**ECG BIOMETRIC AUTHENTICATION: A COMPARATIVE ANALYSIS**

**ABSTRACT**

The main theme of this project is to authenticate the user by using ECG signals. Electrocardiogram (ECG) is an electric signal of cardiac activity posing highly discriminative properties related to human recognition. ECG based authentication has gained much success in recent times however discriminant feature extraction and efficient pattern classification still encounter numerous challenges. In these present situations authentication methods became an indispensable urgent task to protect the integrity of the devices and the sensitive data. Passwords have provided to control the important data, but have shown their inherent vulnerabilities. We propose an authentication method, which can effectively provide the access to the user, which is known as ‘ECG Biometric Authentication’. This authentication mainly involves filtering type, segmentation, feature extraction, and health status on ECG biometric by using the evaluation metrics.

**Keywords:** ECG Biometric, Authentication.

**CHAPTER 1**

**INTRODUCTION**

Being the most commonly used biometric trait by humans, face recognition has become an active research topic for many decades now and it has found great application in consumer electronics and software. Face owes its reputation mainly to being easily and non-intrusively accessible compared to other biometric traits like finger print or iris. However, this advantage becomes a weakness in malicious circumstances, enabling attackers to create copies and spoof face recognition systems without any difficulties. Spoofing attack is the act of outwitting a biometric system by presenting a fake evidence in order to gain authentication [1]. It is relatively simple to forge such an attack for facial recognition systems, due to the fact that the photographs or videos of a valid user can be easily captured from a distance or obtained via internet, e.g. through social networks. Valid users (simply users or clients) can be defined as the persons that are enrolled in a face recognition system. An attacker can attempt to gain access by simply showing their printed photos or replaying their recorded videos to the sensor.

This apparent vulnerability of face has evoked great interest in the biometric community and many papers have been published on countermeasure studies. Mainly as a result of their simplicity and low-cost, the previously mentioned photo print and video replay attacks [2] constitute the focus of research activities in this domain. Existing anti-spoofing approaches against these type of attacks can be roughly classified into three groups: texture analysis, motion analysis and liveness detection. Assuming the presence of cues like printing artefacts [3] and/or blurring [4], many anti-spoofing techniques examine the texture of the captured face image. Similarly, in a recent study [5], micro-texture analysis using multi-scale local binary patterns is proposed. It can be argued that this type of approaches highly depends on the quality of the printed image or video display. The second group of methods aims to detect spoofing attacks by analysing the motion in the scene based on the fact that planar objects like a sheet of paper or a mobile phone screen move in a significantly different way compared to real faces. For example, in [6], the trajectories of small regions of face images are examined to be classified as real or fake. In a similar manner, by computing geometric invariants of a set of automatically located facial points, Marsico et al. [7] exploit the same phenomenon. Finally in the last group of methods, liveness of the face is determined based on live-face specific gestures such as eye blinking [8] or lip movements [9].

However, approaches of this kind are bound to fail in the case of video replay attacks or even more simply, with photographic masks which are actually high resolution facial prints worn on face after the eyes and mouth regions are cut out, as claimed in [10]. Similarly in [11], it is again shown that with eyes cut out from the photos, traditional visible liveness detection method still detects blinking, in other words, cannot distinguish a photo attack. Recently, several studies have been published that present methodical and reproducible analyses of several of these and some other methods, with a shared purpose of providing comparable results on public databases [12]–[14]. Work on fraud detection capabilities for face is still limited and a substantial part of it is based on the flatness of the captured surface in front of the sensor during an attack. This is also true for approaches that examine the 3D nature of the face by employing additional devices, which is much more realistic now with the introduction of affordable consumer depth cameras like Kinect. For instance, in [15], 3D data acquired with a low-cost sensor is utilized to localize face and at the same time to test its authenticity to decrease their system’s vulnerability to spoofing attacks.

Unfortunately, methods that depend on the assumption of a planar surface for a fake face are rendered futile in case of 3D facial mask attacks [16]. With the help of the advancements in 3D manufacturing technologies, easily attainable facial masks take the spoofing attacks one step further and introduce new challenges for counter measure studies. To the best of our knowledge, there have been very few studies published addressing this issue and they are detailed in the next section. The provision of security can entail the protection of sensitive data, services, or facilities by ensuring that only authorized persons have access. Though passwords provide some protection against illegitimate access, they are often so simple that they can be guessed or easily cracked. While offering improved security, complex passwords can be difficult to remember and consequently often “stored” via less secure means. Furthermore, the same password is often used across multiple applications or platforms meaning a cracked password can enable a fraudster to access multiple resources. An attractive alternative to passwords involves biometric recognition. Biometrics refer to a person’s behavioral and biological characteristics such as their face, fingerprint, iris, voice, hand geometry, and gait. Biometric traits can be highly discriminative yet less easily lost or stolen [1]. Despite their appeal, however, biometric systems are vulnerable to malicious attacks [2]. Among them are spoofing attacks, also called presentation attacks, which refer to persons masquerading as others to gain illegitimate access to sensitive or protected resources. As an example, a fraudster could fool or spoof a face-recognition system using a photograph, a video, or a three-dimensional (3-D) mask bearing resemblance to a legitimate individual.

Even though the threat of spoofing is now well recognized, the problem is far from being solved, thus antispoofing research warrants far greater attention in the future. This tutorial article introduces the problem of spoofing and related research to develop antispoofing solutions. The focus is an evaluation methodology for assessing both the effect of spoofing and the performance of spoofing countermeasures. A case study in face recognition is included to illustrate the application of the evaluation methodology in practice. Finally, the article also includes a summary of the lessons learned through our own research and outlines a number of research priorities for the future. Most of the material is based upon antispoofing research performed in the scope of the European TABULA RASA research project (http://www.tabularasa-euproject.org), which was identified as a success story by the European Commission (http://europa.eu/ rapid/press-release\_MEMO-13-924\_en.htm). The presentation is self-contained and aimed at both the generally knowledgeable and nonspecialist.

The article aims to provide an overview of the research problem, not a comprehensive survey of the plethora of antispoofing techniques in the literature; such surveys can be found elsewhere, e.g., for fingerprint recognition [3], face recognition [4], and speaker recognition [5]. The intention is also to stimulate further work, particularly the development of standard metrics, protocols, and data sets for evaluating progress. Biometrics The term biometrics is derived from the Greek words bio (life) and metric (to measure). The goal of a biometric recognition system is to determine or verify the identity of an individual from his/her behavioral and/or biological characteristics. Applications include criminal identification, airport checking, computer or mobile device log-in, building and critical infrastructure access control, digital multimedia rights control, transaction authentication, voice mail, and secure teleworking. Various biometrics have been investigated, from the most conventional including fingerprint, iris, face, and voice, to more emerging modalities such as gait, hand-grip, ear, and electroencephalograms.

Each modality has its own strengths and weaknesses [1]. For example, face recognition is among the most socially accepted biometric; face recognition is a natural method of identification used every day by humans. In contrast, while fingerprint and iris recognition may be more reliable, they are also more intrusive. In practice, the choice of biometric modality depends on the application. Biometric systems typically function in one of two distinct modes: 1) verification (or authentication) and 2) identification. An authentication system aims to confirm or deny a claimed identity (one-to-one matching), whereas an identification system aims to identify a specific individual (one-to-many matching). Although there are some differences between the two modes, their most basic operation, namely that of feature-to-reference comparison, is identical and consists of the following steps illustrated in Figure 1. First, a biometric sample (e.g., a face image) is acquired from a sensor (e.g., a digital camera).

Biometric features (e.g., facial intensity, color, or texture) are then extracted from the sample. These can be a set of parameters (or coefficients) that provide a compact representation of the biometric sample, which is more discriminative and amenable to pattern recognition. Biometric features should minimize variations due to acquisition or environmental factors (e.g., facial expression, pose, and illumination) [Fig1] A generic biometric system. Sensor Biometric Data Biometric Feature Score Database Comparator Decision Biometric Reference Feature Extractor while discriminating between the biometrics collected from different individuals. To determine or verify the identity corresponding to a given biometric sample, the features are compared to a single (verification) or set of (identification) biometric references acquired previously during an enrollment phase. These comparisons are made by a comparator that produces a score reflecting the similarity between features and references. The decision is an acceptance or rejection in the case of verification, or the identity of the closest match in the case of identification.

In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain access to the system. Based on the observations that 2D face recognition systems are vulnerable to spoofing attacks, researchers started to work on countermeasures to reduce the impact of spoofing attacks on face recognition performances. There have been studies on countermeasures to detect photograph and video spoofing, which are 2D face attacks [1 - 3]. Mask attacks to face recognition systems, which are 3D face attacks, is a considerably new subject. To the best our knowledge, the impact of mask attacks on face recognition has not been analyzed yet. The main reason for this delay is due to the unavailability of public mask attacks databases. In this paper, it is the first time that the impact of mask spoofing is analyzed on face recognition using the mask database which was prepared within the context of the European Union (EU) research project TABULA RASA [4]. The preparation of a mask attacks database is much more difficult and expensive than the preparation of photo or video attacks databases. Initially, to prepare a high quality mask, a 3D scanner is necessary to obtain the 3D model of the target person, which are generally high-cost devices. The procedure continues with manufacturing of the masks which Figure 1. Example sample for fabric mask. In the second column, the mask is worn on the face.

The picture is taken from [5] is also an expensive procedure. The mask attacks database which is used in this study was created by MORPHO [6]. Since the database includes many high-quality mask samples, it is possible to detect the performances of face recognition systems, accurately, under mask attacks. The mask database consists of both the 3D scans and the corresponding 2D texture images. Thanks to the nature of this database, in this paper, we are able to conduct the benchmark evaluations for each of 2D, 2.5D and 3D face recognition. The aim of this study is not to propose a new face recognition method, but instead to show the impact of mask attacks on existing face recognition methods. The paper is organized as follows: Section 2 gives brief information on the mask database which is used in this study. Section 3 explains the face recognition systems which are selected to test the performance of these systems under mask attacks.

Biometric systems have been deployed around the world and have been extensively used in the past decades. However the potential of fooling or spoofing this technology is widely admitted. Nowadays biometric spoof detection is an active research area and there has been a lot of efforts towards a promising approach to ensure the presence of a real legitimate user. There are different attack points in a biometric system. The first vulnerable point is the sensor used in the biometric system. Biometric systems and in particular fingerprint can be spoofed by presenting synthetic samples to the sensor e.g. gummy fingers that have fingerprint impressions. There M. Komeili and D. Hatzinakos are with the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada. E-mail: {mkomeili, dimitris}@ece.utoronto.ca N. Armanfard is with the Department of Electrical and Computer Engineering, McMaster University, Hamilton, Ontario, Canada. E-mail: armanfn@mcmaster.ca has been a huge literature on other vulnerabilities that for example bypass feature extraction or matcher, or manipulate database or communication channel.

However, in such cases, some information about the system such as feature extraction, matcher, database and/or physical access to some of those components is necessary. In contrast, fooling the sensor using a fake biometric sample does not need any specific information about internal mechanism of the biometric system. In addition, sensor level attacks are in analog domain and hence many solutions such as cryptography and watermarking that are in digital domain are not useful. This highlights the importance of developing biometric spoofing countermeasures to classify an input sample as live or fake that is focus of this study. Investigating other types of attacks is out of scope of this study. Liveness detection has been an active area in the past decade and numerous approaches have been proposed in the literature to solve this problem. Considering the results reported in LivDet2009 [1], LivDet2011 [2], LivDet2013 [3] and LivDet2015 [4], liveness detection is still an open problem and performance of the existing approaches does not satisfy requirements of many practical applications [5]. The mainstream of the current approaches use some training samples artificially created via certain spoofing process and work well on test samples created by the same process involved in training, but their performance on a novel type of spoof is questionable.

In practice, the way that a fake biometric is fabricated is unknown. In this study we approach the problem from a different perspective by incorporating electrocardiogram (ECG). ECG is among the newer additions to the biometric family and unlike the conventional biometrics such as fingerprint, iris and face, ECG is a vital signal and presence of the ECG automatically ensures the liveness [6]–[12]. In addition, conventional biometrics can be easily stolen from people. For example, fingerprints may be left behind whenever we touch a glass surface. Even iris images can be captured from a few meters distance. Not to mention face images which can be captured from a longer distance. However, compared to the conventional biometrics, if not impossible it is far more difficult to steal someone’s ECG. Beside its advantages, accuracy of ECG is not as good as some other mature biometrics such as fingerprint [13], [14]. Therefore, we seek to fuse ECG and fingerprint to improve the recognition rate and more importantly the liveness detection performance. Fusion of ECG and fingerprint is not a new idea. In [15] and [16] it has been suggested to combine ECG with other biometrics such as face and fingerprint to get a better recognition rate.

But, all these works were restricted to analyzing recognition rate and have failed to consider spoof attacks. The improved verification rate in the conventional fusion approach is because when input samples of one trait have poor quality and hence less informative, the other trait will help the system to still identify the user. However, this opens up the possibility of spoofing because such system may accept a fake copy of an authentic fingerprint even if ECG does not match. This contradicts the main motivation in utilizing ECG which is liveness detection. This issue has been overlooked in the previous works [15], [16]. In this paper, we offer an alternative to the conventional fusion of ECG and fingerprint by proposing to fuse ECG with fingerprint for liveness detection. To this end, we combine ECG recognition score with fingerprint liveness detection score instead of fingerprint recognition score. This greatly improves the accuracy of liveness detection task. Figure 1 shows an overview of the proposed framework which will be explained in detail in section III. In this context, we use terms “fingerprint liveness detection” and “fingerprint recognition” to indicate two blocks in the proposed system as shown in Figure 1. Our ECG signals are collected from fingertips as shown in Figure 2. Majority of previous works on ECG recognition have been based on signals collected form chest area [17]–[21] or lower rib cage [22] and only a few works have been done based on fingertip ECG signals, e.g. [23], [24]. Fingertip ECG has two advantages: first, it eliminates the need for user to undress for electrode placement; second, it makes the fingerprint a natural choice to be fused with ECG.

The main contributions of this paper are as follows: In order to get the most out of ECG, we fuse it with a fingerprint liveness detection method for liveness detection purpose and also fuse it with a fingerprint recognition method for recognition purpose. Although the latter has been previously investigated, e.g. in [15] and [16], to the best of our knowledge, the former has not been explored in the previous literature. In addition, the proposed system is capable of automatically adapting ECG and fingerprint templates to operational data. Since ECG is a time dependent signal and its waveform might be affected by factors like diet and emotion, template updating is crucial to maintain the performance of the system in long term without requiring re-enrolling or retraining the system from scratch and to the best of our knowledge this has not been investigated in the literature. Another shortcoming of the previous works on ECG [7], [22], [25]–[31] is lack of a proper stopping criterion to limit the length of recording sessions. Previous works usually limits the length of sessions by fixing the number of recorded heartbeats to a predefined threshold.

Therefore, the number of recorded heartbeats is the same for all subjects which does not consider the fact that some subjects have a very stable ECG and do not need as many samples as other subjects with less stable ECG. In this paper, we present an easy-to-compute yet effective criterion based on local averaging and correlation that measures heartbeat consistency (HC) in successive heartbeats. The rest of this paper is organized as follows: Section II briefly reviews the previous works on ECG recognition, fusion of ECG and fingerprint as well as fingerprint liveness detection.

Biometric technology has been used widely in personal identification applications. As compared with the traditional security methods like passcodes, biometric technology brings about convenience which uses human intrinsic characteristics for individual identification [1], [2]. Face recognition is one of the most common biometric features because information from the face can be extracted easily without any physical contact. It has been successfully demonstrated in many personal identification applications, e.g. law enforcement, surveillance, information security, smart card authentication and entertainment [3]–[7]. Since traditional face recognition systems do not consider the existence of an adversary, many studies have revealed that these systems are vulnerable to spoofing attacks [8]–[10] in which an attacker obtains an illegitimate access to a system by camouflaging as an authorized person. A well-known example is a 2D spoofing attack, which misleads a system by using a 2D facial duplicate of a valid user.

As an image or a video of a person is easily obtainable and highly reproducible [11], [12], 2D spoofing attack is one of the most common attacks. There are three types of 2D spoofing attacks, namely photo attack, video attack and mimic mask attack. Photo attack evades the detection by using a picture of a legitimate user on a piece of paper [13], [14], or an electronic screen [15], while video attack misleads the system by using a video of an authorized person on electronic devices [16], [17]. In mimic mask attack, an adversary camouflages as an authorized person by wearing a 2D mask [18]. Face liveness detection [19], which is also referred to face spoofing detection, has been devised to defend against 2D spoofing attack. Face liveness detection determines whether an image is taken from a real or fake subject before face recognition process starts. Suspected images are filtered and will not be passed to the recognition system. Previous works on face liveness detection mainly focus on software-based methods which analyze liveness clues, including texture [20], [21], structure information [22], [23] and liveness sign [24], of the subjects, and quality of captured images [15], [25], [26].

These methods are generally sensitive to environmental factors [19], [27], for instance, bad illumination condition and noisy images. Thus, their detection accuracy decreases significantly under such circumstances. In addition, computational complexity of calculating some liveness clue is high, e.g. facial dynamic is calculated based on consecutive frames [28]. Although asking users to speak [29] or shake their heads [30] improves the accuracy of the detection, it also reduces efficiency due to longer detection duration and uncooperative users. On the other hand, a device is embedded in a recognition system in hardware-based methods [31], [32] to capture additional information of the subjects, e.g. temperature. Nevertheless, some of the additional hardware is costly and difficult to install. Our preliminary study [33], which only analyzes the difference of the hair on foreheads between real and fake faces, showed that flash increases the differentiation between a legitimate person and the 2D spoofing attack.

However, the study only focused on video attack in a particular environmental setting in which the ambient illumination is normal, and the distance between the camera and the background is short. The usefulness of flash on detecting other 2D spoofing attacks remains unclear. Moreover, the proposed model is sensitive to the hair on the forehead and may not be practical since users have different hair styles. Therefore in this paper we provide a complete investigation on how the use of flash can improve 2D spoofing attack detection. The literature review of face liveness detection and also 2D spoofing attack is introduced in In the proposed model, a pair of images is taken from a subject in the detection, one with flash and the other without flash. Features of our method are carefully designed in order to provide accurate and robust prediction with low time complexity. The descriptor based on uniform local binary patterns is applied to measure the textural information from the face, and another three descriptors are proposed to capture the structure information of a face using the standard deviation and the mean of grayscale difference between the images with and without flash.

Then, the subject is classified as either legitimate or malicious class based on the difference between the images with and without flash measured by the four descriptors. Unlike hardware-based methods, our method requires only flash which is economical and easy to install in existing face recognition systems. The proposed method is expected to be more accurate and robust than the software-based method since flash enhances the differentiation between real and fake faces and reduces the influence of ambient illumination. In addition, the time complexity of extracting the four descriptors is low and no user cooperation is required. Our method takes advantage of both software and hardware based methods. The discussion on the reasons why considering the difference between the images with and without flash is helpful in face liveness detection based on the Lambertian reflectance law is also provided.

**CHAPTER 2**

**LITERATURE REVIEW**

**[1] Nesli Erdogmus and Sebastien Marcel:** Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Vulnerability of recognition systems to spoofing attacks (presentation attacks) is still an open security issue in biometrics domain and among all biometric traits, face is exposed to the most serious threat, since it is particularly easy to access and reproduce. In this paper, many different types of face spoofing attacks have been examined and various algorithms have been proposed to detect them. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. However, with the advancements in 3D reconstruction and printing technologies, this assumption can no longer be maintained. In this paper, we aim to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type. In order to assess the spoofing performance of 3D masks against 2D, 2.5D, and 3D face recognition and to analyze various texture-based countermeasures using both 2D and 2.5D data, a parallel study with comprehensive experiments is performed on two data sets: the Morph database which is not publicly available and the newly distributed 3D mask attack database.

**Summary:** Spoofing attacks continue to be a security threat for biometric recognition systems and face is among the most vulnerable traits due to its high accessibility. Majority of previous studies in face spoofing focus on preventing 2D attacks performed by displaying printed photos or replaying recorded videos on mobile devices. However, utilization of 3D masks for face spoofing attacks has become easier and cheaper with the advancements in 3D reconstruction and printing technologies.

**[2] A. Hadid, N. Evans, S. Marcel and J. Fierrez:**

Biometrics already form a significant component of current and emerging identification technologies. Biometrics systems aim to determine or verify the identity of an individual from their behavioral and/or biological characteristics. Despite significant progress, some biometric systems fail to meet the multitude of stringent security and robustness requirements to support their deployment in some practical scenarios. Among current concerns are vulnerabilities to spoofing? persons who masquerade as others to gain illegitimate accesses to protected data, services, or facilities. While the study of spoofing, or rather anti spoofing, has attracted growing interest in recent years, the problem is far from being solved and will require far greater attention in the coming years. This tutorial article presents an introduction to spoofing and anti-spoofing research. It describes the vulnerabilities, presents an evaluation methodology for the assessment of spoofing and countermeasures, and outlines research priorities for the future.

**Summary:** Unless they are equipped with suitable countermeasures, all biometric systems were shown to be vulnerable to spoofing. Even so, some modalities (e.g., gait) are more robust than others (e.g., fingerprint), however, this should not be interpreted as meaning they are more reliable; in the absence of spoofing, fingerprint recognition generally outperforms gait recognition. Multimodal biometric systems are also vulnerable and can be overcome by the spoofing of only a single modality.

**[3] N. Kose and J. Dugelay:** There are several types of spoofing attacks to face recognition systems such as photograph, video or mask attacks. To the best of our knowledge, the impact of mask spoofing on face recognition has not been analysed yet. The reason for this delay is mainly due to the unavailability of public mask attacks databases. In this study, we use a 2D+3D mask database which was prepared for a research project in which the authors are all involved. This paper provides new results by demonstrating the impact of mask attacks on 2D, 2.5D and 3D face recognition systems. The results show that face recognition systems are vulnerable to mask attacks, thus countermeasures have to be developed to reduce the impact of mask attacks on face recognition. The results also show that 2D texture analysis provides more information than 3D face shape analysis in order to develop a countermeasure against high-quality mask attacks.

**Summary:** In this study, a 2D+3D face mask attack database is used which was prepared for TABULA RASA research project. It is used to evaluate the performances of the state-of-the art face recognition techniques under spoofing attacks. The novelty of this study is, it is the first time that the impact of mask spoofing is analyzed on 2D, 2.5D and 3D face recognition. **[4]** **Majid Komeili, Narges Armanfard, and Dimitrios Hatzinakos:**

Fingerprints have been extensively used for biometric recognition around the world. However, fingerprints are not secrets, and an adversary can synthesis a fake finger to spoof the biometric system. The mainstream of the current fingerprint spoof detection methods are basically binary classifier trained on some real and fake samples. While they perform well on detecting fake samples created by using the same methods used for training, their performance degrades when encountering fake samples created by a novel spoofing method. In this paper, we approach the problem from a different perspective by incorporating electrocardiogram (ECG). Compared with the conventional biometrics, stealing someone's ECG is far more difficult if not impossible. Considering that ECG is a vital signal and motivated by its inherent liveness, we propose to combine it with a fingerprint liveness detection algorithm. The combination is natural as both ECG and fingerprints can be captured from fingertips. In the proposed framework, the ECG and fingerprint are combined not only for authentication purpose but also for liveness detection. We also examine automatic template updating using ECG and fingerprint. In addition, we propose a stopping criterion that reduces the average waiting time for signal acquisition.

**Summary:** ECG can be recorded from fingertips. Therefore, fingerprint is the natural choice to be fused with ECG. On the other side fingerprint is vulnerable to spoof attacks and ECG has inherent liveness detection. This paper presented a unified approach for fusion of fingerprint and ECG that fills the gap between these two sides. To get the most out of ECG, the proposed system fuses ECG with a conventional fingerprint liveness detection method for a better liveness detection performance, and also fuses it with a fingerprint recognition method for a better recognition rate.

**[5]Patrick PK Chan, Weiwen Liu, Danni Chen, Daniel S Yeung, Fei Zhang, Xizhao Wang, and Chien-Chang Hsu:**

Face recognition technique has been widely applied to personal identification systems due to its satisfying performance. However, its security may be a crucial issue, since many studies have shown that face recognition systems may be vulnerable in an adversarial environment, in which an adversary can camouflage as a legitimate user in order to mislead the system. Although face liveness detection methods have been proposed to distinguish real and fake faces, they are either time-consuming, costly, or sensitive to noise and illumination. This paper proposes a face liveness detection method with flash against 2D spoofing attack. Flash not only can enhance the differentiation between legitimate and illegitimate users, but it also reduces the influence of environmental factors. Two images are taken from a subject, one with flash and another without flash. Four texture and 2D structure descriptors with low computational complexity are used to capture information of the two images in our model. Advantages of our method include low installation cost of flash and no user cooperation required. A data set of 50 subjects collected under different scenarios is used in the experiments to evaluate the proposed method. The experimental results indicate that the proposed model performs better than existing liveness detection methods in different environmental scenarios. This paper confirms that the use of flash successfully improves face liveness detection in terms of accuracy, robustness, and running time.

**Summary:** A dataset containing 50 subjects with 2D spoofing attacks, including paper photo, iPad photo, video, 2D mask and curved mask attack, are collected. In order to compare with the thermal image method, thermal images of 21 subjects with real and five types of attacks are also collected. Our method is also compared experimentally with five software-based and one hardware-based liveness detection methods. The experimental results show that the proposed method is better in terms of accuracy and running time.

**[8]Nima Karimian, Zimu Guo, Mark Tehranipoor, and Domenic Forte:**

Traditional passwords are inadequate as cryptographic keys, as they are easy to forge and are vulnerable to guessing. Human biometrics have been proposed as a promising alternative due to their intrinsic nature. Electrocardiogram (ECG) is an emerging biometric that is extremely difficult to forge and circumvent, but has not yet been heavily investigated for cryptographic key generation. ECG has challenges with respect to immunity to noise, abnormalities, etc. In this paper, we propose a novel key generation approach that extracts keys from real valued ECG features with high reliability and entropy in mind. Our technique, called interval optimized mapping bit allocation (IOMBA), is applied to normal and abnormal ECG signals under multiple session conditions. We also investigate IOMBA in the context of different feature extraction methods, such as wavelet, discrete cosine transform, etc. to find the best method for feature extraction. Experiments of IOMBA show that 217-bit, 38-bit, and 100-bit keys with 99.9%, 97.4%, and 95% average reliability and high entropy can be extracted from normal, abnormal, and multiple session ECG signals, respectively. By allowing more errors or lowering entropy, key lengths can be further increased by tunable parameters of IOMBA which can be useful in other applications. While IOMBA is demonstrated on ECG, it should be useful for other biometrics as well.

**[12]Pei-Lun Hong, Jyun-Ya Hsiao, Chi-Hsun Chung, Yao-Min Feng, and Shun-Chi Wu:**

Biometric technologies offer much convenience over the conventional approaches to identity recognition, but security and privacy concerns also accompany their applications. In this paper, an electrocardiogram (ECG)-based identification scheme is proposed to relieve such concerns. With the help of a deep learning (DL) technique, the identity of an unknown beat bundle can be determined without the need for biometric template construction. Thus, the disclosure of the physiological and pathological condition of an individual from his/her stolen templates will no longer be possible. Furthermore, the problem of being vulnerable to unregistered subjects in this DL-based recognition system is also addressed. Experiments with real and synthesized ECGs are used to illustrate the efficacy of the proposed scheme. An identification rate of 97.84% for the 200 registered subjects with a false-positive identification rate of 0.69% under the attack of 1,000 synthesized single-lead ECGs was achieved.

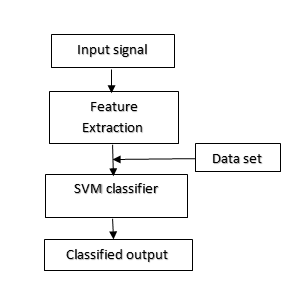
**CHAPTER 3**

**EXISTING METHOD**

For obtaining intra-body propagation signals, the technology for intra-body communication was utilized. There have been proposed three transmission modes for the intrabody communication: the simple circuit type, the electrostatic coupling type, and the waveguide type. Particularly, the waveguide type regards a human body as a waveguide and an input signal at an input electrode pair is propagated to an output electrode pair as an electromagnetic wave. In addition, the waveguide type is insensitive to environmental disturbances and can transmit wide frequency band signals.

In this paper, for measuring intra-body propagation signals we utilize the waveguide type, which consists of general-purpose measuring instruments: a signal generator, digital oscilloscope as a detector and body surface electrodes with gelled pads. The measurement site is antebrachial region for making the measurement easy. A white noisesignal is passed through one electrode pair from the signal generator. On the other hand, a leaked electromagnetic wave is propagated and then extracted at the digital oscilloscope through another electrode pair. While measuring arms are kept in the air since the amplitude of the propagated signal is reduced when the arms are set on the desk.

As individual features, we extract the spectrum of the intra-body propagation signal using the FFT. Spectra of a subject on five days, that is, intravariation of the intra-body propagation spectrum is observed. It is confirmed that these spectral distribution have some commonality but partly differ, for example, at 80-100 MHz. Therefore, it is anticipated that the intra-variation of the intra-body propagation spectrum is relatively large. Next, we show the spectra of five subjects (A, B, C, D, and E) where inter-variation of the intra-body propagation spectrum is observed. Detailed observation suggests that individuals have different distribution of the spectrum but for instance, spectra of the subjects: C and E are similar at 0-50 MHz; therefore,

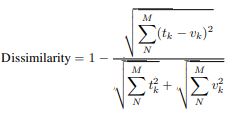


**Fig: Block diagram of existing method**.

It is assumed that the inter-variation is not all that large. From the above comparisons, the spectrum of the intrabody propagation signal is expected to be as individual features while for that it is necessary to examine which frequency bands should be used for better verification performance since some have large intra-variation, and some have small inter-variation.

Verification is performed based on the dissimilarity of the intra-body propagation spectrum. The flow diagram of the verification is depicted in. First of all, templates are prepared as comparison targets in the enrollment stage. An intra-body propagation signal of a user is measured and then an amplitude spectrum is extracted. Repeating it L times and then ensemble-averaging the L amplitude spectra, the template for the user is obtained. However, the intra-variation of the intra-body propagation spectrum is large.

Therefore, smoothing is applied to the spectrum. Concretely, sampled data obtained in a single measurement are divided into several subgroups, a spectrum is extracted in each subgroup, and then spectra in all subgroups are ensemble-averaged. As the number of subgroups is increased, the effect of the smoothing might be elevated but the number of data for FFT analysis is decreased and it results in reduction of frequency resolution and thereby might degrade the verification performance. The smoothed spectrum and its mean value are stored as the template. This procedure is performed for all users in advance to verification. On the other hand, in the verification stage, each user declares who oneself is by giving his/her name or ID number to the system, which specifies the template. And the intrabody propagation signal for verification (verification signal) is measured and then the smoothed spectrum and its mean value are extracted in the same way as templates. Next, normalization is performed by equalizing the mean value of the verification spectrum with that of the template, and the dissimilarity is calculated as



Where tk, vk are the amplitude spectrum of the verification signal and the template, respectively. k is a frequency index, and M and N are respectively upper and lower limits of the frequency band used in the verification. The numerator of the second term in the right-hand side corresponds to Euclidian distance between the verification spectrum and the template. The denominator is their power spectra; therefore, the distance is normalized and as a result the dissimilarity always falls within 0 and 1. Finally, the dissimilarity is compared with a threshold. If the dissimilarity is smaller than the threshold, the user presented the verification signal is regarded as genuine.

As described above, the verification based on the Euclidian distance is simple but not adequate for employing the authentication using the intra-body propagation signal in practical applications, so that we introduce the support vector machine (SVM) into the verification process in order to improve the verification performance further. As a pattern classification method based on supervised learning, the SVM has been proposed. The SVM learns a separating hyperplane which maximizes the distance (margin) between two classes and so performs higher separation capability for unlearned data of the classes an illustration of the separating hyperplane of two classes: C1 and C2. However, the two classes in practical applications are almost linearlyinseparable. Therefore, they are transformed to higherdimensional space by using a kernel function and thereby become linearly-separable there. In general, the polynomial kernel, Gaussian kernel, and RBF kernel are used as the kernel function.

The flowchart of verification with the SVM is shown. In advance to the verification, the enrollment (learning) phase is performed. For preparing learning data, intrabody propagation signals for all users are measured and then their spectra are extracted and smoothed and normalized. The smoothing is the same as the conventional method. In the normalization, mean values of all amplitude spectra are adjusted to one. User specific models are constructed by supervising the classification of the user’s own data and others’ ones to +1 and -1, respectively. In the verification (testing) phase, a spectrum of a user is input to the corresponding model, that is, already-learned SVM and then the SVM output a predictive value. If the value has positive sign, the spectrum is regarded as of the genuine user. Inversely, if the value is negative, the user is regarded as an imposter.

**CHAPTER 4**

**PROPOSED METHOD**

This proposed method is implemented to protect the data and devices securely. We use ECG based dataset for authentication which is collected from the given paper. We have enrollment and verification stages. The signal is plotted form this given database. Then we apply the IIR butterworth filter for filtering operation. Non fiducial is used for feature extraction. Daubechies wavelet is applied in two phases. After that network random algorithm is performed for biometric authentication. The below diagram represent the block diagram of the proposed method.

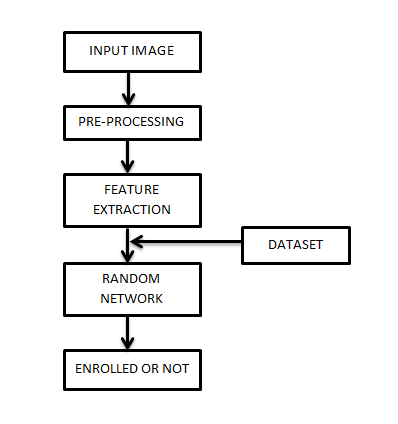


Figure: Block diagram of proposed method.

**Butterworth filter:**

This type of [signal processing filter](https://en.wikipedia.org/wiki/Filter_(signal_processing)) designed to have a [frequency response](https://en.wikipedia.org/wiki/Frequency_response) as flat as possible in the [passband](https://en.wikipedia.org/wiki/Passband). It is also referred to as a maximally flat magnitude filter. It was first described in 1930 by the British [engineer](https://en.wikipedia.org/wiki/Engineer) and [physicist](https://en.wikipedia.org/wiki/Physicist) [Stephen Butterworth](https://en.wikipedia.org/wiki/Stephen_Butterworth) in his paper entitled "On the Theory of Filter Amplifiers". Butterworth had a reputation for solving "impossible" mathematical problems. At the time, [filter design](https://en.wikipedia.org/wiki/Filter_design) required a considerable amount of designer experience due to limitations of the [theory then in use](https://en.wikipedia.org/wiki/Image_parameter_filter). The filter was not in common use for over 30 years after its publication. Butterworth stated that: "An ideal electrical filter should not only completely reject the unwanted frequencies but should also have uniform sensitivity for the wanted frequencies".

Such an ideal filter cannot be achieved, but Butterworth showed that successively closer approximations were obtained with increasing numbers of filter elements of the right values. At the time, filters generated substantial ripple in the passband, and the choice of component values was highly interactive. Butterworth showed that a [low pass filter](https://en.wikipedia.org/wiki/Low_pass_filter) could be designed whose cutoff frequency was normalized to 1 radian per second and whose frequency response ([gain](https://en.wikipedia.org/wiki/Gain_(electronics))) was



Where ω is the [angular frequency](https://en.wikipedia.org/wiki/Angular_frequency) in radians per second and n is the number of [poles](https://en.wikipedia.org/wiki/Pole_(complex_analysis)) in the filter equal to the number of reactive elements in a passive filter. If ω = 1, the amplitude response of this type of filter in the passband is 1/√2 ≈ 0.707, which is half power or −3 dB Butterworth only dealt with filters with an even number of poles in his paper. He may have been unaware that such filters could be designed with an odd number of poles. He built his higher order filters from 2-pole filters separated by vacuum tube amplifiers. His plot of the frequency response of 2, 4, 6, 8, and 10 pole filters is shown as A, B, C, D, and E in his original graph.

Butterworth solved the equations for two- and four-pole filters, showing how the latter could be cascaded when separated by [vacuum tube](https://en.wikipedia.org/wiki/Vacuum_tube) [amplifiers](https://en.wikipedia.org/wiki/Amplifier) and so enabling the construction of higher-order filters despite [inductor](https://en.wikipedia.org/wiki/Inductor) losses. In 1930, low-loss core materials such as [molypermalloy](https://en.wikipedia.org/wiki/Molypermalloy_Powder_Core) had not been discovered and air-cored audio inductors were rather lossy. Butterworth discovered that it was possible to adjust the component values of the filter to compensate for the winding resistance of the inductors. He used coil forms of 1.25″ diameter and 3″ length with plug-in terminals. Associated capacitors and resistors were contained inside the wound coil form. The coil formed part of the plate load resistor. Two poles were used per vacuum tube and RC coupling was used to the grid of the following tube. Butterworth also showed that the basic low-pass filter could be modified to give [low-pass](https://en.wikipedia.org/wiki/Low-pass_filter), [high-pass](https://en.wikipedia.org/wiki/High-pass_filter), [band-pass](https://en.wikipedia.org/wiki/Band-pass_filter) and [band-stop](https://en.wikipedia.org/wiki/Band-stop_filter) functionality.

The frequency response of the Butterworth filter is maximally flat (i.e. has no [ripples](https://en.wikipedia.org/wiki/Ripple_(filters))) in the passband and rolls off towards zero in the stopband. When viewed on a logarithmic [Bode plot](https://en.wikipedia.org/wiki/Bode_plot), the response slopes off linearly towards negative infinity. A first-order filter's response rolls off at −6 dB per [octave](https://en.wikipedia.org/wiki/Octave_(electronics)) (−20 dB per [decade](https://en.wikipedia.org/wiki/Decade_(log_scale))) (all first-order lowpass filters have the same normalized frequency response). A second-order filter decreases at −12 dB per octave, a third-order at −18 dB and so on. Butterworth filters have a monotonically changing magnitude function with ω, unlike other filter types that have non-monotonic ripple in the passband and/or the stopband. Compared with a [Chebyshev](https://en.wikipedia.org/wiki/Chebyshev_filter) Type I/Type II filter or an [elliptic filter](https://en.wikipedia.org/wiki/Elliptic_filter), the Butterworth filter has a slower [roll-off](https://en.wikipedia.org/wiki/Roll-off), and thus will require a higher order to implement a particular [stopband](https://en.wikipedia.org/wiki/Stopband) specification, but Butterworth filters have a more linear phase response in the pass-band than Chebyshev Type I/Type II and elliptic filters can achieve.

**Daubechies wavelets:**

The Daubechies wavelets, based on the work of [Ingrid Daubechies](https://en.wikipedia.org/wiki/Ingrid_Daubechies), are a family of [orthogonal wavelets](https://en.wikipedia.org/wiki/Orthogonal_wavelet) defining a [discrete wavelet transform](https://en.wikipedia.org/wiki/Discrete_wavelet_transform) and characterized by a maximal number of vanishing [moments](https://en.wikipedia.org/wiki/Moment_(mathematics)) for some given [support](https://en.wikipedia.org/wiki/Support_(mathematics)). With each wavelet type of this class, there is a scaling function (called the father wavelet) which generates an orthogonal [multi resolution analysis](https://en.wikipedia.org/wiki/Multiresolution_analysis).

In general the Daubechies wavelets are chosen to have the highest number A of vanishing moments, (this does not imply the best smoothness) for given support width (number of coefficients) 2A.[[1]](https://en.wikipedia.org/wiki/Daubechies_wavelet#cite_note-1) There are two naming schemes in use, DN using the length or number of taps, and dbA referring to the number of vanishing moments. So D4 and db2 are the same wavelet transform.Among the 2A−1 possible solutions of the algebraic equations for the moment and orthogonality conditions, the one is chosen whose scaling filter has external phase. The wavelet transform is also easy to put into practice using the [fast wavelet transform](https://en.wikipedia.org/wiki/Fast_wavelet_transform). Daubechies wavelets are widely used in solving a broad range of problems, e.g. self-similarity properties of a signal or [fractal](https://en.wikipedia.org/wiki/Fractal) problems, signal discontinuities, etc.

The Daubechies wavelets are not defined in terms of the resulting scaling and wavelet functions; in fact, they are not possible to write down in [closed form](https://en.wikipedia.org/wiki/Closed_form_expression). The graphs below are generated using the [cascade algorithm](https://en.wikipedia.org/wiki/Cascade_algorithm), a numeric technique consisting of inverse-transforming [1 0 0 0 0 ... ] an appropriate number of times. Note that the spectra shown here are not the frequency response of the high and low pass filters, but rather the amplitudes of the continuous Fourier transforms of the scaling (blue) and wavelet (red) functions. Daubechies orthogonal wavelets D2–D20 resp. db1–db10 are commonly used. The index number refers to the number N of coefficients. Each wavelet has a number of zero moments or vanishing moments equal to half the number of coefficients. For example, D2 has one vanishing moment, D4 has two, etc.

A vanishing moment limits the wavelets ability to represent [polynomial](https://en.wikipedia.org/wiki/Polynomial) behaviour or information in a signal. For example, D2, with one vanishing moment, easily encodes polynomials of one coefficient, or constant signal components. D4 encodes polynomials with two coefficients, i.e. constant and linear signal components; and D6 encodes 3-polynomials, i.e. constant, linear and [quadratic](https://en.wikipedia.org/wiki/Quadratic_polynomial) signal components. This ability to encode signals is nonetheless subject to the phenomenon of scale leakage, and the lack of shift-invariance, which raise from the discrete shifting operation (below) during application of the transform. Sub-sequences which represent linear, [quadratic](https://en.wikipedia.org/wiki/Quadratic_polynomial) (for example) signal components are treated differently by the transform depending on whether the points align with even- or odd-numbered locations in the sequence. The lack of the important property of [shift-invariance](https://en.wikipedia.org/wiki/Translational_invariance), has led to the development of several different versions of a [shift-invariant (discrete) wavelet transform](https://en.wikipedia.org/wiki/Shift_invariant_wavelet_transform).

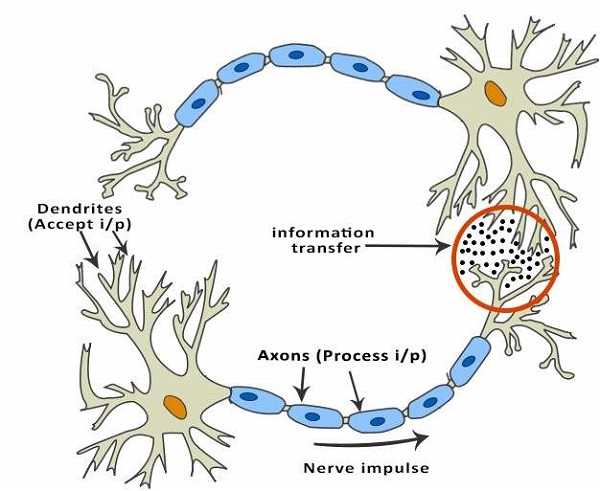
**ANN:**

An artificial neural network is an adaptive system that learns by using interconnected nodes or neurons in a layered structure that resembles a human brain. A neural network can learn from data so it can be trained to recognize patterns, classify data, and forecast future events.

A neural network breaks down the input into layers of abstraction. It can be trained using many examples to recognize patterns in speech or images, for example, just as the human brain does. Its behavior is defined by the way its individual elements are connected and by the strength, or weights, of those connections. These weights are automatically adjusted during training according to a specified learning rule until the artificial neural network performs the desired task correctly.

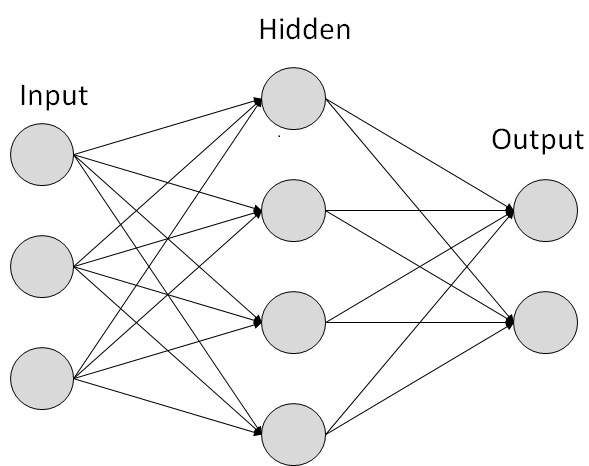
## Structure of ANN:

The idea of ANNs is based on the belief that working of human brain by making the right connections can be imitated using silicon and wires as living neurons and dendrites. The human brain is composed of 86 billion nerve cells called neurons. They are connected to other thousand cells by Axons. Stimuli from external environment or inputs from sensory organs are accepted by dendrites. These inputs create electric impulses, which quickly travel through the neural network. A neuron can then send the message to other neuron to handle the issue or does not send it forward. ANNs are composed of multiple nodes, which imitate biological neurons of human brain. The neurons are connected by links and they interact with each other. The nodes can take input data and perform simple operations on the data. The result of these operations is passed to other neurons. The output at each node is called its activation or node value. Each link is associated with weight. ANNs are capable of learning, which takes place by altering weight values. The simple ANN can be shows in Fig: 2.



**Fig: 3 Simple ANN**

This artificial neuron can be considered as a node and interconnection of nodes is called as network. Each node is connected by a link with numerical weights and these weights are stored in the neural network and updated through the process called learning. An ANN essentially has three layers of neurons namely, input layer, output layer and hidden layer. The block diagram can be shown below Fig: 3.



**Fig: 4 Block Diagram of ANN.**

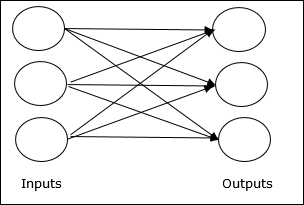
## Types of Artificial Neural Networks:

There are two Artificial Neural Network topologies Feed Forward and Feedback.

### Feed Forward ANN:

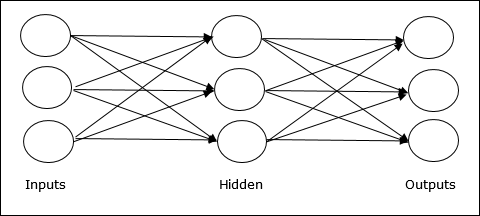
In this ANN, the information flow is unidirectional. A unit sends information to other unit from which it does not receive any information. There are no feedback loops. They are used in pattern generation/recognition/classification. They have fixed inputs and outputs. It is a non-recurrent network having processing units/nodes in layers and all the nodes in a layer are connected with the nodes of the previous layers. The connection has different weights upon them. It may be divided into the following two types

* **Single layer feed forward network:**The concept is of feed forward ANN having only one weighted layer. In other words, we can say the input layer is fully connected to the output layer. The block diagram can be shown below Fig: 4.



**Fig: 5 Block Diagram of Single layer feed forward network.**

* **Multilayer feed forward network:** The concept is of feed forward ANN having more than one weighted layer. As this network has one or more layers between the input and the output layer, it is called hidden layers. The Block diagram can be shown below Fig: 5.

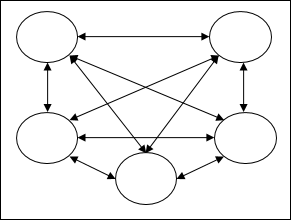


**Fig: 6 Block Diagram of Multilayer feed forward network**

### Feedback Network:

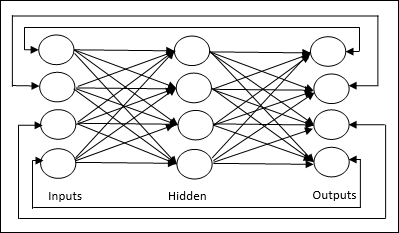
As the name suggests, a feedback network has feedback paths, which means the signal can flow in both directions using loops. This makes it a non-linear dynamic system, which changes continuously until it reaches a state of equilibrium. It may be divided into the following types −

* **Recurrent networks:** They are feedback networks with closed loops. Following are the two types of recurrent networks.
* **Fully recurrent network:** It is the simplest neural network architecture because all nodes are connected to all other nodes and each node works as both input and output. The Block diagram can be shown below Fig: 6.



**Fig: 7 Block Diagram of Fully recurrent network.**

* **Jordan network:** It is a closed loop network in which the output will go to the input again as feedback as shown in the following diagram. The Block diagram can be shown below Fig: 7.



**Fig: 8 Block Diagram of Jordan network.**

## Machine Learning in ANN:

The procedure that consists in estimating the parameters of neurons (setting up the weights) so that the whole network can perform a specific task is called learning. ANNs are capable of learning and they need to be trained. There are several learning strategies −

* **Supervised Learning:**   It involves a teacher that is scholar than the ANN itself. For example, the teacher feeds some example data about which the teacher already knows the answers. For example, pattern recognizing. The ANN comes up with guesses while recognizing. Then the teacher provides the ANN with the answers. The network then compares it guesses with the teacher’s “correct” answers and makes adjustments according to errors.
* **Unsupervised Learning:**  It is required when there is no example data set with known answers. For example, searching for a hidden pattern. In this case, clustering i.e. dividing a set of elements into groups according to some unknown pattern is carried out based on the existing data sets present.
* **Reinforcement Learning:** This strategy built on observation. The ANN makes a decision by observing its environment. If the observation is negative, the network adjusts its weights to be able to make a different required decision the next time.

**CHAPTER 5**

**ADVANTAGES AND APPLICATIONS**

**Advantages:**

* Gives the better authentication results of biometric.
* Accuracy is more.

**Applications:**

There are numerous applications for the use of Biometric Technology, but the most common ones are as follows:

* Logical Access Control.
* Physical Access Control.
* Time and Attendance.
* Law Enforcement.
* Surveillance.

**CHAPTER 6**

**SOFTWARE & HARDWARE REQUIREMENTS**

**INTRODUCTION TO MATLAB**

**What Is MATLAB?**

The name MATLAB stands for Matrix Laboratory. The software is built up around vectors and matrices. This makes the software particularly useful for linear algebra but MATLAB is also a great tool for solving algebraic and differential equations and for numerical integration. MATLAB has powerful graphic tools and can produce nice pictures in both 2D and 3D. It is also a programming language, and is one of the easiest programming languages for writing mathematical programs. Such variables make MATLAB an outstanding research and education instrument.

In reality, the original MATLAB was developed to proceed to provide instant access to the differentiated programs available through the LINPACK (linear system package) and EISPACK (Eigen system package) project development projects. It combines the machine, visualization, and software application. Furthermore, MATLAB is a groundbreaking developmental instructional methodology: it has data management systems, offers built tools for configuration and initialization, and promotes object-oriented programming. Compared to traditional programming languages (e.g., C, FORTRAN), MATLAB has several improvements for solving various problems.

MATLAB abilities a family of add-on software program utility software application software program software utility software-unique solutions called toolboxes. Very essential to maximum customers of MATLAB, toolboxes assist you to studies and observe specialized technology. Toolboxes are entire collections of MATLAB abilities (M-files) that increase the MATLAB surroundings to remedy precise schooling of problems. Areas in which toolboxes are to be had embody signal processing, manipulate systems, neural networks, fuzzy correct judgment, wavelets, simulation, and hundreds of others.

It has powerful built-in procedures that make a wide range of simulations possible. User interface instructions that make the presentation of outcomes instantly accessible are also convenient to use. In packages referred to as toolboxes, particular requirements are gathered. Signal processing software tools, symbolic computation, operations research, simulation, optimization, and many other computational engineering and technology fields are available. MATLAB is an incremental innovation whose basic information element is an array with no material selection necessary. Through 1984, the software kit has been available commercially and is now known as a standard instrument at most educational institutions and companies around the globe.

**Brief History of MATLAB:**

In the late 1970s, Cleve Molar, the chairperson of the computer programming professor at the University of New Mexico, began the creation of MATLAB. The first MATLAB ® was not a software application; it was a basic matrix simulator that was immersive. No applications, no toolboxes, no illustrations and no ODEs or FFTs appeared present. He built it to give the students to have access to LINPACK and EISPACK without studying FORTRAN. A sequence of scientific journals by J. was the computational justification for the first edition of MATLAB. Authored between 1965 and 1970 by H. Wilkinson and 18 of his associates and later compiled in the Handbook for Automatic Computation, Volume II, Linear Algebra, edited by Wilkinson and C. From Reinsch. Such papers introduce algorithm is used to solve the matrix standard curve and own meaning concerns, incorporated in Algol 60.

I taught mathematical procedures and quantitative simulation at the University of New Mexico in the 1970s and early 1980s and expected my colleagues to have simple access to LINPACK and EISPACK without having to write FORTRAN programmers. I meant not heading through all the centralized data storage and continuous edit-compile-link-load-execute phase by "quick access," which was typically necessary on the centralized personal Throughout a visit by molar to Stanford University in 1983, Jack Little, an engineer, was introduced to it. He joined molar and Steve Bangert, recognizing his commercial ability. To progress its advancement, they tried to rewrite MATLAB in C and produced Math Works in 1984. These re-written repositories are recognized as JACKPAC. In 2000, MATLAB was redesigned using such a newer array, LAPACK, of matrix manipulation databases. MATLAB had first been implemented by control engineering academics and organizations, Little's specialization, but soon spread to several other fields. It is once again used throughout education, particularly in linear algebra teaching and numerical methods, and is common among researchers involved in the manufacture of images. EISPACK and LINPACK:

In 1970, the U.S. was suggested by a group of researchers at Argonne National Laboratory. National Science Foundation (NSF) to investigate the methods, costs, and resources needed in some problematic ways to enhance, evaluate, and spread information high-quality mathematical software and to evaluate, certify, disseminate, and help computational software applications. By transforming the Algol instructions for eigenvalue problem issues in the training manual into FORTRAN and experimenting systematically on processing and functionality, the group has developed EISPACK (Matrix Eigen system Package). In 1971, the first version of EISPACK was announced, and in 1976, the second.

Four of us, Jack Dongarra, Pete Stewart, Jim Bunch, and myself, submitted a further research study to the NSF in 1975 that would explore methodology for quantitative computer programming. The programmer itself, called LINPACK, for Linear Equation Bundle, will be a natural consequence. Higher minimum wage was also the center of this project. LINPACK appeared in FORTRAN; the interpretation from Algol was not included. In every one of the four mathematical segmented images, the kit generated 44 sub processes. The LINPACK and EISPACK ventures have been failures in a way. To explore the methods, costs, and expertise needed to develop, validate, and distribute high-quality quantitative software, we suggested research programs to the NSF. We've never written a study or document describing those targets. We were only making apps.

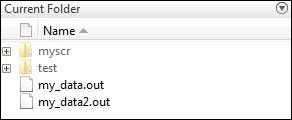
So, I researched the book Algorithms + Data Structures = Programs by Nicklaus Wirth and discovered how and where to parse software packages. The very first MATLAB I wrote was an acronym for Matrix Laboratory in FORTRAN, except the only data form being the matrix. The challenge became a kind of pleasure, a new component of mathematics learning for me and content to be used for my learners. There was never any coordinated external support and, undoubtedly, no marketing plan. This first MATLAB was just a matrix calculation that was collaborative. All designated vocabulary and functionality are shown in this screenshot of the start-up screen. Just 71 are here. You would have to get the encryption keys from me to implement some method, construct a FORTRAN regular expression, add your regular expression to the parsing table, and reinstalling MATLAB.

**Starting MATLAB:**

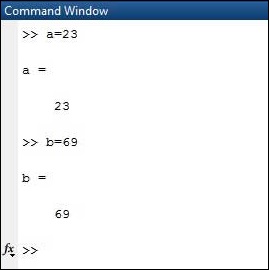
You can access MATLAB after signing across your database by double-clicking on your Computers desktop's MATLAB easily identify (MATLAB 7.0.4). A special monitor, designated the MATLAB workspace, emerges whenever you start MATLAB. A window that includes other applications is the desktop. The major tools within or accessible from the desktop are:

* The Command Window
* The Command History
* The Workspace
* The Current Directory
* The Help Browser

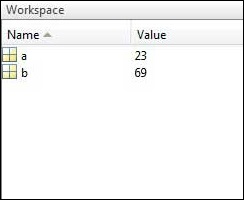
**Current Folder:** This panel allows you to access the project folders and files.



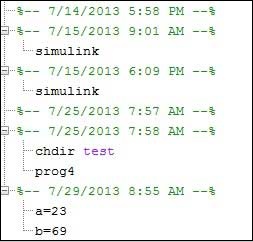
**Command Window:** This is the main area where commands can be entered at the command line. It is indicated by the command prompt (>>).



**Workspace:**  The workspace shows all the variables created and/or imported from files.



**Command History:** This panel shows or return commands that are entered at the command line.



**Help Browser:**

The critical way to get assist online is to use the MATLAB help browser, opened as a separate window every through clicking at the question mark photograph (?) on the computing tool toolbar, or through manner of typing assist browser on the spark off in the command window. The assist Browser is an internet browser blanketed into the MATLAB computing tool that shows a Hypertext Markup Language (HTML) files. The Help Browser consists of panes, the help navigator pane, used to find out information, and the show pane, used to view the information. Self-explanatory tabs apart from navigator pane are used to performs are searching out.

**MATLAB language:**

With controlled flow statements, features, data structures, input / output, and object-oriented programming functions, this is an elevated-level matrix / array language. It enables both software development in the small and programming in the big to easily produce fast and dirty throw-away programmers to construct full large and complex distributed applications.

**MATLAB working environment:**

This is the collection of software and equipment you work with it as a user or designer of MATLAB. It includes the facilities for handling and importing and exporting information for the parameters in your environment. It also contains features for M-files, MATLAB applications, creation, management, monitoring, and characterization.

**MATLAB mathematical function library:**

This is a large set of optimization models extending from mathematical objects such as number, sinus, quadratic formula, and complicated arithmetic, toward more advanced functions such as inverse matrix, matrix eigenvalues, transformations of Bessel, and rapid transformations of quantum mechanics.

**MATLAB Application Program Interface (API):**

This is a framework that helps you to write MATLAB-interacting C and FORTRAN programmers. This includes services for accessing MATLAB (dynamic linking) procedures, accessing MATLAB as a virtual engine, and learning to read MAT-files.

**MATLAB DESKTOP:**

MATLAB Desktop is the precept MATLAB utility window. The computing tool includes five sub home windows, the command window, the workspace browser, the modern-day-day list window, the command records window, and one or greater decide domestic windows, which is probably confirmed high-quality on the identical time due to the truth the client suggests a photo. The command window is in which the character types MATLAB instructions and expressions at the spark off (>>) and in which the output of these commands is displayed. MATLAB defines the workspace because the set of variables that the client creates in a bit consultation. The workspace browser suggests those variables and some facts about them. Double clicking on a variable within the workspace browser launches the Array Editor, which may be used to gain statistics and profits instances edit exceptional homes of the variable.

The modern-day-day-day Directory tab above the workspace tab suggests the contents of the cutting-edge list, whose path is shown inside the modern-day list window. For example, in the home windows on foot machine the path is probably as follows: C:MATLABWork, indicating that listing “artwork” is a subdirectory of the number one list “MATLAB”; WHICH IS INSTALLED IN DRIVE C. Clicking on the arrow within the modern list window suggests a listing of these days used paths. Clicking at the button to the right of the window permits the individual to trade the present day listing. MATLAB uses a seeking out path to find out M-documents and one-of-a-type MATLAB associated documents, which can be put together in directories within the computer document tool. Any report run in MATLAB need to be dwelling in the modern-day-day listing or in a list that is on is looking for course. By default, the documents supplied with MATLAB and math works toolboxes are included inside the searching out direction. The first-rate manner to look which directories are on the searching out route. The satisfactory manner to appearance which directories are speedy the quest route, or to characteristic or regulate a searching for course, is to pick out outset path from the File menu the computing device, and then use the set course talk discipline. It is proper exercise to feature any generally used directories to the hunt route to avoid again and again having the exchange the cutting-edge-day listing.

The Command History Window contains a file of the instructions a person has entered in the command window, together with every contemporary-day and former MATLAB periods. Previously entered MATLAB instructions can be determined on and re-completed from the command statistics window thru proper clicking on a command or series of commands. This movement launches a menu from which to select numerous options similarly to executing the commands. This is useful to select out abilities options in addition to executing the instructions. This is a beneficial feature at the equal time as experimenting with numerous commands in a piece session.

**Using the MATLAB Editor to create M-Files:**

The MATLAB editorial manager is every a literary substance proofreader particular for growing M-facts and a graphical MATLAB debugger. The supervisor can seem in a window through command facts technique for itself, or it is probably a right-clicking inside the PC. M-information this gadget signified through the use of the expansion .M, as in pixel up .M. The MATLAB editorial supervisor window has a few draw down menus for obligations collectively with sparing, seeing, and troubleshooting facts. Since it plays more than one easy tests and furthermore affects utilization of shade to separate among exclusive variables of code, this article editorial supervisor is often supported due to reality the system of a need for composing and altering M-talents. To open the manager, type the at the enact opens the M-document filename. M in a supervisor window, sorted out for enhancing. As stated earlier than, the file should be inside the cutting-edge posting, or in a posting in the are seeking out direction.

## Features of MATLAB:

Following are the basic features of MATLAB.

* It is a high-level language for numerical computation, visualization and application development.
* It also provides an interactive environment for iterative exploration, design and problem solving.
* It provides vast library of mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, numerical integration and solving ordinary differential equations.
* It provides built-in graphics for visualizing data and tools for creating custom plots.
* MATLAB's programming interface gives development tools for improving code quality maintainability and maximizing performance.
* It provides tools for building applications with custom graphical interfaces.
* It provides functions for integrating MATLAB based algorithms with external applications and languages such as C, Java, .NET and Microsoft Excel.

## Uses of MATLAB:

MATLAB is widely used as a computational tool in science and engineering encompassing the fields of physics, chemistry, math and all engineering streams. It is used in a range of applications including

* Signal Processing and Communications
* Image and Video Processing
* Control Systems
* Test and Measurement
* Computational Finance
* Computational Biology

**Applications of MATLAB:**

MATLAB can also be used as tool to model specific electronic networks, but MATLAB's major advancement enable it a much more successful framework for artificial intelligence, robotics, image analysis, wireless networking, machine learning, data analytics, etc. While it is mainly used throughout the field of software engineering by circuit departments and mechanics to overcome a simple number of difficulties, its implementation is extensive. It is a tool that enables computation, programming and graphically visualizing the results. The basic data element of MATLAB as the name suggests is the Matrix or an array. MATLAB toolboxes are professionally built and enable you to turn your imaginations into reality. MATLAB programming is quite similar to C programming and just requires a little brush up of your basic programming skills to start working.

Below are a few applications of MATLAB –

* **Statistics and machine learning (ML)**

**For developers, this software tool in MATLAB can become very useful. Statistical approaches may be quickly applied, including such quantitative or descriptive statistics. The circumstance with artificial intelligence is like that. To overcome modern-day challenges, various variants can indeed be implemented. For big data technologies, the architectures used would also be used.**

* **Curve fitting**

The toolbox for numerical integration includes determining the sequence of data occurrences. After receiving a specific trend which can be a curve or surface, it is difficult to predict the future patterns. It is possible to plot further, measure complex numbers, correlations, interpolation, etc.

* **Control systems**

Technologies can be acquired by design. It is necessary to achieve considerations including certain closed-loop, open-loop, its compatibility and testability, Bode map, Nyquist plot, etc. It is possible to imagine different switching strategies such as PD, PI and PID. Throughout the time domain or frequency domain, analysis has been performed.

* **Signal Processing**

Signals and machines and signal processing are demonstrated in various disciplines of technology. But MATLAB offers the chance for this to be properly visualized. It is possible to perform numerous transforms on any transmitted criterion, along with Laplace, Z, etc. It is possible to verify number theory. In the time domain or frequency domain, analysis has been performed. It is possible to use several built-in features.

* **Mapping**

In different domains, geography has many applications. For instance, the distributed database tool is very significant in Big Data, which has several applications in the real world. Data mapping may be performed through theft investigation or fraudulent financial identification, multiple regressions, emergency analysis, social networking modelling techniques, data tracking, etc.

* **Deep learning**

It's an artificial intelligence category which could be used for speech recognition, identification of financial crime, and interpretation of medical images. It is possible to use techniques such as data set, artificial neural networks (ANN), probabilistic reasoning or a variation of such techniques.

* **Financial analysis**

Before beginning any venture, an entrepreneur must perform a comprehensive questionnaire and financial review to prepare the line of treatment. In MATLAB, the equipment required though are all appropriate. Characteristics can be defined, such as competitiveness, financial stability, profitability, and consistency. It is possible to determine company valuation, financial analysis, return on investment, etc.

* **Image processing**

Bar code generators, portrait (face attractiveness, obscuring the background, face detection), image enhancement, etc., seem to be the most important requirement we experience almost every day. In transmitting information from far distant channels and obtaining and interpreting that in the same way, digital image processing also plays a very important role. There are appropriate implementations to benefit these all implementations.

* **Text analysis**

Subjectivity analysis has been performed based on the text. For just about any text submitted within the next few milliseconds, generally provides millions of search engine results. Due to various text processing, all of this is conceivable. In forensic evidence, handwritten identification can be accomplished. No restriction to the specification and only one application that can do most of anything.

* **Electric vehicles designing**

Often used autonomous vehicle modelling although with a difference in device inputs to analyses its effectiveness. Comparative analysis of acceleration torque, constructing and designed to simulate an engine, things of that nature.

* **Aerospace**

This toolbox in MATLAB is used for analyzing the navigation and to visualize flight simulator.

* **Audio toolbox**

It offers audio processing, speech interpretation, and acoustic measurement instruments. It also offers applications for extraction of audio and speech features and manipulation of audio signals.

**Hardware:**

**Operating Systems:**

• Windows 10

• Windows 7 Service Pack 1

• Windows Server 2019

• Windows Server 2016

**Processors:**

Minimum: Any Intel or AMD x86-64 processor

Recommended: Any Intel or AMD x86-64 processor with four logical cores and AVX2 instruction set support

**Disk:**

Minimum: 2.9 GB of HDD space for MATLAB only, 5-8 GB for a typical installation

Recommended: An SSD is recommended a full installation of all Math Works products may take up to 29 GB of disk space

**RAM:**

Minimum: 4 GB

Recommended: 8 GB

**CHAPTER 7**

**DIGITAL IMAGE PROCESSING**

**Digital image processing:**

Digital Image Processing includes image processing techniques using a computer programmer. We could also assume that machine learning algorithms are used to retrieve some helpful information in terms of accuracy and speed image.

**Image:**

In other words, a two-dimensional array explicitly considered to be significant which characterize an image. The picture consists of a specific number of objects, some of which, at a specific position, has a specific meaning. Such techniques are referred to as components of images, elements of images, and pixels.

A Pixel is most widely used to denote the elements of an Image. To be processed digitally, it has to be **sampled** and transformed into a matrix of numbers. Since a computer represents the numbers using finite precision, these numbers have to be **quantized** to be represented digitally. Digital image processing consists of the manipulation of those finite precision numbers. The processing of digital images can be divided into several classes: **image enhancement, image restoration, image analysis,** and image compression.

**How a digital image is formed?**

Since capturing an image from a camera is a physical process. The sunlight is used as a source of energy. A sensor array is used for the acquisition of the image. So when the sunlight falls upon the object, then the amount of light reflected by that object is sensed by the sensors, and a continuous voltage signal is generated by the amount of sensed data. In order to create a digital image, we need to convert this data into a digital form. This involves sampling and quantization. (They are discussed later on). The result of sampling and quantization results in a two dimensional array or matrix of numbers which are nothing but a digital image.

**Image processing mainly include the following steps:**

* Importing the image via image acquisition tools.
* Analyzing and manipulating the image.
* Output in which result can be altered image or a report which is based on analyzingthat image.

An image can be portrayed as a - dimensional trademark f(x, y), in which x and y are spatial directions, and the sufficiency of any combine of instructions (x, y) is known as the pressure or darkish degree of the image at that inconvenience. Whenever x, y and the abundance estimations of f are on the entire confined discrete quantities, we call the picture a virtual photo. The district of DIP alludes to getting ready computerized photo through strategies for to method for MATLAB. Manner of the use of advanced pc. Computerized image incorporates of a confined form of things, every one in every of which has a chosen location and fee. The components are alluded to as pixels.

Vision is the maximum innovative of our sensor, so it isn't sudden that photograph play the unmarried greatest important component in human conviction. Nonetheless, in appraisal to humans, who are controlled to the visible band of the EM variety imaging machines cover nearly the complete EM range, starting from gamma to radio waves. They can highlight also on previews created with the valuable useful manual of benefits that people aren't conscious of accomplice with airship picture. There isn't commonly any present settlement among creators concerning in which photo managing stops and specific associated districts nearby aspect photo evaluation& workstation imaginative and prescient start.

In a few instances a difference is made through the use of characterizing picture handling as an area wherein each the information and yield at a way are snap shots. This is constraining and predominantly manufactured restriction. The district of image investigation (photograph getting to know) is in amongst photograph getting ready and PC imaginative and insightful. There aren't any easy restrictions in the continuum from picture preparing at one prevent to complete ingenious and sensible on the inverse. In any case, one precious worldview is to revel in as a primary challenge three types of automatic procedures in this continuum: low-, mid-, and radical affirmation methodologies. Low-certificate way includes crude obligations which incorporates image preparing to reduce clamor, appraisal improvement and photo cleansing. A low-certificates approach is described through the way that very it inputs and yields are previews.

Mid-degree method on photographs incorporates of commitments which exemplify division, depiction of that question decrease them to a form becoming for pc getting ready and category of man or woman devices. A mid-degree method is portrayed thru technique for the reality that its resources of info broadly speaking are images anyway its yields are residences extricated from the ones photographs. At lengthy remaining better-degree making ready carries "Making history" of a meeting of analyzed gadgets, as in photo assessment and at the a broadened path give up of the continuum performing the psychological abilities often connected with human imaginative and prescient. Computerized image making ready, as formally depicted is utilized accurately in a huge kind of locales of astonishing social and financial price.

**PHASES OF IMAGE PROCESSING:**

* **Acquisition:**

It could be as simple as being given an image which is in digital form. The main work involves: a) Scaling b) Color conversion (RGB to Gray or vice-versa).

* **Image enhancement:**

It has been used to remove certain secret information from an image and is qualitative, among all the easiest and most desirable in the field of medical imaging.

* **Image restoration:**

It should be about an image's attractiveness, although it is analytical (restoration is defined as a mathematical or probability theory framework or deterioration of the image).

* **Color image processing:**

This concerns with pseudo coloring and colored versions of full color image processing that are specific to image processing.

* **Wavelets and Multi-resolution processing:**

It is foundation of representing images in various degrees.

* **Image compression:**

It requires the creation of certain roles to carry out this activity. This deals specifically with image size and resolution.

* **Morphological processing:**

It communicates with resources that are effective in texture classification & definition for automatically extracting components.

* **Segmentation:**

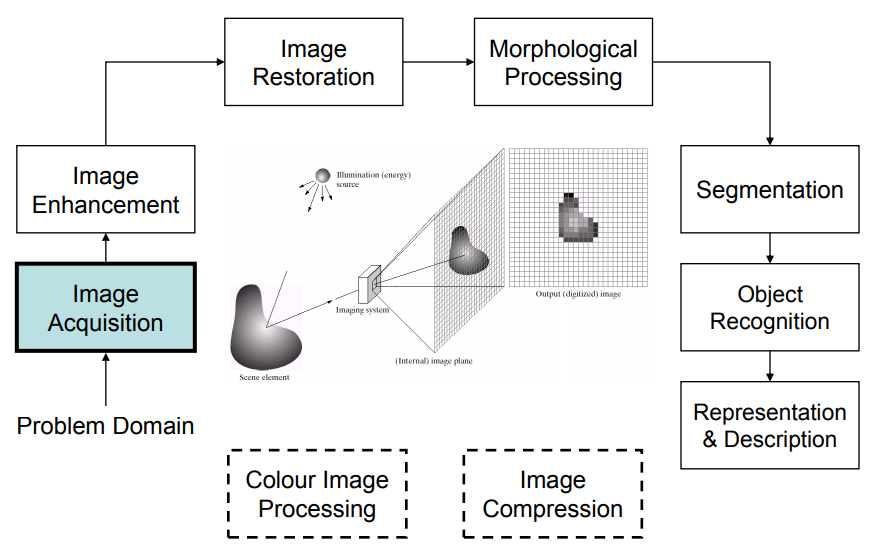
It includes partitioning an image into its constituent parts or objects. Autonomous segmentation is the most difficult task in Image Processing.

* **Representation and description:**

It approaches the categorization stage performance, only the possible solution to convert original information into data collected is to pick a representation.

* **Object detection and recognition:**

It is a process that assigns a label to an object based on its descriptor.



**Color image:**

It may be spoken to with the aid of techniques for manner of three capacities, R (xylem) for purple, G (xylem) for inexperienced and B (xylem) for blue. An image may be nonstop with renowned to the x and y arranges and moreover in sufficiency. Changing over this type of picture to digital form requires that the guidelines in addition to the adequacy to be digitized. Digitizing the set up's qualities is called analyzing. Digitizing the abundancy esteems is known as quantization.

**Grayscale image:**

There are eight sections and 256 tons of grey in the image; 1 = black and 255 = white. It takes 8 times further storage than that of a line-art picture to save. For example, it could be used in the printing department for exhibiting black and white photographs.

**Image Types:**

The tool compartment underpins 4 types of images:

1 .Intensity of pixels;

2. Twofold images;

3. Filed images;

4. R G B images.

Most monochrome image making ready sports are finished utilizing parallel or force pix, so our underlying highlight is on these image composes. Filed and RGB shading images.

**Intensity Images:**

A profundity picture is a measurements lattice whose traits were scaled to talk to goals. At the point while the components of a profundity photo are of class unit8, or elegance unit sixteen, they have complete quantity traits in the collection [0,255] and [0, 65535], for my part. On the off danger that the picture is of class twofold, the qualities are skimming phase numbers. Estimations of scaled, twofold pressure images are within the assortment [0, 1] by means of methods for subculture.

**Binary Images:**

Double depictions have a completely unique because of this in MATLAB.A parallel photograph is a sensible cluster 0s and1s.Thus, a variety of 1s whose features are of measurements excellence, say unit8, and isn't always concept approximately as a twofold image in MATLAB .A numeric show off is modified to paired the utilization of spotlight coherent. In this manner, if A can be a numeric showcase along problem 1s, we make a cluster B using the announcement.

B=logical (A)

In the event that A contains of elements separated from 0s and 1s.Use of the intelligent capability changes over all nonzero segments to sensible 1s and all sections with rate 0 to coherent 0s. Utilizing social and valid administrators further makes clever well-known shows. To take a look at if a cluster is coherent we make use of I practical trademark: is logical(c). In the occasion that c is a coherent show off, this trademark restores a 1.Otherwise returns a zero. Consistent cluster is probably modified over to numeric reveals the utilization of the statistics style transformation presents.

**Indexed Images:**

Framework define a m\*3 kinds of magnificence twofold containing skimming trouble esteems within the assortment [0, 1].The duration m of the guide are identical to the huge sort of shades it characterizes. Each line of manual suggests the blood pink, green and blue brought materials of a solitary shading. A recorded pix makes utilization of "coordinate mapping" of pixel electricity esteems shading map esteems. The tinge of every pixel is resolved through way of using the relating rate the whole range grid x as a pointer in to delineate. On the off danger that x is of modernity twofold ,at that factor the majority of its segments with values masses substantially less than or indistinguishable to no less than one difficulty to the crucial column in delineate, brought materials with fee 2 thing to the second line et cetera. In the event that x is of complexity devices or unit 16, at that factor all delivered substances fee zero thing to the important line in outline, introduced materials with charge 1 aspect to the second et cetera.

**RGB Image:**

A RGB shading photograph is a M\*N\*three exhibit of tinge pixels wherein each coloration pixel is triplet much like the purple, inexperienced and blue brought materials of a RGB image, at a particular spatial area. A RGB image is probably considered as stack of three dim scale pics that after advocated in to the darkish pink, green and blue contributions of a tinge display screen. Deliver a shading picture at the show. Tradition the three previews shaping a RGB color image are alluded to as the red, unpracticed and blue brought

Substances pictures. The information fashion of the brought materials images comes to a decision their form of qualities. On the off hazard that a RGB image is of modernity twofold the type of traits is [0, 1]. Correspondingly the sort of characteristics is [0,255] or [0, 65535].For RGB pics of modernity gadgets or unit sixteen individually. The form of bits use to speaks to the pixel estimations of the aspect pictures makes a decision the bit profundity of a RGB photo. For instance, if every aspect image is an 8bit picture, the evaluating RGB photo is expressed to be 24 bits profound. For the most part, the collection of bits in all inconvenience snap shots is the indistinguishable. For this case the type of feasible shading in a RGB photograph is (2^b) ^three, in which in b is numerous bits in the entirety about. For the 8bit case the amount is 16,777,216 colorations.

**Advantages of digital image:**

* Image processing is simplest and most cost-effective. For processing, one consumes less effort, and therefore less film and many other equipment for photography.
* The processing of photographs seems to be more sustainable. To collect and handle digital images, no manufacturing or correcting substances are required. Conversely, while processing digital images, printing ink is necessary.
* One can automatically see whether the picture is successful or not while taking a digital image. It is simple to copy a digital image, as well as the image’s quality continues to improve unless it has been processed.
* For example, the image is compressed by preserving an image in jpg format. The compressed image will indeed be recompressed by resaving the image as a jpg file, because with every saving, the quality of the image will get even worse.
* It is becoming quicker to patch and retouch pictures. With a new Healing Brush Product, it is necessary to perfect face irregularities in a few seconds in the new Photoshop 7.
* The costly reconstruction is cheaper and faster (especially in comparison to preserving the image with a backup camera).
* The image can be used in a variety of formats by adjusting the image files and quality.

**Applications of Digital Image Processing:**

Some of the major fields in which digital image processing is widely used are mentioned below.

* Image sharpening and restoration
* Medical field
* Remote sensing
* Transmission and encoding
* Machine/Robot vision
* Color processing
* Pattern recognition
* Video processing
* Microscopic Imaging

**CHAPTER 8**

**RESULTS**

Electromyogram (EMG) is generated from the electrical activity of the muscles and appears as rapid fluctuations which are much faster than the ECG waves. The below diagram represent the generated ECG signal.

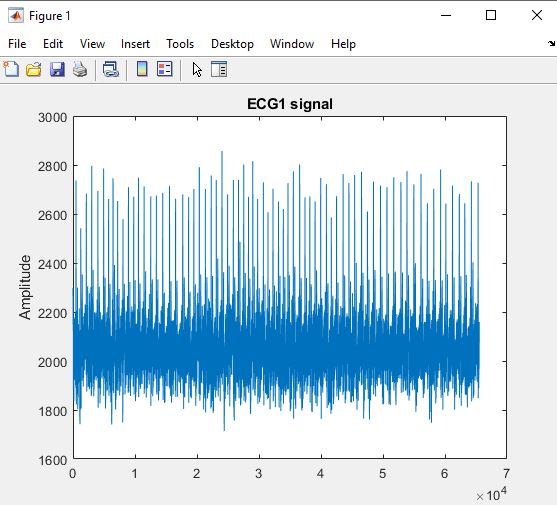
****

Figure1: ECG1 signal

This type of [signal processing filter](https://en.wikipedia.org/wiki/Filter_(signal_processing)) designed to have a [frequency response](https://en.wikipedia.org/wiki/Frequency_response) as flat as possible in the [pass band](https://en.wikipedia.org/wiki/Passband). It is also referred to as a maximally flat magnitude filter. The below figure represent the IIR butterworth filter.

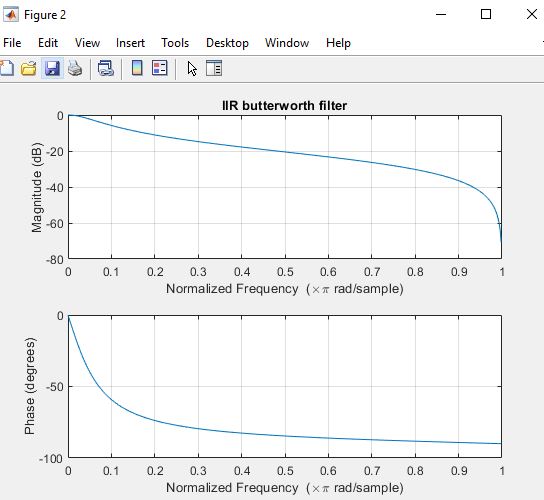
****

Figure2: IIR butterworth filter

The below diagram represent the generated ECG signal for verification phase.

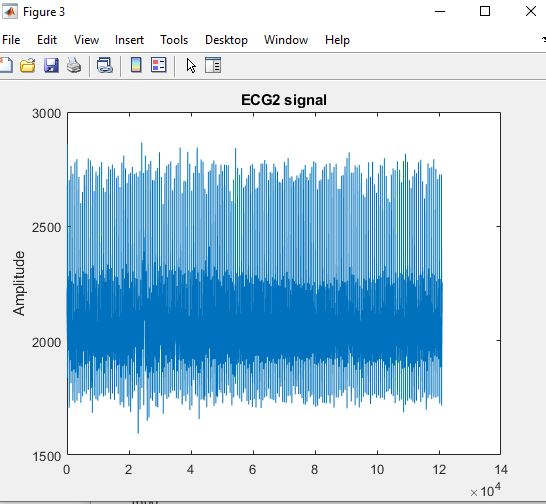
****

Figure3: ECG2 signal

The below figure represent the IIR butterworth filter for verification phase.

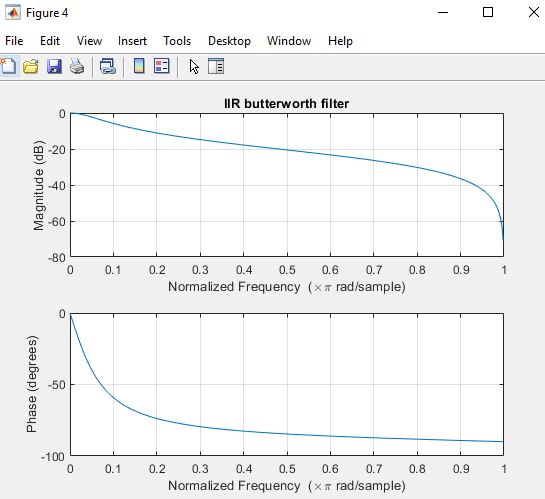
****

Figure4: IIR butterworth filter

Dynamic Time Warping (DTW) is a technique that compares two sequences that do not necessarily need to be the same lengths. After matching is performed.

****

Figure5: Dialog box represents matching or not.

Finally we calculate the accuracy of proposed implementation between filtered input signal and dynamic time warping.

****

Figure 6: Parameter calculation.

**CHAPTER 8**

**CONCLUSION**

In this paper, we completely evaluate the impact of filtering type, segmentation, feature extraction and health status on ECG biometric by using the evaluation metrics such as accuracy, FAR, FRR, and ERR. To protect the devices and data ECG dataset is used for authentication purpose. In other words, several experimental results were conducted to evaluate the impact of such important techniques for ECG biometric systems. This paper presents that our new proposed approach shows better performance when compared with the existing method.

**CHAPTER 9**

**FUTURE SCOPE**

In future work, by taking the biometrics ECG signals in live and by using segmentation technique we can perform the biometric authentication.

**REFERENCES**

[1] Nesli Erdogmus and Sebastien Marcel. Spoofing face recognition with 3d masks. IEEE transactions on information forensics and security, 9(7):1084–1097, 2014.

[2] Abdenour Hadid, Nicholas Evans, Sébastien Marcel, and Julian Fierrez. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine, 32(5):20–30, 2015.

[3] Neslihan Kose and Jean-Luc Dugelay. On the vulnerability of face recognition systems to spoofing mask attacks. In 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, pages 2357– 2361. IEEE, 2013.

[4] Javier Galbally, Raffaele Cappelli, Alessandra Lumini, Guillermo Gonzalez-de Rivera, Davide Maltoni, Julian Fierrez, Javier Ortega-Garcia, and Dario Maio. An evaluation of direct attacks using fake fingers generated from iso templates. Pattern Recognition Letters, 31(8):725–732, 2010.

[5] Zahid Akhtar, Christian Micheloni, and Gian Luca Foresti. Biometric liveness detection: Challenges and research opportunities. IEEE Security & Privacy, 13(5):63–72, 2015.

[6] Majid Komeili, Narges Armanfard, and Dimitrios Hatzinakos. Liveness detection and automatic template updating using fusion of ecg and fingerprint. IEEE Transactions on Information Forensics and Security, 13(7):1810–1822, 2018.

[7] Patrick PK Chan, Weiwen Liu, Danni Chen, Daniel S Yeung, Fei Zhang, Xizhao Wang, and Chien-Chang Hsu. Face liveness detection using a flash against 2d spoofing attack. IEEE Transactions on Information Forensics and Security, 13(2):521–534, 2017.

[8] Nima Karimian, Zimu Guo, Mark Tehranipoor, and Domenic Forte. Highly reliable key generation from Electrocardiogram (ECG). IEEE Transactions on Biomedical Engineering, 64(6):1400–1411, 2016.

[9] José Vicente, Pablo Laguna, Ariadna Bartra, and Raquel Bailón. Drowsiness detection using heart rate variability. Medical & biological engineering & computing, 54(6):927–937, 2016.

[10] Lan-lan Chen, Yu Zhao, Peng-fei Ye, Jian Zhang, and Jun-zhong Zou. Detecting driving stress in physiological signals based on multimodal feature analysis and kernel classifiers. Expert Systems with Applications, 85:279–291, 2017.

[11] Hugo Plácido da Silva, Carlos Carreiras, André Lourenço, Ana Fred, Rui César das Neves, and Rui Ferreira. Off-the-person electrocardiography: performance assessment and clinical correlation. Health and Technology, 4(4):309–318, 2015.

[12] Pei-Lun Hong, Jyun-Ya Hsiao, Chi-Hsun Chung, Yao-Min Feng, and Shun-Chi Wu. Ecg biometric recognition: template-free approaches based on deep learning. In 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pages 2633– 2636. IEEE, 2019.

[13] Ruggero Donida Labati, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. Deep-ecg: convolutional neural networks for ECG biometric recognition. Pattern Recognition Letters, 126:78–85, 2019.

[14] Jin Su Kim, Sung Hyuck Kim, and Sung Bum Pan. Personal recognition using convolutional neural network with ECG coupling image. Journal of Ambient Intelligence and Humanized Computing, pages 1–10, 2019.

[15] Hyun-Soo Choi, Byunghan Lee, and Sungroh Yoon. Biometric authentication using noisy electrocardiograms acquired by mobile sensors. IEEE Access, 4:1266–1273, 2016.

[16] Hanvit Kim and Se Young Chun. Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test. IEEE Access, 7:9232– 9242, 2019.

[17] Ronald Salloum and C-C Jay Kuo. Ecg-based biometrics using recurrent neural networks. In 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 2062–2066. IEEE, 2017.

[18] João Ribeiro Pinto, Jaime S Cardoso, André Lourenço, and Carlos Carreiras. Towards a continuous biometric system based on ECG signals acquired on the steering wheel. Sensors, 17(10):2228, 2017.

[19] Majid Komeili, Wael Louis, Narges Armanfard, and Dimitrios Hatzinakos. Feature selection for nonstationary data: Application to human recognition using medical biometrics. IEEE transactions on cybernetics, 48(5):1446– 1459, 2017.

[20] Iulian B Ciocoiu and Nicolae Cleju. Off-the-person ECG biometrics using convolutional neural networks. In 2019 International Symposium on Signals, Circuits and Systems (ISSCS), pages 1–4. IEEE, 2019.

[21] Yifan Chu, Haibin Shen, and Kejie Huang. ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss. IEEE Access, 7:51598–51607, 2019.

[22] Qingxue Zhang, Dian Zhou, and Xuan Zeng. Heartid: A multiresolution convolutional neural network for ecg-based biometric human identification in smart health applications. Ieee Access, 5:11805–11816, 2017.

[23] Mohamed Hammad, Yashu Liu, and Kuanquan Wang. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. IEEE Access, 7:26527–26542, 2018.

[24] Kuikui Wang, Gongping Yang, Yuwen Huang, and Yilong Yin. Multi-scale differential feature for ECG biometrics with collective matrix factorization. Pattern Recognition, page 107211, 2020.

[25] Yazhao Li, Yanwei Pang, Kongqiao Wang, and Xuelong Li. Toward improving ECG biometric identification using cascaded convolutional neural networks. Neurocomputing, 2020.

[26] Eduardo Jose da Silva Luz, Gladston JP Moreira, Luiz S Oliveira, William Robson Schwartz, and David Menotti. Learning deep off-theperson heart biometrics representations. IEEE Transactions on Information Forensics and Security, 13(5):1258–1270, 2017.

[27] Saeid Wahabi, Shahrzad Pouryayevali, Siddarth Hari, and Dimitrios Hatzinakos. On evaluating ecg biometric systems: Session-dependence and body posture. IEEE Transactions on Information Forensics and Security, 9(11):2002–2013, 2014.

[28] Khairul A Sidek, Ibrahim Khalil, and Herbert F Jelinek. Ecg biometric with abnormal cardiac conditions in remote monitoring system. IEEE Transactions on systems, man, and cybernetics: systems, 44(11):1498– 1509, 2014.

[29] Foteini Agrafioti and Dimitrios Hatzinakos. Ecg biometric analysis in cardiac irregularity conditions. Signal, Image and Video Processing, 3(4):329, 2009.

[30] Sairul I Safie, John J Soraghan, and Lykourgos Petropoulakis. Electrocardiogram (ecg) biometric authentication using pulse active ratio (par). IEEE Transactions on Information Forensics and Security, 6(4):1315– 1322, 2011.

[31] Jun Shen, Shu-Di Bao, Li-Cai Yang, and Ye Li. The plr-dtw method for ecg based biometric identification. In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pages 5248– 5251. IEEE, 2011.

[32] Vu Mai, Ibrahim Khalil, and Christopher Meli. Ecg biometric using multilayer perceptron and radial basis function neural networks. In 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pages 2745–2748. IEEE, 2011.

[33] Song-Kyoo Kim, Chan Yeob Yeun, and Paul D Yoo. An enhanced machine learning-based biometric authentication system using rr-interval framed electrocardiograms. IEEE Access, 7:168669–168674, 2019.

[34] Song-Kyoo Kim, Chan Yeob Yeun, Ernesto Damiani, and Nai-Wei Lo. A machine learning framework for biometric authentication using electrocardiogram. IEEE Access, 7:94858–94868, 2019.

[35] Nima Karimian, Mark Tehranipoor, Damon Woodard, and Domenic Forte. Unlock your heart: Next generation biometric in resource-constrained healthcare systems and iot. IEEE Access, 7:49135–49149, 2019.

[36] Htet Myet Lynn, Sung Bum Pan, and Pankoo Kim. A deep bidirectional gru network model for biometric electrocardiogram classification based on recurrent neural networks. IEEE Access, 7:145395–145405, 2019.

[37] Jikui Liu, Liyan Yin, Chenguang He, Bo Wen, Xi Hong, and Ye Li. A multiscale autoregressive model-based electrocardiogram identification method. IEEE Access, 6:18251–18263, 2018.

[38] Zhidong Zhao, Yefei Zhang, Yanjun Deng, and Xiaohong Zhang. Ecg authentication system design incorporating a convolutional neural network and generalized s-transformation. Computers in biology and medicine, 102:168–179, 2018.

[39] Maryamsadat Hejazi, SAR Al-Haddad, Shaiful Jahari Hashim, Ahmad Fazli Abdul Aziz, and Yashwant Prasad Singh. Non-fiducial based ecg biometric authentication using one-class support vector machine. In 2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), pages 190–194. IEEE, 2017.

[40] Robin Tan and Marek Perkowski. Toward improving electrocardiogram (ecg) biometric verification using mobile sensors: A two-stage classifier approach. Sensors, 17(2):410, 2017.

[41] Joao Pinto and Jaime S. Cardoso. An end-to-end convolutional neural network for ecg-based biometric authentication. In Proceedings of 10th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2019.

[42] Abhishek Ranjan. Permanence of ecg biometric: Experiments using convolutional neural networks. In 2019 International Conference on Biometrics (ICB), pages 1–6. IEEE, 2019.

[43] Rui Li, Gongping Yang, Kuikui Wang, Yuwen Huang, Feng Yuan, and Yilong Yin. Robust ecg biometrics using gnmf and sparse representation. Pattern Recognition Letters, 129:70–76, 2020.

[44] Emna Kalai Zaghouani, Adel Benzina, and Rabah Attia. Ecg based authentication for e-healthcare systems: Towards a secured ecg features transmission. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pages 1777–1783. IEEE, 2017.

[45] Vessela Krasteva, Irena Jekova, and Roger Abächerli. Biometric verification by cross-correlation analysis of 12-lead ecg patterns: Ranking of the most reliable peripheral and chest leads. Journal of electrocardiology, 50(6):847–854, 2017.

[46] Konstantinos N Plataniotis, Dimitrios Hatzinakos, and Jimmy KM Lee. Ecg biometric recognition without fiducial detection. In 2006 Biometrics symposium: Special session on research at the biometric consortium conference, pages 1–6. IEEE, 2006.

[47] Somsanouk Pathoumvanh, Surapan Airphaiboon, and Kazuhiko Hamamoto. Robustness study of ecg biometric identification in heart rate variability conditions. IEEJ Transactions on Electrical and Electronic Engineering, 9(3):294–301, 2014.

[48] Ruggero Donida Labati, Roberto Sassi, and Fabio Scotti. Ecg biometric recognition: Permanence analysis of qrs signals for 24 hours continuous authentication. In 2013 IEEE International Workshop on Information Forensics and Security (WIFS), pages 31–36. IEEE, 2013.

[49] Joana S Paiva, Duarte Dias, and Joao PS Cunha. Beat-id: Towards a computationally low-cost single heartbeat biometric identity check system based on electrocardiogram wave morphology. PloS one, 12(7), 2017.

[50] Mohamed Hammad, Mina Ibrahim, and Mohiy Hadhoud. A novel biometric based on ecg signals and images for human authentication. Int. Arab J. Inf. Technol., 13(6A):959–964, 2016.

[51] Mohamed Hammad, Shanzhuo Zhang, and Kuanquan Wang. A novel twodimensional ecg feature extraction and classification algorithm based on convolution neural network for human authentication. Future Generation Computer Systems, 101:180–196, 2019.

[52] Simon Haykin. Kalman filtering and neural networks, volume 47. John Wiley & Sons, 2004.

[53] Reza Sameni, Mohammad B Shamsollahi, Christian Jutten, and Gari D Clifford. A nonlinear bayesian filtering framework for ecg denoising. IEEE Transactions on Biomedical Engineering, 54(12):2172–2185, 2007.

[54] Donald J Berndt and James Clifford. Using dynamic time warping to find patterns in time series. In KDD workshop, volume 10, pages 359–370. Seattle, WA, 1994.

[55] Chotirat Ann Ratanamahatana and Eamonn Keogh. Making time-series classification more accurate using learned constraints. In Proceedings of the 2004 SIAM international conference on data mining, pages 11–22. SIAM, 2004.

[56] Miguel A García-González, Ariadna Argelagós-Palau, Mireya FernándezChimeno, and Juan Ramos-Castro. A comparison of heartbeat detectors for the seismocardiogram. In Computing in Cardiology 2013, pages 461– 464. IEEE, 2013.

[57] George B Moody and Roger G Mark. The impact of the mit-bih arrhythmia database. IEEE Engineering in Medicine and Biology Magazine, 20(3):45–50, 2001.

[58] R Bousseljot, D Kreiseler, and A Schnabel. Nutzung der ekgsignaldatenbank cardiodat der ptb über das internet. Biomedizinische Technik/Biomedical Engineering, 40(s1):317–318, 1995.

[59] TS Lugovaya. Biometric human identification based on electrocardiogram. Master’s thesis, Faculty of Computing Technologies and Informatics, Electrotechnical University ‘LETI’, Saint-Petersburg, Russian Federation, 2005.

[60] Hugo Plácido Da Silva, André Lourenço, Ana Fred, Nuno Raposo, and Marta Aires-de Sousa. Check your biosignals here: A new dataset for off-the-person ecg biometrics. Computer methods and programs in biomedicine, 113(2):503–514, 2014.

[61] Nima Karimian, Damon L Woodard, and Domenic Forte. On the vulnerability of ecg verification to online presentation attacks. In 2017 IEEE International Joint Conference on Biometrics (IJCB), pages 143– 151. IEEE, 2017.

[62] N. Karimian, D. Woodard, and D. Forte. Ecg biometric: Spoofing and countermeasures. IEEE Transactions on Biometrics, Behavior, and Identity Science, pages 1–1, 2020.