Palestine Polytechnic University
Collage of Administrative Science and Informatics
Department of Information Technology

OFFLINE HANDWRITTEN SIGNATURE VERIFICATION

Project team:

Asma Sokar Ibtihal hanini Rana Zahdeh

Supervisor:

Abdalfatah Najjar

A final project submitted in partial fulfillment of the Requirements' for the degree of B.Sc in Information Technology

June 2011

Abstract

The main idea of our project is to implement a high level of security personnel identification system using biometrics to create an identity database and to verify the identity of authorized persons. This project aims to use the methodology to verify the authenticity of the signature and the identity of the owner by using image processing techniques. In this project, suggests the main features of the form of the signature, and proposed as a case study, signatures of teachers and the staff of Palestine Polytechnic University.

Since human beings feel comfortable using pens and papers for authentication and authorization in legal transactions, this project presents a method for off line hand written signature verification system. So, it is very necessary to a person's hand written signature to be identified uniquely. The development of this efficient technique is to extract features from Handwritten Signature Image and verify the signature with high resolution. That computed feature is used for verification. Here we use SURF features in offline handwritten signature verification. For each known writer we take a sample of three genuine signatures and extract their SURF descriptors and key points from Handwritten.

On other hand we achieved from this system the verification of handwritten signature using SURF algorithm, finding the match between signatures for the same person, Extract features from signature to compare it between signature, and Determined who owns the signature.

Acknowledgements

We would like to thank everyone who helped us continue this project "***Offline Handwritten Signature Verification***" especially to our Supervisor " Mr Abdalfatah Najjar " for his valuable help and guidance,

We would like also to extend our thanks and gratitude to all teachers and employees at Palestine Polytechnic University, and we would like to send special thanks to everyone who presents any help to us.

Lastly, and most importantly, we wish to thank our parents, they raised us, supported us, and taught us during our whole life. . . .

Contents

3 OFF-LINE SIGNATURE VERIFICATION AND THE PROPOSED ALGORITHM

4 SYSTEM DISIGN

5 SYSTEM IMPLEMENTETION

6 TESTING

7 MAINTINANCE

8 Conclusions and Future Work

List of Figures

List of Tables

Abbreviations

Biometric	Bios metron
HSV	Handwritten Signature Verification
HMM	Hidden Marcov Model
IEEE	Institute of Electrical and Electronics Engineers
FRR	False Rejection Rate
FAR	False Acceptance Rate
FTE	Failure to Enrolle – Rate
ERR	Equal Error Rate
AER	Average Error Rate
SURF	Speeded Up Robust Features
SIFT	Scale Invariant Feature Transform
DB	DataBase
DFD	Data Flow Diagram

Chapter One

Introduction

Contents:

Chapter 1

Introduction

1.1 Overview

The world has witnessed in recent times a new revolution called the information revolution, where it was noted tremendous progress in technology in general and information technology, especially biotechnology, and found many of the techniques to make the world a small village to allow millions of people communicate with each other and exchange cultures, information and expertise and knowledge of various kinds until got Information Technology to behavioral biometrics. And applied in some institutions and large corporations. They also affect market trends in light of the economic openness that the world is witnessing.

The idea of this project is to implement a high level of security personnel identification system using biometrics to create an identity database and to verify the identity of authorized persons. This project aims to use the methodology to verify the authenticity of the signature and the identity of the owner by using image processing techniques. In this project, suggests the main features of the form of the signature, and proposed as a case study, signatures of teachers and the staff of Palestine Polytechnic University. Theses extracted features are used in this project to identify points of matching among the signatures, that have compound signatures into similarity groups based on features .

This help to verify the importance of features extracted in this project. The proposed methodology uses images of a compound signatures , then using image processing to pre-process the images of the signature to isolate the main signature from other parts of signature, and then to extract morphological features from signature image. After that to do the clustering process.

1.2 Biometric Systems in General

Biometric involves the automatic identification of an individual based on the physiological or behavioral characteristics. These physical characteristics are fingerprint, hand geometry, palm print, face, iris, retina, and ear. The behavioral characteristics are: signature, lip movement, speech, keystroke dynamics, gesture and gait. Figure 1.1 shows the classification of these characteristics.

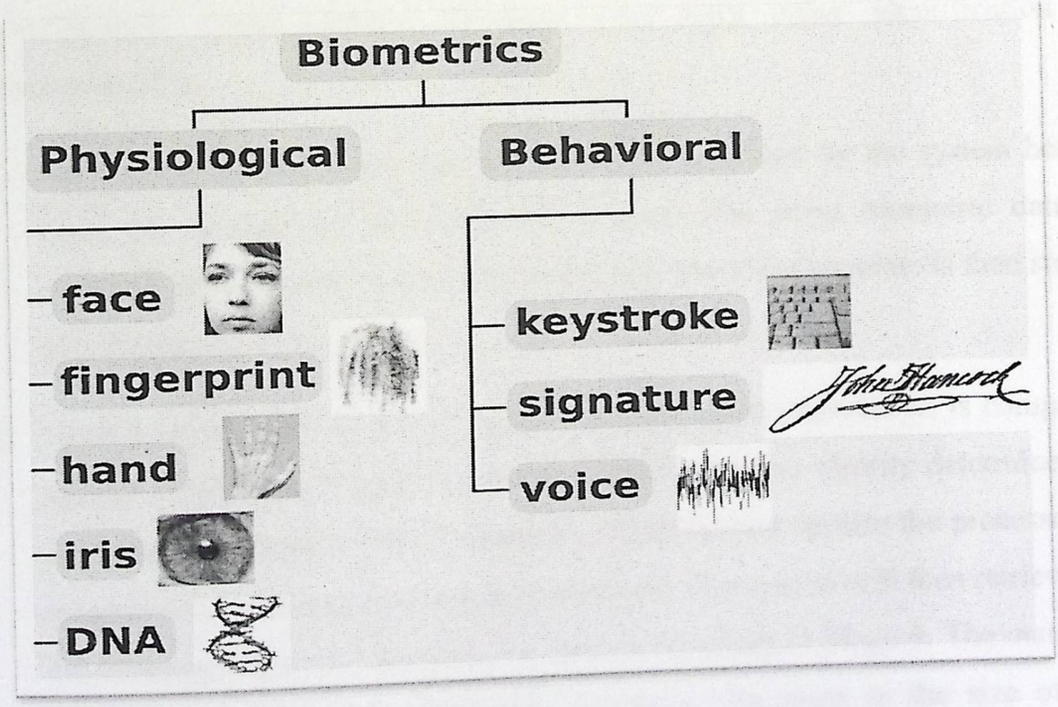


Figure 1.1: physiological or behavioral characteristics [1]

1.2.1 Biometric system Architecture

A biometric system is a system which can determine the authenticity of specific characteristics of a user [2]. Usually, a sensor is used to recognize personal characteristics such as iris, hand, face. Which are fed into the pattern recognition engine to return a result of success or failure. And in behavioral characteristics use algorithm to authentication and verification of person. In general, biometric systems consists of the following four stages: Data acquisition, Signal/Image preprocessing, Feature Extraction and Feature Matching.

1.2.2 Operation Mode of a Biometric System

A biometric system is usually operated in three modes: enrollment, identification and verification. Some systems, however, only have either identification or verification modes.

1. Enrollment- Before a user can be verified or identified by the system he/she must be enrolled by the biometric system. The users biometric data is captured, preprocessed and feature-extracted. The users template is then stored in a database of file system.

2. Identification - One-to-Many transaction: The users information is compared against a database of reference templates and the users identity determined as a match against one of these templates. Identification applies the processes of stages 1-3 to create an identification template. The system will then retrieve all the templates from the database for feature matching in Stage 4. The match is either successful or not. Generally, accuracy, decreases as the size of the database grows

3. Verification - One-to-One transaction: The user effectively claims an identity by providing some information which is typically used to call up a reference number from a database.

1.2.3 Biometric System Evaluation:

For the cost of each biometric system it depends on the accuracy we need for special applications Figure 1.2 shows the relation between the cost and the accuracy of the biometric systems. It is clear that in Handwritten Signature we can get high accuracy with low cost comparing to other biometrics methods. Statistical measures of biometrics can be used to decide which biometric system will best suit your needs. Not knowing the math behind a measurement should not impact one's ability to understand and compare the different statistical measures. The most important biometric statistical measures are:

- **FAR**: Measures the probability that an imposter will authenticate as a legitimate user.
- **FRR**: Measures the probability that a user who makes a legitimate claim about his/her identity will be falsely rejected.
- **FTE**: Measures the probability that an enrollment candidate will be unable to enroll in the biometric system.
- **ERR**: Measures the intrinsic strength of the biometric system and compares the strength of different biometric systems based on their EERs.

For each implementation, one or more of these biometric statistical measures can be important. To decide which ones are important, look at how the biometric system is going to be implemented, as well as how the user population is defined.

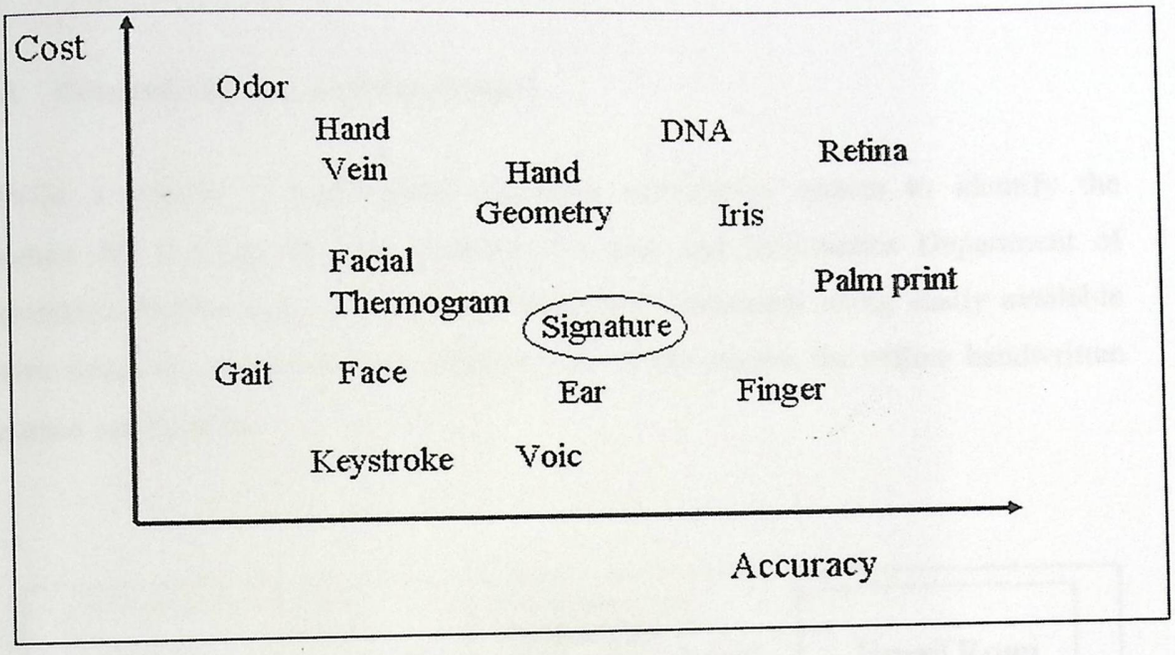


Figure 1.2: Cost and accuracy between biometric [3].

1.3 Problem statement

We are exposed to many situations in our lives may cause us to danger, such as forgery, which is considered as record the identity of the individual and the feature distinguishes it from other. That in all sectors of the economy of universities, banks and other more exposure to forgery handwritten signature. Check forgery case faced by many banks, and also forging the signature in organizations and universities.

Despite this eminent problem of signature forgery there is no economical and reliable automated handwritten signature verification system available to be used across all sectors of the economy to supplement human verification. So the target group in this project is the universities especially.

1.4 Project objectives

1.4.1 General Objectives of the Project

Build a project of handwritten signature verification system to identify the signature for Collage of Administrative Science and Informatics Department of Information Technology in Palestine Polytechnic University using easily available system resources and to find an efficient role of the system for offline handwritten signature verification.

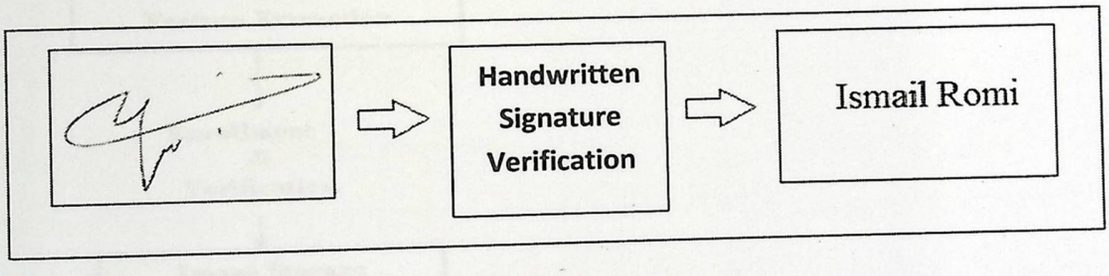


Figure1.3: signature verification

1.4.2 Specific Objectives of the Project

1. Using all the information we get from our study at the University by building a complete usable system in the IT field.
2. Concentrating some concepts in image processing course by apply some processing technique in a real project.
3. Collection of handwritten signature samples to be used as training and testing set.

4. Designing an Algorithm and implementation of signature feature extraction and pattern classification.
5. Testing the accuracy of the verifier.
6. Trying to apply the system on the Palestine Polytechnic University when its required in the registration department.

1.5 Project block diagram

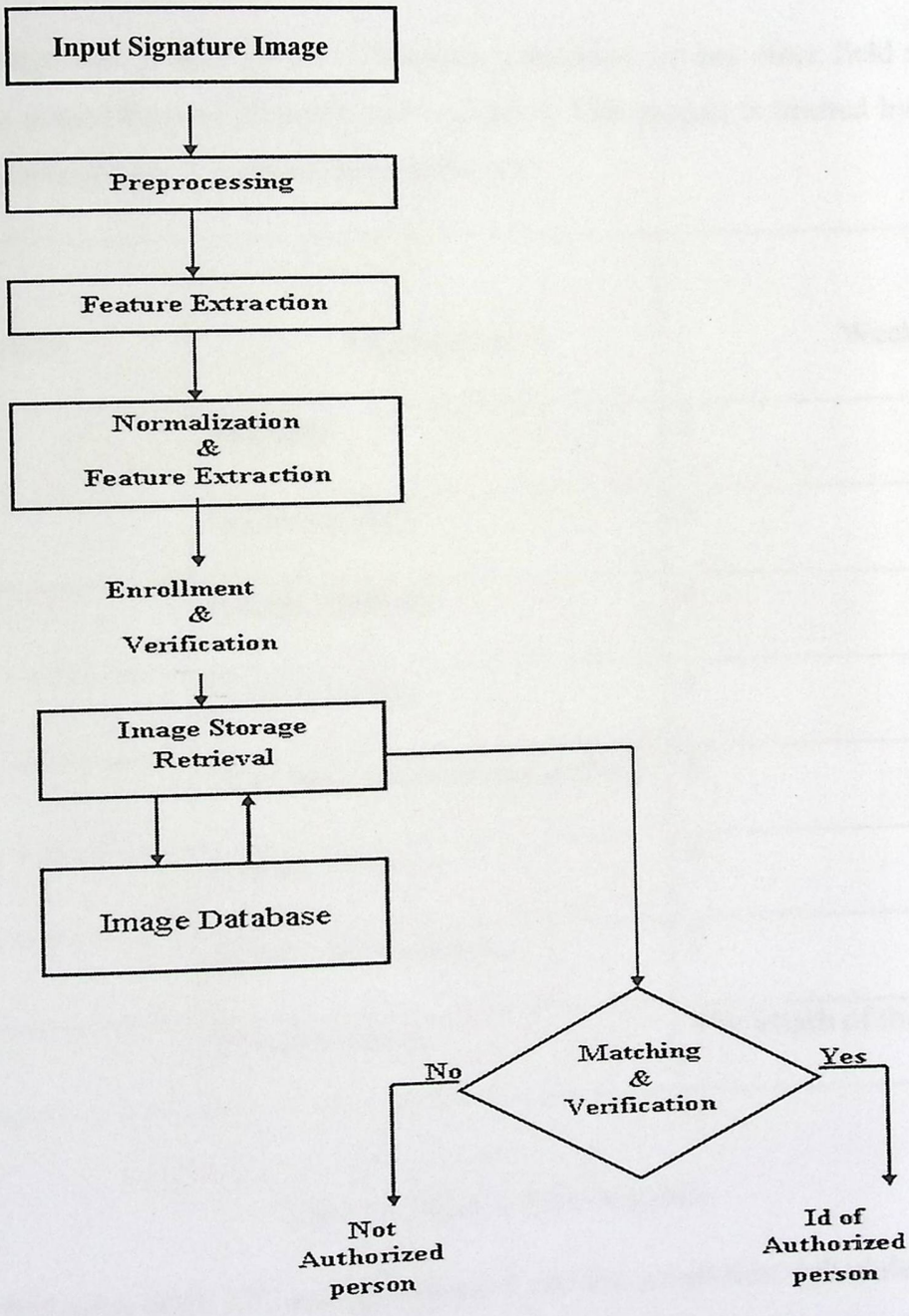


Figure 1.4: General steps of this project

1.6 Scheduling

Time Schedule:

As any project in any field it should be limited to specific time schedule. This project is limited to sixteenth weeks. Project team has managed this time as follow:

- **Project time planning**

Nowadays any project either in business, education, or any other field should be limited to a specific time schedule to be adapted. This project is limited by 16weeks so the following table 1.1 shows these activities.

Activities	Description	Weeks
Activity 1:	Planning	2
Activity 2:	Gathering Data	4
Activity 3:	System Analysis	4
Activity 4:	System Design	6
Activity 5:	Development and Programming	8
Activity 6:	System Testing	4
Activity 7:	System Maintenance	2
Activity 8:	Documentation	The length of the system life

Table 1.1: Time Activity Schedule

The following table 1.2 are the proposed and the actual time schedules needed to accomplish the project based on the" Gant Chart" which is considered as the strongest tool for planning and managing the time needed to order the required tasks .

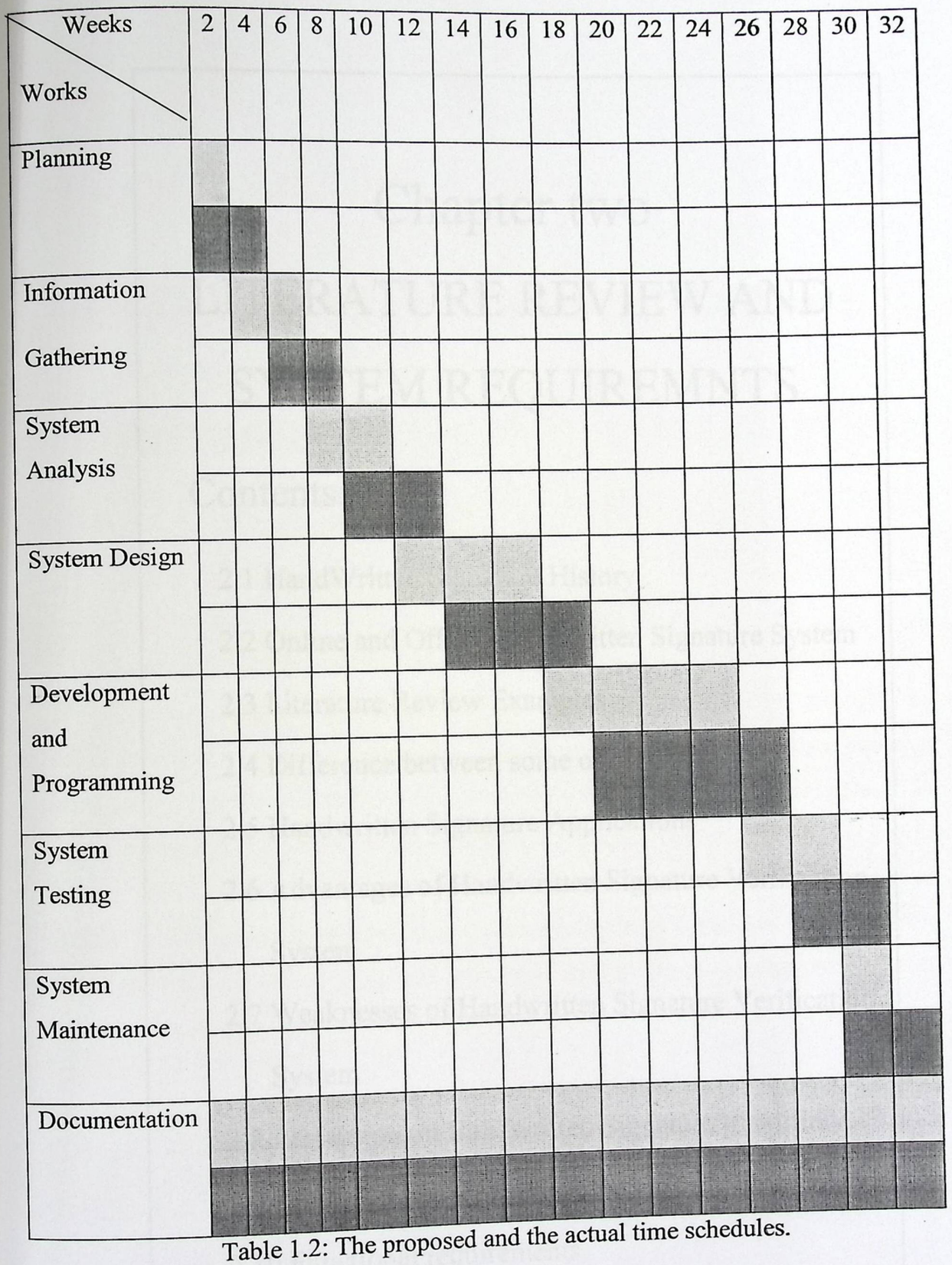


Table 1.2: The proposed and the actual time schedules.

: Expected Time. : Real Time.

Chapter two

LITERATURE REVIEW AND SYSTEM REQUIREMNTS

Contents:

Chapter 2

Literature review and system requirements

2.1 Handwritten Signature History

The importance of Signatures had come from the people's need to save their rights in contracts. Sign has appeared in concrete form significantly through the development of a draw or a particular form on a piece of pottery, leather, paper or manuscript. Signatures also have their own value and history in various cultures. In Japan, for instance, the masters often put their autographs (the so-called seals) on their works: such authors items were much more valuable than the ones manufactured at plants. In Europe masters used to put their handwritten signatures on the works. Scientists have connected signatures with hand writing and graphology which is the study and analysis of handwriting in relation to a person's psychology.

Figure 2.1: piece-of-pottery [4]

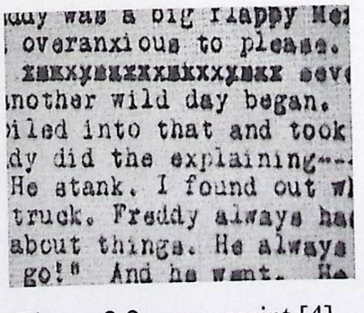


Figure 2.2: manuscript [4]

2.2 Online and Offline Handwritten Signature System

Signature verification is widely studied and discussed using two approaches. Online approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like; pressure, velocity, etc whereas in offline approach stable dynamic variations are not used for verification purpose as in Figure 2.3.

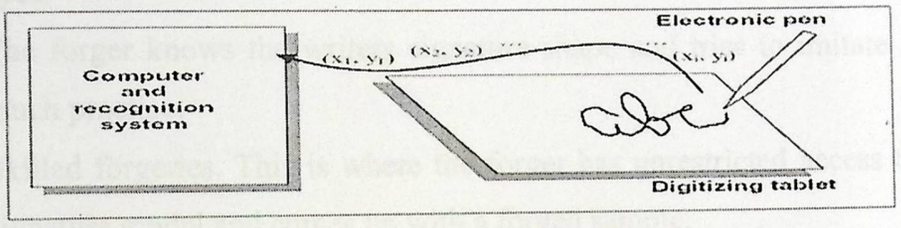


Figure 2.3: Online Signature verification [5].

Offline systems are more applicable and easy to use in comparison with on-line systems in many parts of the world however it is considered more difficult than online verification due to the lack of dynamic information where the input is a static image that is scanned and used for analysis as in Figure 2.4.

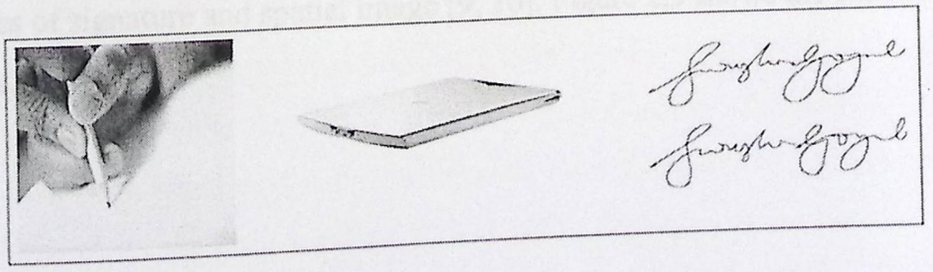


Figure 2.4: Offline Signature verification [6].

2.2.1 Forgeries Types

Both offline and online systems are used to detect various types of forgeries. Signature forgeries are classified as follows [7, 8]:

1. Develop a self-contained system which consists of modules for enrollment of a user, preprocessing the signatures, and comparing.
2. The forger doesn't have the shape of the writer signature but comes up with a scribble of his own. He may derive this from the writers name. This forgery accounts for majority of forgery cases though it's easy to detect with naked eyes.
3. The forger knows the writers signature shape and tries to imitate it without much practice.
4. Skilled forgeries. This is where the forger has unrestricted access to genuine signature model and comes up with a forged sample.

The skilled forgery category has been classified further into amateur and professional forgery. Professional expertise in handwriting analysis has ability to forgery the signature with high quality. The professional forgeries are sub categorized in the context of online verification into home improved and over the shoulder forgeries. Home-improved is when the forger has a paper copy of the signature and has time to practice at home. The imitation is based on static features of the image. Excessive in forgeries shoulder forgeries are produced when immediately the forger has witnessed the writer make a genuine signature, the forger in this case has dynamic properties of signature and spatial image [9, 10]. Figure 2.5 shows the classification of forgeries.

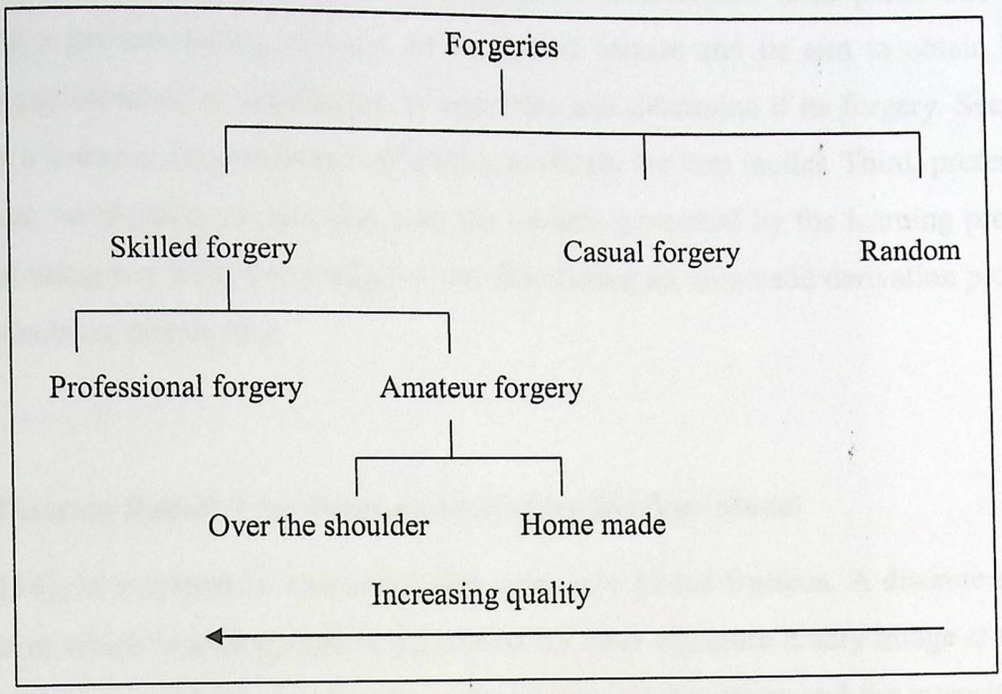


Figure 2.5: Forgery classification [11].

2.3 Literature Review Examples

Handwritten signatures are widely accepted as a means of document authentication, authorization and personal verification. For legality most documents like bank checks, travel passports and academic certificates need to have authorized handwritten signatures. In modern society where fraud is rampant, there is the need for an automatic HSV (Handwritten signature verification) system to complement visual verification.

Many researchers have been pursued in handwriting analysis and pattern matching for a number of years. In the area of HSV, especially offline HSV, different technologies have been used and still the area is being explored. In this section we review some of the recent papers on offline HSV. The approaches used by different researchers differ in the type of features extracted, the training method, the classification and verification model used. The categorization for these approaches done here is influenced by classification used in [12].

2.3.1 HMM and Graphometric features

The approach of Justino [13], It is based on divided into three parts. The first describe a pre-processing process, its to extract feature and its aim to obtain high quality performance to verification of signature and determine if its forgery. Second, display a learning process based on HMM, to obtain the best model. Third, presents a signature verification process that uses the models generated by the learning process without using any prior knowledge of test data (using an automatic derivation process of the decision thresholds).

2.3.2 Discrete Radon Transform and a Hidden Markov Model

In [14], Is a system is introduced that uses only global features. A discrete radon transform which is a sinograph is calculated for each signature binary image at range of 0-360 degree , which is a function of total pixel in the image and the intensity per given pixel calculated using non overlapping beams per angle for X number of angles. Due to this periodicity, it is shift, rotation and scale invariant. A HMM is used to model each writer signature. The method achieves an AER (Average Error Rate) of 18.4% for a set of 440 genuine signatures from 32 writers with 132 skilled forgeries.

2.3.3 Signature Verification Incorporating the Prior Model

In [15], transform the primary classifier via the mapping learnt in the training stage to obtain the final classifier, that's pass in two stages , the first stage the training stage the system learns the mapping between the parameters of classifiers without simple forgeries and those with simple forgeries. Second stage, In the application stage, a primary classifier is trained for a new user without his or her simple forgeries.

The final classifier is obtained by transforming the primary classifier via the mapping learnt in the training stage.

2.3.4 Image Invariants and Dynamic feature

In [16], proposed development of automatic signature classification system. Presented offline and online signature verification system based on dynamic features and the signature invariants. Based on perceptually important points and for each segment extract feature by scale, rotation and displacement invariant. While the speed of pen is used as a dynamic feature of the signature.

2.3.5 Fixed Point Arithmetic

In [17] presents a set of geometric signature features for offline automatic signature verification based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates. The features have been calculated using 16 bits fixed-point arithmetic and tested with different classifiers, such as hidden Markov models, support vector machines, and Euclidean distance classifier. The experiments have shown promising results in the task of discriminating random and simple forgeries.

2.3.6 Shape Descriptor and Multiple Neural Networks

In [18], global features of the signature like the skeleton of the pen trace and the structure of upper and lower envelope are used as shape descriptors. These are obtained by sampling upper and external points from the binary image of the signature.

High pressure regions where the writer made more pressure or emphasis to is generated to a linear function that is be used for maximizing the correlation between the vertical and horizontal projections of the skeleton. For each of the above shape descriptors a multi- layer perception is assigned and the network is trained with a modified back propagation algorithm and the output of each individual network is combined through a fuzzy integral voter. Using a test set of 1000 signatures the approach obtained 90% true verification.

2.4 Comparison between some of methods

Method	FAR	FRR	DataBase
HMM and Graphometric features	0.001%.	9.8%	30 signatures
Discrete Radon Transform and a Hidden Markov Model	1.44%, random, 2.50%, casual,and 22.67% skilled forgeries	2.83%	The first data set contains the signatures of 40 writers with 40 genuine signatures per writer The second data set contains the signatures of 60 writers with 40 training signatures, 10 genuine test signatures, 10 casual forgeries, and 10 skilled forgeries per writer
Shape Descriptor and Multiple Neural Networks	98%, genuine, 96%, simple forgeries, and 90.4% are skilled forgeries		contains data from 1000 signature for 50 person

Table 2.1: Difference between some of methods.

2.5 Handwritten Signature Applications

There are many applications of handwritten signature in our life:

1. In Banks : Offline signature verification has a significant use mainly in establishing the authenticity of bank checks and other official documents, Security system, certificate, contracts, based on the signatures they carry. For instance, thousands of checks are being processed in a day in most banks or

insurance companies; hence there is a great need for the automation of this process.

2. Check authentication.
3. Forensic applications.
4. Signatures inform our study of history. For example, they can be a personal affirmation that an event occurred (e.g., a marriage), a law was put into effect, or a transaction took place.
5. Signing a document can create a feeling of ownership and pride.

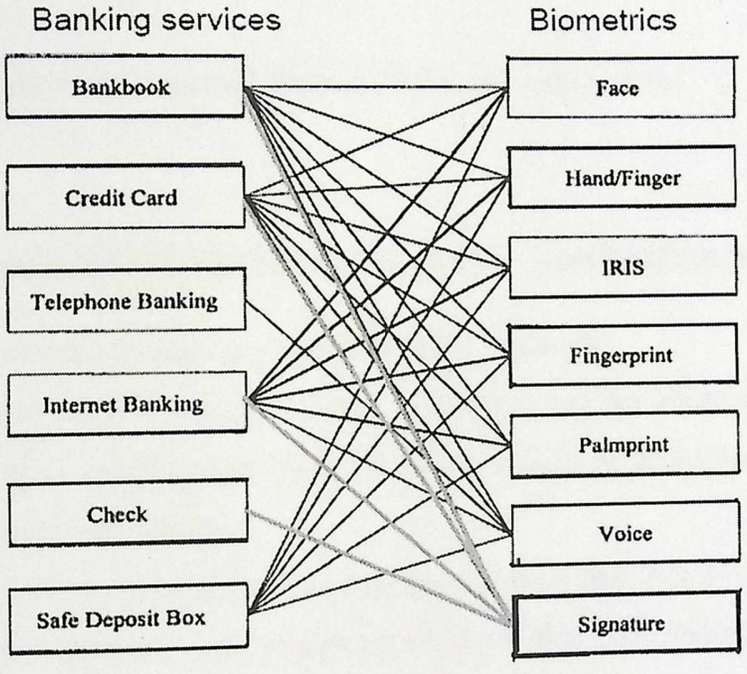


Figure2.6: Handwritten Signature Application examples [19].

2.6 Advantages of Handwritten Signature Verification System

In spite of being natural and intuitive this technology however has certain advantages.

1. Signature verification Natural and intuitive: it is easy to be explained and trusted. The primary advantage that signature verification systems have over other types of biometric technologies is that signatures are already accepted as the common method of identity verification.

2. Well accepted socially and legally. Widely accepted form of identification throughout our history.
3. Require minimal extra hardware.
4. Already acquired in a number of applications.
5. The signature is the most natural and generally established of all the ways in which we seek to confirm our identity.
6. The use of signature verification will minimize the disruption of accepted practices with respect to transactions where personal identity has to be authenticated.
7. When combined with the pen speed, timing, and pressure, it is very difficult to imitate.
8. Measurements of signature characteristics are noninvasive.

2.7 Weaknesses of Handwritten Signature Verification System

1. There are some inconsistencies to a person signature.
2. High intra-class variability, Great variability can be observed in signature according to country, age, time, habits, physiological or mental state, physical and practical conditions.
3. As a result, individuals with muscular illnesses and people who sometimes sign with only their initials might result in a higher False Rejection Rate,
4. Forgeries.

2.8 Perception on Handwritten Signature Identifier

Eight factors affect the determination of a biometric identifier in a particular application: Accuracy, Usability, Smallness, Spoof Proof, Speed, Privacy, Low Cost and Universality [20].

These factors can influence the selection of a biometric system, and coparasion between other. In figure 2.5 displays and summarize.

2.9 Functional requirements

Image	read the input image
Add selected image to database	The input image is added to database and will be used for training.
Database Information	Show information's about the images present in database.
Signature Recognition	Signature matching. The selected input image is processed
Delete Database	remove database from the current directory
Information	show information about this software
Source code Signature Recognition System	how to obtain the complete source code
Exit	quit program

Table 2.2: Describe the Functional requirements

2.10 Non functional requirement

In addition to the Accuracy, usability, accuracy, spoof proof, speed, privacy, and low cost there are some elements of nonfunctional requirements:

- **Distinctiveness:** each relevant person should have only one identifier and no two people should have the same identifier.
- **Performance:** the identifier should not change, nor be changeable, most signatures contain enough steady features to be reliably verified but doesn't achieve a high consistency. Simple for recording and transmission should be easy and not error-prone, cost effective by measuring and storing the identifier should not be unreasonably costly within the context of the application and associated risk.
- **Collectability:** the identifier should be collectible by anyone on any occasion.
- **Acceptability:** its use should conform to contemporary social standards , signature achieve high acceptable , storable so the identifier should capable of being stored.
- **Circumvention:** (exclusive) no other form of identification should be necessary or used.

2.11 Feasibility study:

The following will describes in details the system economic feasibility for all of the system recourses.

2.11.1 System recourses cost:

1. hardware costs:

The following tables list the costs for the hardware recourses required to develop this project:

Element	Unit cost
Computer (Dell Dual-core CPU 2.2GH RAM 3GB)	600$
Printer(laser jet M 1005 3 in 1)	400$
Flash memory(4GB)	10$
Canon Cano Scan LiDE 600F (4800 x 9600dpi*, 48 bit color depth)	99$
Total	1109$

Table 2.3: system hardware cost

2. software costs:

The following table lists the costs for the software recourses required to developed this project:

Element	Unit cost
Microsoft windows	200$
Microsoft office professional 2007	150$
Total	350$

Table 2.4: system software cost

3. Another cost:

There is 50$ is needed to cover another things (travels, papers, printing and pens….etc)

Total system development cost:

Resources	Costs
Costs of physical resources development	1109$
Costs of programming resources development	470$
Costs of other resources	50$
Total	1692$

Table 2.5: Total system development cost

2.11.2 Operational system cost:

1. Hardware costs

The following table lists the costs for the hardware recourses required to operate this project:

Element	Unit cost
Computer	600$
Canon Cano Scan LiDE 600F (4800 x 9600dpi*, 48 bit color depth)	99$
Total	699$

Table 2.6: Operational Hardware cost

2. Software cost:

The following table list the costs for the software recourses required to operate this project :

Element	License cost
Microsoft windows	200$
Microsoft Office professional 2007	150$
Total	350$

Table 2.7: Operational software cost

Total system operational cost:

This table shows total cost of physical resources operation and programming resources operating.

Resource	Cost
Costs of physical resources operation	699$
Costs of programming resources operating	200$
Total	899$

Table 2.8: Total system operational cost

Chapter Three

Off-Line Signature Verification

Contents:

inspection) will examine only a small portion of signatures classified into the third class of uncertain signatures.

3.2.1 Features of the handwritten signature

This section introduces features as a general, the general morphological features of handwritten signature.

3.2.1.1 The features

Features are defined as points represent images in multidimensional feature space which are used to compute the similarity between the images. The images are similar to each other when the images are close to each other in high dimensional space.

Feature extraction can be defined as the process of mapping image from its original space. Some of the methods to extract features are better than other methods in accuracy and time of computation process [22].

Some approaches of features extraction can produce the following features:

1. Uniqueness: images are different to awareness of human have the different features.
2. Invariance: images are similar to awareness of human have the similar features.
3. Stability: the degree of similarity between two images that leads to small degree of similarity in matching features.
4. Efficiency: the feature should be with small size without losing characteristics.
5. Ease of implementation: the feature extraction should be with efficient consecutively.

3.2.1.2 General Handwritten signature features:

In this stage feature Extraction are used for verification stage. Features will have to be extract from both sample images and Test image. Four new Feature Extraction procedures for signature image verification are introduced here.

1- Global features:

Width, Height, Duration, Orientation

2- Local features:

X-coordinates, Y-coordinates, Curvature

3- Dynamic features:

Velocity, Acceleration, Pressure, Pressure changing

4- Other features:

Number of segments, Critical points, etc

3.2.2 Basic Procedure for Offline Handwritten Signature Verification:

1. Preprocessing the Raw data - Make signature fixed to resize and rotation
2. Template generation from given signature. - The generated template include:
    a) What kinds of feature are chosen?
    b) The features.
    c) Distance measures.
    d) The threshold for decision.
3. Verification according to the template.
    a) Preprocess the raw data of the given signature.
    b) Extract features and compare distances with those in the template.
    c) Make decision according to the threshold specified in the template.

During enrollment, user supplies a number of reference signatures which are used by a profile generator to create a profile on the system for that user. Profile contains the reference signatures and similarity values. Similarity between two signatures is calculated using the dynamic programming algorithm. Similarities among all reference signatures are further transformed to calculate similarity scores (distances) which describe variations within reference signatures. Verification engine is responsible for the verification of a given test signature, based on the dissimilarity between the test and the reference set signatures.

Verification engine is used to authenticate a given (test) signature against the claimed ID. Firstly, reference set signatures and similarity values corresponding to the claimed ID, are retrieved from the system's database. Then, using dynamic programming algorithm, the test signature is compared with each reference set signature. Comparison results in a number of dissimilarity values (distances), which further normalized and presented to a classified as a feature vector. We have experimented with a linear classifier used in conjunction with Principal Component Analysis, to classify a test signature as genuine or forgery.

3.3 Algorithm

3.3.1 Introduction

For any object there are many features such as interesting points on the object, which can be extracted to provide a feature description of the object. This description can then be used when attempting to locate the object in an image containing many other objects. There are many considerations when extracting these features and how to record them. SURF image features provide a set of features of an object that are not affected by many of the complications experienced in other methods, While allowing for an object to be recognized in a larger image, SURF image features allow for objects in multiple images of the same location, taken from different positions within the environment to be recognized. SURF features are also very resilient to the effects of noise in the image.

This project deals with verifying the offline signature. Many method are currently available for verifying the offline signature. We have come out with an approach, using the SURF algorithm which create an image pyramid, filter the pyramids suitable for the detection of interesting points, select feature , then compare with another image features to find matches.

In this project the SURF features will be considered. The implementation will be done in VB.NET(2010) and using the Emgucv-windows-x86 library.

3.2.2 Speeded Up Robust Features (SURF) algorithm

The algorithm that computes SURF, contain of two basic steps- interest point detection and interest point description- both takes several steps.

In the interest point detection step, first integrated the image. The output of the integration, same of the integral image, is used as the basis of the subsequence scale-space analysis. The responses obtained from the scale-space analysis are used to localize the interest points. In the interest point description step, the localized interest point are assigned orientations and then have their feature described.

This work-flow is shown in figure:

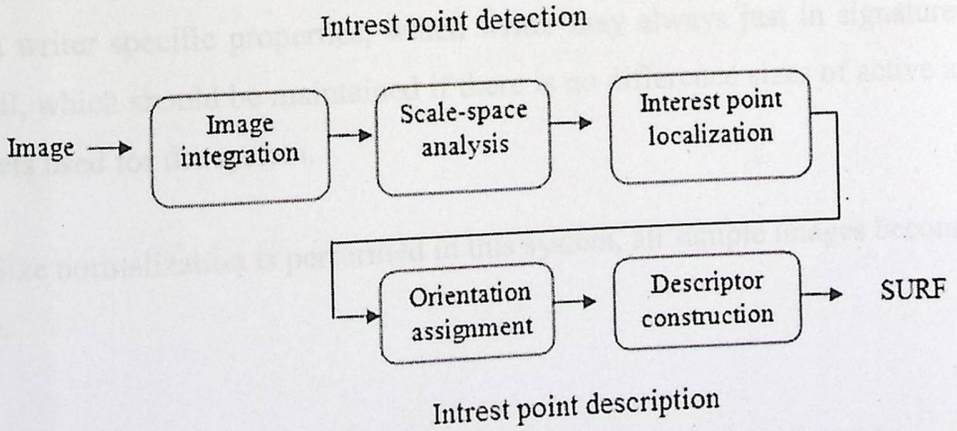


Figure 3.2: the work-flow of the algorithm computing SURF [23].

3.4 Preprocessing

Any ordinary scanner with enough resolution can be used as an image acquisition device. Scanning hardware may introduce noise to a signature image. Another source of noise may be speckled paper background on which the signature is signed. Noise on a signature image may thwart feature extraction process; hence it needs to be removed. However preprocessing methods should be selected carefully as they may remove signature properties peculiar to a signer.

3.4.1 Normalization

In this project the user have to sign on tablets with deferent active regions, and normalization for signature size will be required. In usual persons scale their signatures to Compatible with area available for the signature. Nevertheless difference in size between the two signatures been comparable may be a problem. In general, signatures are normalized with regard to each of width and height, but the measurement does not have always solution to the problem since the signing may be a different aspect ratio. Instead, you can normalize the size of the signature, according to one of the dimensions (width or height) that does not remove the entirely the size of distinctive writer. It also known as that the people do not scale their signatures on an equal footing as regard to the width and height, and considered the size of signature to be a writer specific properties, which writer may always just in signatures, large or small, which should be maintained if there is no difference sizes of active areas of the tablets used for the system.

Size normalization is performed in this system, all sample images become the same size.

3.5 Feature Extraction

- **Interest Point Based Feature Extraction:** Interest points need to be found at different scales, where scale spaces are often implemented as an image pyramid. The pyramid levels are obtained by Gaussian smoothing and sub-sampling.

  For reducing image size, in SURF the scale space is rather analyzed by up-scaling the integral image based filter sizes in combination with a fast Hessian matrix based approach. As the processing time of the filters used in SURF is size invariant, it allows for simultaneous processing and negates the need to subsample the image hence providing performance increase.

- **Grid-Based Feature Extraction:** Usually, a main drawback of an interest point based feature extraction is the large number of false positive detections. This drawback can be overcome by the use of hypothesis rejection methods.

- **Local Feature Descriptors:** generally, to describe each pixel or position (local feature descriptors) in an image through its local content .

  They are supposed to be robust to small deformations or localization errors, and give us a possibility of finding the corresponding pixel locations in images which capture the same amount of information about the spatial intensity patterns under different conditions.

In this system we will use Interest Point and detect feature of signature to verify it.

Speeded Up Robust Features (SURF) the 64-dimensional SURF descriptor are similar to SIFT descriptor, and when the interest point neighborhood SURF descriptor focuses on the spatial distribution of gradient information, by interest point detection approaches or in a regular grid the interest points itself can be localized.

The SURF descriptor is invariant to scale, rotation, brightness, and after reduction to unit length, contrast.

3.6 Verification

Verification is the process of testing whether a claimed signature is of the same (class) writer as the set of signatures enrolled in the system for that class. Verification involved loading the template Visual Studio 2010 file enrolled in the system and comparing its stored parameters with those calculated by the outlier detection process.

Chapter Four

System Design

Contents:

Chapter 4

System Design

4.1 Introduction

In this chapter we will explain the graphic content system that demonstrates relationship of system in environment , data flow diagram in the system, usecase of system, Flowchart of approach, design functions of the system (explain each function from system functions), design screens (design the screen that allow of user interact with system) and test plan (stages that the system will pass it during the test phase).

4.2 Graphic Context diagram

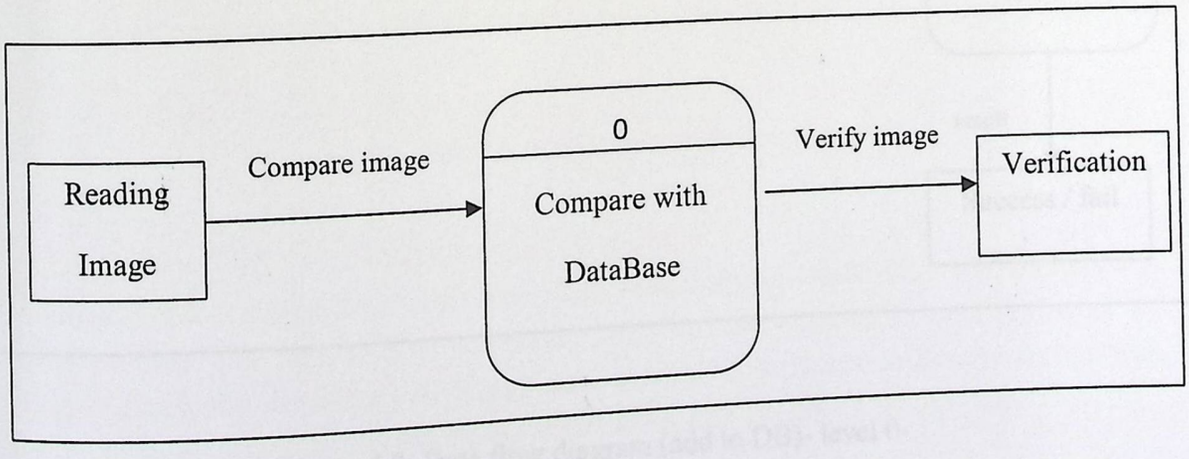


Figure 4.1: Context diagram of the system

In figure 4.1 show Graphic Content System , Shows the system and its relationship with the environment. Start , the user put the paper containing the signature in the scanner , then the system use image processing to extract signature, and finally displayed the result on the screen.

4.3 Data flow diagram in the system

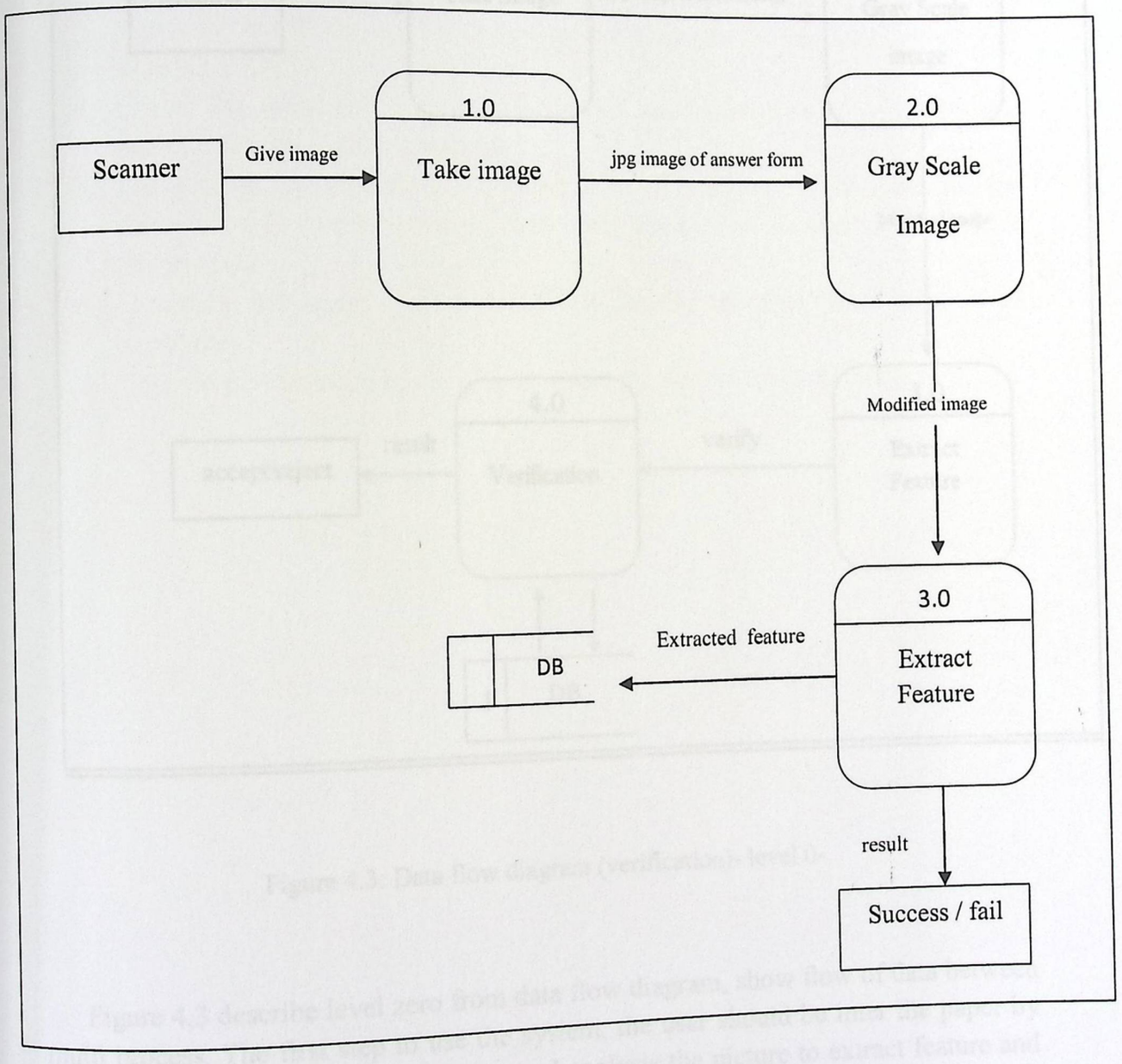


Figure 4.2: Data flow diagram (add to DB)- level 0-

Figure 4.2 describe level zero from data flow diagram , show flow of data between multi process. The first step to use the system, the user should be interring the paper by scanner, and use the binary of image and analysis the picture.

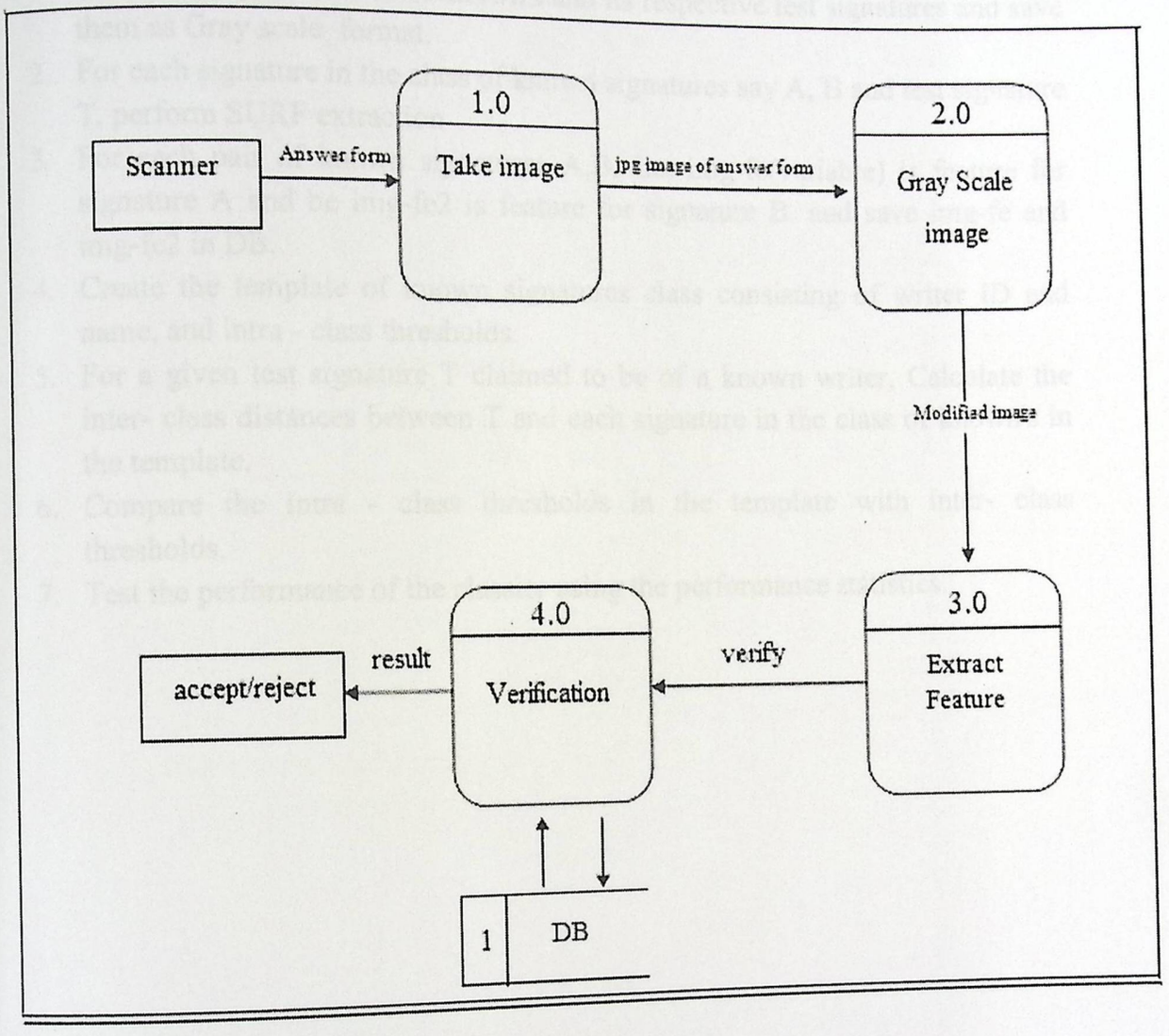


Figure 4.3: Data flow diagram (verification)- level 0-

Figure 4.3 describe level zero from data flow diagram, show flow of data between multi process. The first step to use the system, the user should be inter the paper by scanner , and use the binary of image and analysis the picture to extract feature and verification by match with feature in the database and finally show the result.

4.4 Pseudocode Steps

1. Given the set of known signatures and test signatures signed in a document, scan and crop each class of known's and its respective test signatures and save them as Gray scale format.
2. For each signature in the class of known signatures say A, B and test signature T, perform SURF extraction
3. For each pair of known signatures A,B, Let img-fe(variable) is feature for signature A and be img-fe2 is feature for signature B. and save img-fe and img-fe2 in DB.
4. Create the template of known signatures class consisting of writer ID and name, and intra - class thresholds.
5. For a given test signature T claimed to be of a known writer, Calculate the inter- class distances between T and each signature in the class of known's in the template.
6. Compare the intra - class thresholds in the template with inter- class thresholds.
7. Test the performance of the classier using the performance statistics.

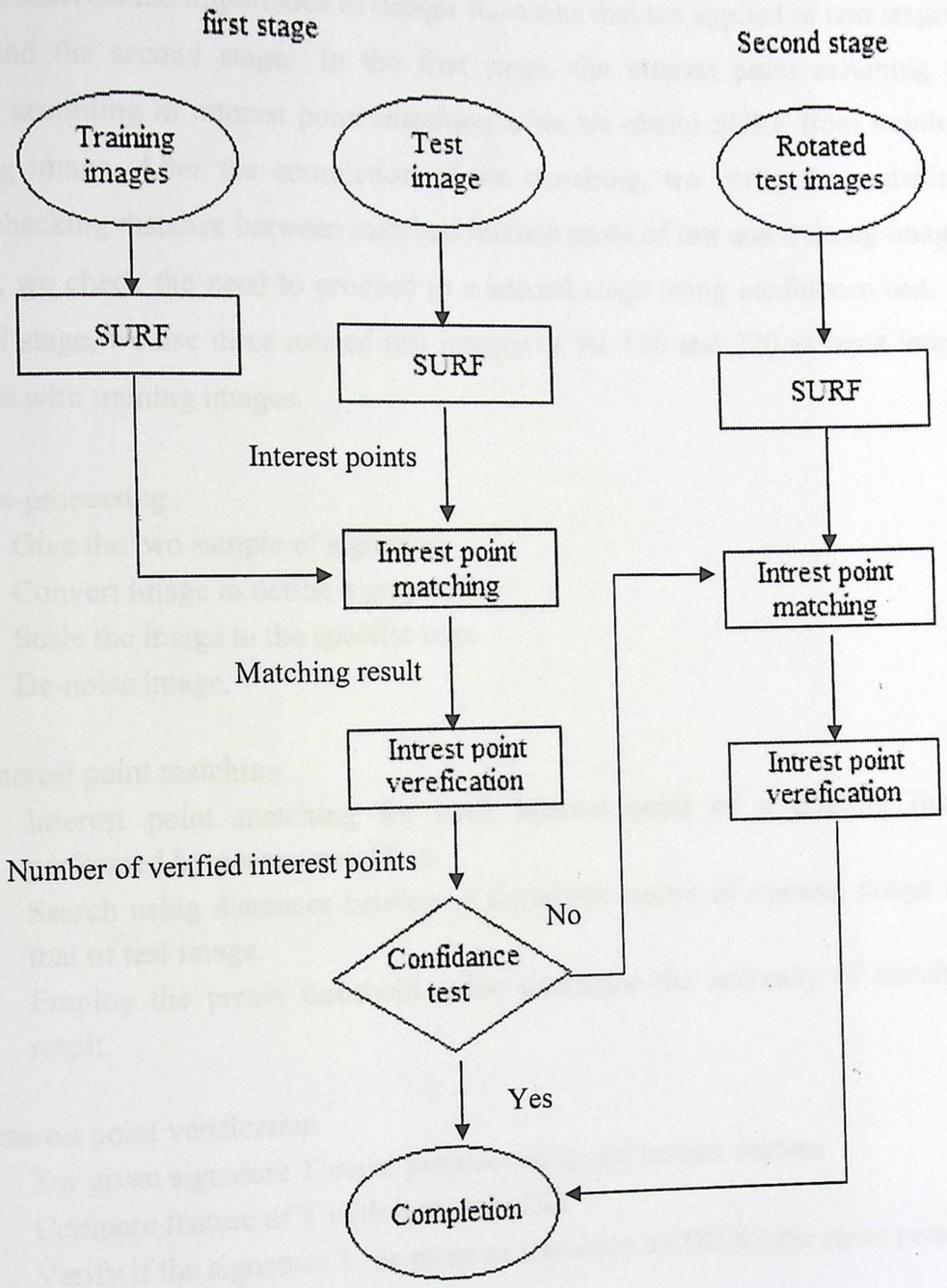


Figure 4.4: Flow chart of the system

4.5 Design functions of the system

We will describe the importance of design functions that are applied in two stages, the first and the second stage. In the first stage, the interest point matching is performed according in interest point matching .after we obtain SURF from training and testing image. After the completion of the matching, we verify the matching result by checking distance between matched interest point of test and training image. After that, we check the need to proceed to a second stage using confidence test. In the second stage, we use three rotated test images of 90, 180 and 270 as input image to compare with training images.

1. Pre-processing
   - Give the two sample of signature.
   - Convert image to define a gray color.
   - Scale the image to the specific size.
   - De-noise image.

2. Interest point matching
   - Interest point matching for each interest point of a training image performed by nearest neighbor.
   - Search using distances between a descriptor vector of training image and that of test image.
   - Employ the preset threshold value guarantee the accuracy of matching result.

3. Interest point verification
   - For given signature T make preprocessing and extract feature.
   - Compare feature of T with feature in DB.
   - Verify if the signature T the same as signature on DB for the same person
   - Show result exist or not exist

4.6 Design screens

4.6.1 Main screen

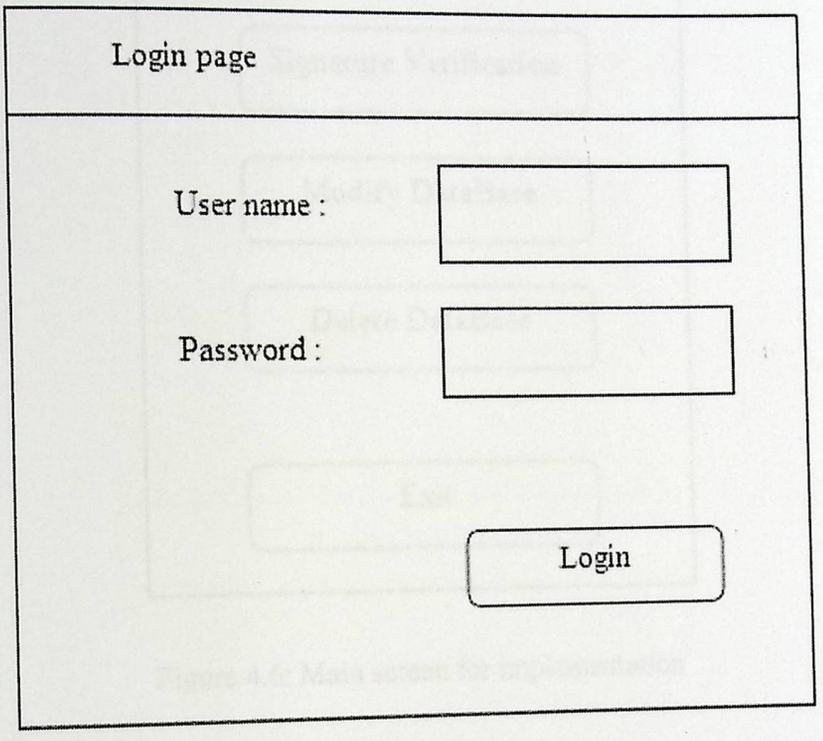


Figure 4.5: Main screen for Login

This page allows the administrator to access to the system to be able to do his own operations and the exercise his permissions.

4.6.3 Screen for add to DataBase

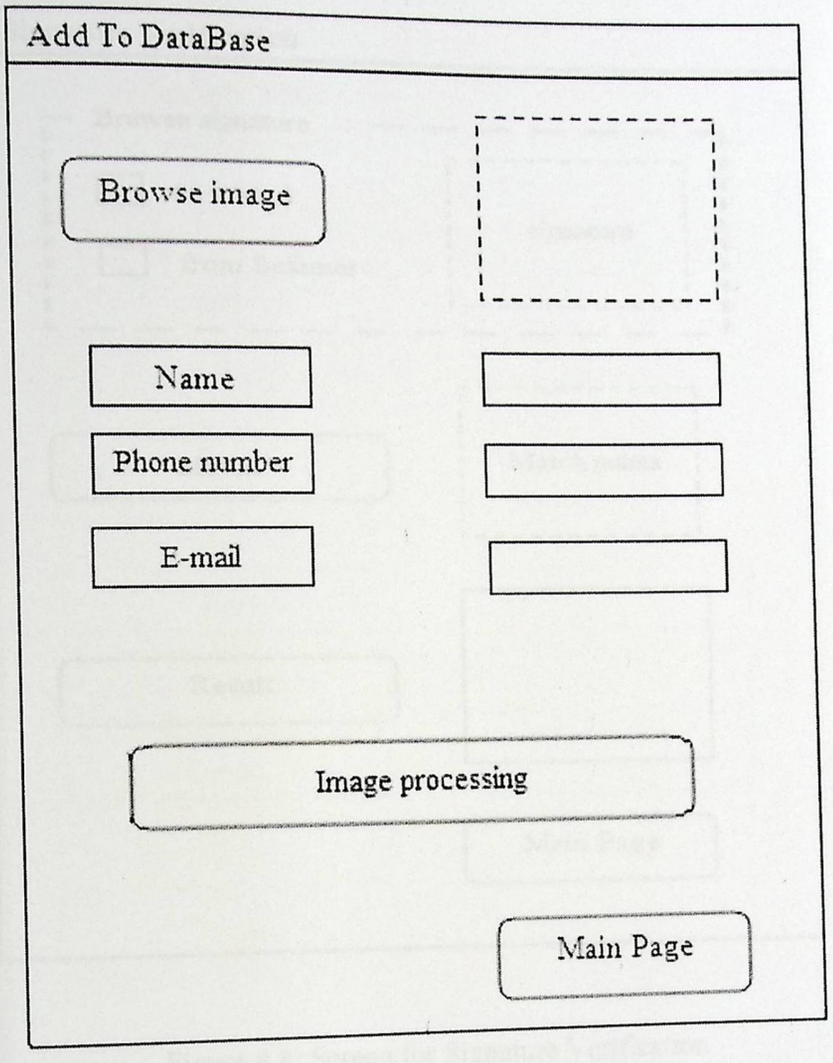


Figure 4.7: Screen to add signature in DB

Figure 4.7 Show the main step to create signature in DB that include:

1. Buttons (Browse Image, Image Process, Add to DataBase and Main Page) ,
2. PictureBox received image of signature.
3. TextBox until enter data about who owns signature (Name, Phone Number and E-mail).

4.6.5 Modify on DataBase

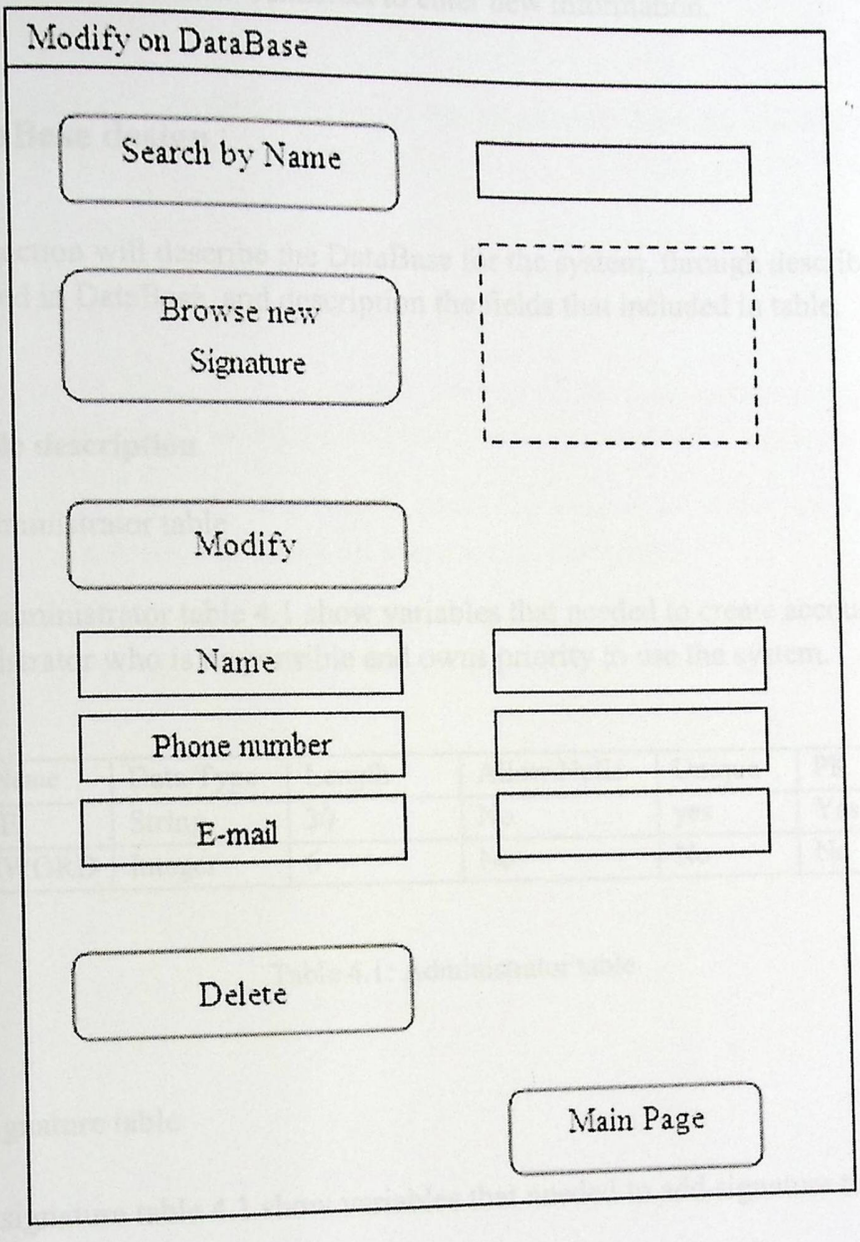


Figure 4.9: Modify on DataBase

Figure 4.9 Show the main step to search, modify and delete signature in database that include:

1. Buttons (Search by name, Browse new signature, Modify , Delete and Main Page) .
2. PictureBox to Browse new signature

3. TextBox to search about name enter name on TextBox and click on Search. And other TextBoxs to enter new information.

4.7 DataBase design

In this section will describe the DataBase for the system, through describe the table that included in DataBase, and description the fields that included in table.

4.7.1 Table description

1. Administrator table

In administrator table 4.1 show variables that needed to create account for administrator who is responsible and owns priority to use the system.

Field Name	Data Type	Length	Allow Nulls	Unique	PK
NAME	String	30	No	yes	Yes
PASSWORD	Integer	6	No	No	No

Table 4.1: Administrator table

2. Signature table

In signature table 4.1 show variables that needed to add signature to DataBase

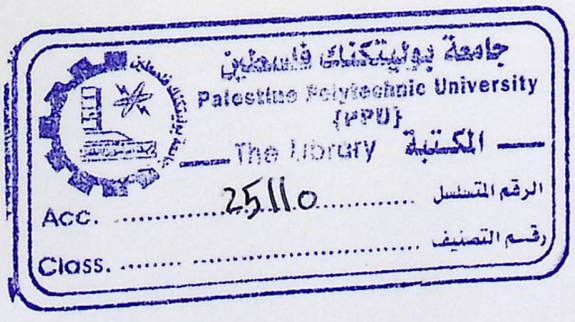
Field Name	Data Type	Length	Allow Nulls	Unique	PK
ID	Integer	6	No	Yes	Yes
NAME	String	50	Yes	No	No
Phoneno	integer	10	Yes	yes	No
Email	string	30	Yes	Yes	No
IMG	Image	16	Yes	No	No
IMG_FE	Image	16	Yes	No	No

Table 4.2: signature table

4.8 Test plan

Will be displayed on a plan to examine the system and this plan include unit testing integration testing and system testing.

1. Unit testing: here is check every unit that is exist separately from other units and these units are examined to validate the system and is free of any problems during the operation process.
2. Integration Testing: here is check integration between system component that is through check interact between system component and system screens.
3. System Testing: in this system check the system as single unit until sure it work correctly, and check all operation of the system.
4. Accept Testing: after check the all system units that work in an integrated and compatible, then checking the acceptable of the system from the user.



Chapter Five

Implementation System

Contents:

Chapter 5

System Implementation

5.1 Introduction

Application stage is an important stage in the development of the system, which is where the transition from the conceptual stage of the analysis and design of the system to the practical stage in which they are preparing resources and equipment to carry out crisis programming system and its construction as a whole. In this chapter will clarify the sources and reactions of equipment and software crisis for the application of the system and building the database.

5.2 Source code for the development of the system

In this part of code is the preparation of equipment and all the programs that we need through process system development and of the operating system

1. Microsoft windows 7 ultimate
2. Microsoft office 2007
3. Microsoft Visual Studio.Net 2010
4. VB.NET
5. SQL Server 2008
6. EmgU library

Chapter 5

System Implementation

5.1 Introduction

Application stage is an important stage in the development of the system, which is where the transition from the conceptual stage of the analysis and design of the system to the practical stage in which they are preparing resources and equipment to carry out crisis programming system and its construction as a whole. In this chapter will clarify the sources and reactions of equipment and software crisis for the application of the system and building the database.

5.2 Source code for the development of the system

In this part of code is the preparation of equipment and all the programs that we need through process system development and of the operating system

1. Microsoft windows 7 ultimate
2. Microsoft office 2007
3. Microsoft Visual Studio.Net 2010
4. VB.NET
5. SQL Server 2008
6. EmgU library

5.2.1 Operating System (Microsoft windows 7 ultimate)

This system is characterized by a strong and high quality in performance and have a protection system that enables privacy and safety for t he user. Also have good function in sharing of folder and verify the identity of the user and support many of application and Special software and support multimedia programming.

5.2.2 Microsoft office 2007

Microsoft office 2007 use for Documentation stage , Microsoft PowerPoint 2007 and Microsoft office Visio to do all the necessary designs and drawings and shapes , and Microsoft office Excel 2007 for do diagrams.

5.2.3 Working Environment (Microsoft Visual Studio.Net 2010)

Programming environment is one of Microsoft's products are considered the most powerful environments for programming languages because it support to deal with the databases needed by the program as effective and fast. Also, Visual STudio.NET is a tool for the development of the environment of .NET that It is a complete development environment possible to do design, develop, detect and correct errors and activation of different applications.

The most important features of Visual Studio .NET:

1. The ability to deal with and correct errors.
2. Build the tools of Web applications and Windows tools and access to databases.
3. Supports many programming languages
    - Microsoft VB.NET
    - Microsoft visual C++
    - c#

5.2.4 VB.NET

Programming language used in programming system and it is a programming framework that builds on .NET framework.

5.2.5 SQL Server 2008

One of Microsoft's products that work to manage database and control it (insert, delete and update data) and use it to build tables that will use in the system to input data or update it. The strength and effectiveness of the system in connection between Microsoft SQL server and Visual studio .NET as integrated without make any problem in the system or data that exist in database.

5.2.6 EmgU library

"Emgu CV is a cross platform .Net wrapper to the Intel OpenCV image-processing library. Allowing OpenCV functions to be called from .NET compatible languages such as C#, VB, VC++, Iron Python etc. The wrapper can be compiled in Mono and run on Linux / Mac OS X" [24].

OpenCV is a library of C++ functions which lends itself well to real time computer vision. It provides functionality for reading data from image files, video files as well as live video feeds direct from a webcam or other vision device. The library is well supported and works on both Linux and Windows [25]

5.3 Operation of the system.

After completing the preparation of programs and tools needed by the system, and the creation of the database and lists of input, output, and processing,and writing code for each list, the system is ready to run, and the ability to implementing its functions and show results to the user, and insert data from the user and stored in the database and perform operations required.

Chapter Six

System Testing

Contents:

Chapter Six

System Testing

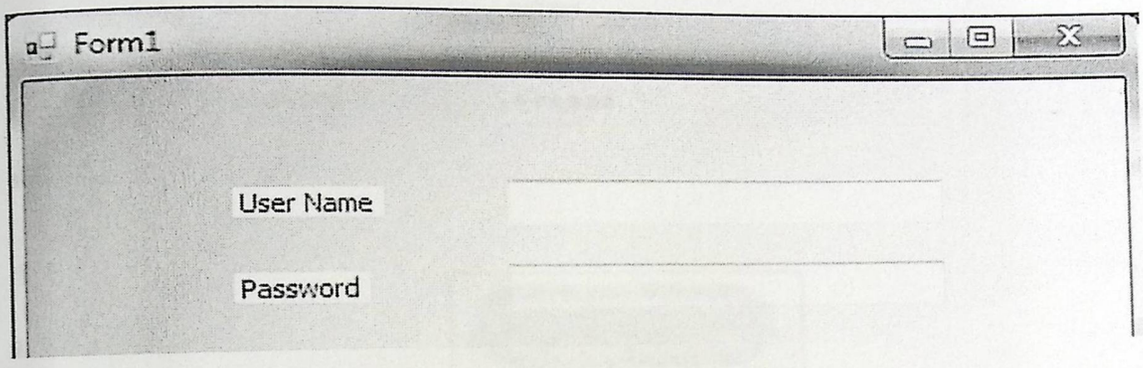
Contents:

6.2 Examine units and models

As each process was examined separately from the other process to make sure it works properly and as expected.

Examples of processes that have been examined:

- **Login examination**



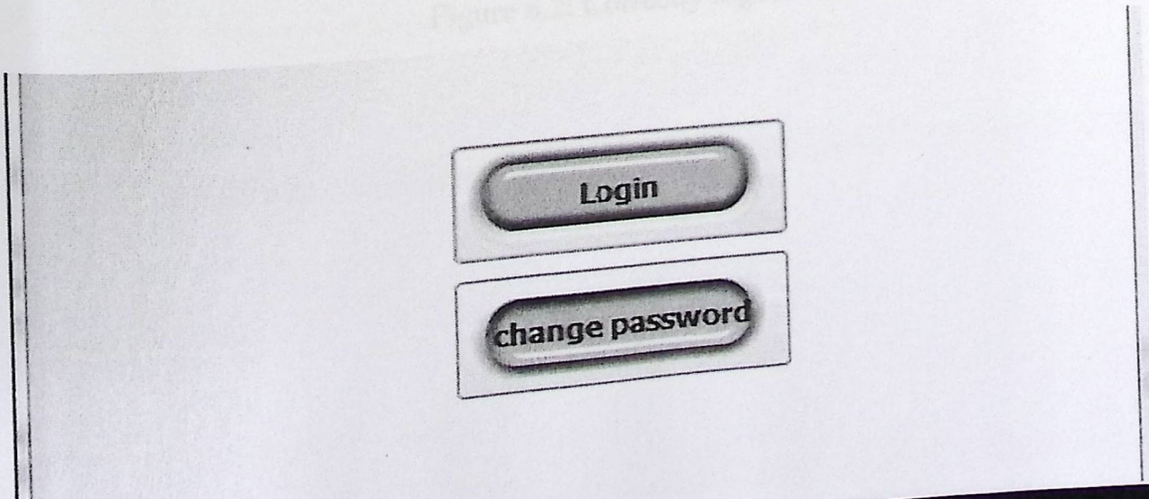


Figure 6.1: Login examination

1. Correctly login

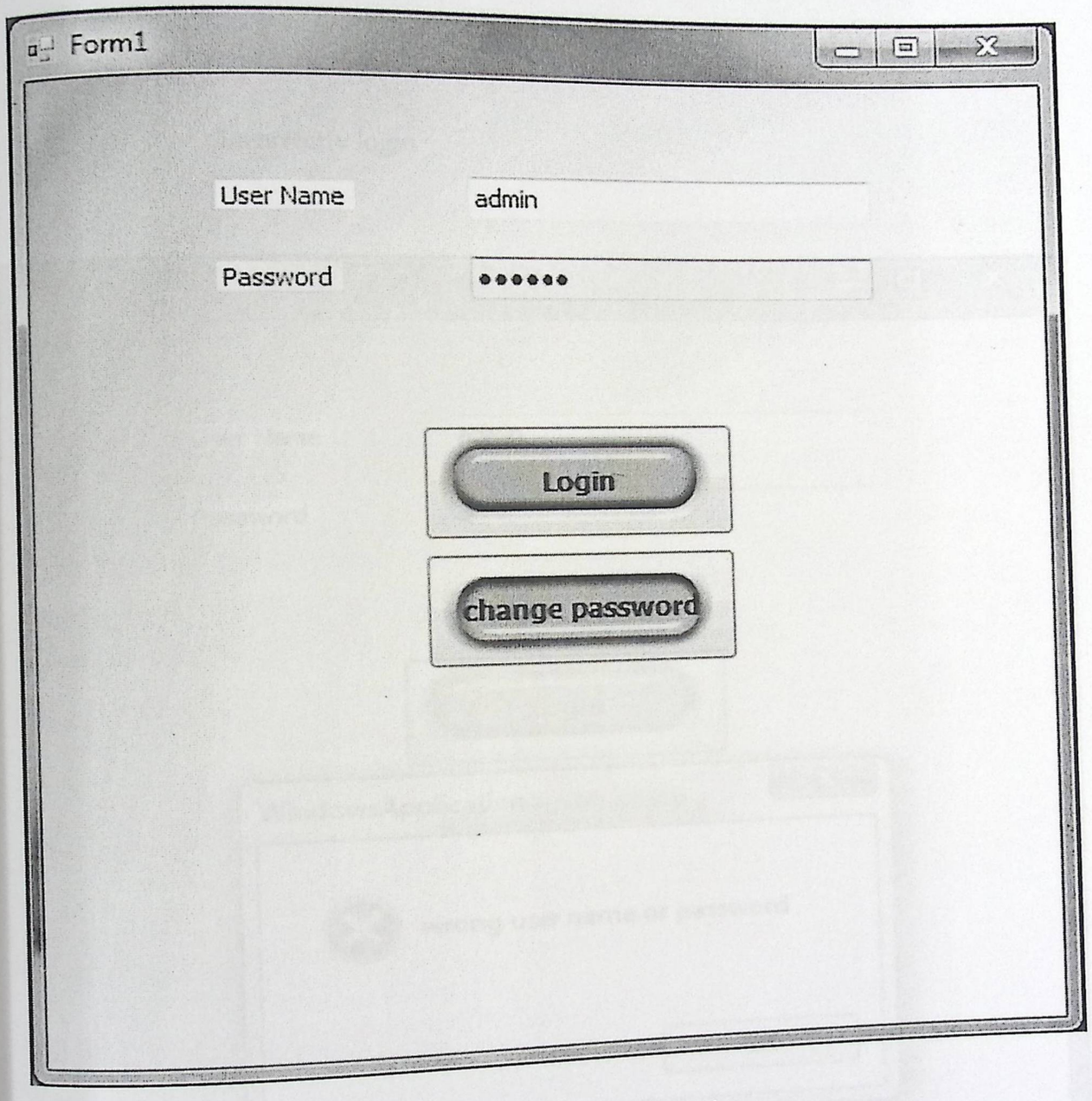
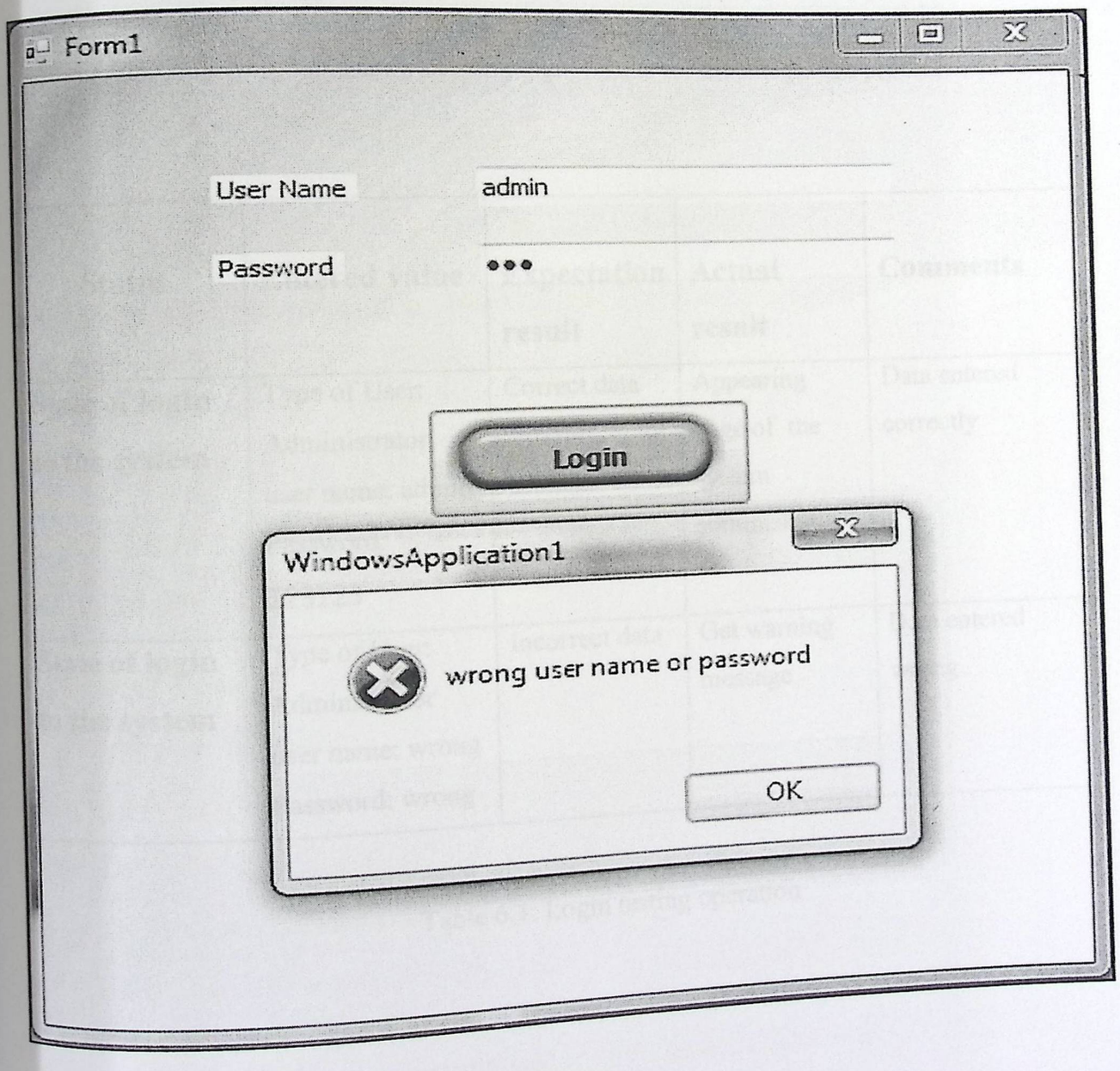


Figure 6.2: Correctly login

2. Incorrectly login



2. Incorrectly login

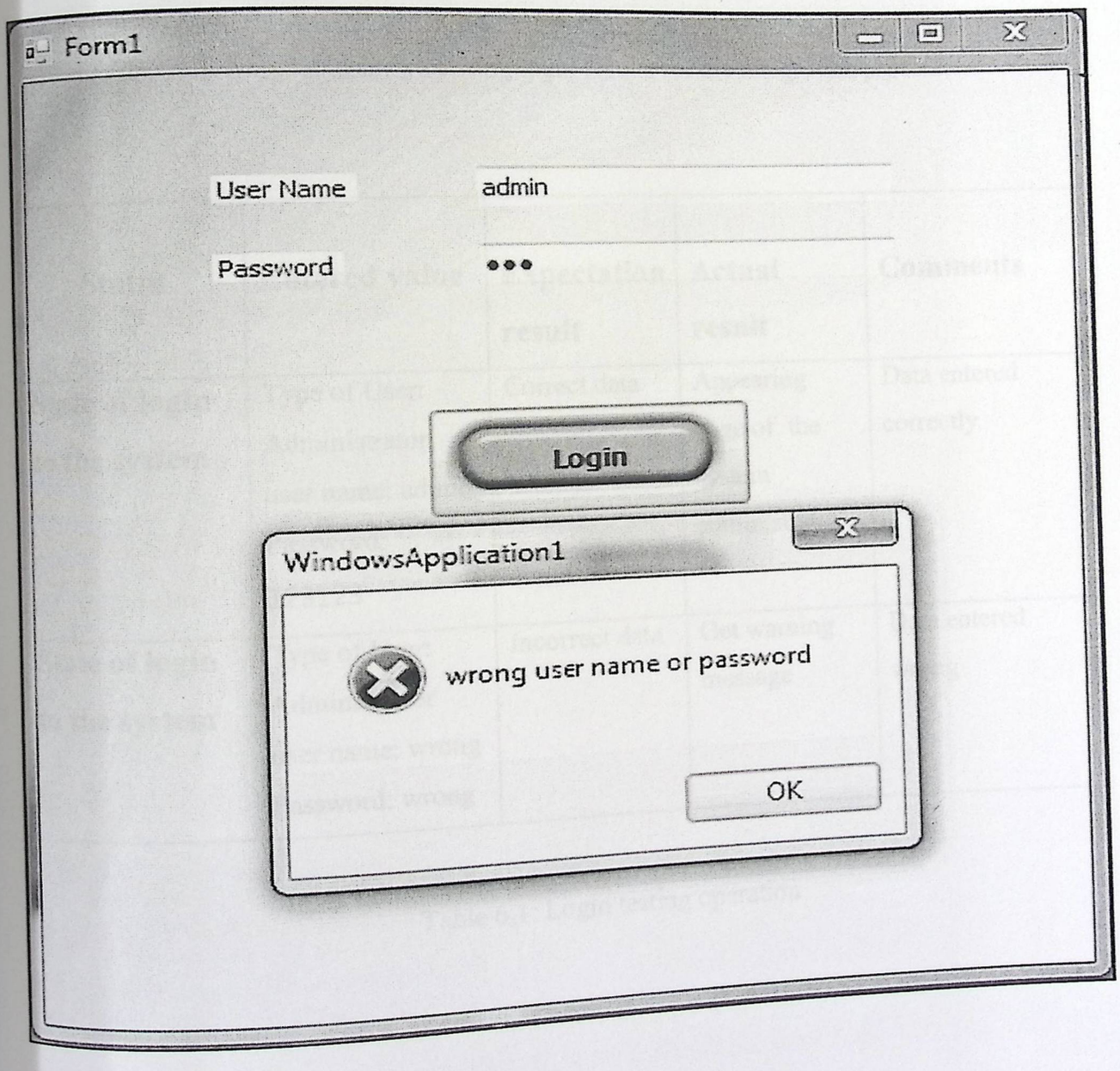


Figure 6.3: Incorrectly login

- In the first case Figure (6.2) a user entered name and password correctly then.

- In the second case Figure (6.3) has been entered incorrectly username or password.

The following table shows testing login results for the integration process:

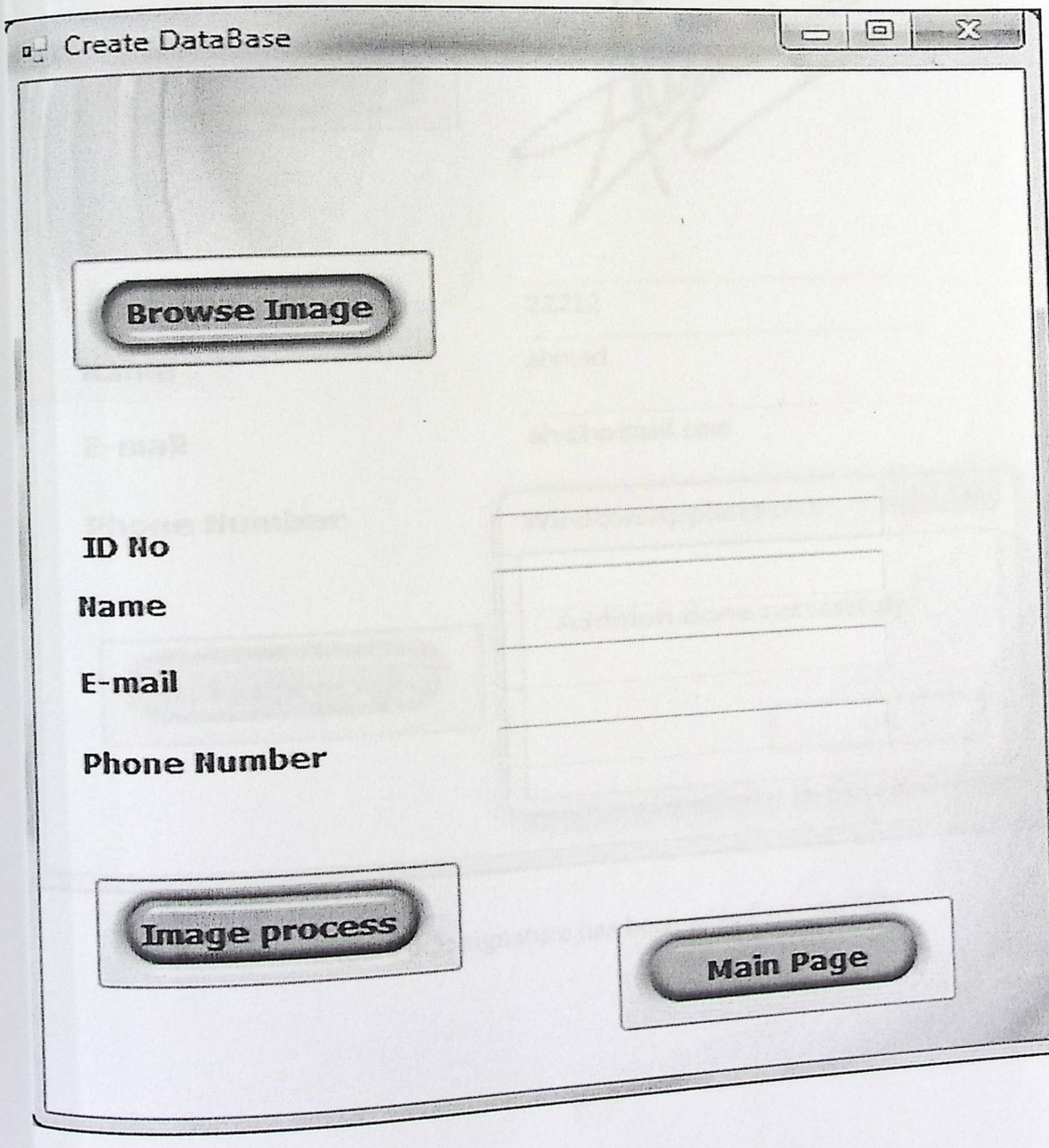
Status	Entered value	Expectation result	Actual result	Comments
State of login to the system	Type of User: Administrator user name: admin Password: 123123	Correct data	Appearing page of the system administrator	Data entered correctly
State of login to the system	Type of User: Administrator user name: wrong Password: wrong	Incorrect data	Get warning message	Data entered wrong

Table 6.1: Login testing operation

6.3 Integration testing

In this section were tested integration between the different parts of the system and examining the interaction between these parts, and examples of parts that were examined integration, including:

- Test adding a new image(signature):



The following figure shows that the signature has been added with fail method because redundancy of ID:

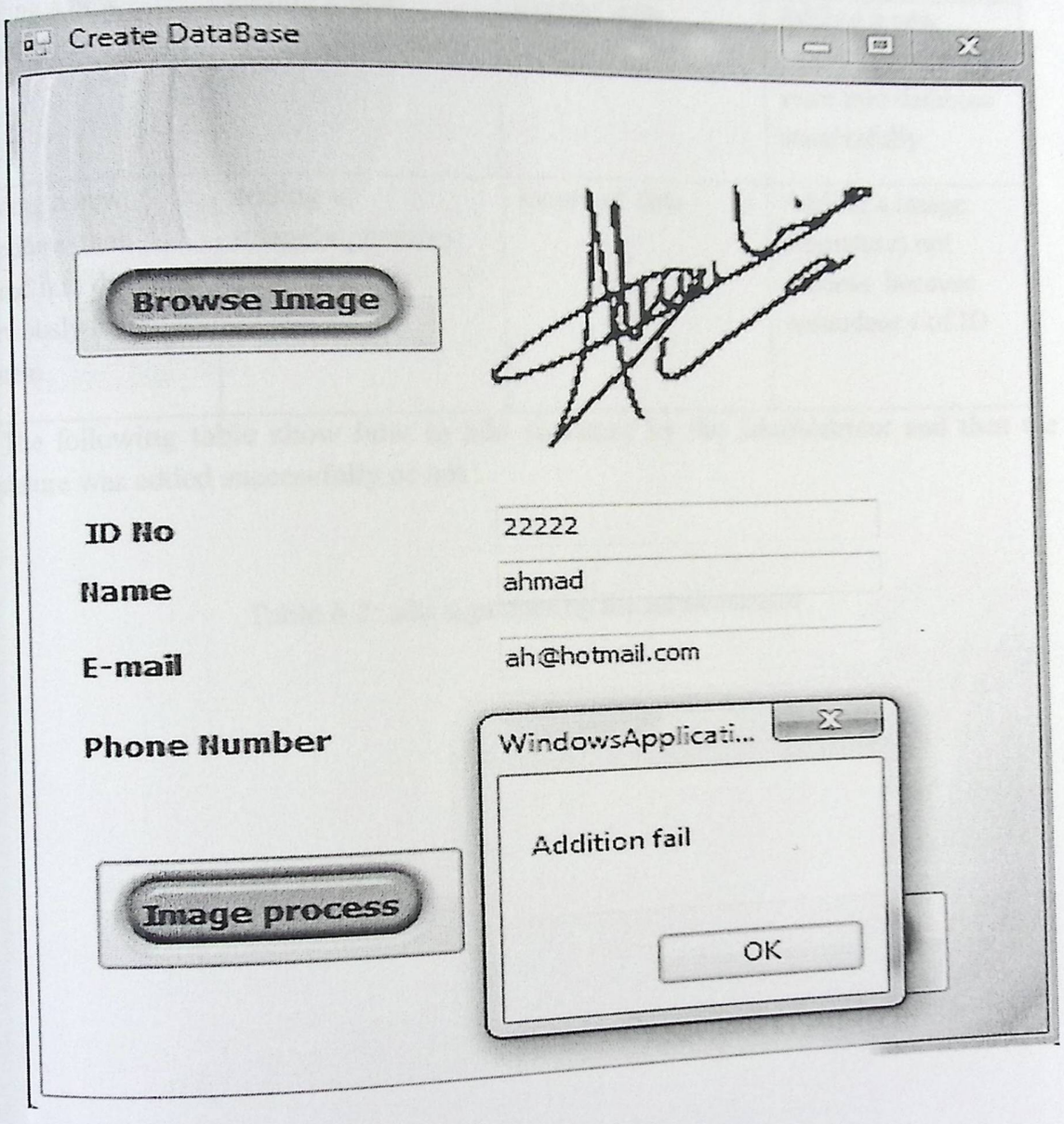


Figure 6.6: signature has been added with fail method

The following figure shows that the signature has been added with fail method because redundancy of ID:

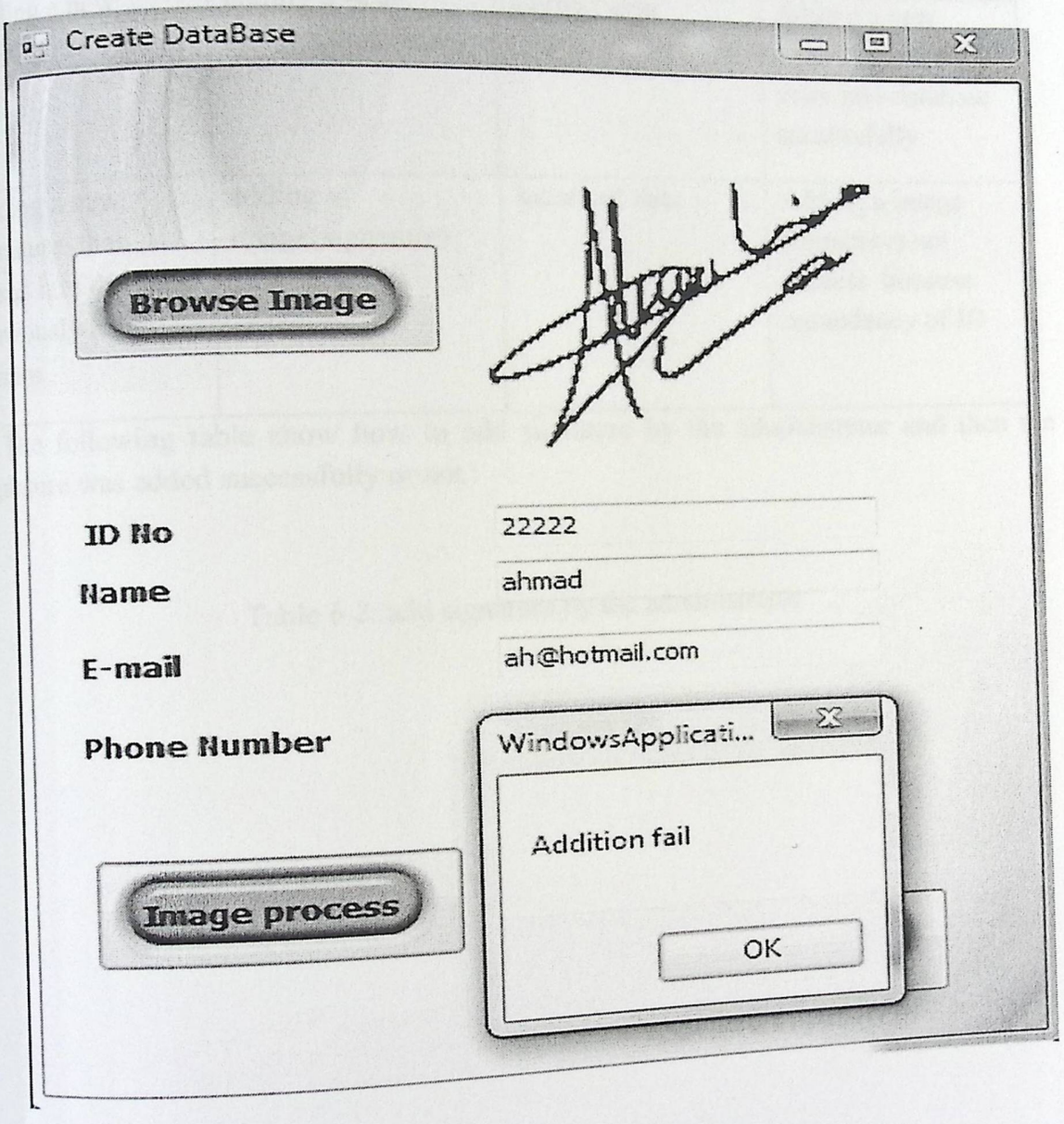


Figure 6.6: signature has been added with fail method

State	Data entered	Expected Result	Actual Result
Adding a new signature to system	adding a new image(signature)	Correct data	Adding a new image (signature) store into database successfully
Adding a new signature that stored into database previously to system	adding a image(signature)	Incorrect data	Adding a image (signature) not success because redundancy of ID

The following table show how to add signature by the administrator and then the signature was added successfully or not :

Table 6.2: add signature by the administrator

6.4 System testing

In this section we examined the system as a single unit to make sure that it works correctly and without errors. And we examined all operations of the system, with noting its impact on other parts of the system, for example Examine the process of changing password of a user and examine the content of the database after the process:

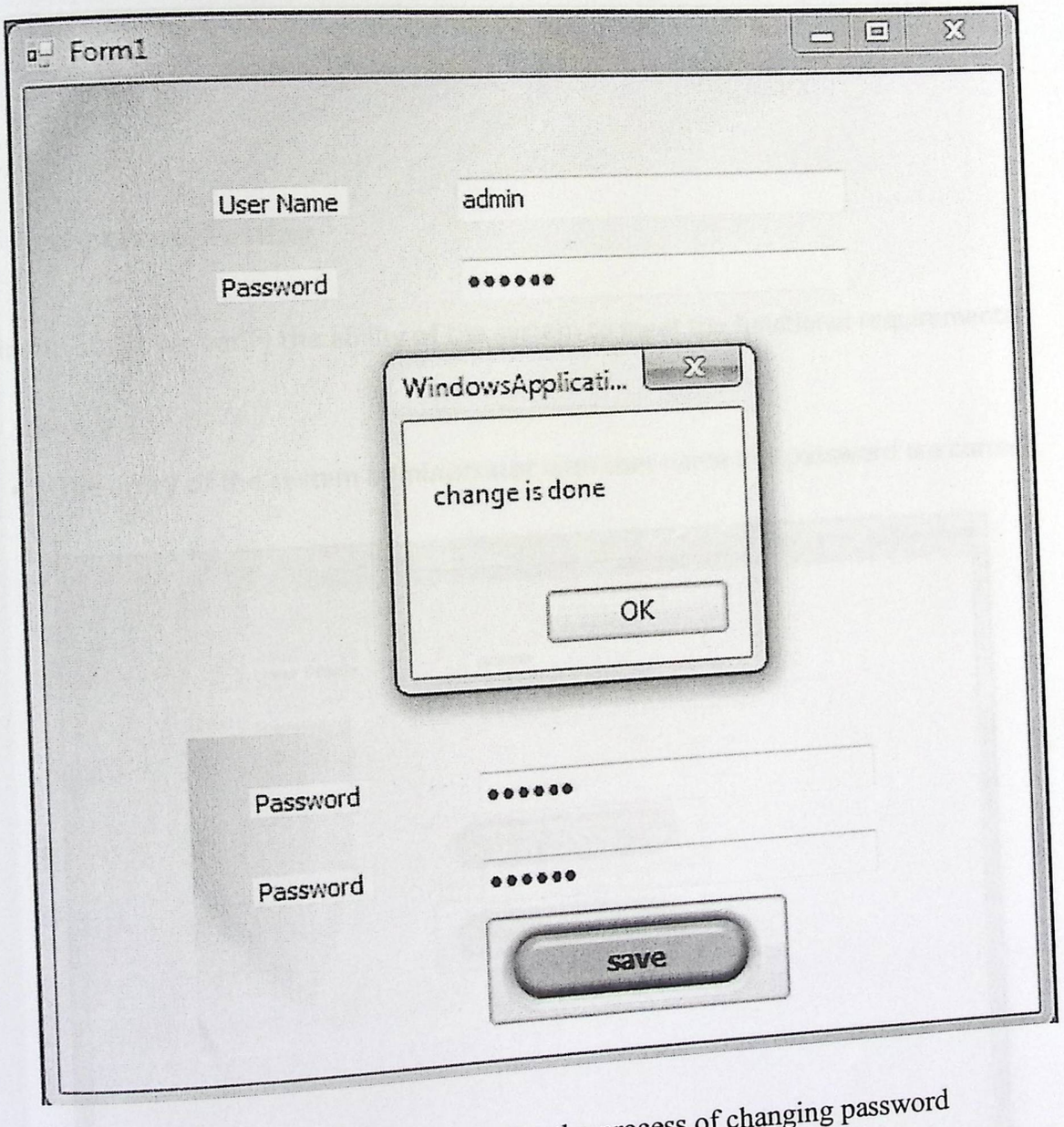


Figure 6.7: Examine the process of changing password

6.4 System testing

In this section we examined the system as a single unit to make sure that it works correctly and without errors. And we examined all operations of the system, with noting its impact on other parts of the system, for example Examine the process of changing password of a user and examine the content of the database after the process:

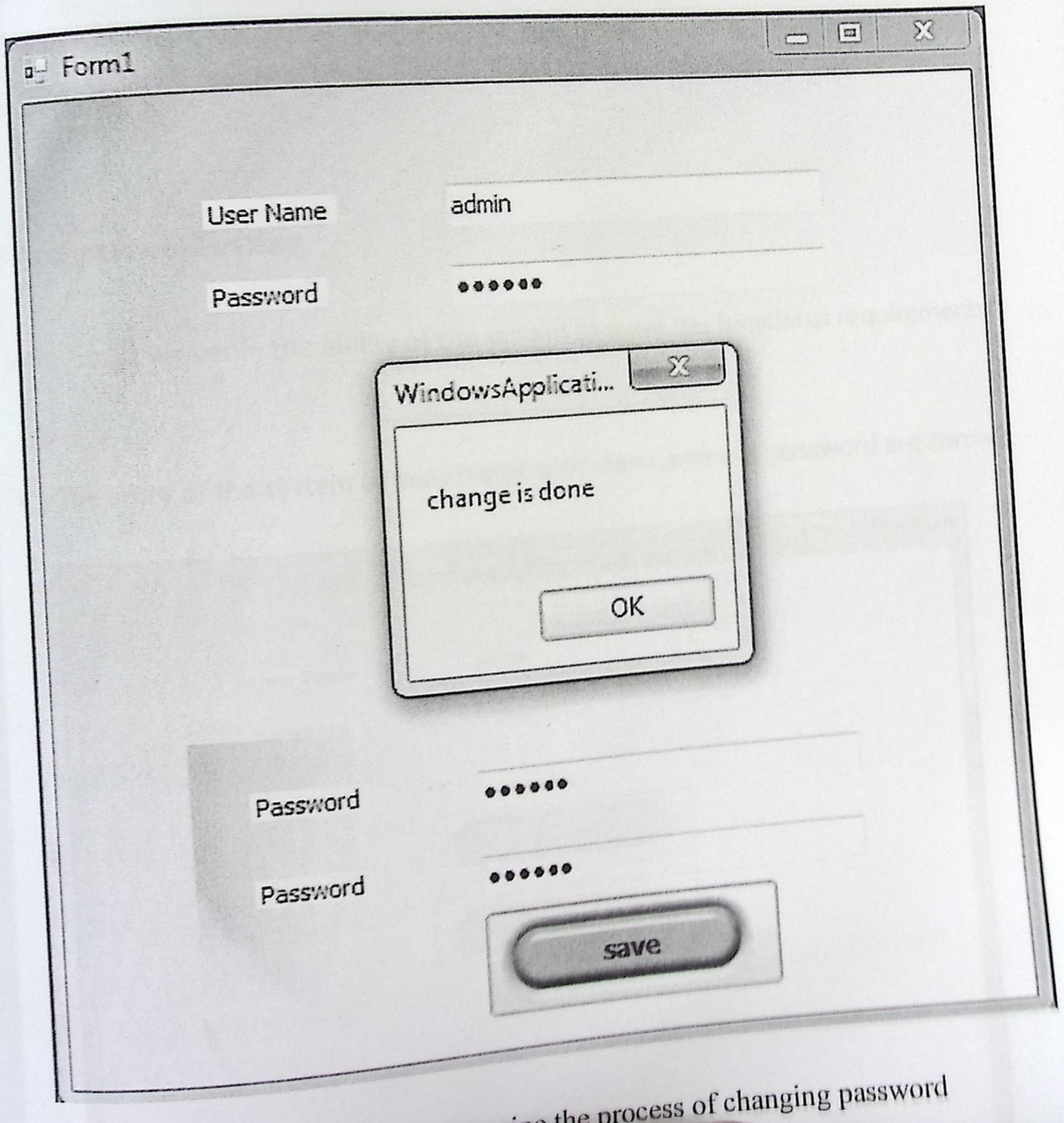


Figure 6.7: Examine the process of changing password

We note in this form that the new password added to the database:

	id	username	password
▶	1	admin	123123
*	NULL	NULL	NULL

Table 6.3: new password added to the database

6.5 Acceptance Testing

In this stage we verify the ability of the system to meet the functional requirements.

- The entry of the system administrator with user name and password are correct

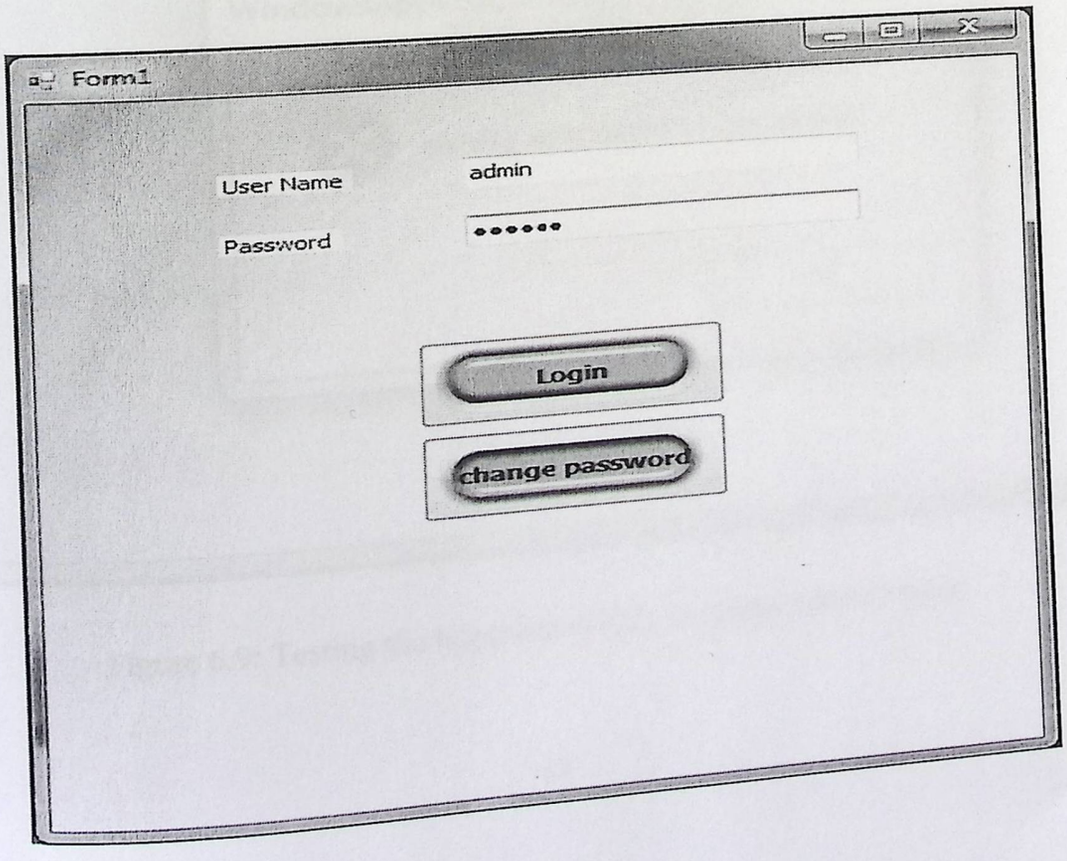


Figure 6.10: Signature verification in our system

- Successfully Signature verification in our system: if the signature that we browse it found in database, then the system bring the name, phone, email for the person who own this signature. On other hand the system can do match percent between the original signature and browsing signature.

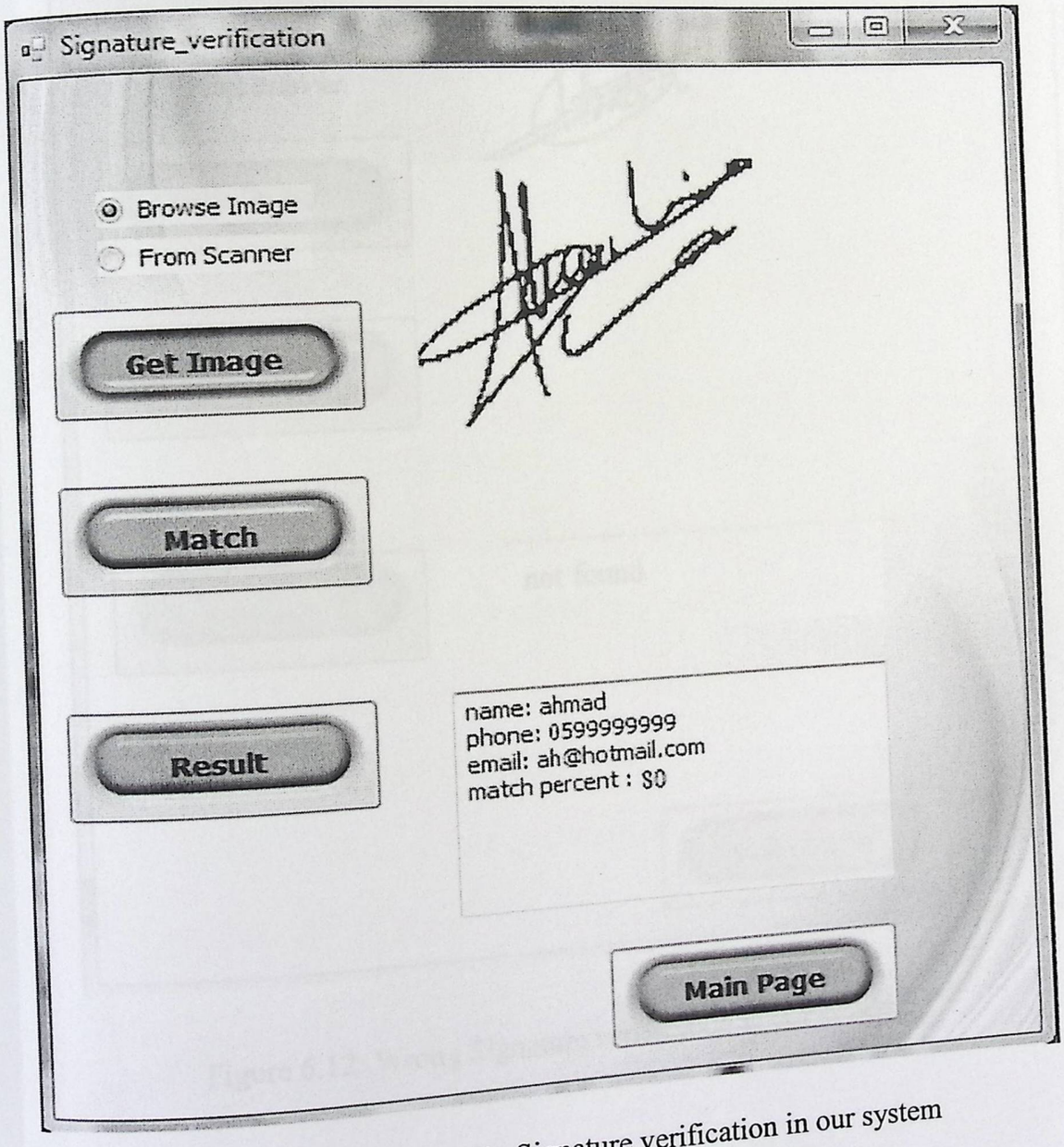


Figure 6.11: Successfully Signature verification in our system

Chapter Seven
Maintenance

Contents:

7.4 Maintenance of the SQL Server 2008

Can control the server and the SQL database system and follow-up errors and problems through the Log file stored in the database, and also can control the powers of the users and add a new user and give specific terms of reference through the screen of the Console Windows.

7.5 Maintenance of the Internet Information Server (IIS)

IIS service is the main entrance to the process of deploying applications on the Intranet or the Internet as one of the most important requirements for the download. Visual Studio.Net Therefore, the successful deployment of efficient and effective applications needed depends primarily on the basic accuracy and confidentiality enjoyed by the IIS. And can control the characteristics of the IIS by Prosperity panel domain.

7.6 How to deal with errors

When you run the system by the user there are several problems or errors may arise at work, the user can not be resolved or knowledge of their causes. In this case, the user must contact the author using and explain the problem to him.

Chapter 8

Conclusion and future work

8.1 Introduction

After the completion of the process of development system, the team of work are achieve results and goals that has aspires to achieved its previously planned. in addition reach for conclusions to help for development of system and Increase efficiency and effectiveness in system.

8.2 Conclusions

Handwritten signature verification is approach in the field of image processing. this project open the way for apply another algorithm on signature Specially it is not apply here.

8.2.1 Project achievements

In this point the main achievements of our project are discussed and the ways of achieving it.

- The project succeed of verify of handwritten signature using SURF algorithm .
- Finding the match between signatures for the same person.
- Extract features from signature to compare it between signatures.
- Determined who owns the signature.

8.2.2 Project problems

Many problems faced us during implementing this project.

- DataBase of signature

  Numbers of sample of signature because was needed large number of sample. and there is no sufficient sample.

- SURF algorithm

  Apply SURF algorithm on signature because it is not previously applied.

- Vector

  We faced problem when determined the value of Vector because it is need a high accuracy.

- Forgery.

  Signature easier to be forged than other biometric attributes such as fingerprint, iris, etc.

8.3 Results of Signature Verification

Signature Verification using 3 signatures of each of the 30 signers, totaling to 150 signatures, 3 signature in DataBase and 2 used it in testing. Tests using a similarity measure between the coefficient vectors.

Nature of signature	Sample	False Acceptance Ratio	False Rejection Ratio	Time of match
Original	20	20%	80%	4 second
Original	40	22.5%	77.5%	6 second

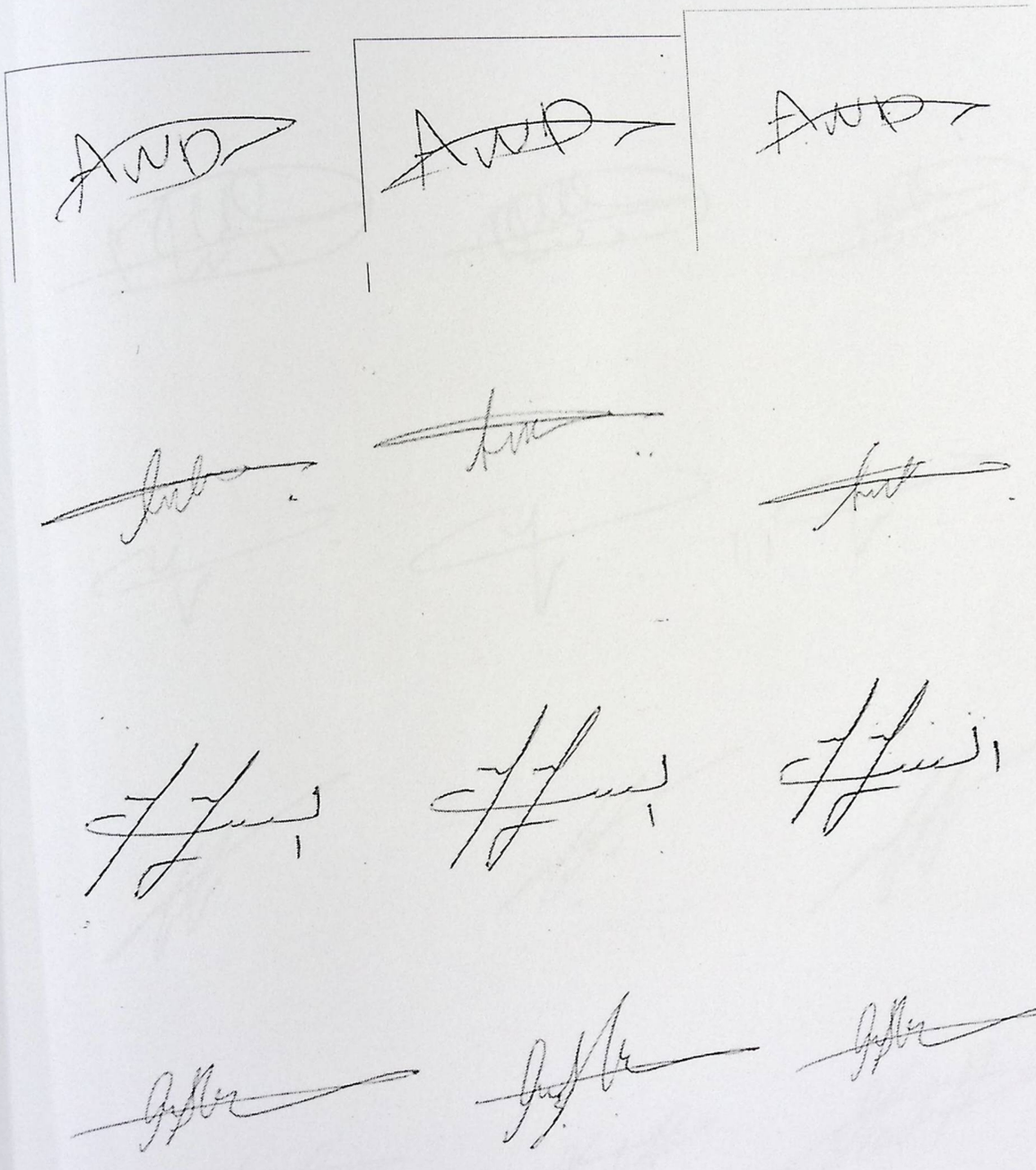
Table 8.1 : Results of Signature Verification

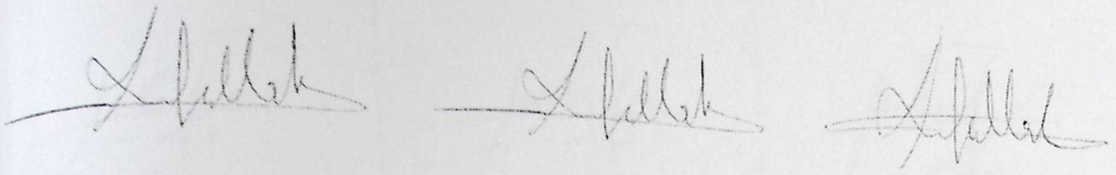
8.4 Future work

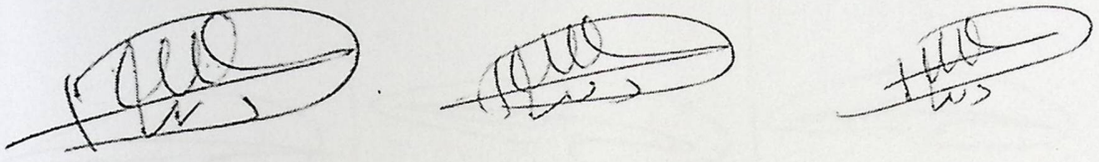
In the future many changes could help in obtaining better results; by using another algorithm to obtaining better accuracy. And Building system takes into new several things, such as:

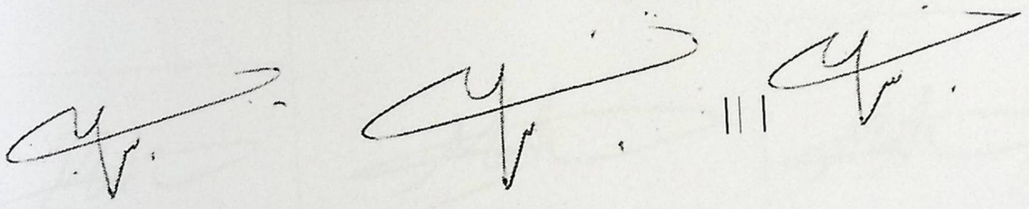
- That takes the psychological status of person because nerves and diseases affecting the signature.
- Takes signature from paper that contain many word and the system can determined the place of signature and take it only.
- Develop the current system to become more efficient.

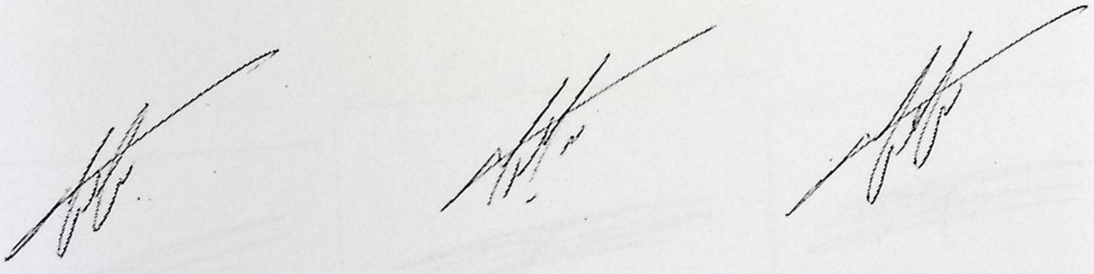
Appendix Signatures

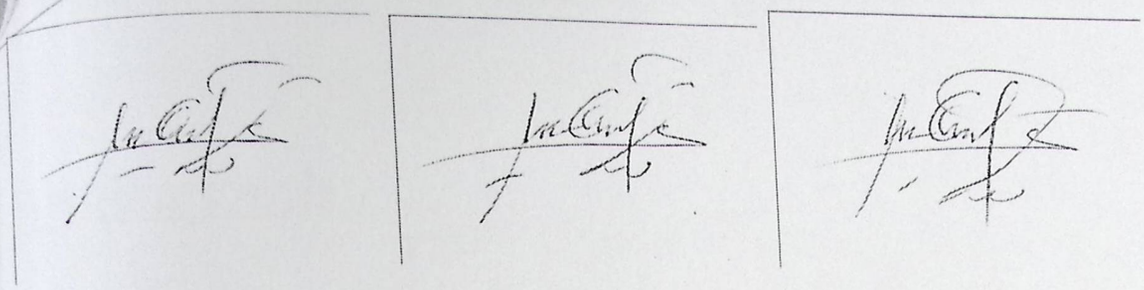


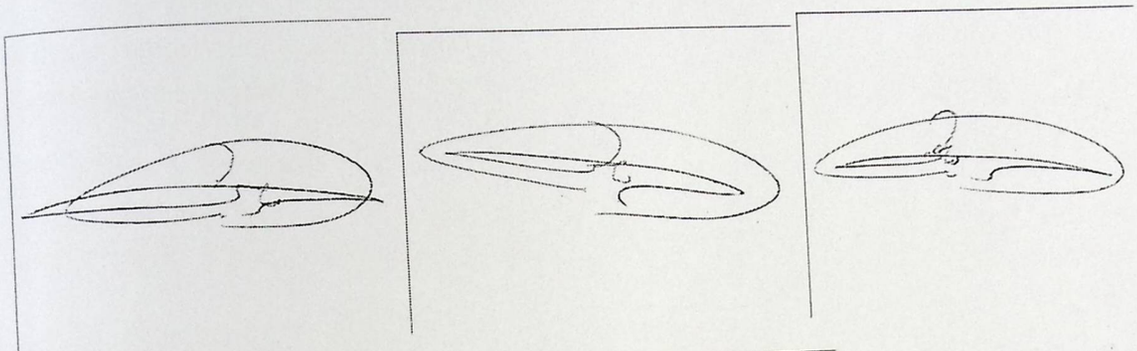


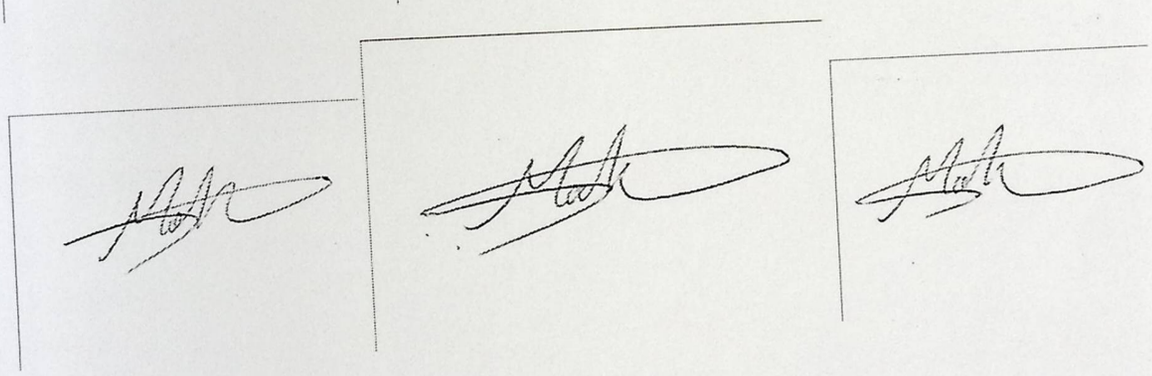


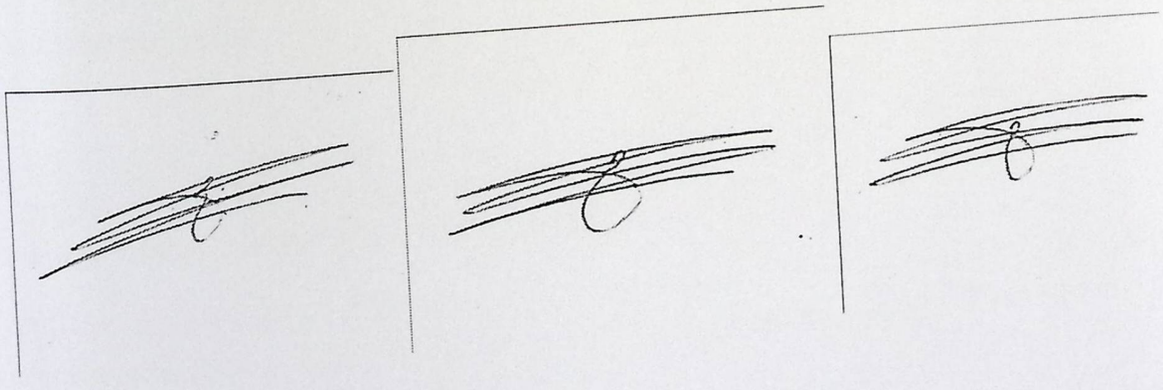


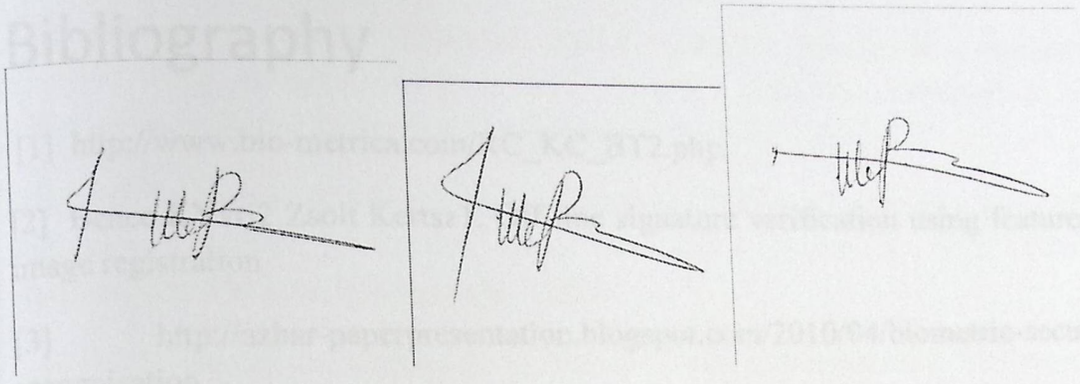












Bibliography

[1] http://www.bio-metrica.com/RC_KC_BT2.php.

[2] Bence KYvri2 Zsolt Kertsz1. Off-line signature verification using feature based image registration.

[3] http://azhar-paperpresentation.blogspot.com/2010/04/biometric-security-iris recognisation.

[4]http://www.google.ae/search?um=1&hl=ar&biw=1291&bih=540&tbm=isch&sa=1 &q=piece+of+pottery

[5] Sharath Pankanti Nalini K Ratha Ruud Bolle, Jonathan H. Connell. Guideto Biometrics. Springer Sceince Busness Media Inc. 233 Spring Street Nea York, NY, 10013, USA, 1 edition, 2004.

[6] R. Plamondon and S. N. Srihari. On-line and off-line handwriting recognition. IEEE Trans.on Pattern Analysis and machine Intelligence, 22(1):6384, 2000.

[7] Bence KYvri2 Zsolt Kertsz1. Off-line signature verification using featurebased image registration.

[8] R. Plamondon and S. N. Srihari. On-line and off-line handwriting recognition.IEEE Trans.on Pattern Analysis and machine Intelligence, 22(1):6384, 2000.

[9] Rasha Abbas and Victor Ciesielski. A prototype system for off-line signa-ture verification using multilayered feed forward neural networks. SMC'97,February 1995.

[10] S. N. Srihari and A. Xu. Learning strategies and classification methods foroffline signature verification. roceedings of the 7th internationalWorkshop onFrontiers in handwriting recognition, 2004.

[11] A. E. Yocoubi. F. Bortolozi. E. R. Justino. and R. Sabourin. An off-linesignature verification system using hmm and graphometric features. 4th IAPRInternational on Document Analysis Systems, DAS 2000.

[12] B. Herbst. J. Coetzer. and J. Preez. Online signature verification using thediscrete radon transform and a hidden markov model. EURASIP. Journal onApplied Signal Processing, 4, 2000.

[13] Z. Lin. W. Liang. and R. C. Zhao. Offline signature verification incorpo-rating the prior model. International Conference on Machine Learning and Cybernetics, 3, 2003.

[14] HT. S . enturk. E. Ozgunduz. and E. Karshgil. Handwritten signature verification using image invariants and dynamic features. Proceedings of the 13thEuropean Signal Processing Conference EUSIPCO, 2005.

[15] HB. A. Jesus. A. Migual. and M. Traveiso. Doff-line geometric parame-ters for automatic signature verification using fixed point arithemetic. IEEETrans.Pattern Analysis and Machine Intelligence, 7, 2005.

[16] G. F. Russel. A. Heilper. B. A. Smith. J. Hu. D.Markman. J. E. Graham.T. G. Zimmerman. and C. Drews. Retail application of signature verification.Proceedings of SPIE 2004, 5404,:206214, 2004. Bibliography 46

[17] . Bolle A. Jain and S. Pankanti (eds). Biometric Personal Identification inNetworked Society. Kluwer Academic Publishers, Boston Hardbound, 1999.

[18] A. K. Jain and S. Pankanti. An introduction to biometric recognition. IEEE Transactions on Circuit and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics, 14(1):4–20, January 2004.

[19] Ashish Dhawan ,Aditi R. Ganesan"Handwritten SignatureVerification "

[20] GD. Lowe. Distinctive image features from scale- invariant keypoints. International Journal of Computer Vision, 60(2):91, 2004.

[21] S. C. Han S. W. Kim S. K. H. M. Park, Y. Kim and C. H. Kang. An biometric identification system by extracting hand vein patterns. Journal of the Korean Physical Society, 38(3):268–272, 2001.

[22] (Tamimi, 2006, p.22)

[23]http://books.google.ps/books?id=7ZHqiQ6K7gUC&pg=PA289&lpg=PA289&dq =work- flow+of+the+algorithm+computing+SURF(+interest+point+detection)

[24] https://www.ohloh.net/p/EmguCV

[25] Open Source Computer Vision Library. Provides a simple API for working with images and videos in C++. Available from: http://opencvlibrary.sourceforge.net/