

FINGERPRINT MATCHING USING SIFT FEATURES

A Proposal



|  |  |
| --- | --- |
| ID | FULL NAME |
| 10736694 | Terence Ugo Nacciarone Quashie |
| 10729461 | Abdul-Aziz Abubakar Saddick |

Table of Contents

[Background 2](#_Toc109742635)

[Introduction 2](#_Toc109742636)

[Objectives 2](#_Toc109742637)

[Method And Design 2](#_Toc109742638)

[Sample Data 2](#_Toc109742639)

[Procedure 3](#_Toc109742640)

[Analyses 3](#_Toc109742641)

[Conclusion and Findings 3](#_Toc109742642)

# Introduction

In 1983 when the Home Ministry Office, UK concluded that no two individuals can have the same fingerprints, it set in motion a series of events that led\* to the widespread use of fingerprint pattern systems, known as the AFIS (Automatic Fingerprint Identification Systems). These systems are actively used by law enforcement agencies all over the world today. In fact, these fingerprint matching systems have become so successful in criminal investigations that the term fingerprint has become synonymous with the word inherent characteristic or unique characteristic.

The success of fingerprint identification systems has spurred a wide spiral of its application beyond the forensic domain to “second generation” geared towards civilization application such as biometric authentication. The second generation of fingerprint identification systems operate automatically and are deployed in more mainstream applications that deal with a larger cross-section of society such as unlocking mobile phones or gaining access to a secure app such as a banking or blockchain app. **(LINK SOMETHING ABOUT SMART HOMES HERE AS A SECOND EXAMPLE).**

It is an undeniable fact that the current implementations of fingerprint identification systems (rephrase?) have positively reduced cases of identity theft in our society. However, the “million-dollar” question still remains; “Will these fingerprint biometric technologies work all the time? Will they work everywhere and, in all contexts, reliably identify and authenticate a person”. These are questions that have pushed researchers to develop newer and more efficient methods of automatic fingerprint identification and matching.

One of the design criteria for building such an automatic and reliable fingerprint verification systems is that the underlying sensing, representation and matching technologies must be very robust. It is essential that these individual components have little to no degradation in their performance in the long term. One way to address these requirements of robust performance is to adopt a robust representation scheme that captures all discriminatory information to a high degree of accuracy.

The most popular representation of these discriminatory information is through local landmarks known as **minutiae**. This method evolved from the system of visually matching fingerprints used by forensic experts. **The minutiae-based algorithm** works by locating these local landmarks where fingerprint ridges either terminate or bifurcate and then match minutiae relative placement between a given fingerprint sample and the stored template. A good quality fingerprint contains between 25 and 100 minutiae depending on sensor resolution and finger placement on the sensor. The minutiae-based system is a well-known method for fingerprint verification.

Although the minutiae based-system is plenty robust and the most widely used method of fingerprint verification, it struggles when given poor quality fingerprint impressions arising from dry fingers or fingers mutilated by scars and scratches. There is also anecdotal evidence that a fraction of the population may have fingerprints with relatively small number of minutiae thereby making it more vulnerable to failures.

This short-coming of the minutiae-based system meant that there was need to extend characteristic feature matching beyond minutiae points. For this, techniques such as the **Scale Invariant Feature Transformation (SIFT)** was introduced, an object matching algorithm. SIFT works by constructing a scale space from which descriptors are extracted and used in the matching process.

Using a public domain fingerprint dataset, this project will implement the two algorithms and compare their performance and useability.

# Introduction

Fingerprint Recognition is an automated method used to match fingerprint features against already stored samples for the purpose of identity verification. It is one of the most well-known biometrics and by far the most used biometric solution for authentication on computerized systems (Biometric Solutions, 2016). Fingerprint features on the other hand are graphical features embedded in fingerprint ridges and valleys. Also included are minute patterns like bifurcation, ridge spots and ridge ends. These ridges and valleys can be recognized over fingertip surfaces.

Various methods of fingerprint matching exist such as minutiae-based systems, and while these methods have shown fairly high accuracies, further improvements are needed for an improved performance, especially in applications involving large scale databases. In an effort to improve the currently existing method, the ***Scale Invariant Feature Transformation* (SIFT)** method was created.This method involves extracting various feature points in a scale space and performing matching based on the texture information around characteristic points using the SIFT operator. Using a public domain fingerprint dataset, a SIFT based fingerprint matching system and compare its performance to conventional minutiae-based system.

# Objectives

1. Implement the Scale Invariant Feature Transformation (SIFT) algorithm using python programming language
2. Match two exact fingerprints using this algorithm
3. Measure its effectiveness against minutiae methods by distorting some parts of the image

# Method And Design

## Sample Data

The Kaggle [Sokoto Coventry Fingerprint (SOCOFing)](https://www.kaggle.com/datasets/ruizgara/socofing) dataset will be used in the undertaking of this project. The database contains over 6,000 (Six Thousand) sampled fingerprint images, as well over 14,000 (Fourteen Thousand) alterations of these fingerprint images. A sample will be taken from this pool and compared with their altered version using the SIFT algorithm.

## Procedure

A theoretical approach will be done detailing the important constituents of the SIFT algorithm including its advantages as well as it’s time complexity. Following these characteristics, the algorithm will be implemented using the **Python Programming language** with a Graphical User Interface *(GUI)* built with **PyQt5.**

## Analyses

The accuracy and speed of matching will be compared and from this a graph will be generated showing the false acceptance rate of each method.

# Conclusion and Findings

This project will demonstrate that the SIFT algorithm is very efficient at matching fingerprints more efficiently than the currently existing minutiae-based methods of matching.