Fingerprint Identification System

P. Ananta Lakshmi

Srinivasa Institute of Technology& Science, Kadapa

Abstract

A finger print identification system uses digital imaging and algorithms to rapidly and accurately compare finger prints against a data base for identification purposes, commonly used by law enforcement.

Key word : Minutiae, Latent prints, Ten print, Palm print, NAFIS, Interpol's AFIS.

1.1 INTRODUCTION TO IMAGE PROCESSING

In the initial stages of computing, data was mainly composed of numerical figures. As technology advanced, textual information gained significance. In the present era, data encompasses a wide range of formats, including audio, music, spoken language, images, and computer-generated graphics, all of which are extensively utilized.Each of these data types functions as a signal, which is essentially a function that conveys information. Before delving into digital image processing, it is essential to explore its historical background.

The emergence of digital image processing as a field occurred relatively late in computer history, largely due to the need for graphical operating systems to support its development. Additionally, digital image processing demands meticulous optimization, particularly for real-time applications. Throughout history, as people have used electronic mediasuch as telegraphs, telephones, television, and radarto communicate, Researchers have acknowledged that signals can be modified by the systems responsible for their capture, transmission, or processing. These systems frequently introduce various interferences, such as noise, distortion, or artifacts, which can degrade the overall quality of the signal.

Signal processing focuses on understanding these effects and developing methods to correct them. The goal is to embed specific information within a signal and later extract it accurately. Some signals represent natural occurrences, while others are artificially created. By combining these technologies, we can capture natural signals, process them, and transmit them in various waysa process known as digital image processing.

Human vision allows us to perceive and interpret our environment. Computer vision seeks to replicate this ability by enabling machines to interpret images electronically. However, this is a challenging task because while humans perceive the world in three dimensions (3D), most visual sensors, such as TV cameras, capture two-dimensional (2D) images. This transformation from 3D to 2D results in a significant loss of information, making computer vision a complex and intricate field of study.

1.2 DIGITAL IMAGE PROCESSING

Ezra Pound describes an image as a fusion of intellect and emotion captured in a single moment. In the context of image processing, an image is defined as a two-dimensional function of light intensity, represented as f(x, y), where x and y denote spatial coordinates. The function's value at any specific point (x, y) indicates the brightness or gray level at that position in the image.Typically, the x-axis runs horizontally, while the y-axis is oriented vertically. The origin of the coordinate system is typically located at the top-left corner of the image. In this setup, the x-axis extends horizontally from left to right, while the y-axis progresses vertically from top to bottom.

Image processing involves manipulating images in various ways, whether to enhance quality, restore details, extract useful information, or alter the image's structure. It falls under the broader category of signal processing, explicitly dealing with visual data. The primary objective of image processing is to refine image quality for better human perception or to make the image more suitable for computer-based analysis and interpretation.

A digital image, denoted as f(x, y), is a representation that has been discretized in terms of both spatial coordinates and intensity levels. It is typically structured as a matrix, where each element corresponds to a specific point in the image. The row and column indices determine the location of the point, while the value stored in the matrix represents the gray level or intensity at that position.Digital Image Processing (DIP) involves modifying digital images through computational techniques. This multidisciplinary field combines principles from optics, surface physics, visual perception, computer science, and mathematics. In DIP, an image is transformed into a numerical array of pixels, each representing a specific physical attribute like scene radiance. These numerical values are stored in digital memory and analyzed using computers or specialized digital devices.

Digital images can be categorized into three main types: binary, monochrome, and color images. Binary images contain only two intensity levels, representing bright areas as 0s and dark areas as 1s. Monochrome images, or grayscale images, have pixel values that range within a specific intensity scale. Color images, on the other hand, store information on both brightness and color. Each pixel in a color image records the intensity of three primary colors, red, green, and blue (RGB), which combine to produce the final visual representation.

Fundamental Steps:

Outputs of these processes generallyvare images

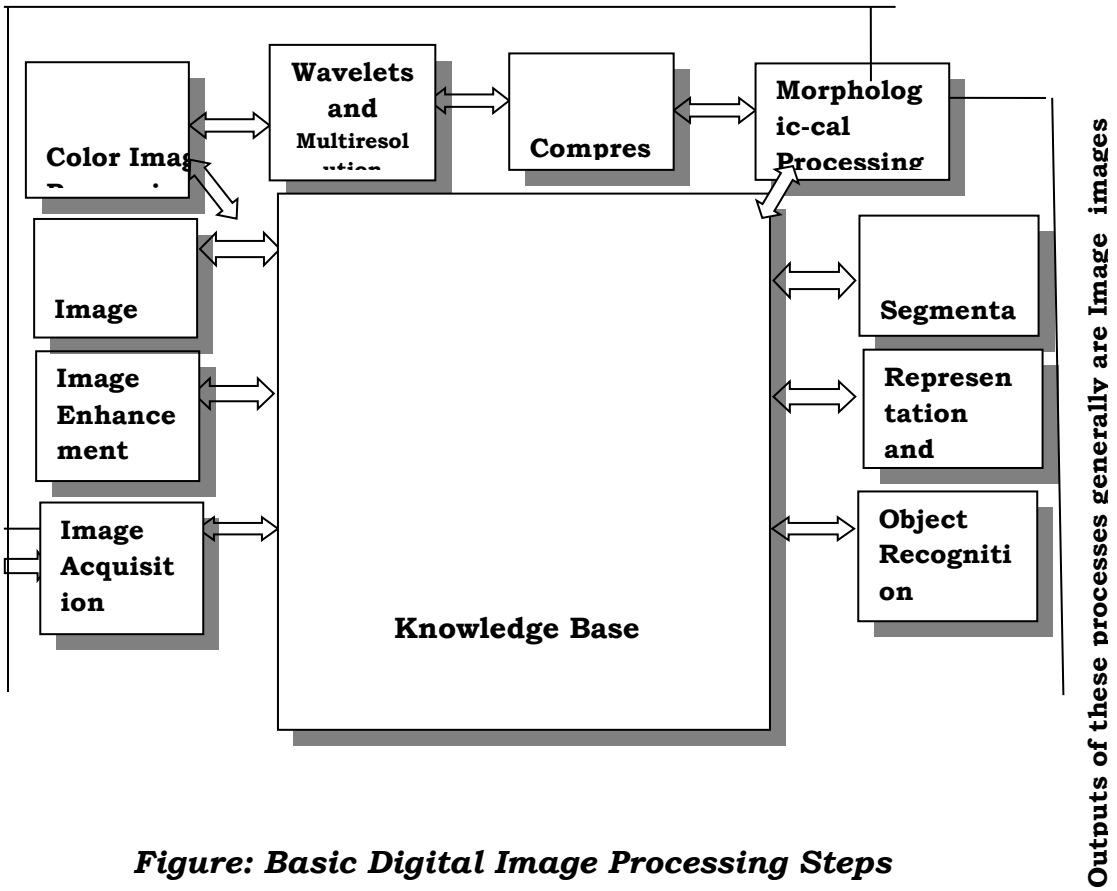


Figure: Basic Digital Image Processing Steps

Digital image processing involves several essential steps that can be applied to images for various purposes, depending on the desired outcomes. These steps include:

1.2.1 Image Acquisition

The process of acquiring an image generally involves preprocessing steps like scaling. A sensor, such as a monochrome or color TV camera, captures the image, which is then transformed into a digital format for further processing.If the sensor or camera produces an analog output, an analog-to-digital converter transforms the data into a digital representation.

1.2.2 Image improvement

Image enhancement is a fundamental and visually appealing aspect of digital image processing. Its main objective is to improve the visibility of important details or highlight specific features within an image. These techniques help in refining image quality, making subtle elements more distinguishable and enhancing overall

clarity for better interpretation.These methods are designed to improve the visual appeal or clarity of an image, making it easier to analyze. Since the effectiveness of enhancement depends on the intended application and user preference, it is considered a highly subjective area of image processing.

1.2.3 ImageRestoration

Image processing enhances the visual quality of an image. However, unlike enhancement, which is a subjective process influenced by personal preferences, image restoration is an objective approach. Restoration techniques rely on mathematical and probabilistic models to correct distortions or degradation in an image, aiming to recover its original form as accurately as possible.

1.2.4 ColorImage Processing

The rapidly expanding use of digital photographs on the Internet is making this field more and more significant.

1.2.5Wavelets

This concept serves as a fundamental approach to representing images at different levels of resolution. Unlike Fourier Transforms, which use sinusoids as their basic functions, the wavelet transform relies on small wave-like functions known as “wavelets.” These wavelets have varying frequencies and are confined to a limited duration, making them well-suited for analyzing both localized and detailed image features.

1.2.6Compression

This process helps minimize the storage space needed to save an image or the bandwidth required for transmission. Most computer users encounter image compression through common file formats, such as the widely used JPG extension, which follows the Joint Photographic Experts Group's (JPEG) compression specification.

1.2.7 The Process of Morphology

These tools are used to extract specific components of an image that are essential for representing and describing its shape. At this stage, the focus shifts from producing an image to identifying and analyzing its key attributes.

1.2.8 Image Segmentation

This process divides an image into its fundamental components or distinct objects. Generally, the higher the precision of the segmentation, the greater the chances of successful recognition.

1.2.9Representation & Description

It determines whether data should be represented using boundaries or entire regions. Boundary representation emphasizes the external shape features, such as edges, corners, and points of curvature. In contrast, region representation highlights internal characteristics, including texture patterns or skeletal structure.

The process of description, also known as feature selection, involves identifying and extracting specific attributes that provide meaningful quantitative information. These attributes play a crucial role in distinguishing different categories of objects and aiding in their classification.

1.2.10 Object Recognition

This process involves identifying an object by assigning it a specific label (such as "vehicle") based on its unique characteristics or features.

1.2.11 Knowledge Base

In an image processing system, information about the specific problem domain is embedded within a knowledge database. This database serves as a structured repository that helps the system interpret, analyze, and process images based on predefined rules and patterns.

1.3 USEOF DIGITAL IMAGE PROCESSING

Applications for digital image processing are numerous and span many different domains, such as microscopy, video communications, remote sensing, astronomy, and medical imaging. The following are some of its primary uses:

Planetary scientists utilize image processing techniques to enhance images of celestial bodies such as Mars and Venus, providing more precise and more detailed visual data for research and exploration. In the medical field, doctors use this technology to process and analyze CAT scans and MRI images, enabling accurate diagnoses and better treatment planning.

One of the earliest uses of digital images involved transmitting digitized newspaper photographs via submarine cables between London and New York. This demonstrated the potential of digital imaging in communication and media.

A centralapplication area for digital image processing is machine perception, where techniques are developed to extract meaningful information from images in a format that computers can process. This involves methods such as statistical analysis, Fourier transform coefficients, and multidimensional distance measurements.

In educational settings, laboratory-based image processing can enhance student engagement and make scientific concepts more relevant to their learning experience. Additionally, in archaeology, image processing helps restore and preserve damaged or blurred historical photographs and artifacts.

Beyond these areas, digital image processing is widely used in fields such as astronomy, geography, biology, defense, and law enforcement. Its ability to enhance, analyze, and interpret images makes it an essential tool in scientific research, security, and various technological advancements.

1.4 TYPES OF NOISE

Real-world images often suffer from random distortions, commonly referred to as noise. This deterioration may depend on or independent of the image content, and it may happen at any point during the image capture, transmission, or processing process. One of the most commonly used models for noise is white noise, which serves as a general approximation of image degradation due to its mathematical simplicity in calculations. A specific type of white noise is Gaussian noise, where the pixel values follow a normal distribution, represented by a Gaussian probability density function.

Quantization noise arises when an image is processed using an insufficient number of quantization levels, leading to a loss of detail and accuracy. Another type of noise, known as impulsive noise, appears as random bright or dark pixels that stand out significantly from their surrounding areas. Salt-and-pepper noise is a type of impulsive noise that affects image clarity and appears as randomly positioned black and white pixels. This type of noise is especially noticeable in binary images, where it disrupts the contrast between black and white regions.

In digital images, each pixel carries information about color composition, typically regarding three primary components: Red, Green, and Blue (RGB). These values determine the final appearance of the image and play a crucial role in processing and correcting noise-related distortions.

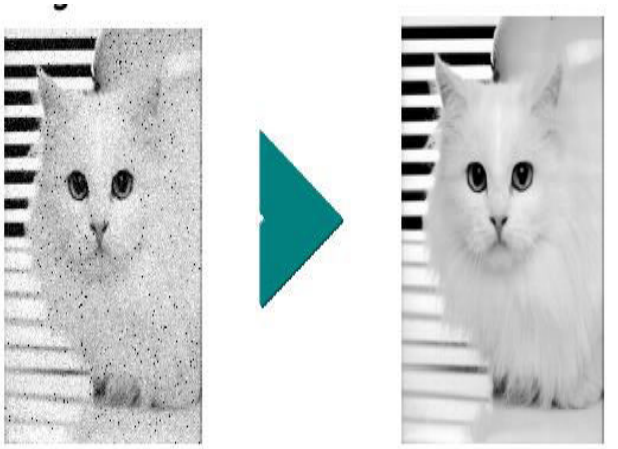
Fig: Image noise

Digital photos, especially those captured by digital cameras, can exhibit discernible noise. It describes the erratic changes in colour or brightness brought on by the internal circuitry and camera sensor. Moreover, the inherent shot noise in an ideal photon detector or film grain can be the source of noise.

In most cases, image noise is considered an unwanted artifact because it reduces the accuracy and clarity of an image. The term "noise" is borrowed from audio terminology, where it signifies unwanted sound; however, in the context of images, it remains visually disruptive rather than audible. Despite being generally undesirable, noise can sometimes be useful in specific applications, such as dithering, where controlled noise is added to improve the visual appearance of images.

Image enhancement is one of the most fundamental and widely used techniques in digital image processing. The primary goal of enhancement methods is to improve an image by revealing hidden details or emphasizing specific features of interest. Since enhancement techniques depend on the intended application and individual preferences, this area of image processing is highly subjective.

Example:



1.4.1 Gaussian Noise

The addition of wideband or white noise with a consistent spectral density (measured in watts per hertz) and an amplitude that follows a Gaussian distribution is the prominent communication disruption in Additive White Gaussian Noise (AWGN), a popular channel model. Factors such as fading, frequency selectivity, interference, nonlinearity, and dispersion are not included in this model. However, it offers a mathematically simple and helpful approach for understanding system behavior before incorporating these complexities.

The thermal motion of atoms in conductors (sometimes referred to as thermal noise or Johnson-Nyquist noise), shot noise, black body radiation from the Earth and other warm objects, and celestial sources like the Sun are some of the natural sources of wideband Gaussian noise. When it comes to describing communication channels in satellite and deep-space broadcasts, the AWGN model works exceptionally well. However, it is not ideal for most terrestrial communication links, which are often affected by multipath propagation, terrain obstructions, and interference. In such cases, AWGN simulates background noise alongside other factors such as multipath effects, terrain-related disruptions, and interference from various sources.

Amplifier noise, another common type of Gaussian noise, is typically additive and independent at each pixel. It is not influenced by signal intensity and is mainly caused by Johnson-Nyquist noise, including reset noise from capacitors, also known as "kTC noise." In digital color cameras, the blue channel often has higher noise levels due to increased amplification compared to the red and green channels. This amplifier noise significantly contributes to "read noise" in image sensors, which affects the uniformity of dark regions in an image.

Gaussian noise is characterized by a probability distribution that follows a normal (Gaussian) distribution. When the noise values at different time intervals are statistically independent and uncorrelated, it is referred to as white Gaussian noise. However, Gaussian noise alone does not imply whiteness; the term "white Gaussian noise" is necessary to specify both the amplitude distribution and the lack of correlation.

In the context of image processing, Gaussian noise causes each pixel's intensity to deviate slightly from its original value. A histogram representing the degree of distortion across different pixel values typically follows a normal distribution. The central limit theorem, which asserts that the total of several independent noise sources tends to approximate a Gaussian distribution, makes Gaussian noise, while there are other kinds of noise distributions, a good model. Although noise between pixels may be correlated or uncorrelated in real-world applications, it is frequently considered to be independently and identically distributed (i.i.d.), which means that the noise variation in each pixel is independent of the noise variations in the others.

1.4.2 Salt and Pepper Noise

Salt and pepper noise, also known as impulsive noise, appears as random black and white specks scattered throughout an image. This type of noise occurs when certain pixels differ significantly in intensity from their neighboring pixels, with no correlation to the surrounding colors. Typically, only a small fraction of the image is affected. The name "salt and pepper" originates from the visual effect of these disturbances, resembling white (salt) and black (pepper) specks on the image.

Common causes of salt-and-pepper noise include dust particles inside a camera lens, faulty or overheated CCD sensors, and transmission errors in digital processing. This noise can also result from analog-to-digital conversion issues or bit errors during data transfer. When present, it creates bright spots in darker areas and dark spots in brighter regions.

To minimize salt and pepper noise, techniques such as dark frame subtraction and pixel interpolation can be used. These methods help detect and correct corruptedpixels, improving image clarity by reducing unwanted disturbances.

Fig: image with salt & pepper noise

Salt and pepper noise is a common type of distortion that appears in images as randomly distributed black and white pixels. This noise often results from sudden interruptions, such as errors in data transmission or faulty sensor switching. To effectively reduce this type of noise, filtering techniques like the median filter or the contra-harmonic mean filter are commonly used. These methods help restore image quality by smoothing out the noise while preserving important details.

1.4.3 Speckle Noise

The overall quality of radar and synthetic aperture radar (SAR) images is decreased by speckle noise, a form of granular distortion that happens naturally. This noise is caused by random fluctuations in the reflected signal from objects smaller than a single image processing unit in conventional radar. In specific regions of an image, it frequently raises the average grey level.

In SAR imaging, speckle noise is more pronounced, making image analysis and interpretation more challenging. The coherent processing of signals reflected from several dispersed targets is what causes this phenomenon. For example, backscattered signals from small-scale surface disturbances, like gravity-capillary ripples, produce speckle noise in SAR oceanography, which distorts the image beneath the fundamental sea wave patterns.

Various techniques have been developed to reduce speckle noise, each relying on different mathematical models. One widely used approach is multi-look processing, which minimizes noise by averaging multiple observations of a target in a single radar sweep. Another method involves filtering, which can be either adaptive or non-adaptive. Adaptive filters adjust their parameters based on local speckle levels, preserving edges and details in high-texture areas like forests or urban

landscapes. Non-adaptive filters, while easier to implement and less computationally demanding, apply uniform filtering across the image, potentially blurring details.

Non-adaptive speckle filters typically rely on either mean-based or median-based calculations within a selected pixel region. Median-based filtering is generally more effective at reducing noise while maintaining edge clarity. There are several adaptive speckle filtering methods, including the Refined Gamma Maximum-A-Posteriori (RGMAP) filter, the Lee filter, and the Frost filter.

These methods operate under three key assumptions:

- Speckle noise is multiplicative, meaning its intensity is proportional to the local gray level.
- The mean and variance of a single pixel correspond to those of its surrounding region.
- The noise and the actual image signal are statistically independent.

The Lee filter transforms the multiplicative noise model into an additive one, simplifying the noise reduction process. It's interesting to note that speckle patterns can occasionally yield helpful information, especially when researching dynamic and laser speckle phenomena, where changes in the pattern over time can indicate surface activity.

Speckle patterns emerge from the interference of multiple wavefronts and have been a subject of scientific investigation since Newton’s era. With the advent of laser technology, speckle effects have gained practical significance in various fields. A typical example is the random pattern seen when a laser beam scatters off a rough surface. Other instances include the distorted view of a star through atmospheric interference, sunlight scattering off a fingernail, and radio waves reflecting off rough surfaces like the ground or ocean. Speckle noise is also present in ultrasonic imaging and optical fiber outputs, where shifting mode velocities or attenuation differences lead to dynamic speckle variations over time.

1.4.4 Shot Noise

In the brighter areas of an image captured by a sensor, the primary source of noise is often due to statistical quantum fluctuations. This variation occurs in the number of photons detected at a specific exposure level and is referred to as photon shot noise. The intensity of shot noise follows a root-mean-square relationship with the square root of the image brightness, and the noise at each pixel is independent of

the others. Shot noise is typically modeled by a Poisson distribution, which in many cases closely resembles a Gaussian distribution.

Beyond photon shot noise, image sensors can also experience additional noise caused by Dark shot noise, often referred to as dark-current shot noise, is the result of dark leakage current. This occurs due to the spontaneous charge generation within the sensor, with "hot pixels" exhibiting the highest dark current levels. To mitigate this, dark frame subtraction can be used to remove the fixed dark charge component, leaving behind only the random noise component. Nevertheless, hot pixels may become more noticeable if dark-frame subtraction is not used or if the exposure duration is prolonged above the sensor's linear charge capacity, resulting in observable salt-and-pepper noise in the finished picture.

1.4.5 Noise from Quantisation (Uniform Noise)

Quantization noise occurs when the continuous pixel values of an image are converted into a limited number of discrete levels during the quantization process. This type of noise generally follows a uniform distribution and may depend on the signal itself. However, if other noise sources are sufficiently strong to introduce dithering, or if dithering is intentionally applied, the noise becomes independent of the signal.

1.4.6 Film Grain Noise

Grain in photographic film is a signal-dependent noise type that is closely associated with shot noise. The resulting pattern of dark grains will be random if the grains in a film are evenly spaced throughout an area and each grain has an independent chance of turning into a dark silver grain when it absorbs photons. In situations where the chance of development is minimal, this randomness closely matches the Poisson distribution, which is typical of shot noise, and it follows a binomial distribution. Nonetheless, as a valid approximation, a Gaussian distribution is frequently employed.

Film grain is generally considered an isotropic noise source, lacking a specific orientation. The randomness is further influenced by the irregular distribution of silver halide grains in the film, which contributes to the overall noise effect.

1.4.7 Anisotropic Noise

Certain types of noise in images exhibit a distinct directional pattern. For instance, image sensors may experience row or column noise, where disturbances

appear consistently along horizontal or vertical lines. In traditional film photography, scratches on the film serve as an example of anisotropic noise, as they follow a specific orientation rather than being randomly distributed across the image.

1.4.8 In Digital Cameras

The image on the left was captured with an exposure time of more than 10 seconds in low-light conditions, while the image on the right was taken with sufficient lighting and a much shorter exposure time of 0.1 seconds. In low-light environments, achieving proper exposure typically requires longer shutter speeds, increased ISO sensitivity (gain), or a combination of both. However, extended exposure times on most cameras can result in increased salt-and-pepper noise due to leakage currents in photodiodes.

One method to reduce this type of noise is dark frame subtraction, which can significantly minimize salt-and-pepper artifacts; however, it comes at the cost of doubling the variance of read noise, resulting in a 41% increase in its standard deviation. Additionally, banding noise similar to shadow noise can appear when shadows are brightened or during color balance adjustments. As exposure time decreases, the impact of both read noise and shot noise becomes more pronounced, requiring higher ISO settings to compensate.

2.1 Altered Fingerprints: Analysis And Detection

The extensive use of Automated Fingerprint Identification Systems (AFIS) in law enforcement and border security has emphasized the importance of safeguarding these systems from potential threats. While various security concerns, such as identity fraud using fake fingerprints, have been explored, the issue of fingerprint modification or distortion has received limited attention. Fingerprint obfuscation involves the intentional alteration of fingerprint patterns to conceal an individual's identity. Numerous cases of such modifications have been documented in media reports. Traditional fingerprint quality assessment tools, such as NFIQ, may

not always identify altered fingerprints, as the quality of the image might not be significantly affected by these changes. This study contributes to the field by: (1) compiling case studies of individuals who have altered their fingerprints to bypass AFIS, (2) analyzing how fingerprint alterations affect the accuracy of commercial fingerprint matching systems, (3) categorizing fingerprint modifications into three main types and proposing countermeasures, (4) developing an automated technique for detecting altered fingerprints by examining orientation fields and minutiae distribution, and (5) assessing the effectiveness of the proposed method alongside the NFIQ algorithm using a comprehensive database of altered fingerprints obtained from a law enforcement agency. Experimental findings demonstrate the viability of the proposed approach in identifying fingerprint alterations and underscore the need for further research in this area.

Index Terms—Fingerprints, AFIS, obfuscation, alteration, ridge pattern, minutiae distribution, imagequality, fingerprintness.

INTRODUCTION:

Law enforcement agencies have successfully used fingerprint recognitionto identify suspects and victims foralmost 100years.Recentadvances in automated fingerprint identification technology,coupled withthe growing need for reliable person identification,have resulted in an increased use of fingerprints in both government and civilian applications such as border control, employment background checks,andsecurefacility access[2].The FBI's IAFIS service [4] and the US-VISIT's IDENT program [3] are two instances of extensive fingerprint systems in the US government sphere.

Because fingerprint identification technology is so successful at correctly identifying people, some people have taken drastic steps to get around these systems. The main goal of fingerprint alteration [5] is to avoid detection by employing methods that range from plastic surgery to abrading, chopping, and burning fingertips (see Fig. 1). The employment of fake fingerprints to conceal one's identity is a major "attack" on a border control biometric system since it negates the technology's primary function, which is to enable the identification of people on a watch list.

Note that phoney fingerprints are not the same as changed fingerprints. One widely known way to get around fingerprint systems is to create fake fingers, which

can be manufactured of silicone, adhesive, or latex. However, altered fingerprints are actual fingers that are used to hide one's identity so that a biometric system cannot identify them. Alternated fingers are used to conceal one's own identity, whilst fake fingers are usually employed to assume the identity of another person. Numerous hardware [11] and software [10] solutions have been put forth to identify attacks based on fake fingers. Nevertheless, the issue of changed fingerprints has not yet been examined in the literature, and no methods for identifying them have been documented. Moreover, research in this field has been hindered by the absence of accessible databases containing changed fingerprint scans. Highlighting the significance of the issue, analysing changed fingerprints, and suggesting an automatic detection strategy for them are some of the objectives of this research.

The problem with the changed fingerprints discussed above is part of a larger class of attacks called biometric obfuscation.

Obfuscation is the intentional attempt by a person to conceal his identify from a biometric system by changing the biometric characteristic before the system has it. Examples include employing abrasive material to mutilate the ridges on one's fingerprint, wearing theatrical lenses to change the texture of the eye, or undergoing surgery to change facial features like the nose and lips. For the following reasons, we shall focus on the issue of fingerprint obfuscation in this study: 1) Compared to other biometric modalities, fingerprint-based biometric systems are far more common for large-scale identification;2) Unlike, say, one's iris or face, where a more involved surgical procedure might be required, it is relatively easy to alter one's fingerprints using chemicals and abrasives; and 3) law enforcement and immigration officials frequently come across mutilated fingerprints in a number of countries, which emphasises how urgent it is to find a solution to this issue.

The first step in identifying fingerprint alteration is creating an automated method to identify changed fingerprints. If the accompanying photos are in fact of low quality, fingerprint quality assessment procedures that are employed in the majority of fingerprint recognition systems, such as the open source NFIQ (NIST Fingerprint Image Quality) software [12], may be helpful in identifying altered fingerprints. However, as seen in Figs. 10 and 11, not all photos of changed fingerprints are of low quality. Existing algorithms for evaluating fingerprint quality [13] are restricted in their ability to identify whether an image is a natural fingerprint or an altered fingerprint since they are made to determine whether an image contains

enough information (such as minutiae) for matching.For instance, the NFIQ score indicates that the synthesised ridge pattern in Fig. 2 is of the highest quality, despite the fact that it is unlikely to be found on fingertips. The automatic detector needs to meet the following three criteria since the changed fingerprints are probably going to be found in extensive national identity or border control systems:

1. The method needs to be incredibly quick due to the high throughput requirements of these systems. Stated differently, it shouldn't significantly raise the matcher's computational load. Approximately one million fingerprint matches may be processed every second by the most advanced Automated Fingerprint Identification Systems (AFIS). This suggests that the decision logic and feature extraction process used to automatically identify changed fingerprints must be straightforward.

2. There would be very few people with changed fingerprints that AFIS will come across in operating circumstances. In light of this, the modified fingerprint detection method ought to function at a very low false positive rate, perhaps 1% or less. A secondary inspection stage will be used to subjects who are suspected of having changed fingerprints.

3. Any AFIS should be able to incorporate the modified fingerprint detector with ease. 1. According to NFIQ, there are five different quality levels, with 1 denoting the highest quality. The remainder of the document is structured as follows: Some of the situations where law enforcement agencies have come across altered fingerprints are listed in Section 2. Three distinct types of altered fingerprints and possible countermeasures are presented in Section 3, which also looks into how fingerprint alteration affects matching performance. Section 4 presents the suggested method for identifying changed fingerprints, and Section 5 assesses it. Section 6 concludes by suggesting potential lines of inquiry for this subject.

2.2 BACKGROUND

Fingerprint modification has a lengthy history. In 1933, it was found that murderer and bank robber Gus Winkler had cut and ripped the flesh of his fingers, altering the fingerprints of his left hand except for the thumb [5]. Furthermore, the pattern type of one finger was switched from double loop to left loop (see Fig. 3a). A man called Alexander Guzman was apprehended by Florida authorities in 1995 for possessing a forged passport; more recently, concealed fingerprints were found on him (see Fig. 3b).

Following a two-week search that involved painstakingly reconstructing the damaged fingerprints and looking through the 71 million records in the FBI database, Alexander Guzman's recreated fingerprints were connected to those of drug-related absconding criminal Jose Izquierdo [15]. Three steps were involved in his fingerprint mutilation procedure: cutting a "Z" form on the fingertip, moving two triangle skin patches, and sewing them back. A cocaine dealer called Marc George was arrested in September 2005 after border officers saw that he was limping after surgery (see Fig. 1a) [16].

Fingerprints have been found to be altered by someone other than criminals. A woman managed to avoid the Japanese immigration AFIS in December 2009 by

Figure 3: Inked impressions before and after fingerprint alteration (a) of Jose Izquierdo [15] (by switching two parts of a “Z” shaped cut on the fingertip) and (b) of Gus Winkler [5] (pattern type is changed from double loop to left loop). Her left and right hands' fingerprints were surgically switched [21].Although shewasoriginally arrested forfaking amarriage license, scars onher hands made thepolicesuspicious.It has even been possible to modify fingerprints on a much wider scale using a group of people. According to reports from EURODAC [23], a fingerprint system used throughout the European Union to identify asylum seekers, hundreds of asylum seekers have burned, abraded, and sliced their fingertips to avoid recognition [19], [20].

Fingerprint modification cases that have been documented are listed in Table 1. It is highly impossible to quantify the precise number of people who have successfully escaped recognition by biometric systems due to fingerprint alteration, even while the number of examples with altered fingerprints that have been made public is not very high. Nearly all of the individuals who were found to have changed their fingerprints were found in some other way other than by AFIS [16], [21].

2.3 Analysis of Alteredfingerprints

Using a database of altered fingerprints that we were given by a law

enforcement agency, we first 1) determine how fingerprint alteration affects matching performance, 2) categorise altered fingerprints into three types (obliteration, distortion, and imitation; see Figs. 9, 10, and 11), and 3) assess the value of an existing fingerprint quality measure in terms of altered fingerprint detection.

2.3.1 Database

The database contains 4,433 altered fingerprints from 535 ten-print cards that belong to 270 individuals. It's possible that not every instance of the ten fingers on a ten print card was altered. Figure 4 displays the distribution of the number of altered fingers on a card.the ten print cards, five out of ten had all ten fingerprints altered, and eighty-five percent had more than five altered fingerprints. Ten print cards range from one to sixteen for each subject; 87 of the 270 subjects have more than one ten print card because of multiple arrests. Pre-altered (natural) and post-altered fingerprint pairs total 1,335 for subjects with more than ten print cards. An example of 10 print cards of a topic that have been edited both before and after is displayed in Fig. 5. 3.2 The fingerprint identification systems' weakness.

Since fingerprint tampering undermines the core tenet that a person's fingerprints remain consistent throughout their lifespan, it poses a severe threat to AFIS. We compared 1,335 altered fingerprints to their corresponding pre-altered fingerprints using a commercial matcher, VeriFinger SDK 4.2 [24], in order to determine how susceptible AFIS is to fingerprint manipulation. The VeriFinger SDK was utilised to obtain genuine and impostor match score distributions in order to create a baseline utilising the NIST SD4 database [25], which comprises 2,000 fingers with two impressions per finger.
The score distributions for authentic and imposter matches in NIST SD4 as well as pre/post-altered fingerprint pair matches by type are displayed in Fig. 6. Here, the salient observations are: For every method of manipulation, the pre/post-altered fingerprint pair match score distributions resemble the imposter score distribution. As seen in our database, fingerprint alteration is not always effective in avoiding AFIS, as indicated by heavy tails in pre/post-altered match score distributions.

The genuine match scores of 83% of the pre/post-altered fingerprint pairs fell below the 41 threshold, corresponding to a 0% False Acceptance Rate (FAR) on NIST SD4. This indicates that most changed fingerprints cannot be connected to their real partners using AFIS. Examples of how changing a fingerprint prevents it from

matching its real mate are shown in Fig. 7. The ridge structure is destroyed during the fingerprint mutilation process, making it impossible to retrieve minutiae in this region (Fig. 7a). Furthermore, the spatial distribution of the minutiae is changed by extreme ridge distortion, such as ridge structure alteration (Fig. 7b) or ridge deformation brought on by scars.

The efficacy of fingerprint modification in avoiding AFIS is not guaranteed (see Fig. 8). As long as 3. It should be noted that although the analysis is based on a particular fingerprint matcher, the outcomes of fingerprint change will probably have a comparable impact on all commercial matchers. The ridge pattern, which the criminals attempt to alter through fingerprint tampering, is used for matching by VeriFinger and other cutting-edge fingerprint matchers. Pre/post changed fingerprint mates can be successfully matched since there are enough details that can be recovered in the unaffected area.

2.3.3 Types of Altered Fingerprints

Based on the modifications made to the ridge pattern, we divide fingerprints into three groups. This classification will help us in the ways listed below: 1) Gaining a deeper knowledge of the types of changes that may occur, 2) identifying modified fingerprints by simulating distinct subcategories, and 3) developing methods for repairing altered fingerprints.

The exclusive classification of 4,433 mutated fingerprints in our database is displayed in Table 2. It should be noted that this classification is subjective and based on our analysis of the ridge patterns in a significant number of altered fingerprint photos in the database; it is not based on the alteration technique, which we do not know.

2.3.3.1 Obliteration

The patterns of friction ridges on fingertips can be destroyed by abrading [26], cutting [5], burning [18], [19], [20], [27], applying powerful chemicals (Fig. 1c), and transplanting smooth skin [16]. Fingerprints can also be erased by additional causes such skin conditions like leprosy [28] and adverse chemical reactions from cancer treatments [29]. The structure of the friction ridge is hardly discernible inside the destroyed area. Table 2 shows that the most common type of modification is obliteration.

This can be due to the fact that obliteration, which totally eliminates ridge structures, is far easier to do than distortion/imitation, which necessitates surgery. Furthermore, erased fingerprints are far easier for human examiners to detect than altered or mimicked fingerprints.

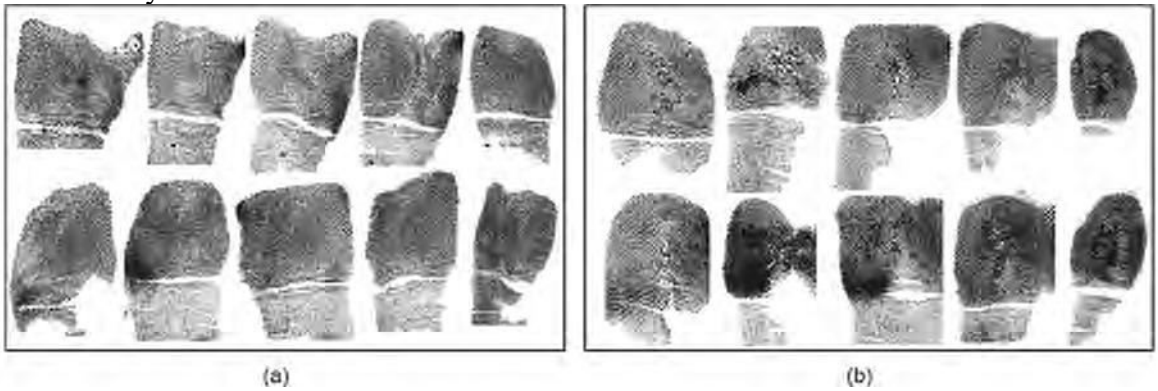
Depending on the extent of the damage, obliterated fingerprints may avoid detection by fingerprint quality control software. Although AFIS is likely to successfully match the damaged fingerprint to the original mated fingerprint (Fig. 8a), if the affected finger area is small, the current fingerprint quality assessment software might not identify it as altered (the fingerprint in Fig. 9a has an acceptable NFIQ value of 3). However, fingerprint quality control tools may easily identify the damage if the altered area is large enough. The erased fingerprint in Figure 9b, for instance, has the lowest NFIQ score, which is 5.

Treating fingerprints as latent images, performing AFIS search with manually indicated features, and implementing a suitable fusion strategy for 10 print searches may be required to identify people whose fingerprints are completely obliterated [30]. Rarely does the dermal papillary surface exhibit the same pattern as the epidermal. The pattern may be used for identification even if the surface of the finger is completely injured [31].

2.3.3.2 Distortion

In order to create abnormal ridge patterns on fingertips, parts of the skin on the fingertip can be removed and either grafted back in different locations (Fig. 10a) or replaced with friction ridge skin from the palm or sole (Fig. 10b). Unusual ridge patterns that are absent from natural fingerprints can be seen in distorted fingerprints. These anomalies include sudden shifts in the orientation field along the scars or an irregular spatial distribution of singular points.

Keep in mind that natural fingerprints typically only exhibit orientation field discontinuity at isolated locations.



(a) (b)

Fig.5.Mated pre/post-altered tenprint cards fromasubject. (a)Pre-altered fingerprints. (b)Post-altered fingerprints.

Because their global ridge pattern is irregular but their local ridge structure is still close to that of actual fingerprints, distorted fingerprints can also pass the fingerprint quality test. For example, when skin patches inside a finger are swapped, the resulting distorted fingerprint (Fig. 10a) maintains the same ridge attribute (e.g., ridge frequency and width) across the fingerprint area. The maximum quality level, NFIQ of 1, is given to Fig. 10a. Similarly, NFIQ ¼ 2, the second-highest quality level, is applied to the modified fingerprint in Fig. 10b.

Fingerprints altered via a "Z" cut are especially intriguing since they allow for reconstructing the original fingerprint before alteration, preserving the original ridge structure. The fingerprint quality control software that is currently in use has to be updated to detect the deformed fingerprints. Following identification, AFIS may profit from the following measures: After 1) determining the fingerprint's unaffected regions and manually noting the features (i.e., the minutiae) in these regions, recreate the original fingerprint as in the "Z" cut case [15].

2.3.3.3 Imitation

Even after a complex fingerprint altering process, the friction ridge patterns on fingertips can retain their fingerprint-like appearance: 1) The skin is pulled and sewn back together after a section of it is removed (Fig. 1a, 2) The entire fingertip is
90
transplanted, or 2) the excised portion is filled with friction ridge skin from other body areas to match the remaining ridge structure (Fig. 11b). According to [21], AFIS could be avoided by simply switching the skin on the fingertips of the left and right hands.

In addition to passing the fingerprint quality evaluation tools, fake fingerprints can also fool human examiners. Pre- and post-altered fingerprint mates are displayed in Fig. 11. The only indication of a potential change is a tiny scar. The modified fingerprint in Fig. 11a appears to be an arch-type fingerprint due to its extremely smooth orientation field across the whole fingerprint region. This fingerprint has the highest value, with an NFIQ of 1. Its pre-altered partner is, in fact, of the right loop type, but the match score between these two fingerprints is only 19.

Remember that 41 was the match score criterion corresponding to the matcher's 0% FAR. A remarkable surgical technique was employed to alter the

fingerprint shown in Fig. 11b, resulting in a pattern with a highly natural ridge flow, even across the surgical scars. This fingerprint exhibits the highest NFIQ value of 1 and has a match score of only 28 when comparing the pre- and post-modification fingerprint pairs.To accurately match the altered fingerprints in Fig. 11, it is crucial to develop algorithms capable of handling distortions and inconsistencies. When fingerprints from different fingers are interchanged, matching without relying on finger position, such as allowing a left thumbprint to be compared with a right index finger, could aid in uncovering a person's true identity, though it would significantly increase the matching time.

2.3.4 Effectiveness of Fingerprint Quality Assessment Algorithm

The NFIQ program [12],recognized as the de facto standard for fingerprint quality assessment, was utilized to evaluate the quality of both altered and natural fingerprints. This analysis aimed to determine the effectiveness of widely used fingerprint quality control software in identifying altered fingerprints.We used the 27,000 fingerprints in NIST SD14 to build a database of natural fingerprints [33]. We can see from the NFIQ value histograms for natural and modified fingerprints in Fig. 12 that:

Examples of fingerprint alteration significantly lowering the matching score with the pre-altered mates are shown in Fig. 7. (a) Mutilation across a vast region. (b) The transformation of the ridge. The match score between these fake fingerprints and their real mates is zero. Red-filled squares show matching minutiae between the pre- and post-altered fingerprints, while all squares show minutiae taken from the image.

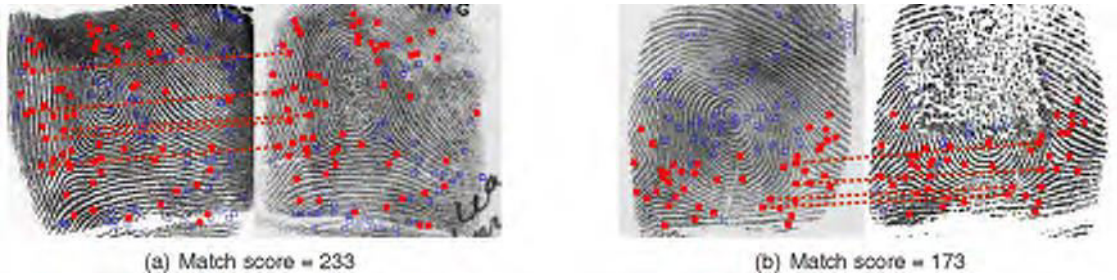


Figure 8 presents examples where fingerprint mates remain correctly matched despite fingerprint alterations. These cases demonstrate the robustness of the matching process, ensuring accurate identification even when modifications occur.(a) Change with no ridge distortion and a tiny damaged area. (a) Despite significant fingerprint alteration, there are enough details in the unchanged area. Dotted lines only link a small number of comparable minutiae.

1. Only a small fraction of natural fingerprints have the lowest quality level of 5, however a large number of changed fingerprints do. Specifically, the largest amount of the obliterated finger prints is at the NFIQ level of 5. On the other hand, the portion of the distorted and copied fingerprints at level 5 is rather minor.

2. Many altered fingerprints have good quality; a considerable percentage of deformed and copied fingerprints have the highest quality level, and approximately 7% of altered fingerprints have the highest quality level of 1 overall.

3. A true result will be obtained if the NFIQ value of 5 is applied as a criterion for identifying altered fingerprints.

Fig.9.Fingerprint obliteration. Examples of(a)scar and (b)mutilation.

Figure 10. Distortion of fingerprints. Examples of (a) transplantation from another friction ridge skin, such as the palm, and (b) transplantation from within a finger via "Z" cut.

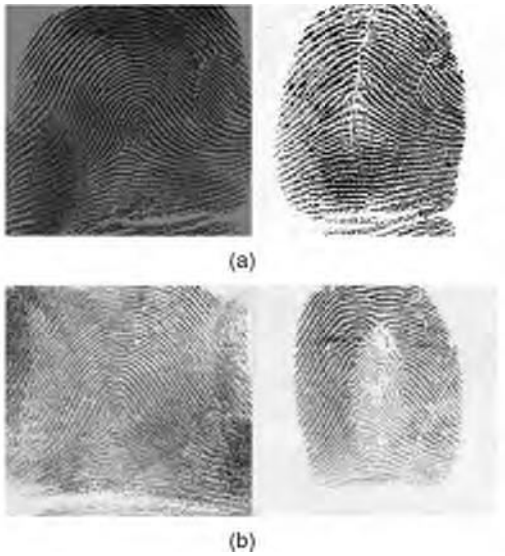
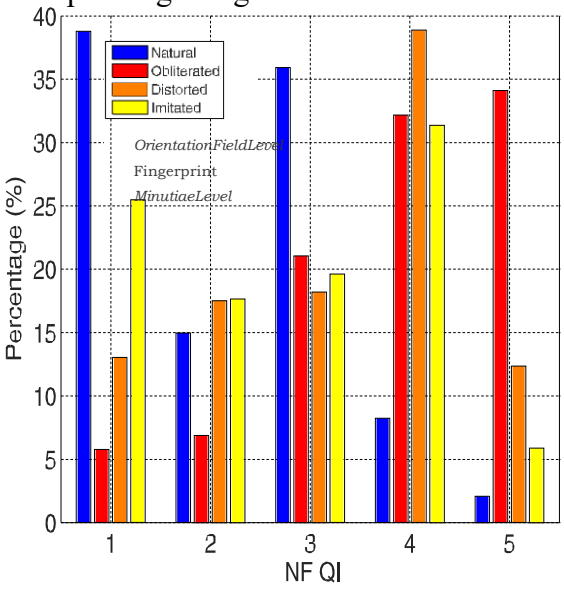


Figure 11. Imitation of fingerprints. Its pre-altered fingerprint is on the left, while its post-altered fingerprint is on the right. (a) Excision of a section of skin. (b) Beautiful transplanting using skin from another friction ridge.



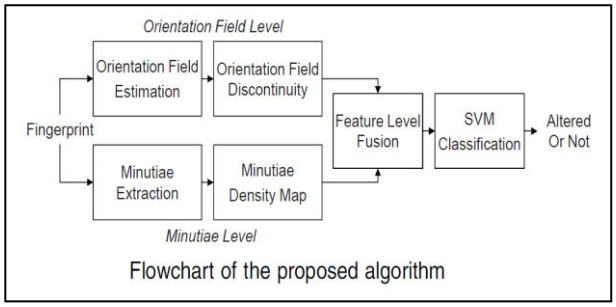


Figure 12 shows the histograms of NFIQ values for 4,433 altered fingerprints in our database based on the type of alteration and 27,000 natural fingerprints in NIST SD14. Remember that the best quality is indicated by NFIQ ¼ 1. A false positive rate of 2.1 percent occurs when a natural fingerprint is mistakenly identified as an altered fingerprint, whereas a positive rate of 31.6 percent occurs when an altered fingerprint is successfully classified as such.

2.4 Automatic Alteration Fingerprint Detection

We shown in the preceding section that the NFIQ algorithm is not appropriate for identifying altered fingerprints, particularly those that are imitation and distortion.

In actuality, any fingerprint image quality evaluation method that relies on evaluating local picture quality finds it extremely difficult to identify distorted and copied fingerprints. This section examines the issue of automatically detecting changes by examining the minutiae distribution and ridge orientation field. Fig. 13 shows the suggested alteration detector's flowchart.

2.4.1 Analysis of Orientation Field

The orientation field describes the ridge flow of fingerprints and is defined as the local ridge orientation in the range ½0; Þ. High-quality fingerprints have a smooth orientation field, except for regions near the unique points (such as the core and delta). Many orientation field models have been developed as a result of this property, combining the global orientation field model for the continuous flow field of the fingerprint with the local orientation field model around the single spots [34], [35], and [36]. The global orientation field model represents either.

1. Normalisation. The NIST Biometric Image Software (NBIS) is used to normalise an input fingerprint picture to 512x480 pixels by cropping a rectangular portion of the fingerprint that is centred on the fingerprint and aligned along the longitudinal direction of the finger [37]. This stage makes sure that the features that are extracted in the next stages are unaffected by the finger's translation and rotation.

2. Estimation of orientation fields. The gradient-based approach is used to calculate the fingerprint's orientation field, ðx; yÞ [38]. A 16x16 averaging filter is used to smooth the initial orientation field, and then the orientations are averaged in 8x8 pixel blocks. The dynamic range of grey values in local blocks of the fingerprint image is measured to create a foreground mask, and morphological procedures are carried out to fill in the gaps and eliminate isolated blocks.

3.Orientation field approximation. The orientation fieldðx;yÞisapproximated byapolynomial model toobtain^x;yÞ.

4.Feature extraction.The error map, "ðx;yÞ, is computed astheabsolute differencebetweenðx;yÞand^x;yÞand used toconstruct thefeature vector.More details ofSteps 3and 4aregiven below.

2.4.1.1 Orientation Field Approximation

A collection of polynomial functions is utilised to represent the global orientation field; this approach is both computationally efficient and offers a good approximation for orientation field modelling. Let the orientation field be

represented by ðx; yÞ. Then, polynomials of order n can be used to represent the cosine and sine components of the twofold orientation at ðx; yÞ:

$$g_c^n(x,y) \triangleq \sin 2\theta(x,y) - \sum_{i=0}^{n}\sum_{j=0}^{i} a_{i,j}x^i y^{i-j}$$

$$g_s^n(x,y) \triangleq \cos 2\theta(x,y) - \sum_{i=0}^{n}\sum_{j=0}^{i} b_{i,j}x^i y^{i-j}$$

where the polynomial coefficients for$g_c^n(x,y)$ and $g_s^n(x,y)$are denoted by ai;j and bi;j, respectively. The model's ability to depict sudden changes in the orientation field improves with the polynomials' order. The orientation field that the models approximate differs significantly from the actual orientation field when the polynomial model's order is too low. It is not necessary for the polynomial model to have a particularly high order, though, as models with an order of six or higher do not significantly alter the fitting outcomes. Therefore, we choose 6 (n ¼ 6) as the polynomial model's order. The least squares approach can be used to estimate the polynomial coefficients ai;j and bi;j using the orientation field _ðx; yÞ that was acquired in Step 2.

To keep things simple, we use matrix form to describe (1) and (2):

$$g_c(x,y) - x^t a, g_s(x,y) - x^t b$$

Where $x - [i, x, y, x^2, xy, y^2 \ldots\ldots x^n \ldots\ldots y^n]^T$, a and b are the corresponding vectors. One way to formulate the estimation problem for a and b is as

where $g_{c-}\begin{bmatrix} g_c(x1,y1) \\ g_c(x2,y2) \\ . \\ . \\ g_c(xn,yn) \end{bmatrix}, g_{s-}\begin{bmatrix} g_s(x1,y1) \\ g_s(x2,y2) \\ . \\ . \\ g_s(xn,yn) \end{bmatrix}$ and $x\text{-}\begin{bmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_n^T \end{bmatrix}$

Finally, the orientation field is approximated by the polynomial model.

$$\hat{\theta}(x,y) - 1/2\tan^{-1}(\hat{g_s}(x,y)/\hat{g_c}(x,y))$$

Where $g_c(x,y) - x^t a, g_s(x,y) - x^t b$.

3.1 Feature Extraction

A low-order polynomial model effectively captures smooth, global variations in the orientation field but struggles to represent sudden changes in localized areas, such as fingerprint cores and deltas. In altered fingerprint regions, including severely scarred (Fig. 9a), mutilated (Fig. 9b), and deformed ridge areas (Figs. 10a and 10b), ridge flow patterns can become irregular. The difference between the estimated and actual orientation fields helps identify the position and extent of abrupt ridge flow changes. After eliminating two columns from the edges of the erroneous map, 60 blocks remain.

Local geographic region histograms form the feature vector derived from the error map [39]. The error map consists of a 3×3 grid, where each cell measures 20×20 blocks. Within each cell, the histogram of the error map is computed using 21 bins spanning the range [0,1]. The final feature vector, which has 189 dimensions, is obtained by summing the histograms from all nine cells. Here, T represents a predefined threshold. Figure 15 illustrates the fine-grained density maps of three modified and natural fingerprints.The minutiae in a natural fingerprint are evenly spaced and scattered. However, the minutiae distributions in the modified fingerprints are very different; 1) Because of ridge discontinuity, a large number of bogus minutiae are extracted along scars and in the erased region; 2) When a new ridge-like pattern is generated after alteration, an excessive number of minutiae arise. These illustrations show how the distribution of minutiae can help identify tampered fingerprints.

The feature vector is generated from the minutiae density map using local histograms within 3×3 cells. Subsequently, the histograms from each cell are merged to integrate feature vectors derived from both the minutiae density map and the orientation field discontinuity map. These combined features are then utilized as input for a support vector machine (SVM) to perform classification.

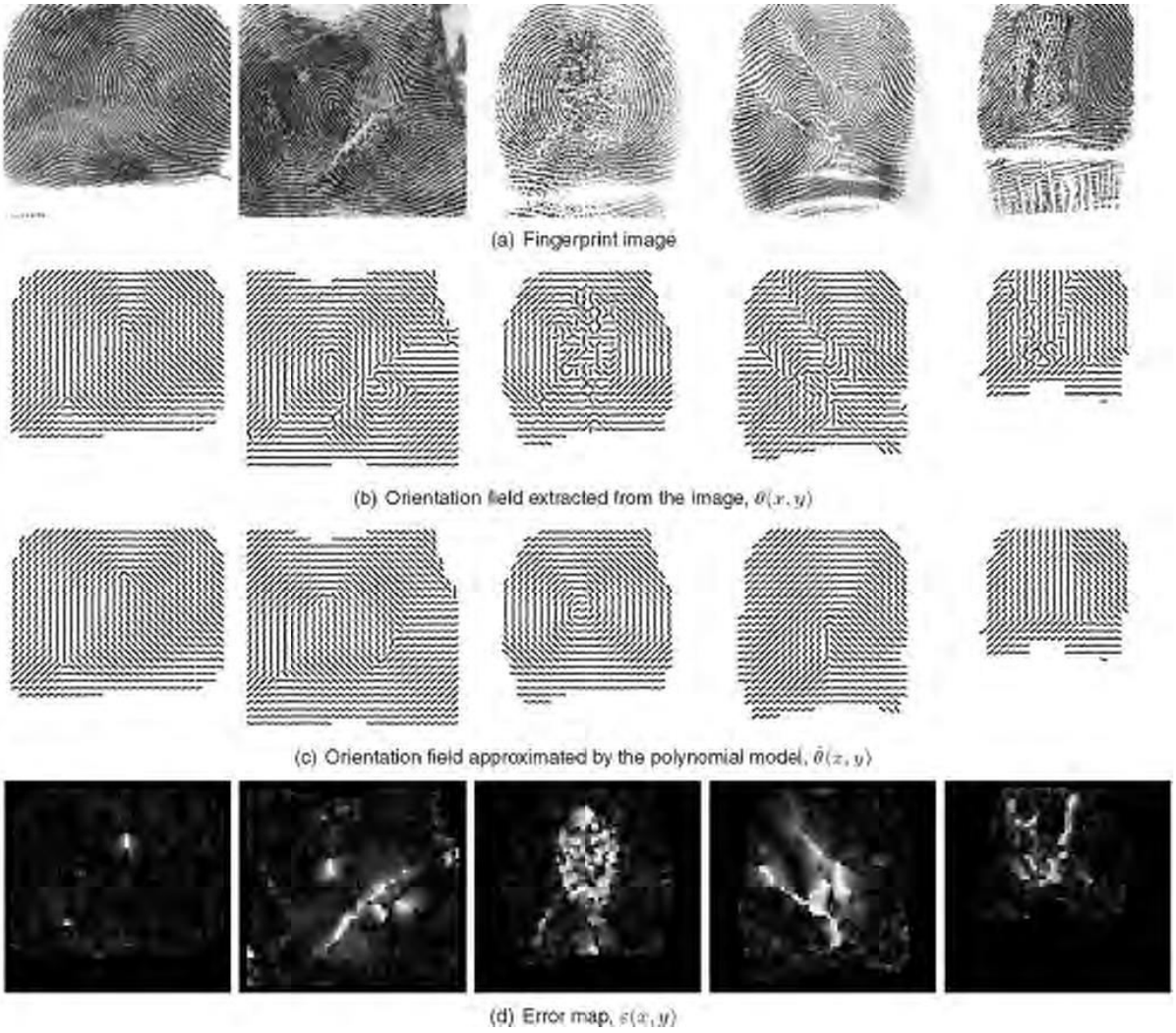
3.2 Minutiae Distribution Analysis

A minutia in a fingerprint represents specific ridge features, such as ridge endings or bifurcations. Nearly all fingerprint recognition systems rely on minutiae for matching. Besides the irregularities observed in the orientation field, it has been noted that the minutiae distribution in altered fingerprints often deviates from that of natural fingerprints. Utilizing minutiae extracted through the open-source minutiae

extractor in NBIS, a density map of the minutiae is generated using the Parzen window method along with the corresponding coefficient vectors.It is possible to formulate the problem of estimating a and b as a uniform kernel function. Let Sm represent the fingerprint's minutiae, or the location of the minutiae: The minutiae density map from Sm is then calculated in the manner described below: A 30x30 pixel Gaussian filter with a 10 pixel standard deviation smoothes low-pass filtering.

4 Experiments

Two levels of evaluation were used for the suggested algorithm: We evaluate fingerprint differentiation at both the individual finger level and the subject level, which includes all ten fingers. At the finger level, we examine the capability to distinguish between unaltered and modified fingerprints. At the subject level, we analyze the ability to differentiate individuals with natural fingerprints from those whose fingerprints have been altered.



(a) Fingerprint image

(b) Orientation field extracted from the image, $\theta(x, y)$

(c) Orientation field approximated by the polynomial model, $\tilde{\theta}(x, y)$

(d) Error map, $e(x, y)$

Fig.14.Orientation fielddiscontinuity. Column1:Natural fingerprint(NISTSD14, F0000001). Scarred fingerprint (Column 2). Column 3: Fingerprint mutated. Column 4: "Z" cut-distorted fingerprint. Column 5: A fingerprint that has been distorted through transplantation from another friction ridge skin.

The subject level performance makes use of this application domain information because the majority of AIFS used in border control, national ID, and law enforcement applications process each of a person's ten fingerprints.

4.1 finger-Level Evaluation

The modified fingerprint database we have access to contains 4,433 fingerprints from 535 ten print cards. To build a non-altered fingerprint database, we use 27,000 fingerprints from the 2,700 ten print cards in the NIST SD14 database [33].Each finger in this database has two impressions, referred to as file and search; our tests employ the file impression.

10-fold cross-validation is employed for classification using LIBSVM [40] with a radial basis kernel function. The LIBSVM scores are linearly scaled to fall between ½0 and 1. The normalised score is referred to as an indicator of the input fingerprint's fingerprintness. The system sounds an alert to suggest that an input image may be a manipulated fingerprint when its fingerprintness falls below a preset threshold value. This image is considered a true positive if it is, in fact, a changed finger print; if not, it is considered a false positive. In the same way, a genuine negative means that a natural fingerprint is appropriately identified as such, while a false negative means that an altered fingerprint is not identified as such.

The Receiver Operating Characteristic (ROC) curves for the NFIQ software and the recommended technique for detecting altered fingerprints are displayed in Figure 16. In NIST SD14, natural fingerprints with an NFIQ value of 5 are classified as altered fingerprints, resulting in a false positive rate of 2.1 percent and a true positive rate of 70.2%, although the NFIQ's true positive rate is only 31.6 percent. Fig. 16a shows the ROC curves of the NFIQ algorithm and three techniques for detecting altered fingerprints: minutiae distribution, orientation field discontinuity, and their feature level fusion. Fig. 16b shows the ROC curves for the NFIQ algorithm and the proposed fusion algorithm by modification type. While NFIQ can only detect bliterated fingerprints, the suggested approach can detect both obliterated and warped fingerprints with comparable accuracy.

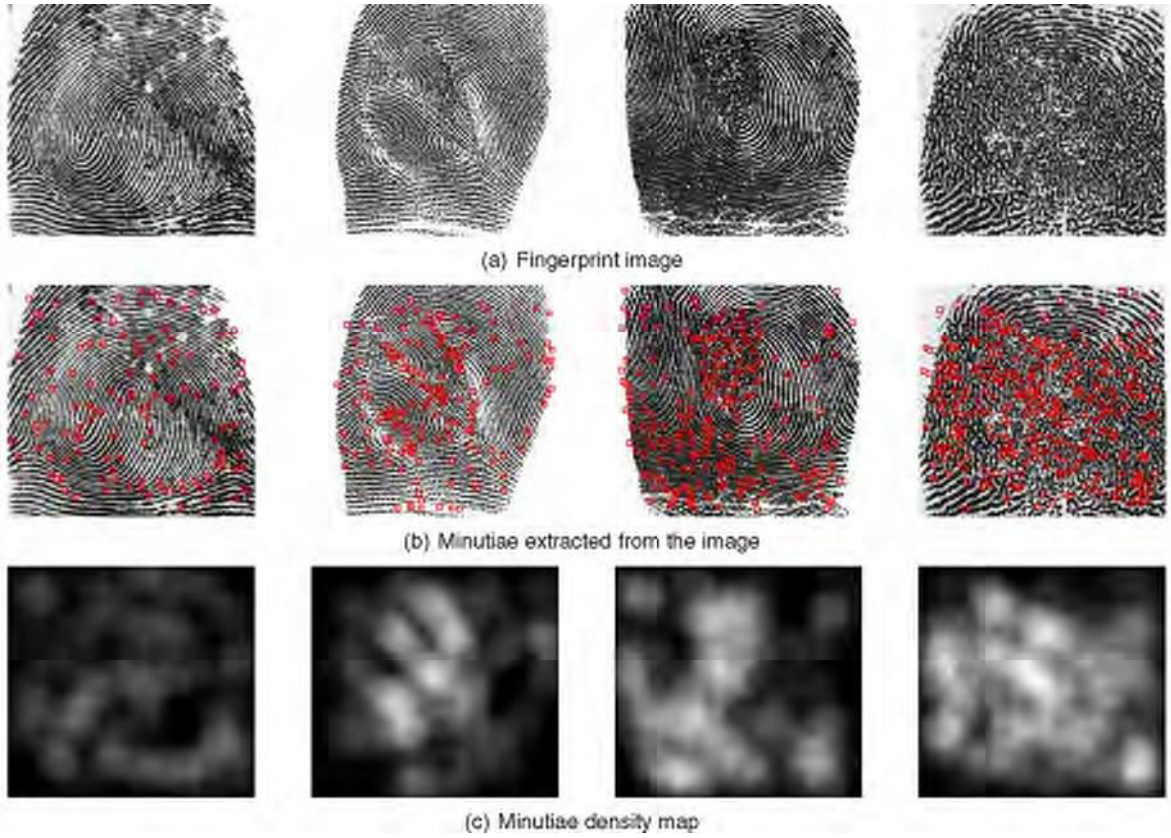


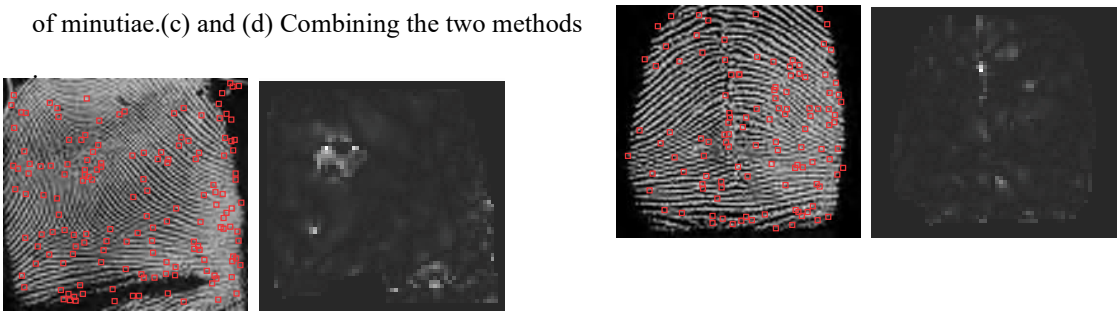
Figure 15. Map of minutiae density. Column 1: Natural fingerprint (F0001826, NIST SD14). Column 2: Deformed fingerprint with intricate details surrounding scars. Column 3: The revised area's obliterated fingerprint with a dense dispersion of minutiae. Column 4: The ridge-like pattern created by the change resulted in an obliterated fingerprint with extensive minutiae dispersed over the whole affected area. Take note that the same greyscale range is used for the minutiae density maps.

However, both algorithms struggle with fingerprint impersonation. With a false positive rate of 1% and a threshold value of 0.60 for the fingerprintness score, 270 of the 27,000 fingerprints in NIST SD14 would be mistakenly classified as altered fingerprints. Fig. 17 shows instances of correctly detected changes using the proposed method, even if the NFIQ measure indicates that the quality level of these images is acceptable.

Notallofthealtered fingerprints canbedetected bytheproposed algorithm. Ifthealtered areaistoosmall(Fig.18a), the evidence of alteration is difficult to detect. Even at the edge of the modified area, the ridge structure in the replica example is quite natural;There is a negligible anomaly in the minutiae density along scars, and the orientation field is continuous (Fig. 18b).

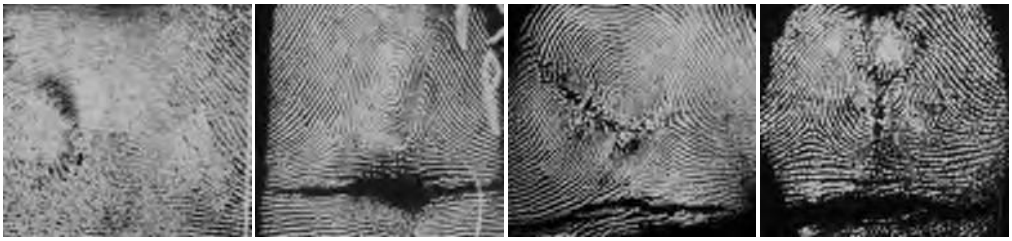
The ROC curves for the recommended algorithm and the NFIQ criterion for detecting fingerprint changes are displayed in Figure 16. (a) The ROC curves for the three approaches in the NFIQ algorithm and the recommended algorithm. (b) The ROC curves for the proposed fusion method and the NFIQ algorithm for each type of altered fingerprint. The ROC curve for the NFIQ criterion is shown as a collection of points because its output can only accept one of the five quality levels (the range of false positive rate represented here only shows one point).

Figure 17. Cases of true positive detection by (a) discontinuity in the orientation field. (b) Distribution of minutiae.(c) and (d) Combining the two methods



(a) Fingerprintness = 0.92, NFIQ = 1 (b) Fingerprintness = 0.86, NFIQ = 1

False negative examples of the suggested technique are shown in Figure 18. Each example's minutiae and orientation field discontinuities are displayed. (a) A fingerprint containing a little patch of changed information. (b) Fingerprint imitation. It should be noted that NFIQ is likewise unable to identify these two modified fingerprints.



(a) Fingerprintness = 0.33 NFIQ = 5 (b) Fingerprintness = 0.57 NFIQ = 1 (c) Fingerprintness = 0.58 NFIQ = 2 (d) Fingerprintness = 0.52 NFIQ = 3

False positive instances of the suggested approach are shown in Fig. 19. Inadequate ridge patterns: (a) F0010811, NIST SD14. Fingerprints that may have been changed include (b) F0019979, (c) F0002962, and (d) F0018103.

Have an NFIQ of 4 or 5. It is acceptable to raise alarms regarding low-quality photographs because 1) they need to be manually validated and 2) criminals may purposefully submit low-quality fingerprints to the fingerprint system in order to evade detection [41]. All three of the NFIQ ¼ 1 or 2 false positive examples (two are displayed in Figs. 19b and 19c) seem to have been modified.

4.2 SUBJECT-LEVEL ASSESSMENT

When someone uses fingerprint alteration, we found in our database of altered fingerprints that they attempt to change as TABLE 3 NFIQ Distribution for False Positives Detected.

at the Rate of1Percent by the Proposed Algorithm

NFIQ Value	1	2	3	4	5
Number of Images	2	1	39	145	83

the greatest number of fingers (Fig. 4). This makes sense because a combination of match scores from all 10 fingerprints is usually used for identification in large-scale AFIS applications. Therefore, it is unlikely that changing one or two fingerprints will alter the identification determination. In light of this finding, we carry out the subject level detection for modified fingerprints using the subsequent decision level fusion rule. A person is said to have changed fingerprints if six or more of their fingerprints are found to have altered. Subjects with less than six altered fingerprints are not considered a threat to AFIS because even five (out of 10) normal fingerprints are usually sufficient for correct identification.

2,700 ten print cards in NIST SD14 and 453 ten print cards with more than five changed fingerprints are used for the topic level evaluation. The ROC curves of the suggested method, which includes three different approaches, and the NFIQ criterion for identifying people with altered fingerprints are displayed in Fig. 20. The proposed algorithm attains a true positive rate of 66.4%, significantly outperforming

the NFIQ criterion, which has a true positive rate of 26.5%. Additionally, the algorithm maintains a false positive rate of 0.3%. According to the NFIQ criterion, individuals with six or more fingerprints classified as NFIQ = 5 in the NIST SD14 dataset are identified as those who have altered their fingerprints.

Figure 21 presents an instance of a ten-print card where the subject-level decision is accurately determined. Despite up to nine fingers exhibiting alterations, the subject-level fusion algorithm successfully identifies the individual. However, one altered finger goes undetected due to the smooth orientation field and the absence of irregularities in the minutiae distribution within the modified region.

For individuals who have not intentionally altered their fingerprints or have only a few that have been affected due to accidents or occupational hazards, combining multiple fingerprints can help reduce the false positive rate. An example of this scenario is illustrated in Fig. 22. However, in this case, six out of ten fingerprints have an NFIQ score of 5, which may lead to an unfair alarm being triggered based on the NFIQ criteria.

Another government organisation has given us access to a tiny database of changed fingerprints (254 pictures). The image format, including compression method, image resolution, and image kind (single finger impressions, slap impressions, and 10 print cards), varies more in this database. As a result, we present a distinct report on the detection performance for this database. After training an SVM with all 4,433 images from our initially modified fingerprint dataset, we conducted tests on this second small database. Furthermore, a comparison was performed using the same NFIQ criterion. The proposed method achieves a true positive rate of 33.1% at a false positive rate of 2.1%, whereas the NFIQ criterion yields a true positive rate of 9.4%.

TESTING

One of the most important parts of computer programming is testing and debugging programs; without functional programs, the system will never generate the intended result. When user development is asked to help find all flaws and bugs, testing is done most effectively. Testing is done using the sample data. When it comes to testing, the quality of the data is more important than its quantity. The purpose of testing is to make sure the system was functioning correctly and effectively before live operation directives.

5.1 TEST CASE PREPARATION

Before delivering the final product, software undergoes testing to identify and resolve as many defects as possible after the source code is developed. The goal is to design multiple test scenarios that maximize the chances of detecting errors and ensuring the software's reliability.

Two viewpoints are used to test software:

Techniques for designing "white-box" test cases are used to exercise internalsoftware logic. The "block-box test case design techniques" are used to exercise software requirements.

5.1.1 White-Box Testing

White-box testing focuses on evaluating the intended functionality of a product. It involves conducting tests to determine whether each function serves a meaningful purpose while simultaneously identifying any potential defects within those functions.

A software engineer can design test cases using white-box testing techniques to verify that each independent path within a module is executed at least once. This approach helps ensure comprehensive code coverage, identifying potential issues and improving the overall reliability of the software.

1. Perform true and false side-condition testing on all logical decisions.
2. Test each loop by exercising it within its operational constraints and at its boundaries.
3. To ensure validity-data flow testing, practise internal data structures.

Test Case 1: User input

Input	User inserting image
Process	Checks whether image is inserted.
Expected output	Successfully allow to further process, otherwise reinsert the image.

5.1.2 Black-Box Testing

Black-box testing concentrates on the software's functional requirements. Black-box testing looks for mistakes in the following areas:

1. Missing or inaccurate functions.
2. Mistakes in the interface.
3. Mistakes in external database access or data structures.
4. Errors in performance.
5. Errors in initialisation and termination.

5.1.3 Test cases

Test Case 2: Preprocessing

Input	crack detection part& range exceeded part
Process	Checks the values and removes noise and set the range.
Expected output	Successfully noise is removed and rage is set

Test Case 3: Orientation

Input	From the part of image that degree of it has changed
Process	Reads the crack values and set the image in a derived form called as rotation variant
Expected output	Successfully getting the output image with proper angle

Test Case 4:Feature Extraction

Input	From the ridges detection part
Process	Reads the ridge values and remove those ridges from the image
Expected output	Successfully getting the output image without ridges

Test Case 5: Minutiae Distribution

Input	From the over lapping detection part
Process	Reads the overlapping values and remove those over lap pings from the image
Expected output	Successfully getting the output image without over lappings

Test Case 6: Matching

Input	Two images are inserted
Process	Reads the values of two images and compare them to check that they are equal or not
Expected output	Successfully the two images are compared

5.2 TEST CASE VERIFICATION

5.2.1 Unit Testing

During this testing process, each module is evaluated individually before being integrated into the complete system. Unit testing focuses on verifying the smallest software design unit to ensure its functionality. This method is also referred to as module testing, where each component is tested separately to identify and resolve potential issues before full system integration.This testing is done during the actual programming stage. Every module is found to function satisfactorily in this testing step with respect to the expected output from the module. There are some validation checks for fields also. It is very easy to find error debut in the system.

5.2.2 Integration Testing

Data can be lost via an interface, and when two modules are merged, one module may negatively impact the other subfunctions and fail to generate the intended principal functions. Integrated testing is a systematic approach used to develop the interface and identify defects within a system. This process involves testing with sample data to evaluate the functionality and ensure seamless interaction between integrated components.The combination of the aforementioned test cases will be displayed in the test case verification that follows.

Test case 4: Image inserting, Crack Detection & Filling

Input	User image inserting
Process	Reads the image and pixel values by using pixel grabber and read the crack areas and it will indicate it with different color and by using neighboring pixels it will fill the crack area
Expected output	Successfully getting the output image without cracks

5.2.3 Validation and system testing

While validation can be defined in various ways, the simplest explanation is that it is achieved when the software functions as expected by the user.A battery of black-box tests is used to validate software and show that it complies with specifications. A test plan describes the test technique and the kinds of tests that will be administered. outlines the precise test scenario that will be utilised to show that the requirements are being met.

The procedure and the plan are both made to make sure that all functional

requirements are met. All requirements are met, including human engineering, accurate documentation, behaviour characteristics, and performance requirements.

One of two circumstances may occur following the completion of each validation test case.

i. The performance characteristics or function meet the specifications and are approved.

ii. A list of deficiencies is created after a specification deviation isdiscovered.

6 Conclusions And Future Work

Because of the success of AFIS and its widespread use worldwide, some people have gone to great lengths to change their fingerprints in order to avoid detection. Fingerprint spoofing involves the use of a fake fingerprint to impersonate someone else and is distinct from fingerprint alteration or obfuscation. While spoofing has been widely studied in research, fingerprint alteration where individuals modify their fingerprints to evade identification has been documented in various cases. However, the concept of obfuscation remains largely unexplored in biometric studies.

Figure 21. An actual positive illustration of the suggested algorithm's subject-level detection. Even if one of the altered fingerprints was not discovered, this subject is still highly confidently identified as having altered fingerprints because the other nine (boxed) fingerprints are correctly identified as altered. Using the NFIQ criterion, none of the ten fingerprints are found to be altered.

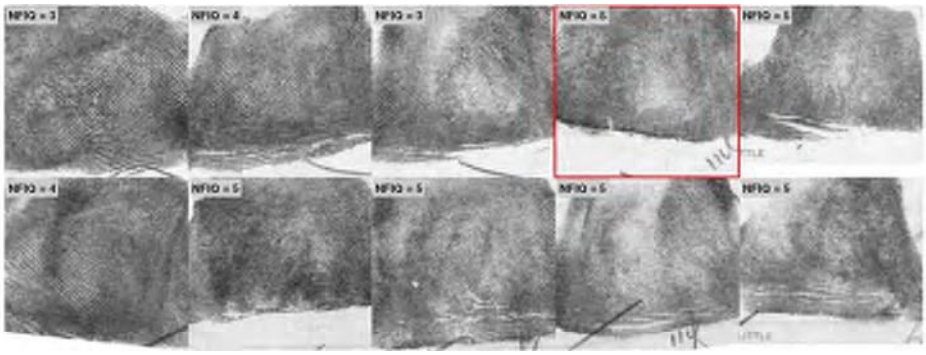


Figure 22 presents a true negative example at the subject level, as identified by the proposed algorithm (NIST SD14, F0000121-F0000130). The algorithm classifies the subject's nine fingerprints as natural, allowing them to pass the alteration detector. However, the NFIQ criterion incorrectly flags this subject, generating a false alarm due to six fingerprints receiving an NFIQ score of 5.

However, other biometric modalities (such face and iris) may experience obfuscation.this problem isespecially significant inthe caseoffingerprints due to thewidespread deployment of AFIS in both government and civilian applications and theease with which fingerprints canbeobfuscated.

The problem of fingerprint manipulation has been introduced, and a quantitative analysis of the threat posed by altered fingerprints to a commercial fingerprint matcher has been conducted. We also tested the capacity of NFIQ, a popular program for evaluating the quality of fingerprint images, to identify changed fingerprints. Due to the NFIQ's poor ability to distinguish between altered and real fingerprints, we developed a method to automatically identify altered fingerprints based on minutiae distribution and fingerprint orientation field properties. The three fundamental conditions for a modification detection algorithm are satisfied by the suggested algorithm, It is predicated on the characteristics extracted from the minutiae and orientation field: The first three advantages include easy AFIS integration, fast operation time, and a high true positive rate at low false positive rate. The proposed approach and the NFIQ criterion were assessed using a large public domain fingerprint database (NIST SD14) and a modified fingerprint database provided by a law enforcement agency. The suggested approach can accurately identify 66.4 percent of the subjects with changed fingerprints at a false positive rate of 0.3 percent, whereas the NFIQ algorithm detects 26.5 percent of these subjects. The following avenues for further extension of this study are possible:

1. Automatically identify the type of modification so that the proper

countermeasures can be implemented.

2. Recreate fingerprints that have been changed. For some types of changed fingerprints, reconstruction is possible if the ridge patterns are locally damaged or the ridge structure is still intact in the finger but may be in a different location.
3. Compare their modified fingerprints to those of their unmodified partners. A matcher designed specifically for altered fingerprints can be made to link them to unmodified mates in the database using whatever information is included in the altered fingerprints.
4. To counteract the growing threat of people avoiding AFIS, use multibiometrics [42]. The FBI's NGI [43] and the Department of Defense's ABIS [44] are two examples of federal agencies in the United States that have implemented or intend to implement multibiometrics in their identity management systems. But it's also possible to successfully change other biometric characteristics. According to reports, cataract surgery can lower the accuracy of iris identification systems [46] and plastic surgery can drastically impair the performance of face recognition systems [45]. A thorough investigation of potential alteration strategies for each significant biometric characteristic is required in order to address the issue of avoiding identification by changing biometric traits.

7. REFERENCES

[1] J. Feng, A.K. Jain, and A. Ross, "Detecting Altered Fingerprints," Proc. 20th Int'l Conf. Pattern Recognition, pp. 1622-1625, Aug. 2010.

[2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, second ed. Springer-Verlag, 2009.

[3] The U.S. Department of Homeland Security, US-VISIT, http://www.dhs.gov/usvisit, 2011.

[4] The Fed. Bureau of Investigation (FBI), Integrated Automated Fingerprint Identification System (IAFIS), http://www.fbi.gov/hq/cjisd/iafis.htm, 2011.

[5] H. Cummins, "Attempts to Alter and Obliterate Finger-prints," J. Am. Inst. Criminal Law and Criminology, vol. 25, pp. 982-991, 1935.

[6] Surgically Altered Fingerprints, http://www.clpex.com/images/FeetMutilation/L4.JPG, 2011.

[7]K.singh,AlteredFingerprints, Forensic/fingerprints/research/alteredfingerprints.pdf, 2008.

[8]M. Hall, "Criminals Go to Extremes to Hide Identities," USA Today, http://www.usatoday.com/news/nation/2007-11-06-criminal-extreme_N.htm, Nov. 2007.

[9] Criminals Cutting off Fingertips to Hide IDs, http://www. thebostonchannel.com/news/15478914/detail.html, 2008.

[10] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 360-373, Sept. 2006.

[11] K.A. Nixon and R.K. Rowe, "Multispectral Fingerprint Imaging for Spoof Detection," Proc. SPIE, Biometric Technology for Human Identification II, A.K. Jain and N.K. Ratha, eds., pp. 214-225, 2005.

[12] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint Image Quality," NISTIR 7151, http://fingerprint.nist.gov/NFIS/ ir_7151.pdf, Aug. 2004.

[13] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun, "A Comparative Study of Fingerprint Image-Quality Estimation Methods," IEEE Trans. Information Forensics and Security, vol. 2, no. 4, pp.

[14] R. Cappelli, D. Maio, and D. Maltoni, "Synthetic Fingerprint-Database Generation," Proc. 16th Int'l Conf. Pattern Recognition, pp. 744-747, Aug. 2002.

15]K. Wertheim, "An Extreme Case of Fingerprint Mutilation," J. Forensic Identification, vol. 48, no. 4, pp. 466-477, 1998. [16] History ofFingerprintremoval, http://jimfisher.edinboro.edu/forensics/fire/print.html, 2011.

[17] J. Patten, Savvy Criminals Obliterating Fingerprints to Avoid Identification, http://www.eagletribune.com/punews/local_ story_062071408.html, 2008.

[18] Woman Alters Fingerprints to Deceive Taiwan Immigration Fingerprin t Identifi cation Sys tem Oct. 2008.

[19]Sweden Refugees Mutilate Fingers, http://news.bbc.co.uk/2/hi/ europe/3593895.stm, 2004.[20] Asylum Seekers Torch Skin off Their

Fingertips So They Can't BeID'd by Police, http://www.mirror.co.uk/sunday-mirror/2008/06/29/asylum-seekers-torch-skin-off-their-fingertips-so-they-can-t-be-id-d-by-police-98487-20624559/, 2008.

[21] Surgically Altered Fingerprints Help Woman Evade Immigration, http://abcnews.go.com/Technology/GadgetGuide/surgically- altered-fingerprints-woman-evade-immigration/story?id=9302505, 2011.

[22] Three Charged with Conspiring to Mutilate Fingerprints of Illegal Aliens, http://www.eagletribune.com/local/x739950408/Three- charged-with-conspiring-to-mutilate-fingerprints-of-illegal-aliens, July 2010.

[23] EURODAC: a European Union-Wide Electronic System for the Identification of Asylum-Seekers, http://ec.europa.eu/justice_ home/fsj/asylum/identification/fsj_asylum_identification_ en.htm, 2011.

[24] Neurotechnology Inc., VeriFinger, http://www.neurotechnology. com/vf_sdk.html, 2011.

[25] NIST Special Database 4, NIST 8-Bit Gray Scale Images of Fingerprint Imageg Groups GS), nistsd4.htm, 2011.

[26] J.W. Burks, "The Effect of Dermabrasion on Fingerprints: A Preliminary Report," Archives of Dermatology, vol. 77, no. 1, pp. 8-11, 1958.
27] Men in Black, http://www.imdb.com/title/tt0119654/, 1997.

[28] M.V. de Water, "Can Fingerprints Be Forged?" The Science News-Letter, vol. 29, no. 774, pp. 90-92, 1936.

[29] M. Wong, S.-P. Choo, and E.-H. Tan, "Travel Warning with Capecitabine," Annals of Oncology, vol. 20, p. 1281, 2009.

[30] K. Nandakumar, A.K. Jain, and A. Ross, "Fusion in Multi-biometric Identification Systems: What about the Missing Data?," Proc. Second Int'l Conf. Biometrics, pp. 743-752, June 2009.

[31] H. Plotnick and H. Pinkus, "The Epidermal versus the Dermal Fingerprint: An Experimental and Anatomical Study," Archives of Dermatology, vol. 77, no. 1, pp. 12-17, 1958.

[32] Altered Fingerprints Detected in Illegal Immigration Attempts, http://www.japantoday.com/category/crime/view/altered-

fingerprints-dete cted-in-illegal-immigration-attempts, 2011.[33] NIST

Special Database 14, NIST Mated Fingerprint Card Pairs 2(MFCP2), http://www.nist.gov/srd/nistsd14.htm. 2011.

[34] J. Zhou and J. Gu, "A Model-Based Method for the Computation of Fingerprints' Orientation Field," IEEE Trans. Image Processing, vol. 13, no. 6, pp. 821-835, 2004.

[35] S. Huckemann, T. Hotz, and A. Munk, "Global Models for the Orientation Field of Fingerprints: An Approach Based on Quadratic Differentials," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 30, no. 9, pp. 1507-1519, Sept. 2008.

[36] Y. Wang and J. Hu, "Global Ridge Orientation Modeling for Partial Fingerprint Identification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 33, no. 1, pp. 72-87, Jan. 2010

[37] C. Watson, M. Garris, E. Tabassi, C. Wilson, R.M. McCabe, S.Janet, and K Ko, "NIST Biometric Image Software.