CHAPTER

6
TRIANGULAR GEOMETRIC FEATURES FOR OFFLINE SIGNATURE VERIFICATION

Mohd Shafry Mohd Rahim, Fazliaty Edora Fadzli, and Aida Ali

6.1 INTRODUCTION

Handwritten signatures are widely accepted as a biometric trait for personal authentication. Over the past decade, numerous solutions have been proposed to address the limitations of offline signature verification. However, many previous studies failed to achieve high accuracy, as their approaches primarily relied on global and local features without fully exploring geometric properties. To address this gap, the present research proposes a novel feature based on geometric concepts aimed at improving verification accuracy. Specifically, triangle attributes are utilised due to their inherent properties—orientation, angles, and transformation—that are beneficial for distinguishing between genuine and forged signatures.

A new primary feature set is introduced using a triangulation-based geometric model, which includes the sides, angles, and perimeter of a triangle constructed from the centre of gravity of the signature image. The sides are computed using Euclidean distance, while the angles are derived using either the Law of Sines or the Law of Cosines. The perimeter is calculated as the sum of the triangle's sides.

To evaluate the effectiveness of this feature set for classification, both the Euclidean classifier and a voting-based classifier were employed to detect forgery tendencies (Tram & Chau, 2024). The classification process was carried out using the proposed triangular geometric features in combination with selected global features.

6.2 UNDERSTANDING THE BASICS

Offline signature verification presents several challenges due to the nature of the input, which typically consists of a scanned image of a signature on paper or other physical media (Singla & Mittal, 2025). These inputs often contain less discriminative information, making it difficult to distinguish between genuine and forged signatures. While genuine signatures from the same individual may exhibit slight variations, the differences between a forgery and an authentic signature can be subtle and hard to detect. This makes automatic offline signature verification a highly complex pattern recognition problem.

This chapter discusses the problem of signature verification, a biometric identification method that utilises the unique attributes of an individual's signature. Since a signature can consist of symbols, lines, curves, or a group of letters, it is generally treated as an image. Unlike character recognition, signature verification deals with stylised, often unreadable representations that reflect the individual's writing style. Signatures are distinct from typical handwriting, often serving as symbolic identifiers rather than literal text. As such, a signature should be analysed as a complete image reflecting the unique writing patterns of an individual, rather than as a combination of letters or words. Given that each person typically has a unique handwritten signature, their identity can often be verified through these personalised writing traits.

Over the past decade, various methods have been proposed to improve the performance of offline signature verification systems and to address their limitations. Despite these efforts, achieving high accuracy remains a significant challenge. For such systems to be practical and widely accepted, they must demonstrate a high degree of reliability.

However, compared to online signature verification, offline systems still fall short in terms of accuracy. Studies have shown that most offline systems average around 90% accuracy, which is considered insufficient for critical biometric authentication applications.

Offline signature verification is one of the earliest problems in pattern classification, involving the task of distinguishing between genuine and forged signatures written on paper. In contrast, online signature verification systems collect data directly from electronic devices such as tablets, capturing dynamic writing information like pen speed, pressure, and the number of strokes. This dynamic data provides valuable features for verification. However, offline systems rely on static images of signatures captured using scanners or cameras, which lack dynamic information. As a result, only simple features can be extracted from these scanned images, making the verification process more challenging.

Several factors contribute to the complexity of offline signature verification. First, scanned images often contain noise, such as salt-and-pepper artefacts, introduced by the scanning hardware or the texture of the paper. Such noise can interfere with the image processing and feature extraction stages. Additionally, physical issues like paper folds may leave marks that are mistakenly interpreted as signature features, leading to inaccurate results. Variations in pen type and tip width also introduce inconsistencies in the shape and style of signatures, potentially causing the system to misclassify signatures from the same person.

Another major challenge is the limited amount of training data available for each writer. This scarcity makes it difficult for the system to learn an accurate representation of an individual's signature. Furthermore, intrapersonal variability—natural variations in a person's own signature—complicates the task. Even genuine signers rarely produce identical signatures every time due to slight inconsistencies. On the other hand, interpersonal similarities—where signatures from different individuals resemble one another—pose a risk of skilled or traced forgeries being falsely accepted as genuine.