of knowledge” [1]. The significant effect of technology for human grants the ability to control and adapt to their environments and simplify their lives. This began with the conversion of natural resources into simple tools and now includes the development of techniques, crafts, systems or methods of organization in order to solve a problem or serve some purpose. Technology under distinct improvisation can assist human in general in adapting to their lives as well as contribute to the improvisation of the standard of living and provide basic needs and necessity to people from all walks of life. Without the improvisations, developments and advancements of technology, man would be lacking of many comfort and securities in their daily lives.

One aspect of a human’s life that has been greatly influenced by technology is security. Security can generally be defined as a “measure taken to guard against espionage or sabotage, crime, attack, or escape” [2]. Security is an important factor that many fail to prioritize. be it at home or offices. In homes, the need for security would be to ensure the safety of the residents as well as the physical property against thefts, robbery as well as physical harm that can be inflicted by external parties.
In addition, Security is also used to ensure that there is no breach or trespassing into properties or homes. It is the backbone of an organization to safeguard business against possible threats towards materials, confidential information and intellectual properties of an organization. Organizations tend to deal with much information regarding their own business or information regarding clients and customers. These types of information are confidential and the safety of the information is a high priority for organizations. Some businesses deal with money, assets and financial funds.

These monetary assets have to be guarded as the misuse of information can result in the loss of funds. There is also the risk of physical breach of security such as fraud and robberies. The situation is asymmetric since the “host” must cover all points of attack while the attacker would only need to identify a single weak point upon which to concentrate in order to breach or overcome the security system installed.

One of the most commonly used forms of security is locks. Locks have been vastly used to secure or guard properties, devices and other types of valuables. Many different types of locks have evolved over the many years. It started from the very basic locks which was made of wood and rope until the modern dead bolt or magnetic locks. All locks have one common similarity which is the need of using a key to release the locking mechanism. This has made locks to become renowned for their ease to break into.
With the advancement of technology, homes and businesses which fail to keep abreast with the latest security methods will find themselves increasingly vulnerable to criminal attacks. In an attempt to ensure all properties are safest and secure, digital locks were designed to provide home and business owners with the essential security measures required in such a modern age. Digital locks are now widely used compared to conventional locks as it eliminates the need for the traditional key. Digital locks are largely used in banks and organizations especially in areas that tightly guarded. This security measure is to ensure that confidential information, valuable assets and data is not prone to be breached or stolen. This was the beginning of the keyless access security system. Keyless security systems were then extensively developed to replace the conventional locks that were previously used as they provided a better form of security.

At times, a breach of security happens due to reasons such as stolen passwords or by system hacking. Conventional digital locks only receive password and does not have any other form of additional security in case the passwords integrity have been breached. This is one of the shortcomings with the keyless access technology. There have been cases where passwords have been hacked, given or sold to assist the breach of security in past. This has sparked a large interest in using biometric features as verification tools whereby certain parts of the human body are used as a password.

Biometric verification can be classified as a process by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. These traits include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures [3]. Fingerprinting is probably the most well-known biometric. Some fingerprint applications and devices can detect when a live finger is presented. The devices analyze the position of tiny points on the fingerprint, called minutiae. Minutiae are the end points and intersections of ridges. Many fingerprint devices do not actually store the image of the prints, as this can require a great amount of memory and storage. Instead, a series of numbers stemming from calculations derived from the unique points of intersections, swirls, and arcs that make up the fingerprint are saved [3].
Besides fingerprints verification, retinal scans can be used to direct a low-intensity beam of light through the pupil and to the back of the eye to record and measure the vein patterns of the eye to further enhance verification process. Low reject rates and nearly a zero percent false accept rate makes retinal scans are one of the most accurate biometric measurement performers. However, users are required to stand close to the device and focus on a target. This makes the biometric application unattractive to some users in addition to the inconvenience it brings for individuals who had undergone eye operations [3].

On the other hand, Iris scanning is the less intrusive of the eye pattern biometrics. It is one of the most uniquely identifiable biometric characteristics, with a higher than average template matching performance. Iris scanning requires no intimate contact between the user and the reader, and can be accomplished successfully while wearing eye glasses. Iris scanning technology uses a camera to photograph the iris in the front of the eye. Subjects do not have to focus their eyes on a target and can stand as far as three feet away from the camera [3].

Biometric verification has evolved greatly due to the advancement of computerized databases and the digitization of analog data, allowing for almost instantaneous verification. The human face belongs to the most common biometrics, since humans recognize faces throughout their whole lives and naturally have the ability to differentiate between different face. Face recognition has been studied for many years in the context of biometrics. Face recognition systems show many advantages, among others easy implementation, easy cooperation with other biometric systems, availability of face databases. Facial recognition systems measure characteristics as the distance between facial features (from pupil to pupil) or the dimensions of the features themselves (such as the width of the mouth). The majority of these systems look for characteristics and not a complete image which uses the eyes as an anchor point and measure distances between the eye, from the center of the eye to the tip of the nose, to the tip of the chin, etc.
Facial scanning concentrates on distinctive features or characteristics of the human face, including its thermal pattern. It examines the areas of the face that are less vulnerable to alterations such as eye sockets, cheekbones, and sides of the mouth. Glare and eyeglasses are common causes of error rates in facial recognition. False accept rates are sometimes caused by factors such as recalcitrant users, contact lenses, lighting, and variations in bone structure for different ethnicities. For proper enrollment, facial scanning also requires consistent lighting [3].

Using biometric verification to enhance the digital locking system will be a new method to increase the security measures required in a modern age. This new system will be able to increase or enhance existing systems and act as a platform for further developments in biometric verifications. With this advancement in technology, the biometric verification digital lock system will be the sole project as such and not similar to any of the previous projects and inventions.

1.2 Problem Statement

There are currently some commercial digital locks using biometric verifications such as fingerprint security, retina eye security and this research will be done in the interest of implementing a more secured access system and expanding the commercial application of digital locks for the betterment of people and property in mind. However, towards the betterment of a security system in areas where threat is a concern, this project would be an innovation with the foundation of a study in the conventional digital lock, biometric verification systems and possible threats towards materials, confidential information and intellectual properties. A fair challenge in developing this integrated system is eagerly expected as to many of the previous system never match closely and more enhancements is now added.
1.3 Final Project Objectives

The aim of this project would be to develop a digital lock device with built in biometric verification function as a security measure. This will serve as a platform for a more established security. The frontline to security is to safeguard properties and intellectual properties against thefts and fraudulent activities. Hence, with the integrations to develop a digital lock device with built in biometric verification, it will serve as supportive layers to establish and enhance the existing systems.

A face recognition technique that would be suitable to the system design needs to be selected and the technique taken into consideration shall ensure that verification can be done effectively within the needed function scope. The technique chosen would have to be able to recognize the features of a person and verify by comparing with an initial database.

Once the electronic part of the circuit has been designed, the circuit is drawn using Proteus and its functions is simulated to check if it functions correctly as designed. This is important to ensure that the system that is designed would be functional.

Developing and testing the designed device into working prototype so that real-time testing can be done. A prototype has to be built in order to allow real time testing of the device. The functions can then be tested when the device functions as desired.

In short, the aims and objectives would be:

1. To integrate a digital lock device with a camera and to function as a single working unit.
2. To select a facial recognition technique and design a practical biometric verification system.
3. To stimulate the facial recognition access device using software tools and incorporated into the system hardware.
4. To develop and test prototype.
1.4 Final Project Scopes and Limitations

This research will require the integration of two current systems that is used commercially. It would also help improve the current security systems used in most organizations as there would be two layers of security that has to be bypassed before access is granted to the individual. This system will coincide with the “Defense in Depth” method. This system is a process where multiple layers of security are used to ensure that the security cannot be easily breached. The intruder would have to breach more than a layer of security since the system requires verification through password and face recognition. This multi layered system would make the system even more of a secure access device. Defense in depth is process not a product. It’s proactive approach to thinking about security from the inside out. Certain architectural approaches such as centralized security overlays lend themselves well to solve today interior security problems. Security continues to be an ongoing process and constant vigilance play equally important roles in building the best security [4].
1.5 Final Project Outline

Figure 1.1: Proposed System Design

Figure 1 shows the flow in designing the proposed digital locking system with biometric verification. Firstly, the proposed design is evaluated based on its function and design. Enhancements are then planned for the design and its usage is then justified. The digital lock with camera circuit is then designed. Troubleshooting is then done if there are problems involved in designing the circuit or alternatives and improvements. A source code is written using Matlab for face recognition and suitable outputs. The design is
evaluated to ensure if further modification or improvement is needed. A prototype is then developed and tested.

1.6 Conclusion

The presence of the digital lock with biometric verification systems would help in deterring crimes and theft in vulnerable business areas and homes. For this reason, more and more households and businesses can be equipped with the proposed system with the hopes of protecting their properties against breach of security. This will enable them to guard against frauds and loss of intellectual properties. Besides serving as a good platform for a secured security, the presence of digital lock with biometric verification would also mark another milestone in the improvisation as well as further developments in the era of technology.
CHAPTER 2

LITERATURE REVIEW

2.1 Preliminary Remarks

The locks main function is to prevent unauthorized access to a wide range of items such as computers, data, building, money and weapons, thereby reducing crime and increasing safety. PINs(Personal Identification Numbers), signatures, ID cards, Credit cards and driving licenses are examples of common means of identification and access. But they can be forgotten, mislaid, falsified or stolen, hence when such devices or methods are used, it does not necessarily ensure that the user is actually the person authorized to use it. In contrast (with the exception of performing surgery) it is nearly impossible to steal a biometric or transfer on between individuals. Biometric verification provides an identifier that unique to each and every individual that is non–intrusive and user–friendly. The automation of biometric verification offers considerable scope for simplifying and making secure a variety of processes [5].

In conclusion, this system would be an alternative security measure and with proper development, it is able to eliminate the need of the elements below:

- Carrying the documents
- Remembering and entering passwords and PINs
- Carrying keys or ID cards to gain access into restricted areas
- Having a security officer to monitor the staffs entering or exiting the premise.
2.2 Domain Research

The first concept of face recognition was developed in the 1960’s and it was a semi–automated system. The system required the administrator to locate the features (eyes, ears, nose and mouth) on photographs before it calculates distances and ratios to a common referenced point, which were then compared to the reference data. This method was used by Goldstein, Harmon and Lesk [6] who use 21 subjective markers such as hair color and lip thickness to automate the recognition. Although the system had a specific amount of detail, the data (measurements and locations) had to be manually computed and inputted. In 1980’s, Kirby and Sirovich [7] applied principle component analysis, a standard linear algebra technique to the face recognition problem. Turk and Pentland [8] discovered that while using the eigenfaces technique, the residual error could be used to detect faces in images. The eigenfaces technique is a discovery that enabled real time automated face recognition systems. The technique had then sparked a great interest in developing future face recognition technologies and usages.

These techniques had been developed to produce a system that is accurate and able to track facial features in order for a system designed would be able to function effectively in real–time. These systems work in a basic rule or concept which would be extracting and identifying or verifying by finding the best match from the sequence of images captured by camera using a pre-stored image database.
2.3 Concept

There are two different ways to recognize a person which is verification and identification. Identification is the aim to address the question “who am I?” which would require searching for an individual identity. Identification is more of a challenging problem because it involves 1:X matching which means identifying an identity from an uncountable amount of identities. For instance, in order to identify a person an accumulative amount of details is need to assist the process of identifying. This can be done by picking out an identity from a pool of collective that matches the said person.
On the other hand, verification answers the question “Am I who I say I am?” which would require a 1:1 matching for verification. It functions by confirming or denying a person’s claimed identity. This is done by confirming the features and thereafter linking in to the said person. By comparing the features of several identities within the pool of identities in a database, the identity of the person is verified to be exact or accurate.

2.4 Approach

Different approaches of face recognition for still images can be categorized into three main groups such as holistic approach, feature-based approach, and hybrid approach [9]. These different approaches work using different parameters to detect features in a person’s face.

2.4.1 Holistic approach

In holistic approach, the whole face region is taken into account as input data into face detection system. Examples of holistic methods are eigenfaces (most widely used method for face recognition), probabilistic eigenfaces, fisherfaces, support vector machines, nearest feature lines (NFL) and independent – component analysis approaches. They are based on principal component – analysis (PCA) techniques that can be used to simplify a dataset into lower dimension while retaining the characteristics of dataset [10].

2.4.2 Feature-based approach

In feature-based approaches, local features on face such as nose, and then eyes are segmented and then used as input data for structural classifier. Pure geometry, dynamic link architecture and hidden Markov model methods belong to this category [10].
2.4.3 Hybrid approach

The idea of this method comes from how human vision system perceives both local feature and whole face. There are modular eigenfaces, hybrid local feature, shape normalized, and component based methods in hybrid approach. Thus, when a human face is represented as an image, it is very natural for these features to depict distinguishing characteristics not present in other facial components such as forehead, cheeks and chin [10].

2.5 Face Recognition Techniques

There are a few main techniques that are used in face recognition. This discussion shows the difference in the techniques that can be used in face recognition. The approaches are analyzed in terms of the feature representation that is used to recognize features in the face. The techniques discussed are neural networks, geometrical feature matching, graph matching, eigenfaces as well as fisherface.

2.5.1 Neural Networks

The attractiveness of using neural networks could be due to its non-linearity in the network. Hence, the feature extraction step may be more efficient than the linear Karhunan – Loeve methods which choose a dimensionality reducing linear projection that maximizes the scatter of all projected samples [7]. However, when the number of persons increases, the computing expense will become more demanding. In general, neural network approaches encounter problems when the number of classes (i.e., individuals) increases. Moreover, they are not suitable for a single model image recognition test because multiple model images per person are necessary in order for training the systems to “optimal” parameter setting.
2.5.2 Geometrical Feature Matching

Geometrical feature matching techniques are based on the computation of a set of geometrical features from the picture of a face. The overall configurations can be described by a vector representing the position and size of the main facial features, such as eyes and eyebrows, nose, mouth, and the shape of face outline. One of the pioneering works on automated face recognition by using geometrical features was done by T. Kanade in 1973 [11]. The matching process utilized the information presented in a topological graphic representation of the feature points. After compensating for different centered location, two cost values, the topological cost, and similarity cost, were evaluated. In summary, geometrical feature matching based on precisely measured distances between features may be most useful for finding possible matches in a large database. However, it will be dependent on the accuracy of the feature location algorithms. Current automated face feature location algorithms do not provide a high degree of accuracy and require considerable computational time to the right person was 86% and 94% of the correct person’s faces were in the top three candidate matches.

2.5.3 Graph Matching

Graph matching is another approach to face recognition. M. Lades et al in 1993 [12] presented a dynamic link structure for distortion invariant object recognition, which employed elastic graph matching to find the closest stored graph. Dynamic link architecture is an extension to classical artificial neural networks. Memorized objects are represented in terms of a local power spectrum and whose edges are labeled with geometrical distance vectors. Object recognition can be formulated as elastic graph matching which is performed by stochastic optimization of a matching cost function. In general, dynamic link architecture is superior to other face recognition techniques in terms of rotation invariance; however, the matching process is computationally expensive.
2.5.4 Eigenfaces

Eigenface is one of the most thoroughly investigated approaches to face recognition. It is also known as Karhunen-Loeve expansion, eigenpicture, eigenvector, and principal component. M. Kirby and L. Sirovich [7] used principal component analysis to efficiently represent pictures of faces. They argued that any face images could be approximately reconstructed by a small collection of weights for each face and a standard face picture (eigenpicture). The weights describing each face are obtained by projecting the face image onto the eigenpicture for face detection and identification.

In mathematical terms, eigenfaces are the principal components of the distribution of faces, or the eigenvectors of the covariance matrix of the set of face images. The eigenvectors are ordered to represent different amounts of the variation, respectively, among the faces. Each face can be represented exactly by a linear combination of the eigenfaces. It can also be approximated using only the “best” eigenvectors with the largest eigenvalues. The best \( M \) eigenfaces construct an \( M \) dimensional space, the “face space”. In summary, eigenface appears as a fast, simple, and practical method. However, in general, it does not provide invariance over changes in scale and lighting conditions. In A. Pentland et al [13], experiments with ear and face recognition, using the standard principal component analysis approach, showed that the recognition performance is essentially identical using ear images or face images and combining the two for multimodal recognition results in a statistically significant performance improvement.

Then we need to calculate the average space in face space. Here \( M \) is the number of faces in our set:

\[
\Psi = \frac{1}{M} \sum_{n=1}^{M} \Gamma_n
\]

We then compute each face’s difference from the average:

\[
\Phi_i = \Gamma_i - \Psi
\]
We use these differences to compute a covariance matrix $\Sigma$ for our dataset. The covariance between two sets of data reveals how much the set correlate.

$$\Sigma = \frac{1}{M} \sum_{n=1}^{M} \Phi_n \Phi_n^T = \frac{1}{M} \sum_{n=1}^{M} \begin{pmatrix} \text{var}(p_1) & \cdots & \text{cov}(p_1,p_N) \\ \vdots & \ddots & \vdots \\ \text{cov}(p_N,p_1) & \cdots & \text{var}(p_N) \end{pmatrix} = AA^T$$

Where $A$ and $P_i = \text{pixel I of face n.}$

The eigenfaces that we are looking for are simply the eigenvectors of $C.$ However, since $C$ is of dimension $N$ (the number of pixels in our images), solving for the eigenfaces gets ugly very quickly. Eigenface face recognition would not be possible if we had to do this. This is where the magic behind the eigenface system happens.

After we get the $N$, we need to simplify the initial eigenface basis by using a statistical technique known as Principal Component Analysis (PCA), we can reduce the number of eigenvectors for our covariance matrix from $N$ (the number of pixels in our image) to $M$ (the number of images in our dataset). In general, PCA is used to describe a large dimensional space with a relative small set of vectors. It is a popular technique for finding patterns in data of high dimension, and is used commonly in both face recognition and image compression.

PCA tells us that since we have only $M$ images, we have only $M$ non-trivial eigenvectors. We can solve for these eigenvectors by taking the eigenvectors of a new $M \times M$ matrix:

$$L = A^T A$$

Because of the following math trick:

$$A^T A v_i = \mu_i v_i$$

$$A A^T A v_i = \mu_i A v_i$$
Where $V_i$ is an eigenvector of $L$. From this simple proof we can see that $AV_i$ is an eigenvector of $C$. The $M$ eigenvectors of $L$ are finally used to form the $M$ eigenvectors $U_l$ of $C$ that form our eigenface basis:

$$u_l = \sum_{k=1}^{M} v_{lk} \Phi_k$$

It turns out that only $M-k$ eigenfaces are actually needed to produce a complete basis for the face space, where $k$ is the number of unique individuals in the set of known faces.

In the end, one can get a decent reconstruction of the image using only a few eigenfaces ($M'$), where $M'$ usually ranges anywhere from .1M to .2M. These correspond to the vectors with the highest eigenvalues and represent the most variance within face space.
2.5.5 Fisherface

In 1997, Belhumeur et al [14] proposed fisherfaces method by using PCA and Fisher’s linear discriminant analysis to produce subspace projection matrix that is very similar to that of the eigen space method. However, this method can solve one of the main issues that arise in Pentland [8] eigenfaces method, one of the main drawbacks of eigenface approach is that the scatter being maximized can also be due to within – class scatter, which can increase detection error rate if there is a significant variation in pose or lighting condition within same face images. Considering these changes due to different illumination and head pose are almost always greater than variation due to difference in face identity, a robust detection system should be able to handle the problem. Since, the fisherfaces approach takes advantage of within – class information; minimizing variation within each class, yet maximizing class separation, the problem with variations in the same images such as different lighting conditions can be overcome.
CHAPTER 3

RESEARCH METHODOLOGY

3.1 Preliminary Remarks

The research done from previous literatures has shown that the system proposed can be designed although there would be a fair challenge in integrating the inputs and outputs (hardware) and the processing (program) part of the system. However, there are also constraints that have to be taken into account before the system design can be perfected. The system would have to be designed and simulated to ensure the integration of the two parts of the system can be done without losing the integrity of the system.

3.2 Research Approach

Since the security is still a major concern and traditional methods of deterring theft and intrusion has become obsolete, much effort is being put into the development of multi-layered security measures. This system will coincide with the “Defense in Depth” method and the approach that has been defined in this project is Holistic approach. “Defense in Depth” is a process where multiple layers of security are used to ensure that the security cannot be easily breached, whereas a multiple layers of security means there are more than one type of security so that it becomes more secure and safe. In a way, advancement in this field has sparked many interest as well as development projects to provide multi layered security systems. Any intruder would have to breach more than a layer of security since the system requires verification through password and face recognition.
The main objective of this project is to develop an integrated security system which is made up of a digital lock and integrates face recognition as a secondary security layer. This will serve as a platform for a more established security. The main purpose of frontline to security is to safeguard properties and intellectual properties against thefts and harmful activities. Hence, the developed system would further increase the research into real-time usage of face recognition and improving the quality of the techniques. Coinciding with this, the digital locking technology would go through a significant enhancement and this improvement would put a vast difference between traditional locks and digital locks.

The face recognition technique that has been chosen for this project is the eigenfaces technique. This method provides a high enough accuracy rate to be used in real-time. The detection and recognition ability of this method shows a high reliability among other methods and is suitable for the use in the project. Eigenfaces technique is also able to provide real-time recognition of faces with minimal constraints. Since the eigenfaces is being decided, the face recognition must be on a full – face for recognition process.
3.3 Primary Research

A functional system designed based on the concept would work by:

Figure 3.1. Functional system overview
1. Start

The digital lock is activated and the verification process begins.

2. Input Image

In this stage, an image of the individual would be captured and the facial features are extracted for processing.

3. Image match

The captured image would then be compared with the images in the database to verify the individual’s identity.

4. Input Password

The individual inputs the password into electronic lock.

5. Identity confirmed

If the password matches the individual’s image, then the identity of the individual is confirmed.

6. Lock Release

The locking mechanism release is then triggered so that access can be granted and system is reset awaiting next individual.
CHAPTER 4

METHODOLOGY AND SYSTEM EXPLANATION

4.1 Preliminary Remarks

The system design and methodology that is used to develop the planned system is discussed in this chapter. System development and the components that will be used for construction the circuit are chosen. A simulation of the circuitry and the development of the software are also done to ensure that the system can be developed as intended and the software would function as intended.

4.2 Reasoning on system development

The system is designed to work as multi-layered access system which incorporates face recognition as well as a numerical password input as a security device. This would require combining two systems and integrating them to work as a single unit. Initially the two systems are designed separately as both have different methodologies and functions. The face recognition system would require a more complex processing unit as it runs on an algorithm and requires specific software to execute and run the recognition process while the locking mechanism is designed using a PIC microcontroller that is programmed to base on a fixed logic.

i) Face Recognition

The Face Recognition system is based mainly on an algorithm based program that is written using the Matlab software. The recognition process is done as a verification process where an input image is taken and compared with a database of preprocessed images of the individuals that are allowed access. The verification and matching of the system designed would also have to perform real-time verification process to ensure that access is only given to the specified person and a breach of security can be prevented. Not to forget, the eigenface system is occupied for full – face recognition only.
A laptop or pc is used as a processing unit that would run the verification program and a built-in webcam or external webcam can be used to capture the image that will be used for processing. The face recognition system design can be broken down into several parts.

Firstly, database of images of the individuals that will be granted access by the system needs to set up. This database is called a training set as the system would refer to this training set to compare and match the new input images for verification. The images in the training set have to be preprocessed in order for it to be used in the verification process. The preprocessing includes resizing and de-coloring it to a grayscale image.

When the face recognition program is initiated, an image or a picture of the person is taken to be used in the verification process. This picture is then saved and used for representation and matching in face recognition. The image would then be converted into a specific form of data so that it can be compared and matched with an existing database in the system. This is when the verification process is done to confirm an identity.

Once the verification process is done and if the question “Am I who I say I am?” is answered, then the identity of an individual is confirmed. The system would then grant the access to the individual. If the identity of the individual could not be verified, access would then be denied.

ii) Digital lock

The locking mechanism of the system is based on a PIC microcontroller that would be programmed to receive an input from the verification system and then receive a numerical password which would be used as part of the second verification step before access is granted to the individual.

Once the acknowledgement from the verification system is received showing positive verification, the locking system would then request the password or pin number before granting access to the individual.

If the given password or pin number does not match, the verified picture, or if an incorrect pin was input, then access would be denied.
4.3 Investigation on material/component selection

The circuit is designed based on the functions and the usage of the device hence, the materials or the components that will be used in building the circuit has to be relevant and capable to function as required. Although there are many different types of components but care has to be taken in deciding the components needed based on functions, ease of usage, availability and to ensure that they are cost effective.

**PIC 16F877A microcontroller**

The PIC 16F877A microcontroller is a 40 pin CMOS FLASH-based-8-bit microcontroller that is fairly easy to program and has a memory size of 256 bytes of EEPROM data memory. The microcontroller is used with the SK40C start-up kit by Cytron Technologies. The start-up kit is used to run the PIC as well as program the PIC. The SK40C has an on board 5V voltage regulator (1A maximum), LED as power indicator, a 20MHz crystal and a reset button.
Figure 4.2: PIC 16F877A microcontroller pin diagram

Figure 4.3: SK40C start-up kit by Cytron technologies
4x4 Keypad

A 4x4 Keypad is used as an input device to receive the password or pin number from the individuals that wants to be granted access. There are 16 characters in the 4x4 keypad, 10 which are numerals (0-9), 4 alphabets (A-D) and 2 additional symbols.

Matrix keypads use a combination of four rows and four columns to provide button states to the host device, typically a microcontroller. Underneath each key is a pushbutton, with one end connected to one row, and the other connected to one column. These connections are shown in figure 4.4.

![4x4 Keypad Circuit](image-url)

Figure 4.4: 4x4 Keypad Circuit
In order for the microcontroller to determine which button is pressed, it first needs to pull each of the four columns (pins 1-4) either low or high on at a time, and then poll the states of the four rows (pin 5-8). Depending on the states of the columns, the microcontroller can tell which button is pressed.

For example, say your program pulls all four columns low and then pulls the first row high. It then reads the input states of each column, and reads pin 1 high. This means that a contact has been made between column 4 and row 1, so button ‘A’ has been pressed.

![Figure 4.5: 4x4 Keypad](image)

**LCD screen display**

A 16x2 LCD display is selected to display words for simple notifications and password symbols for the locking system. The LCD has sufficient characters to display numerical and alphabets. The word contrast of the LCD can be adjusted using potential meter for clearer or better viewing depending on the need and lighting conditions.

![Figure 4.6: 16x2 LCD screen display](image)
Relay and buzzer

A relay and buzzer is used as the output of the system to show that the circuit functions as desired. A relay is used for having two different inputs and outputs. For example if I input 1 then the output must be 1 and if I input 2, then the output must be 2. A buzzer is used as an indicator if the output of the system is “right” or “wrong”.

4.4 Design and Simulation

Once the basic system design has been planned out, a more detailed design of the system has to be designed. This design would have to include schematics, software development and simulation of the system that will be implemented. This is an important phase to ensure that system designed is feasible. A simulation is also done to able to test and manipulate a design theoretically before it is practically assembled thus ensuring that the nature that the system would function once it is assembled can anticipated.

Since the system requires the incorporation of codes for the microcontroller and a program to perform the face recognition, the codes and program can be tested during the simulation process. Any changes or manipulation to the system design can also be done if needed and this can be done during the simulation process. Once the design is finalized then the hardware of the design can be implemented.

The first part of the design process is designing the detailed system flowchart that shows the system process. This is to aid in the implementation process as it shows all the steps or process within the system.
IF NO

INPUT IMAGE

ALIGNMENT & MEASUREMENT

REPRESENTATION & MATCHING

IDENTITY VERIFIED? (FACE RECOGNITION)

IF NO

IDENTITY CONFIRMED

LOCK RELEASED

IF YES

INPUT PASSWORD

IF NO

IDENTITY CONFIRMED

LOCK RELEASED

Figure 4.7: Program Flowchart
When the system is initiated, an input image is given to the system and the facial features would be captured for processing. The alignment and measurement of the image is taken into account to ensure that the image taken could be used for verification. The image would then be converted into a specific form of data so that it can be compared and matched with an existing database in the system. This is when the verification process is done to confirm an identity. If the question “Am I who I say I am?” is answered. Then the identity of an individual is confirmed, the system would then grant the access to the individual. If the image is successfully verified, the individual is then required to input the password into electronic lock. The locking mechanism release is then triggered so that access can be granted and system is reset awaiting next individual.
4.5 Hardware design
The schematic of the proposed circuit design is drawn using simulator software called Proteus. The design of the circuit includes the PIC16F877A that would act as the brain of the circuit. External devices such as the LCD, keypad, buzzer and LED are also included in the design. This design would be the basis and the reference when the circuit design is implemented. In addition, there is no interfacing between the Matlab software with the hardware design that has been used in this project and the interfacing would be done by a certain operator.
CHAPTER 5

SYSTEM IMPLEMENTATION & TESTING

5.1 Preliminary Remarks

Once the proposed system has been designed and simulated, the system is then implemented in stages. This is done according to the flowchart that was designed during the planning. The flowchart is a very important part of the project design and contains details of the working process. This is to ensure that all planned aspects of the system can be implemented successfully.

5.2 The working process of the system

5.2.1 Digital lock

The hardware section of the design is the circuitry of the digital lock. The digital lock had been designed previously and the proposed design has to be implemented. In order to build a working prototype, the design could be manipulated using the software and once satisfying results were obtained, the designed schematic is then implemented.

i) Hardware

![Figure 5.1: LCD connections](image)
The figure above shows the connections of the LCD. There are 16 connections to the PIC 16F877A. These connections provide the power, input values and the configurations from the program.

![PIC 16F877A with SK40C startup kit](image)

**Figure 5.2: PIC 16F877A with SK40C startup kit**

The PIC16F877A is the main component that is used to control the locking mechanism and the program that is compiled will be programmed into the microcontroller memory. The microcontroller is mounted on a programming and start-up kit from Cytron Technologies Sdn Bhd. All the main connections from the external peripherals are connected to the microcontroller.

![Relay](image)

**Figure 5.3: Relay**

The relay is used to trigger the magnetic lock to release or stay locked.
In this research, 2 LEDs are used as a representation of the lock. The red LED is used to represent the LOCKED state and the yellow LED is used to represent the UNLOCKED state.

Buzzer is used as another signal of represent the lock. It will beep once if it’s RIGHT and it will beep twice if it's in WRONG.
Figure 5.6: Complete prototype

The completed prototype is built and assembled and tested to ensure that all function are working and that there are no malfunctions.
i) Program Flowchart

START

LCD CONFIGURATION

DISPLAY
“ENTER 6 – DIGIT PASSWORD”

IF NO

PASSWORD CORRECT?

IF YES

DISPLAY
“ACCESS GRANTED”

LOCK RELEASE

DISPLAY
“INVALID PASSWORD”

Figure 5.7: Program Flowchart
The proposed digital lock program is designed according to the flowchart above. The flowchart is used to show all major processes that have to be completed before the locking mechanism is released and granting access to the individual. Therefore, using the flowchart as a guide, the source code for the PIC16F877A is designed for implementation.

ii) Program source code

The important codes that were used in the implementation of the locking mechanism is shown and discussed below. These codes were programmed using MPLab IDE software and are converted in (.hex) format so that it can be programmed into the PIC16F877A. The codes determine how the microcontroller and the circuit as the whole functions.

```c
// ==============================================================
// DIGITAL LOCK SYSTEM WITH BUILT IN CAMERA
// NICHOLAS JOY
//
// ==============================================================

#include<pic.h>
#include<htc.h>

// configuration
__CONFIG (0x3F32);

// define
#define rs RC0
#define e RC1
#define led_data PORTD
#define relay RB1
#define buzzer RB2
```

Initially, the libraries are included in the program. The libraries <pic.h> and <htc.h> is required to program the PIC16F877A. The LCD configuration and the functions that will be used are also initialized in the beginning of the program.
Then the function prototypes and the global variables are initialized. The function prototypes are declared to inform the compiler the function and the type of data will be returned. Global variables are variables that can be accessed and modified from any part of a program. These variables are used as their values are changed during the execution of the program.
In the main program body, the states of the PORTA, PORTB, PORTC, PORTD and PORTE are declared using the binary numbers equivalent to declare the port as an input port and output port. The initial states of the ports and the LCD configurations are also defined as well.

```c
// main function

void main(void)
{

    ADCON1=0b00000110;
    TRISA=0b00011111;
    TRISB=0b00000000;
    TRISD=0b00000000;
    TRISC=0b11110000;
    TRISE=0b00000000;

    PORTC=0;
    PORTD=0;
    relay=0;
    buzzer=0;

    send_config(0b00001001);
    send_config(0b00000010);
    send_config(0b00000110);
    send_config(0b00001100);
    send_config(0b00111000);

    while(1)
    {

        password_count==0;

        lcd_clr();
        delay(1000);
        lcd_goto(0);
        send_string("Awaiting Image");
        lcd_goto(20);
        send_string("Verification");
        delay(300000);

        lcd_clr();
        lcd_goto(0);
        send_string("Please Enter");
        lcd_goto(20);
        send_string("6-Digit Password");
        delay(200000);
```
The PIC 16F877A is programmed to display a string of characters when the system is initiated as well as when requesting for password. The sent string is displayed on 2 lines of the LCD as only 16 characters can be displayed per line.

```c
while (password_count<7) {
    clearrow1();
    scancolumn1();
    clearrow2();
    scancolumn2();
    clearrow3();
    scancolumn3();
    clearrow4();
    scancolumn4();

    if(password_count==6)
    {
        password_count=0;

        if((keyin_char[0]==stalled_char[0])
        && (keyin_char[1]==stalled_char[1])
        && (keyin_char[2]==stalled_char[2])
        && (keyin_char[3]==stalled_char[3])
        && (keyin_char[4]==stalled_char[4])
        {
            lcd_clr();
            lcd_goto(0);
            send_string("ACCESS GRANTED !!");
            relay=1;
            beep_once();
            delay(200000);
            relay=0;
            lcd_clr();
            break;
        }
        else
        {
            lcd_clr();
            lcd_goto(0);
            send_string("INVALID PASSWORD !!");
            beep_twice();
            delay(200000);
            lcd_clr();
            break;
        }
    }

    else
    {
        clearrow1();
        clearrow2();
        clearrow3();
        clearrow4();
        scancolumn1();
        scancolumn2();
        scancolumn3();
        scancolumn4();
    }
}
```

The codes above are used to receive and save the number or characters that are input by the keypad. The functions to scan and clear the inputs are also declared and final verification process of the password is also declared in the body of the program. The code written compares the received inputs and matches it with the preset password. Access is granted if the password matches and access is denied if the passwords do not match.
```c
// scanning function

void clearrow1(void)
{
    RA1=0;
    RE0=1;
    RA5=1;
    RA4=1;
}

void scancolumn1(void)
{
    if (RA0==0)
    {
        while (RA0==0) continue;
        if (password_count==0) lcd_clr();
        lcd_goto(password_count);
        send_char('1');
        keyin_char[password_count]='1';
        password_count+=1;
    }
    else if (RA1==0)
    {
        while (RA1==0) continue;
        if (password_count==0) lcd_clr();
        lcd_goto(password_count);
        send_char('2');
        keyin_char[password_count]='2';
        password_count+=1;
    }
}
```

The scanning functions are used to scan each rows of the keypad for inputs and save the input character. The same is also done to scan the columns for inputs from the keypad and characters are saved. The functions work in a loop and continuously scan the keypad for inputs. The input characters or number are saved and used to compare and verify the password.
5.2.2 Face Recognition

The face recognition program is designed and written to be implemented based on the initial design structure. A flowchart is initially designed incorporating the necessary functions and steps to ensure that the program is designed in a smooth flow. The work process of the program is done on the program flowchart and programming is done using the Matlab software.

i) Flowchart

![Flowchart](image-url)

Figure 5.8: Face Recognition flow chart
Firstly, a training set or a database of images has to be created to be used in the verification process as these images will be used to compare against the new image. The database that will be used is the Olivetti Research laboratories (ORL) & AT&T Laboratories Cambridge face recognition database. The database contains 400 images of 40 different individuals. Each individual has different pictures with slightly varying poses of the face.

This database is used as it is the common database used for most systems testing and is also used for discussion in most literature study done on face recognition. The database is also one of the smaller and much lighter databases available as larger database would require more space and a longer processing time. It is also important that all the images and test images used in the training and for recognition purpose are required to be of the same size with resolution 112 x 92. Training set and test images are also in grayscale and saved in (.pgm) format to reduce the image memory size.

Once the database has been set, the eigenfaces which are designed for the training set has to be calculated. Images are made up pixels, which can be assumed as x amount of rows and y amount of columns. This means that the images can be converted into a large matrix using the pixel values. In this case, the size would be 112 x 92. Images that have been converted to this form are the average or mean faces. Once the average or mean faces have been calculated, mean face value is then deducted from the sample images. This has to be done to the test images as well to be used in recognition.

Upon completion, the eigenvectors or eigenfaces of the images is calculated using the built matrix. The eigenfaces will then be used to generate the face-space values. The values or the weight of these images of the training set would then be used to compare with the new input image. If the weights match the images, the images are considered and hence the system recognizes the new image as it is the same as the training images.
Face Recognition Program

a) Training Set

```matlab
function out=load_database()
% We load the database the first time we run the program.

persistent loaded;
persistent w;
if(isempty(loaded))
    v=zeros(10304,400);
    for i=1:40
        cd(strcat('s',num2str(i)));
        for j=1:10
            a=imread(strcat(num2str(j),'.pgm'));
            v(:,(i-1)*10+j)=reshape(a,size(a,1)*size(a,2),1);
        end
    end
    cd ..
    w=uint8(v); % Convert to unsigned 8 bit numbers to save memory.
end
loaded=1; % Set 'loaded' to avoid loading the database again.
out=w;
```

For testing purposes, a test database is taken from AT&T laboratories Cambridge face recognition database. The database is made up of 400 images and there are 10 different images of each of 40 distinct subjects. For some subjects, the images were taken with facial expressions. (open / closed eyes, smiling / not smiling) and facial details (glasses / no glasses). All the images were taken with the subjects in an upright, frontal position (with tolerance for some side movement). Each image is taken with a resolution of 112 x 92 and is saved in the (.pgm) format.
b) **Main program**

```matlab
data = load('training_set_database.mat'); %loading database
w = load_database(); %loading database size (W)
```

Initially the database of the training set is loaded. The training set is the database of images that have initially taken and stored to be used for comparison. Any new image will be tested and verified through recognition process from the database that already loaded.

```matlab
vid = videoinput('winvideo', 1, 'YUY2_160x120'); %initialize video input
triggerconfig (vid, 'manual'); %configure trigger
vid.FramesPerTrigger = 1;
set (vid, 'TriggerFrameDelay', 20); %Set trigger delay
preview(vid);
start(vid);
trigger(vid) %Triggering snapshot
set (vid, 'ReturnedColorSpace', 'grayscale')
rgbImage = getdata(vid);
stop(vid);

fullImageFileName = fullfile(pwd, 'baru.pgm');
imwrite(rgbImage, fullfile(fullImageFileName);
B = imread('baru.pgm');

r = imresize(B, [112 92]); %Resizing image to 112x92
imwrite(r, 'baru.pgm');

im = r; %r contains the image we use to test the algorithm

tempimg = im(:, :, 1);
r = reshape(tempimg, 10304, 1);
v = w; %v contains the database
N = 50; %number of signatures used for each image
```
The initial conditions of the programs is then set and initialized. This is important that all variables and functions are declared. The program is required to take a snapshot images and process is so that it can be used in the recognition process. Thus, the video input is initialized and the image is converted to grayscale. The image is saved and is resized from 1260x120 to 112x92 so that the pixels and the size will be the same as the database which is used.

```matlab
%% subtracting the mean from v

O=uint8(ones(1,size(v,2))); % is the mean of all images
m=uint8(mean(v,2));

vzm=v-uint8(single(m)*single(O)); % vzm is v with the mean removed

%% calculating eigenvectors of the correlation matrix
% we are picking N of the 400 eigenfaces.

[V,D]=eig(L);
V=single(vzm)*V;
V=V(:,end-1:end-(N-1)); % pick the eigenvalues corresponding to the 10 largest eigenvalues

%% calculating the signature for each image

C=zeros(size(v,2),N);
for i=1:size(V,2);
    C(i,:)=single(vzm(:,i))*V; % each row in C is the signature for one image
end
```

The mean of the input face image and the database is calculated. The mean value is then removed to obtain mean-shifted images. These values are then used to calculate the eigenvectors and eigenvalues of the images. The output of this step is the matrix of eigenvectors. The signature value of each image is then calculated. The signature value of the images can also be said to be the weight of the images that will be used to differentiate each image.
Once the signature values have been obtained, the recognition process is the done. This is done by deducting the mean of the input image with the mean of the images in the training set. If the value of an image in the training set matches the value of the input image, then the pictures are matching and the identity is verified. Both the images are then shown as proof.
5.2.3 Testing and troubleshooting of the system

Testing and troubleshooting is done only on the hardware of the project as the programs used are debugged during the programming and compiling of the programs. Once the hardware of the system has been implemented, the system has to be tested to ensure that it functions as per design.

The system is tested using various methods and the first test is to ensure that all connection and soldered joints are done correctly and there are no loose connections. The next step would be to power the device and check if all of the connections are correct and the components are working in order. This is to ensure that there is no faulty hardware used in the completion of the circuit. This would also narrow down a cause for malfunction the circuit fails to initialize and function.
Another test was to program the PIC16F877A of the circuit with the compiled program. If the programming can be done successfully, then the program functions are tested and checked if they function according to requirement as errors in wiring could cause the system to malfunction.

If the initialization of the program is successful, then the rest of the functions of the circuit is tested such as displaying characters according to program, input of password, output such triggering of relay and buzzer. All the parameters of the program and the circuit is tested.

During the testing phase, another malfunction that was detected is soldering joint of the keypad had given away during testing phase. This was probably due to weak soldering in the initial stage. The connection was re-soldered and tested again. Once re-soldered the keypad function as per normal.

The display that was programmed to display a notification from the program changes too fast and this had to be corrected by increasing the delay in the program itself. The initial program was erased and the new program with the changed delay value was programmed into the PIC16F877A. Then the display is tested again to check if the delay functions as expected.

5.3 Interpretation of Data

In the beginning stages of the implementation of the program, data that were collected had to be interpreted in a different manner due to different functions and methodology. Data conversions had to be done and certain formats of files had to be changed in the course of the program. This had caused some errors to surface and some time was taken to re-evaluate the coding done to perform the functions that were needed without errors.

The eigenface method based on matrix, and the dimensions of the matrix are based on the resolution of the images in the training set and the number of images in the training set. If any image within the training set is changed, it has to be within the same parameters or identical resolution as the rest of the images in the training set. If these parameters are breached, then algorithm would not function. These parameters are also applied to the input image that is used for matching as the difference would violate the parameters.
Some re-evaluation had to be done during the programming as well as the implementation of the hardware due to the timing setting or delay settings as these function according to the clock – cycle of the microcontroller. The changes had to be done in order for the timing to be in – line and according to the clock pulse received by the microcontroller.

There were some circumstances that the result of the recognition was not accurate. This is probably due to the way the eigenface methodology which processes the image as a whole and takes into account the background as well during recognition. This includes circumstances whereby wrong match is being identified or no identical match is found. Therefore, the best way to overcome this is to ensure that when a new image is taken to be used as an input, the background of the image should match the background of the training set images or better still, taken against an empty background. This could eliminate the errors that occurred.

The method’s main weakness would be the lighting factor. Poor lighting or a highly different lighting condition could badly affect the results of the face recognition process. This is because lighting changes the contrast of the image and indirectly changes the values or the weight value of the image during processing. If the weights do not match, the image is considered a different image.
CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

6.1 Preliminary Remarks

This research was designed as an enhancement to strengthen the security system to cope with the continuous threat to many organizations, and even homes. Many of today’s victorious businesses in general have adopted into investing a highly integrated security system to guard their premises. As mentioned earlier, security is definitely the backbone of an organization to safeguard business against possible threats towards materials, confidential information and intellectual properties of an organization. The importance of security has resulted into booming technology in digital system locks or an even tighter security to safeguard their businesses against risks. Along with this advancement in technology, the biometric verification digital lock system will be a favorable project that is in line with the motive of innovation and enhancement.

6.2 Conclusions relating to the Research Objectives

As per stated in the beginning of this project, all the objectives that were expected in the beginning of the study was not fulfilled accordingly towards the completion of this project. An initial study was done on various methods of face recognition was and a feasible project was developed. At this point, the objective to select a facial recognition technique and design a practical biometric verification system was made possible with much trials and tribulations. This was enabled by the simulation of the facial recognition access device using software tools and then wasn’t fully incorporated to the system hardware. A human is needed to simulate the project perfectly. The developed program functions and is able to perform face recognition in real-time. In the final stage, a fully functional prototype was developed as the designed plan as per the proposed study. This shows that the proposed prototype is feasible and could further be developed to be used as a commercial security system.
6.2.1 Recommendations and Suggestions

Although the developed system functions as per proposed, there are several improvements that could be done depending on the circumstance and as well as the general usage of the product. If such system is to be further developed, a larger database or training set which would contain more varying images of the individual could be used to enhance the efficiency of the system.

Using better technology to develop the system to process the recognition such as faster processors, larger storage space and camera of higher quality would collectively enhance the capability of this system to function. Faster processors can reduce the time taken for verification and a larger storage space could include a larger database for initial images. A better camera would allow higher quality or better resolution pictures to be taken and as a result better rate of recognition.

Since the approach taken into consideration processes the whole image and not to the face only, images that will be used for comparisons could be taken in a more controlled environment such a clear background or backing against a wall to avoid other objects to be included in the image. This way, the system would process an image that contains the face of the individual which would automatically enhance the effectiveness and reduce the probability of error occurring during verification.
6.3 Limitations

Limited functionality of system

As this research study is a student project and was done as a proof feasibility, a more practical methodology was used when designing and implementing it. Thus limiting the capabilities of the system to function within the means need to perform its functions and operation. Although the system functions well under most circumstances, there are certain limitations to the system.

Limited quality of output image

One notable limitation of the device itself was the quality of the input image itself. The verification depends on the quality of input image given to the system. Varying light conditions, background color or movement and camera quality affects the effectiveness of the system in recognition as the rate of error is increased. In some instance, where there was slight movement during the image capture, the image would appear blurry and could not be used for recognition.

Limited resources

As mentioned earlier, this is an individual student’s research study which is self-funded. Thus, another limitation was the financial resource that was available and thus the components or devices used in the development and implementation process do not perform as well as expected. For instance, the cost of purchasing the raw material such as PIC, LCD, relay, buzzer, ICSB Programmer is RM440 (Rp1.320.000,00). In addition, the unavailability of the raw materials within Indonesia has resulted the researcher to obtain the product from the nearest neighboring country such as Malaysia. The researcher has to fly directly to obtain the items needed as online purchase does not guarantee that the items would still be in the original condition upon delivery.

As a result, lower grade technology that was used showed that it is very practical to implement the device but it would also be prone to errors. This could be seen in the quality of the device and their output. The cost of purchasing
Duration of research study

The given duration of the research study is only a time period of five months. The researcher has to manage his studies along with this research study which can be very challenging. The limited time given can contribute to the limited overall quality of the research study.

Nature or scope of the chosen research study

The scope of the chosen research study is quite challenging as the digital lock system using PIC is very new. Thus, this is new and is a limitation for the researcher. This requires the researcher to spend more time during the field research and to ensure the successful implementation of the desired product is achieved.

Limited past researches

Due to the fact that the scope chosen is fairly new, thus there is a very limited or past researches related to this scope which can be used by the researcher. This is a huge limitation as considerable amount of time will be spent by the researcher to do research findings in relation to the chosen scope of research study. This can be a huge challenge given the limited time is only five months.
6.3.1 Further Research

Future researchers who display high level of interest in the field of face recognition or image processing as a whole could continue researching on better methods of recognition. Current methods do successfully perform the recognition process but there are too many controlled parameters that need to be fulfilled before a system can be executed. If a new method of recognition could be developed where the recognizing process is much more natural or less controlled, then face recognition would then be the front runner in biometric verification and security systems as a person’s face is almost impossible to duplicate unless thru surgery.

Future works are also dependent on current technological advancement as there may be an alternative recognition method but it is not feasible as the cost of complementing such a system is too high as it requires a higher range or more advanced devices. This can be seen especially in processors as higher range processors are able to process very large amount of data in shorter timeframe therefore a larger database would indeed develop a better system for recognition.

As for security system development purposes, the face recognition system could also be integrated with other biometric verification such as fingerprint or voice recognition. This would further enhance the security filed and it also incorporates the principal of key-less entry where the risk of duplication or breach of security can be inhibited.
6.3.2 Conclusion

The project was managed to be completed as proposed and the integrity of the system was maintained during the implementation. The use of face recognition as a toll for key-less security system has been proven feasible and should be considered as a future in security systems. Having incorporated the multi-layered security system with the implementation of this project, many more such project could be developed as well according to preference. The frontier to security is to protect assets and intellectual properties against thefts and damaging activities. Therefore, this system could further increase the research into real-time usage of face recognition and improving the quality of the techniques. Coinciding with this, the security industry and defense sciences would go through a significant enhancement and this improvement would put a vast difference between traditional locks and digital locks.
REFERENCES


APPENDICES

PROGRAM CODE
function out=load_database()
    % We load the database the first time we run the program.

    persistent loaded;
    persistent w;
    if(isempty(loaded))
        v=zeros(10304,400);
        for i=1:40
            cd(strcat('s',num2str(i)));
            for j=1:10
                a=imread(strcat(num2str(j),'.pgm'));
                v(:,(i-1)*10+j)=reshape(a,size(a,1)*size(a,2),1);
            end
            cd ..
        end
        w=uint8(v); % Convert to unsigned 8 bit numbers to save memory.
    end
    loaded=1; % Set 'loaded' to avoid loading the database again.
    out=w;
% face recognition_ Nicholas Joy

% Loading of training set database
% the training is made up of 400 images.
% the images will be used for the recognition process.

w=load_database(); % loading database
size (w)

%%% initializations
% the initial conditions are initialized.
% the new image input and video configuration.
% that will be used for recognition is set.
vid = videoinput('winvideo', 1, 'YUY2_160x120'); % initialize video input
triggerconfig (vid, 'manual') % configure trigger
vid.FramesPerTrigger = 1;
set (vid,'TriggerFrameDelay',20); % Set trigger delay
preview(vid);
start(vid);
trigger(vid) % Triggering snapshot
set(vid, 'ReturnedColorSpace','grayscale')
rgbImage = getdata(vid);
stop(vid);

fullImageFileName = fullfile(pwd, 'baru.pgm');
imwrite(rgbImage,fullImageFileName);
B=imread('baru.pgm');
r = imresize(B, [112 92]); % Resizing image to 112x92
imwrite(r,'baru.pgm');

im = r; % r contains the image we use to test the algorithm

tempimg = im(:,:,1);
r = reshape(tempimg, 10304,1);
v = w; % v contains the database

N = 50; % number of signatures used for each image

%% subtracting the mean from v

O = uint8(ones(1, size(v, 2))); m = uint8(mean(v, 2)); % m is the mean of all images

vzm = v - uint8(single(m)*single(O)); % vzm is v with the mean removed

%% calculating eigenvectors of the correlation matrix
% we are picking N of the 400 eigenfaces.

L = single(vzm)'*single(vzm);
[V,D] = eig(L);
V = single(vzm)*V;
V = V(:, end-1:end-(N-1)); % pick the eigenvalues corresponding to the % 10 largest eigenvalues

%% calculating the signature for each image
cv = zeros(size(v, 2), N);
for i = 1:size(v, 2);
    cv(i, :) = single(vzm(:, i))' * V; % each row in cv is the signature for one image
end

%% recognition
% now, we run the algorithm and see if we can correctly recognize the face.
figure (1)
subplot(121);
imshow(reshape(r, 112, 92)); title('Looking for ...', 'FontWeight', 'bold', 'Fontsize', 16, 'color', 'red');
subplot(122);
p = r - m; % subtract the mean
s = single(p)' * V;
z = [];
for i = 1:size(v, 2)
    z = [z, norm(cv(i, :) - s, 2)];
    if(rem(i, 20) == 0), imshow(reshape(v(:, i), 112, 92)), end;
    drawnow;
end
[a, i] = min(z);
subplot(122);
imshow(reshape(v(:, i), 112, 92)); title('Found', 'FontWeight', 'bold', 'Fontsize', 16, 'color', 'red');
DIGITAL LOCK SYSTEM WITH BUILT IN CAMERA

NICHOLAS JOY

PROGRAM CODE

// include

#include<pic.h>
#include<htc.h>

// configuration

__CONFIG(0x3F32);

// define

#define rs RB4
#define e RB5
#define led_red RC2
#define led_yellow RC3
#define lcd_data PORTD
#define relay RB1
#define buzzer RB2
// function prototype

void delay(unsigned long data);
void send_config(unsigned char data);
void send_char(unsigned char data);
void e_pulse(void);
void lcd_goto(unsigned char data);
void lcd_clr(void);
void send_string(const char*s);
void clearrow1(void);
void clearrow2(void);
void clearrow3(void);
void clearrow4(void);
void scancolumn1(void);
void scancolumn2(void);
void scancolumn3(void);
void scancolumn4(void);
void beep_once(void);
void beep_twice(void);

// global variable

unsigned char password_count=0;
unsigned char keyin_char[6];
unsigned char stalled_char[6]="866868";
// main function

void main(void)
{
    ADCON1=0b00000110;
    TRISA=0b00001111;
    TRISB=0b00000000;
    TRISD=0b00000000;
    TRISC=0b11111000;
    TRISE=0b00000000;

    PORTC=0;
    PORTD=0;
    relay=0;
    buzzer=0;
    led_yellow=0;
    led_red=0;

    send_config(0b00001001);
    send_config(0b00000010);
    send_config(0b00000110);
    send_config(0b00111000);
    send_config(0b00000110);
    send_config(0b00001100);
    send_config(0b00111000);

    while(1)
    {

password_count==0;

lcd_clr();
delay(1000);
lcd_goto(0);
send_string("AWAITING IMAGE");
lcd_goto(20);
send_string("VERIFICATION");
delay(900000);

lcd_clr();
lcd_goto(0);
send_string("PLEASE ENTER");
lcd_goto(20);
send_string("6-DIGIT PASSWORD");
delay(200000);

while(password_count<7){

clearrow1();
scancolumn1();
clearrow2();
scancolumn2();
clearrow3();
scancolumn3();
clearrow4();
scancolumn4();

if(password_count==6)
{
password_count=0;

{
    lcd_clr();
lcd_goto(0);
    send_string("ACCESS GRANTED !");
    led_yellow=1;
    relay=1;
    beep_once();
    delay(200000);
    relay=0;
    lcd_clr();
    break;
}
else
{
    lcd_clr();
lcd_goto(0);
send_string("INVALID PASSWORD !");
led_red=1;
beep_twice();
delay(200000);
lcd_clr();
break;
}

// scanning function

void clearrow1(void)
{
RE1=0;
RE0=1;
RA5=1;
RA4=1;
}

void clearrow2(void)
void clearrow3(void)
{
    RE1=1;
    RE0=1;
    RA5=0;
    RA4=1;
}

void clearrow4(void)
{
    RE1=1;
    RE0=1;
    RA5=0;
    RA4=1;
}
RA5=1;
RA4=0;

}

void scancolumn1(void)
{
if(RA0==0)
{
while(RA0==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('1');
keyin_char[password_count]='1';
password_count+=1;
}

else if(RA1==0)
{
while(RA1==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('2');
keyin_char[password_count]='2';
password_count+=1;
}

else if(RA2==0)
{
while(RA2==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('3');
keyin_char[password_count]='3';
password_count+=1;
}

else if(RA3==0)
{
while(RA3==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('A');
keyin_char[password_count]='A';
password_count+=1;
}
}
void scancolumn2(void)
{
    if(RA0==0)
    {
        while(RA0==0)continue;
        if(password_count==0)lcd_clr();
        lcd_goto(password_count);
        send_char('4');
        keyin_char[password_count]='4';
        password_count+=1;
    }
    else if(RA1==0)
    {
        while(RA1==0)continue;
        if(password_count==0)lcd_clr();
        lcd_goto(password_count);
        send_char('5');
        keyin_char[password_count]='5';
    }
password_count+=1;

}

else if(RA2==0)
{

while(RA2==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('6');
keyin_char[password_count]='6';
password_count+=1;

}

else if(RA3==0)
{

while(RA3==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('B');
keyin_char[password_count]='B';
password_count+=1;
void scancolumn3(void)
{
    if(RA0==0)
    {
        while(RA0==0)continue;
        if(password_count==0)lcd_clr();
        lcd_goto(password_count);
        send_char('7');
        keyin_char[password_count]='7';
        password_count+=1;
    }

    else if(RA1==0)
    {
        while(RA1==0)continue;
    }
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('8');
keyin_char[password_count]='8';
password_count+=1;
}

else if(RA2==0)
{

while(RA2==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('9');
keyin_char[password_count]='9';
password_count+=1;
}

else if(RA3==0)
{

while(RA3==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('C');
keyin_char[password_count]='C';
password_count+=1;
}

void scancolumn4(void)
{
if(RA0==0)
{
while(RA0==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('*');
keyin_char[password_count]='*';
password_count+=1;
}

else if(RA1==0)
while(RA1==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('0');
keyin_char[password_count]='0';
password_count+=1;

}

else if(RA2==0)
{

while(RA1==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('#');
keyin_char[password_count]='#';
password_count+=1;

}

else if(RA3==0)
{ 

while(RA3==0)continue;
if(password_count==0)lcd_clr();
lcd_goto(password_count);
send_char('D');
keyin_char[password_count]={'D';
password_count+=1;

}
}

// [General Purpose functions]

void delay (unsigned long data)
{

for( ;data>0;data-=1);
}

void beep_once(void)
{

buzzer=1;
delay(8000);}
void beep_twice(void)
{
    buzzer=1;
    delay(8000);
    buzzer=0;
    delay(13000);
    buzzer=1;
    delay(8000);
    buzzer=0;
}

// LCD functions

void send_config(unsigned char data)
{
    rs=0;
    lcd_data=data;
    delay(50);
e_pulse();
}

void send_char(unsigned char data)
{
    rs=1;
lcd_data=data;
delay(50);
e_pulse();
}

void e_pulse(void)
{
    e=1;
delay(50);
e=0;
delay(50);
}

void lcd_goto(unsigned char data)
{

if(data<16)
{
    send_config(0x80+data);
}

else
{
    data=data-20;
    send_config(0xc0+data);
}

}

void lcd_clr(void)
{
    send_config(0x01);
    delay(50);
}

void send_string(const char*s)
unsigned char i = 0;
while (s && *s) send_char(*s++);
}
APPENDICES