LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

GESTURE RECOGNITION FOR INTRUDER DETECTION

Dissertation Report Submitted

By

Shashwat Sagar

To

Department of Computer Science and Technology

In partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance of

Mr. Mohinder Kumar
Asst. Professor

(April 2015)

Abstract

This report contains detailed plan of the dissertation that has been implemented. Biometric authentication in smart phones is relatively new subject of research and is beneficial in many fields and also an evolution for authentication systems. With a common passwords or pins the confidentiality and integrity of the data is in jeopardy as it can be lost or destroyed. As biometrics cannot be replicated or cannot be lost or be stolen. Final product of this proposal will have the ability to use gait biometric system as an authentication process in the smart phones.

CERTIFICATE

This is to certify that **Shashwat Sagar** has completed M.Tech dissertation titled **Gesture Recognition for Intruder Detection** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma. The dissertation proposal is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech Computer Science & Engineering.

Date:

Signature of Advisor

Name: Mohinder Kumar

UID:

Acknowledgement

I would like to gratefully and sincerely thank **Mr. Mohinder Kumar** for his guidance, understanding and patience during my dissertation-II studies at Lovely Professional University. His mentorship was paramount in providing a well-rounded experience considering my long-term career goals. He encouraged me to not only grow as an experimentalist but also as an independent thinker. I am not sure many graduate students are given the opportunity to develop their own individuality and self-sufficiency by being allowed to work with such independence. I would like to thank **Lokesh Ranjan, Vimmi Kaushal, Rahul Roy and Rahul Abhishek** for their co-operation in collecting data samples. I would also like to thank my family and friends that helped me throughout my research and also for their valuable feedbacks throughout research.

DECLARATION

I hereby declare that the dissertation entitled, **“Gesture Recognition for Intruder Detection”** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Shashwat Sagar
Reg. No. 11008506

Table of Contents

List of Tables

List of Figures

Chapter 1

INTRODUCTION

The evolution of biometric systems in today's era is one of the most promising accessibility or authentication techniques provided to the people and also it has caught the imagination of the public eye. As it is easy to measure the characteristics of any human being, it has become feasible for authentication purposes [16]. There are various biometric systems available like- iris, face, fingerprint, eye, hand geometry, signature, voice, keystroke and gait. Out of which gait is one of the best in biometric for accessibility and authentication point of view. There are three different systems for accessibility which are object based, knowledge based and biometric based. In yester years people do have to remember lots of passwords or tokens for gaining access. For example, if any user wants to login into any account or a user wants to access some confidential files, the password should be with the user so as to gain access, so as it can be easily accessible whenever required. This system comes under knowledge based system. So if there exists multiple accounts then there must be multiple passwords for each account, which on the other hand is difficult to remember by the user. Normally users do not use multiple passwords for multiple accounts, one or two passwords are fixed which is easy to remember. Thus the probability of attacks by the attacker on their accounts becomes highly likely.

Object-based system is basically the combination of an object-based and a knowledge- based such as Credit card, ATM card with a given pin code. Since, both knowledge-based system and object-based system contain some kind of token or passwords, hence, it can easily be stolen, lost or forgotten. Therefore, to remove this problem biometric based systems were introduced. Biometrics basically means you. Considering a biometric technique say finger print recognition, if a user has to access anywhere via his finger prints rather than any password or tokens and since the users biometric can never be changed, in this case the finger prints and also we all know that no two user's finger print can be same, it is a unique. This system stores the human biometric in the form of template and then at the time of verification this stored template is matched with the produced biometric data. If there is a match then the user is authorised or is allowed access. Also while using biometrics the probability of attacks is quite less.

Human gait being a vital biometric feature, gait refers, the walking moments of an individual. This technique is basically used for forensics or any high security areas. Gait is very much different from other biometrics because it does not require any physical contact. In rest of the biometrics normally a user has to undergo a physical contact, say, finger-print biometrics. Here, the user has to first present its biometric card to the biometric machine/biometric system and then the user has to produce its biometric, in this case the finger which was used at the time of enrolment. So here comes the physical contract part and also it takes time.

Gait recognition is an effective biometric as compared to traditional biometrics, for human identification. In contrast, gait biometric gives us a possibility for recognition at a distance or at low-resolution. The image can be captured from a distant camera and further is analyzed so as to create template/silhouettes. In simple words we can say that Gait recognition is a very useful biometric feature which is capable of recognizing any human from a particular distance just by looking into their walking patterns.

1.1 Introduction to Biometrics

Basically, biometrics can be either physical or behavioural or even chemical biometrics [4]. In physical biometrics there exists some kinds of measurements or some form of measurements and the biometrics which falls under this category are-face, fingerprints, iris-scans, hand geometry. Behavioural biometrics are typically temporal in nature and it involves a certain type of measurement of some part of a human body or a measurement in which a user performs a certain tasks. Speech, signature, gait, keystroke dynamics falls under this category. In chemical biometrics, which is still an emerging field and involves measuring of chemical cues such as order and the chemical composition of human perspiration.

The biometric system follow some set of stages of operations- captures biometric sample of an individual, extract set of relevant features from captured sample and compare the extracted feature set against the template set in the database [8].

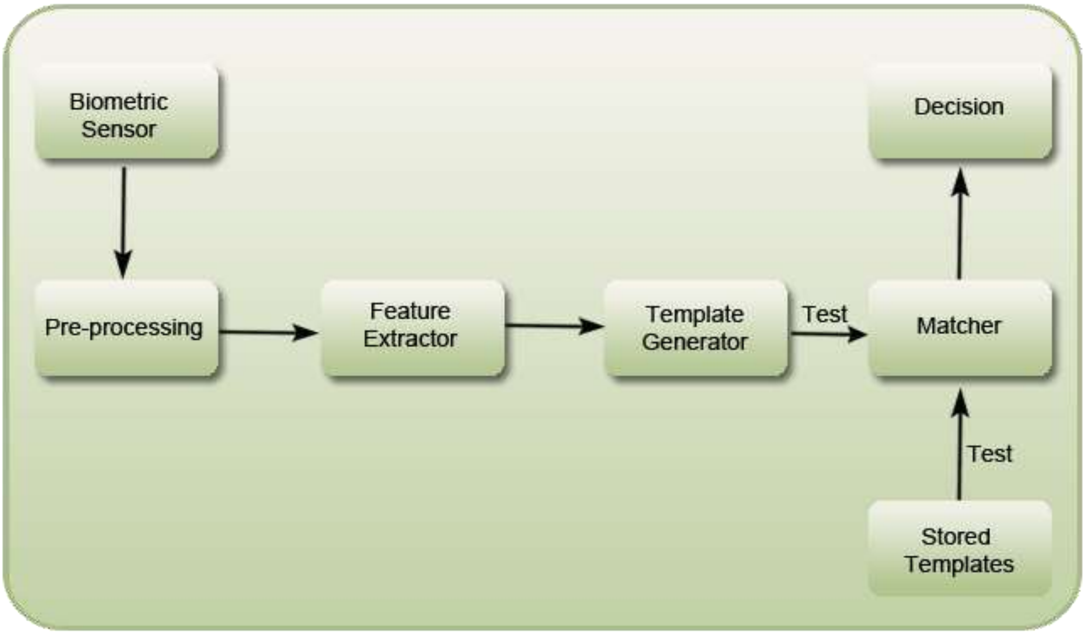


Figure 1: Process of Biometric System [24].

There are two modes in biometrics [1], [8].

- Identification
- Verification

In case of identification the user produces its biometric card to the system and tells “Who am I?”. Whereas, in case of verification when a user produces its card and it tells “Am I who I claim I am?”.

In a biometric system at the time of enrolment and in the time of verification the system generates a template which consists of some values. At enrolment process this value, known as a threshold value, gets stored in the database and at the time of verification a new template is generated based on the biometric provided by the user, and a value is calculated. Now the value generated is compared with the threshold value, if the value is less than threshold value, then the user gets access or else error is displayed or the user will not gain access. There can generate lot of errors at the time of verification, like FMR and FNMR. In case of FMR, suppose a user ‘X’ provides its biometric at the time of verification, and due to some external factors or the internal factors the template does not match the condition with the threshold value of the data which is stored in the database and gets access of another user ‘Y’. Then this phenomenon is known as FMR. Whereas in case of FNMR, suppose a user ‘L’ provides its biometric at the time of verification, and due to some external factors or the internal factors the template does not match the condition with the threshold value of its data which is stored in the database and gets a message that you are not authorized/enrolled. Then this phenomenon is known as FNMR.

False non-matches occur because there is not a sufficiently strong correlation between a user's verification and enrolment templates. This can be attributed to the following as-

- Biometric data of a user is changed somehow.
- How a user presents its biometric data.
- Environment changes in which biometric data is presented.

Also FTER is another type of error which come across at the time of enrolment. It occur when users have insufficiently distinctive or replicable biometric data or when the design of the biometric solution is such that providing consistent data is difficult.

For a biometric system to be successful, the FMR and the FNMR should be equal, which is EER, also referred to as the crossover rate, in the DET curve. That is, it represents the accuracy level at which likelihood of a FMR is the same as the likelihood of a FNMR. EER is generally used as a representation of overall system accuracy, as it is a general indicator of a system's resistance to break-ins and an ability to match templates from authorized users. Also the biometric system can be fallen under attack, mainly the biometric authentication system which do contain some eight typical points of attacks described below and also shown in figure 2.

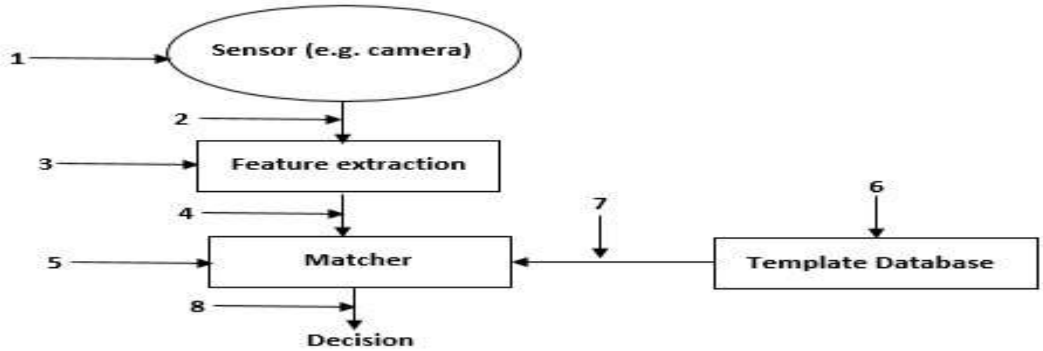


Figure 2: Different type of attacks in biometric system [11].

1) By presenting an imitated biometric or a fake biometric to the sensor.

2) By submitting data of a biometric sample which was previously obtained.

3) The attacker sets its own value so as it matches with the value of feature extractor.

4) The attacker substitutes the value of extracted feature value.

5) The matcher score is changed so as to produce a low or high matching score.

6) By attack on the databases of biometric templates.

7) The data which is in transit are modified.

8) Decision can be altered.

In biometric, the attacks can be performed either on the communication channels between modules or on the specific modules of the system.

1.2 Gait Biometric System

The gait biometric recognition system is described in the following figure 3 –

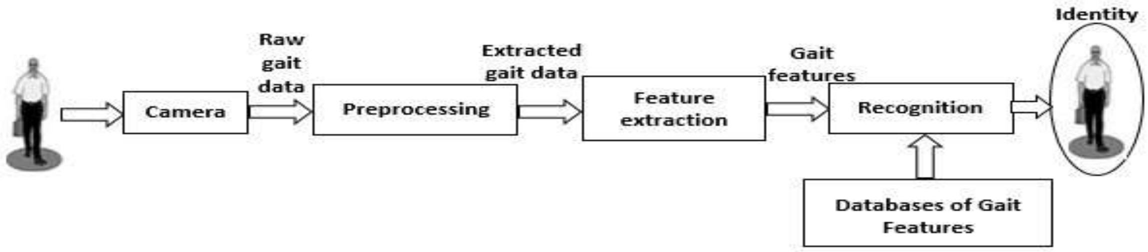


Figure 3: Gait Recognition System [7].

As it is well known that gait biometric can be well used for authentication purposes. Not also this but using gait biometrics one can easily reveal the presence of certain sickness, moods and also the distinguished genders [16]. For identifying the difference between genders the features like shoulder/hip size ratios, torsion of torso among others [5]. Also for gender based classification using gait, different body parts silhouette can be used: head, chest, back, hip and leg [22].

The method of approach for gait recognition are grouped into two different categories, first is model-based approach and the other is model-free approach [13]. In first approach, i.e., in model-based approach, its main focus is the model of a human body and uses the parameters of this model for recognition [7], [13]. This model basically includes motion of high and lower leg rotation, and thus it describes both walking and running. It recover features describing gait dynamics such as strides and kinematics of joints. The only advantage is that it easily derives the gait feature and does not depend on clothing. The disadvantages are as follows- It is difficult to follow in low resolution images because for a system to identify the gait features of a user it needs high resolution images to provide accurate results. So, for this system to be efficient the images should be in high resolution for which image processing will be used and thus the computational complexity will be increased. Also it is very sensitive to noise.

In Model Free Approach [7], [13], it is simple and free and it do not deal with the structure of human motion but it deals directly with image statistics. Also it contain low computational complexity as compared to model-based approach and it is best suited for real-time system. The few model-free approach are [7] - First is, Background Subtraction, here a silhouette is obtained from a video frame of a moving object, i.e., after the subtraction of moving object the silhouette is obtained. Also, it is of two types Recursive and non-recursive. In non-recursive, a sliding window approach is used which is highly adaptive for background estimation. In recursive technique, the buffer is not used for background estimation. A single background model which is based on each input frame is been recursively update. The second approach is Feature extraction, where different type of feature based method are applied so as to obtain a gait feature and those methods are holistic methods. Thirdly, the approach is Silhouette Extraction, as mentioned earlier that silhouette means the outline of someone or something visible in restricted light against a brighter background.

Other technique is BPNN, the three layer Neural Network is used, the first layer is the input layer and the final layer being the output layer and the middle layer, which is also known as the “hidden layer”, as it is hidden from the users’ side. The various computational part are done by the designed network. Also this technique is highly flexible and it follows non-linear modelling. Design of the neural network involves the architecture for the network, an algorithm and the activation function. Gait recognition problem uses BPNN, which consists with one or more hidden layer. This hidden layer is used for reducing complexity and thus increasing computational efficiency. The other technique is PCA [18], [12], the statistical analysis of data is been done so as to find out the principal components on which the data is more likely to vary. It is a classical linear approach so as to reduce data dimensionality and due to which it is most efficiently used in face recognition. LDA do include PCA but just for reducing the dimensionality and then LDA performs optimal classification on low dimensional space. MDA reduces the dimensionality and its main objective is to maximize the distance between different classes and minimize the difference between each class.

The techniques for capturing gait of any individual are divided into three categories [8], [14]. First is MV-based, in which the capturing of image from multiple cameras is done. Generally, multiple high definition cameras are required so as to capture the image of a user on different angles. Here the gait is captured from a distant video camera and this video undergoes various image and video processing for extracting gait feature. The extraction are done on the basis of some parameters like the distance between feet, the distance between pelvis and head, also the maximum distance between feet and a pelvis and the height. Most of the gait recognition algorithms performs over the gait silhouettes. Silhouettes means in the image the background is being removed and the lone silhouette of an individual is extracted and then analysis is done. The sample size while using this recognition technique was limited in earlier times but now the sample size has been increased. The main advantage of this technology is the images can be captured from a distance where all the other biometric fail to cooperate. The main areas of applications are surveillance and the forensics.

The second is FS-based [8], [14], which uses the sensor system which is placed on the floor. A set of sensors are installed on a particular area of the floor, which captures the gait information. This can also include the location information within any building, mostly it is installed in front of the doors. Thus the users gait is captured using all the parameters like pressure, angle, and shoe type. In the third is WS-based [8], [14], it is basically used for mobile unit, were a tracking chip is attached to the users anklet or the waist. Here the data collected via MR sensors and this chip stores all the users gait data and further allows it to gain access as required.

1.3 Challenges and Security in Gait Biometric

We all are very well aware that any system is not 100% secure. So, gait biometric do have to face some challenges, and those challenges are further divided into two main categories [8], by which the gait data can be altered or spoofed. First is the external factor, it means that suppose a user ‘X’ has enrolled gait while the user was wearing casual shoes and now at the time of verification the user wore heels, and this could totally affect the gait template and the false match error will be generated. Also some other external factors are dress code like at the time of enrolment the user was wearing a formal dress but at the time of verification the user wore a casual dress, or object carrying with it like carrying a bag pack or side bag with the user, viewing angles, lighting conditions like in case of day and night, or walking surface, say if the user is walking on a smooth floor or on stairs etc. Secondly the internal factors also do affect the gait like physiological changes in the body like aging, weight problem like weight gain or weight loss, due to sickness, or due to pregnancy.

Normally the greatest myth in this technique is that, it is believed that the imposters are passive and unknowledgeable. There are two types of attacks in this system, one is passive attack and the other one is active attack [8]. In passive attack, it generally refers to FMR error, whereas in active attack the imposter knows some knowledge about the target user and modifies his walking moment and gained access, so this also can come under FMR but here it was intentional. Also the closets person attack and the minimal-effort impersonation attack on gait biometrics is one of the main concern [9]. Also apart from these attacks, physiological and behavioural attacks is also another concerning point. Behavioural biometrics can be unsafe to the mimicking or impersonation attacks. The level of attacks which a biometric system can describe is totally dependent on the resources available to the attackers, such as tools (hardware/software), time, knowledge of the system etc. A minimal-effort impersonation attack are those type of attacks where the attacker only has a common knowledge of the system and no other information. The performance of a biometric system changes when the system is under attack, so to depict this there are four hypothetical DET curve which is given in the figure 4. This DET curve is plotted on FAR versus FRR, which tells us that by changing the threshold value for acceptance, various combinations can be produced of FAR, FRR pairs and thus a graph can be plotted. The first dark curve is for the friendly scenario and the other three dotted curves are in the hostile scenarios.

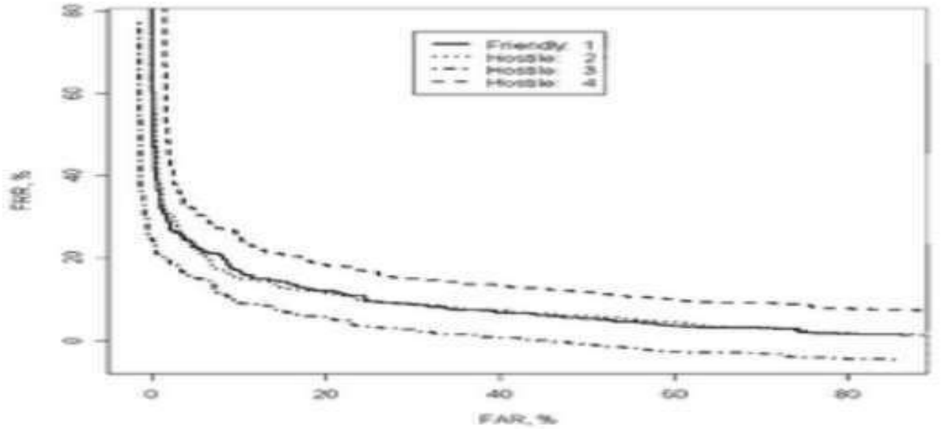


Figure 4: The DET curves showing the performance shift of the biometric system [9].

Although, it is believed that the gait biometric is difficult to hide or replicate, but gait biometrics do have spoofing attacks [11]. Spoofing attacks occurs when an individual tries to imitate the walking style and/or walking style of someone else in order to gain unauthorised access and advantages. The only prior work done on gait spoofing uses only wearable sensors but not video analysis. The spoofing attack was performed using an accelerometer based gait recognition system where the users needed to have devices attached to their legs specifically so as to obtain gait signature. The most appealing way for spoof attack is by wearing same clothes which makes an attacker's body shape appear as the same as the target, and which is most unobtrusive and a straightforward method probably for performing the attack.

1.4 Gait Biometrics in Smartphones

As todays smartphones contains various types of sensors, but the sensor which can read the gait data is the accelerometer sensor [15]. Presents a survey on all the sensors present in the smart phones and how they can be used. Many researchers have worked in this field, earlier only the sensor was attached to various parts of the body to measure the gait data, but now researchers are focusing on the accelerometer sensor in smart phones [6], [17], [20], [21]. The gait data can be easily accessed in the smartphones. Generally, the gait data are extracted either in the form of the data divided into segments and then the features are extracted or the gait cycles thus generated are separated from the sensor data and with these gait cycles Manhattan and Euclidean distances can be calculated or even using PCA.

Chapter 2

LITERATURE REVIEW

In past few years, many researches have done work related to accelerometer sensor. The common motive of all these researches were to capture gait data by placing the sensor on various parts of the body and to improvise the results thus obtained. In the present study an attempt has been made to review the literature on accelerometer sensor on smartphones and also few gait recognition methods.

Derawi, Mohammad and Bours, Patrick. 2013 [6] also used accelerometer inbuilt in smartphones to capture the gait data. But here for the authentication purpose they have combined gait, fingerprint, and password and also holds the future scope for other biometrics to be combined with it. The enrolment process supports walking in multiple direction or forms like normal walking, or walking in rough surface, or inclined walking like walking in stairs. Although it is stated that in previous researches, the position as well as orientation of the sensor-based smartphone was to be fixed, but here, the orientation does not play any role for authentication process only the phones' position is valuable, the user should attach the phone at the very position from where the enrolment process was carried out. Also here activity recognition was included, for this each and every individual was matched with the stored template and test samples were generated.

Zhang, Jian 2013 et al. [14] has proposed a new framework which construct a new-invariant feature for gait recognition. Gait silhouettes have been used so as to normalize the process. The main focus was on one particular paper under the approach of Goffredo, M. 2009 et al. [10] which have some limitations. Those are described below-

- The poses estimation of limbs' is not robust.
- Since the limbs' poses is untraceable and thus it is not applicable to capture the gait silhouettes from front view.
- For the cases of a small view change the performance was worse.

The only advantage is that it performs very well in those areas where the view change is large enough and thus it provides accurate result. The proposed method is a very good method, it does not rely on supervised learning nor does it use multiple cameras. The benefits in this method are-

- It do contain more reliable gait information which will lead to a better recognition performance.
- Because of gait silhouettes it becomes quite easy to extract feature.

The proposed method consists of two stages, namely- a new GTI, which is a part of the view-normalization stage, which represents an original gait information on a sequence of gait silhouettes. A transformation is applied on the GTI so as to get the optimized domain output. Secondly, PSA is applied on the gait silhouettes to get a desired invariant gait feature. The GTI which consists of TILT has two main components-first is the domain transformation and second is the sparse error matrix. Since, the images captured will have some noise factor so to remove this noise factor sparse error matrix is used. It basically excludes the noise created by occlusion, shadow and also silhouette segmentation errors. Also the main purpose is to help the domain transformation to model and deal with the textures which are high rank textures in GTI. Since, the work was on the gait view change so for this to be correctly implemented PSA is used. PSA is a statistical shape analysis which can easily tolerate the change in the orientation of an object. It acts as a process for performing a shape preserving Euclidean transformation on a set of shapes. It has an ability to achieve by properly superimposing similarity measurement between two sets of shapes. This property is useful for gait recognition because gait is a periodic dynamic action. During the superimposition, the positions and the sizes of gait shapes that vary throughout a walking cycle and a distance to camera are adjusted accordingly.

The main contribution is to propose a new framework of view-invariant gait recognition. It includes the following aspects. Firstly, seeking gait information (i.e., GTI) that can be normalized across different views. Secondly, proposing a novel view-normalization process through domain transformation by TILT on GTI. Thirdly, normalizing gait silhouettes based on corresponding domain transformation. Lastly, computing a novel view-invariant gait feature through an improved scheme of PSA on view-normalized gait silhouettes.

Yang, Mingjing 2012 et al. [21] have gait pattern analysis for clinical practice for the diagnosis of neurodegenerative diseases. Here the use of a tri-axial accelerometer is used which is embedded in a smart phone also a minimod accelerometer is used on the bottom of the smartphone's accelerometer and it was attached to the subject's lower back [23]. Each subject underwent three experiments for this work, first they were allowed to stand still and then they were allowed to walk for 25 m in normal heels. After the subject has walked 25 m, it stopped for a second and then underwent another experiment. The gait data was stored in the memory card of the subjects' phone in a plain text format, which includes the anterior-posterior acceleration, the vertical acceleration and the medial-lateral acceleration. For gait pattern analysis a tool was developed which stores the regularity features and the spatiotemporal features. RMS value was calculated so as to remove all the noise from the gait data. The result being that the regularity features had a fair-to-good agreement also RMS features extracted had good features in all the three motions of accelerometer. But the symmetry features had poor agreement and so it indicated that for gait pattern analysis the smart phone can be used based on spatiotemporal features only. Also due to low sampling rate symmetry features and the regularity features should be proceeded with kind attention.

Bustard, John and Nixon, Mark. 2012 et al. [11] The method described for spoofing is same as in facial recognition system using 3D mask. The methods are developed by the USOU and UOULU. In USOU gait recognition system the 3D volumetric data is used to synthesise the silhouettes from a fixed view-point related to the subject. The eight synchronized camera views are used to gather the silhouettes and the 3D volume is synthesised by getting result from standard background subtraction approaches and then applied to the silhouettes. The outcome of this is then passed to a standard gait analysis technique using the average 3D silhouette. This silhouette is used for verification and treated as the feature vector using the Euclidean distance metric. In UOULU gait recognition system, the dynamic texture based gait recognition system, which uses 2D dynamic texture descriptors. This 2D dynamic texture includes LBP-TOP for describing human gait in a spatio-temporal way. A normal walking of a user is considered as a spatio-temporal volume. The spoofing attacks includes various scenarios like- deliberately selection of a target which has a similar build to the attacker, clothing impersonation or combination of these two. The conclusions were that it is indeed a possibility to spoof such systems but it may require a lot of efforts like, impersonating the clothes and to select a target which has a similar build to the attacker and the walking style.

Nickel, Claudia and Bours, Patrick 2011 [17] as accelerometer are used for biometric data to be captured and recent smartphones do have lot of new feature and/or sensors. Accelerometer is a sensor which is present in almost every smart phone. As smart phones are normally used for both business scenarios and private environment, so the integrity of the data can be compromised. Normally, most of the smart phones provide a knowledge-based authentication system. But here, for authentication purpose gait data is used and by using accelerometer the gait data is been captured. For enrolment purpose MBASSy [20] was used and the gait data is stored on the phone itself and when the screen saver is activated the accelerometer collects the gait data. A gait cycle is extracted for last 30 seconds and these are then compared with the reference data. If the outcome is true, then the lock screen is closed or else it isn't and a little changes in the authentication system have been done, the gait data once collected is stored and the feature comparison and extraction is done later.

Goffredo, Michaela and Carter, John. 2011 et al. [2] has done work in forensics taking into consideration of gait recognition, which is also used for surveillance. The location of hip, ankle and knee is used to derive a measure so as to match between the subjects in the image sequences present. As this biometric can be used to solve crimes, as face recognition has proven wrong in many cases of crimes. So, gait biometrics can overcome all the limitations of various biometrics like, face, fingerprint etc. As facial recognition cannot be covered from a large distance, but gait can be easily detected from a large distance. Usually, in crime scenes, the individuals walking moment can be recorded using the surveillance camera. Although, the common thinking is to not get caught, but by using that video the gait features can be extracted and can be easily used so as to determine the culprit.

The technique described here uses the position of human leg, namely the hip, knees and ankle, which is also named as the vertex features. The method used is background independent and thus the various errors like shadow, background clutter, and outdoor factors will not affect the gait data. The main aim of this method is to extract limbs, human joints by prior knowledge, incorporating kinematics and anthropometric gait data. For matching the joint positions a Haar-based template matching method is applied, this method basically deals with the evaluation of the result of convolving selected families of binary templates with image data. The kinematics of the anthropometric gait knowledge and gait are used for refining the accuracy for the extraction of the joint positions and also to limit the search space. A gait cycle is generated, which means that the time interval for the successive instances of the initial foot-to-floor contact for the same foot. Thus a markerless extraction method is applied based on the medical data which helps in describing the angular motion of the hip and knee at different states of a gait cycle. For analysis of gait form video sequences, an instantaneous posture matching algorithm is used. Since, the natural walking of each and every individual is executed in a different way, as confirmed by psychological and medical studies. So, the motion of limb is very unique in each and every instant of a moment and the human kinematic properties can be easily used for efficient identity matching. As a users' gait can be capture while the user is in walking state, i.e., at any point of time at least one foot is in contact with the floor/ground. But in case of running the gait features extraction is difficult because at some or any point of time there is no contact between the neither feet of the individual with the floor/ground. Also in case of forensics, the vertex location method is more favourable because this can be more readily communicated without a technical background.

Bouchrika, Imed & Nixon, Mark S. 2008 et al. [3] has proposed a new method using dynamic features for gait recognition. These dynamic features includes the spatial displacement of the trunk and the angular measurements of the lower limbs. The dynamic features means the cues which describe the kinematics of the locomotion process like the angular motion of the lower limb. Also in gait, static cues are also present, which is basically, the geometry structure of the human body, like user's height and width also the width of different body parts. Since, the static features are dependent on the factors like clothes, bags, shoes etc. Therefore, the static features are not widely used for recognition purpose. The gait feature was extracted by the model-based method so as to automate the extraction process of the joint trajectories. The motion of the joints were captured by the manual gait analysis.

For the extraction process, an algorithm is deployed which uses recursive evidence gathering and the output is in a parameterized form using the equation of Elliptic Fourier Descriptors. The gait knowledge is extracted by the heel strike, which is to reduce the computational load of the algorithm and also to reduce the parameter space dimensionality. After the extraction the other part is the gait feature selection, the Adaptive Sequential Forward Floating Selection search algorithm is deployed and it fully relies on the evaluation function which is used to derive the ideal subset of the features. The results thus obtained from the recognition rate were 82%. The research is carried so as to confirm the early psychological theories which includes the discriminative features for the motion perception which are embedded in gait kinematics.

Gafurov, D. and Snekkenes, Einar. 2007 et al. [9] The main focus was on the vulnerability on Gait Recognition System. Normally, lots of research work is been done regarding the efficiency for the gait recognition, the attacks on this system has not gained wide attention. The discussion about the minimal-effort impersonation attack and the closets person attack on gait biometrics are the main topic. Accelerometer have been used so as to capture gait of an individual which was attached to their respective hip, unlike others used video-camera so as to capture gait feature of an individual. The method for capturing gait of an individual comes under WS-based gait recognition approach. Here, the acceleration of hip in three orthogonal directions, have been recorded which are- forward-backward, up-down and sideways. The primary advantage of WS-based approach is enabling user authentication with unobtrusive, due to which this approach is suggested for user authentication and protection in portable devices and mobile devices.

However, for biometrics to work properly, it is not only enough to be unique but also important to be robust against attacks. As there are two type of biometrics- physiological and behavioural. Behavioural biometrics can be unsafe to the mimicking or impersonation attacks. The level of attacks which a biometric system can describe is totally dependent on the resources available to the attackers, such as tools (hardware/software), time, knowledge of the system etc. In minimal-effort impersonation attack the attacker has only an information about the common knowledge of the system and no other knowledge, like in this case the hip acceleration method, limited time to study the targets' walking style and also number of mimicking attempts to be restricted. The methods constitutes of three parts namely, the analysis of normal walking samples and second is, the scenario of minimal-effort mimicking attack is evaluated and the final part, an attack scenario is conducted. Here, the gait samples have been compared using the cycle method.

References	Year	Journal/ Conference	Problem	Technique	Shortcomings
2	2011	Journal	Gait recognition in forensics	The position of human leg, namely the hip, knees and ankle is used. Maim	At least one foot should be in contact with the ground. At the time of running

				aim is to extract limbs, human joints by prior knowledge and anthropometric gait data.	gait recognition is not possible.
3	2008	Conference	Dynamic features using the spatial displacement of the trunk and the angular measurements of the lower limbs.	Gait feature was extracted using model-based method and motion of joints by manual gait analysis. For extraction a recursive evidence gathering algorithm is used.	The Adaptive Sequential Forward Floating Selection search algorithm is deployed which relies on evaluation function.
6	2013	Conference	Using accelerometer for gait and activity recognition	Extracted gait cycles and calculated Manhattan and Euclidean distances	Only activity recognition can be done using accelerometer or a combination of various biometrics
9	2007	Journal	Spoof on Biometrics	Minimal-effort impersonation attack and closets person attacks	Using WS-based approach it becomes easy to spoof the gait data.
11	2012	Journal	To check if Gait Biometrics can be spoofed or not?	Methods are developed by the USOU and UOULU. A 3D volumetric data is used to synthesise the silhouettes.	Spoof can be done while attacker wears same clothes and same walking style.
14	2013	Journal	A new-invariant feature for gait recognition	GTI is used for original gait information on gait silhouettes. PSA is applied to get invariant gait feature.	Superimposing of the images from two sets of shapes.
17	2011	Conference	Using accelerometer to identify individual	Used MBASSy [20]	The authentication process was activated when the user wants it
21	2012	Conference	Gait pattern analysis for clinical practice	Accelerometer was attached to subjects' lower back. Gait data was calculated using RMS values	Has low sampling rate symmetry features and the regularity features

Table 1: Comparison and summary of the Literature Survey

Chapter 3

SCOPE OF THE STUDY

Now a days, almost every individual have a smart phone and almost each and every smart phone manufacturer provide a knowledge-based authentication method either it can be pin or it may contain password. As these authentication method are not so secure and can be easily attacked, like the password or pin can be stolen. Thus the integrity and confidentiality of that individual's data comes in jeopardy. So to resolve this problem, biometric based authentication module has been used, as in biometric the individual do not have to remember any password or pin or any of this kind and smart phones, with the help of inbuilt sensors can be used to obtain an individual user's biometric data.

Now a days, smart phones have lot of inbuilt features as well as various inbuilt sensors like, for the fingerprint sensor and also the accelerometer. The accelerometer basically acts upon the movement of an individual, so when an individual with its smart phone in the pocket is in acceleration then using accelerometer can be used for storing the gait data. Then this stored data is further compared with the enrolled template, which is stored after the enrolment process has done in the phone. The recent smart phones can use this method as a method for authentication process, as the gait of each and every individual is different and it is almost impossible that the attack on this type of system can be possible. Thus, the biometric based authentication system can be easily embedded with the mobile device.

Chapter 4

OBJECTIVE OF THE STUDY

The objective means the goal of any research. The work represented by this report is fully focused on the study that the biometric system can be used in the smart phones so as to get a better authentication results. As for authentication purpose, in earlier days as well as now a days, knowledge-based system are widely used and the main drawbacks was that it was solely based on a password or a pin, which can either be lost or can be stolen and the privacy of the users' data in is great danger. Also as there may be a common password or pin of the users' each and every account. Therefore, a loss of pin or password may lead to a heavy loss to all the users' private data. The biometrics system were introduced accordingly to remove this delimiters. The objectives of this research work are-

- at the time for enrolment
    1. using accelerometer capture gait data for different input modules (like standing, slow walking, fast walking and normal walking).
    2. the gait data will be stored in the smartphone itself.
- at the time for authentication
    1. user will again give its gait data using accelerometer for all modules.
    2. then this data will be matched from the pre-existed data which is stored in a smartphones.
    3. if both the data are a match then, access is granted or else second attempt will be given

As only fingerprint scan was included in smart phones earlier and the outcome was well addressed. Now the gait biometrics can also be embedded with the smart phones by using the accelerometer sensor. This technique can be easily accessible as biometrics is turning to an evolution in today's world.

Chapter 5

RESEARCH METHODOLOGY

Research methodology means the way of methods being followed in a particular discipline to prove our hypothesis. It is major part of my research. Basically it is a proof of the concept(s) that I will use from some pre-existing validated method. The concepts should be clear enough so that it can be easy to experiment on and the result produced must be reproducible and a valid conclusion.

Proposed system is developed using Android 5.1.1 (API 22) hence minimum required version of Java to run this system is 1.7. Key benefits of using Java are platform independency, dynamic and extensible programming, backward compatibility, object oriented programs, security, efficiency and performance and also the fact that Android OS is fully based on Java and also several APIs are available which can be easily used to ease the programming. The brief description of the tools, which are used to develop this system are described:

5.1 Tools Description

5.1.1 Android 5.1.1 (API 22) [25]-[30]

Android 5.1.1 (API 22) is the latest API version launched by google on 21st April, 2015. The key features is if the device is lost or if it is stolen then it shall remain locked until the owner signs in to their google account, also if the phone is reset to factory mode then also the device will remain locked. Android provides a Java language environment also the apps are designed to run on various platforms like phones, tablets, televisions, phablets and Android Wear. So to achieve this goal different XML layouts are provided for different screen sizes. As Android is based on the Linux Kernel, so each and every applications have a different system identity and thereby they run independently and Linux isolates every applications from each other and also from the system.

5.1.2 Accelerometer Sensor [31], [32]

To develop this system we used accelerometer sensor so as to capture the motion data or gait data. Although in Android lots of motion sensors are available like gravity sensors, accelerometers, rotational vector sensors and gyroscopes. To access these sensors we use Android Sensor Framework which includes several interfaces and classes which helped in accessing the sensors according to the projects requirements. To access accelerometer-

```
Sensor accelerometer = sensorManager
                        .getDefaultSensor(Sensor.TYPE_ACCELEROMETER);
```

Every sensor is associated with a SensorEvent, which stores the data in floating point for all the three axes. If only required to capture the data in any one of the axes are-

```
lastX = event.values[0]; //along x-axis
lastY = event.values[1]; //along y-axis
lastZ = event.values[2]; //along z-axis
```

5.1.3 Eclipse Juno IDE(c) [33]

To develop this project Eclipse Juno IDE (Eclipse 4) with Version: 1.4.1.v20120912-144938-8R7xFOXFLWUl7PpNBh_HIGkb4 is used and its Build id: M20130204-1200. In this project Eclipse ADT [34] a plugin which is used to build Android applications is been provided by the google, which can be included into Eclipse as per following steps:

Step 1: Goto Eclipse and **Help -> Install New Software**.

Step 2: A new window will open as shows in figure 5 wherein under the "**Work with**" text box write the following link "**https://dl-ssl.google.com/android/eclipse**".

Step 3: From the following window click on "**Next**" and the ADT plugin will be installed in the system.

Apart from ADT, SDK packages are needed to install so as to build the applications in different API levels. To install SDK, following steps are to be followed-

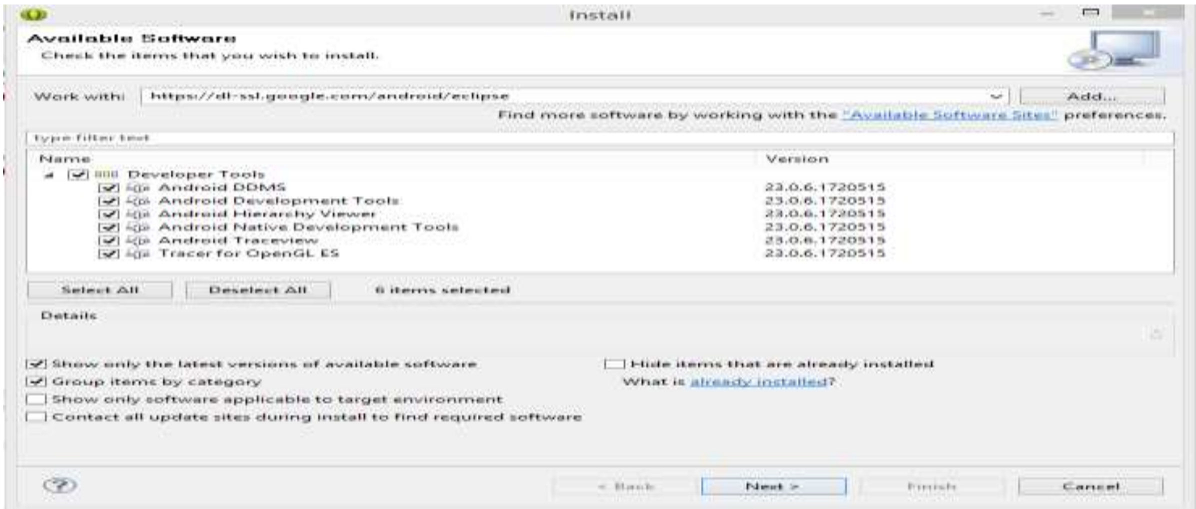
Step 1: Goto "**https://developer.android.com/sdk/installing/index.html**" and click on "**Stand-Alone SDK Tools**".

Step 2: Then click on "**download the SDK now**" link.

Step 3: Under the section "**Other Download Options**" and sub-section "**SDK Tools Only**", download the package according to the platform.

Step 4: After the installation SDK will be installed in the system under the name "**SDK Manager**".

Step 5: To access SDK Manager from the eclipse. **Window -> Android SDK Manager,** and this will provide a window as shown in figure 6, so as to install various APIs as per the requirement of the project.



Available Software

Check the items that you wish to install.

Work with: https://dl-ssl.google.com/android/eclipse

Find more software by working with the "Available Software Sites" preferences.

Name	Version
☑ Developer Tools	
☑ Android DDMS	23.0.6.1720515
☑ Android Development Tools	23.0.6.1720515
☑ Android Hierarchy Viewer	23.0.6.1720515
☑ Android Native Development Tools	23.0.6.1720515
☑ Android Traceview	23.0.6.1720515
☑ Tracer for OpenGL ES	23.0.6.1720515

6 items selected

☑ Show only the latest versions of available software

☑ Group items by category

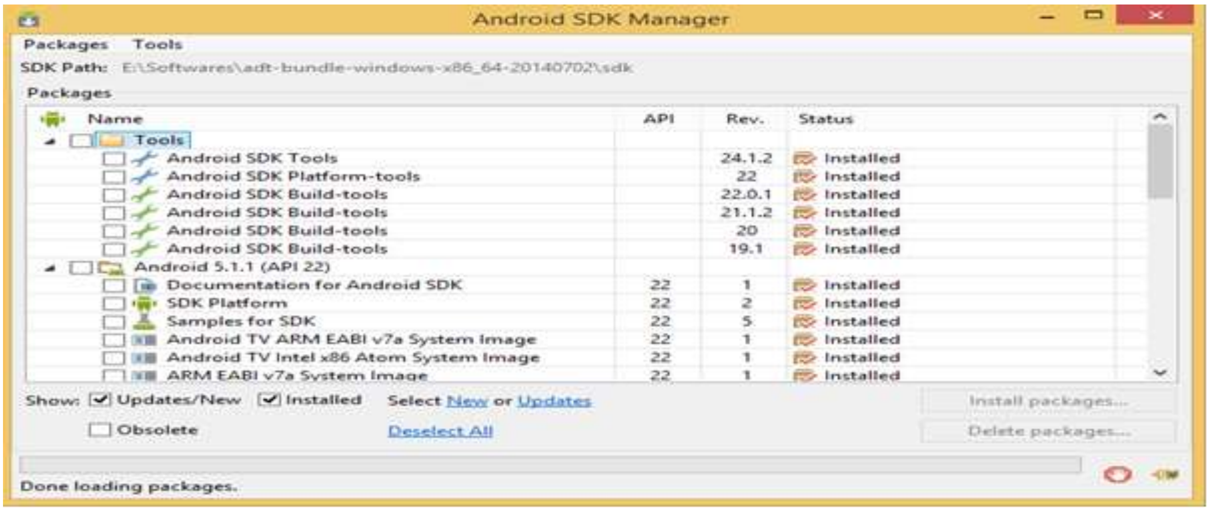
□ Show only software applicable to target environment

□ Contact all update sites during install to find required software

□ Hide items that are already installed

What is already installed?

Figure 5: Installation of ADT plugin



SDK Path: E:\Softwares\adt-bundle-windows-x86_64-20140702\sdk

Packages

Name	API	Rev.	Status
□ Tools			
□ Android SDK Tools		24.1.2	Installed
□ Android SDK Platform-tools		22	Installed
□ Android SDK Build-tools		22.0.1	Installed
□ Android SDK Build-tools		21.1.2	Installed
□ Android SDK Build-tools		20	Installed
□ Android SDK Build-tools		19.1	Installed
□ Android 5.1.1 (API 22)			
□ Documentation for Android SDK	22	1	Installed
□ SDK Platform	22	2	Installed
□ Samples for SDK	22	5	Installed
□ Android TV ARM EABI v7a System Image	22	1	Installed
□ Android TV Intel x86 Atom System Image	22	1	Installed
□ ARM EABI v7a System Image	22	1	Installed

Show: ☑ Updates/New ☑ Installed Select New or Updates

□ Obsolete Deselect All

Done loading packages.

Figure 6: Android SDK Manager

5.2 Proposed System

The proposed system includes two modules- first being the enrolment module and the other being the authentication module. In enrolment module first the user will undergo enrolment and then its gait data will be stored in the phone itself. In the authentication module the user will undergo authentication, but the user will have to provide gait data again, so as it will be compared with the data which is stored in the smartphone. The flow chart of the whole process is described in figure 7-

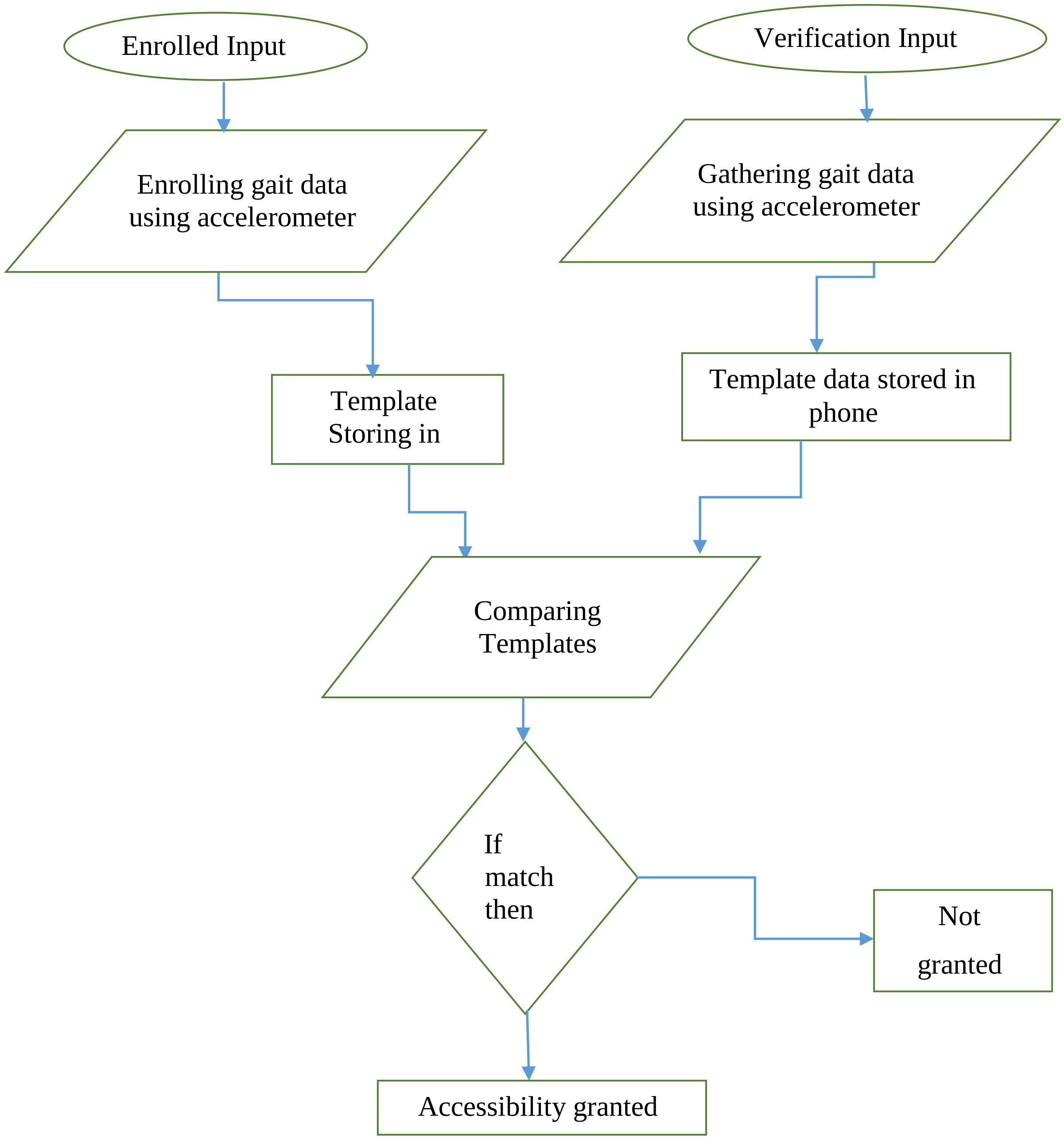


Figure 7: Flow-Chart for problem solving process.

5.2.1 Enrolled Input

The enrolment of the user is done with the help of inbuilt accelerometer. For a user to be enrolled in the system, following sub-modules should be enrolled, first Standing, second Slow Walking and third is Normal Walking.

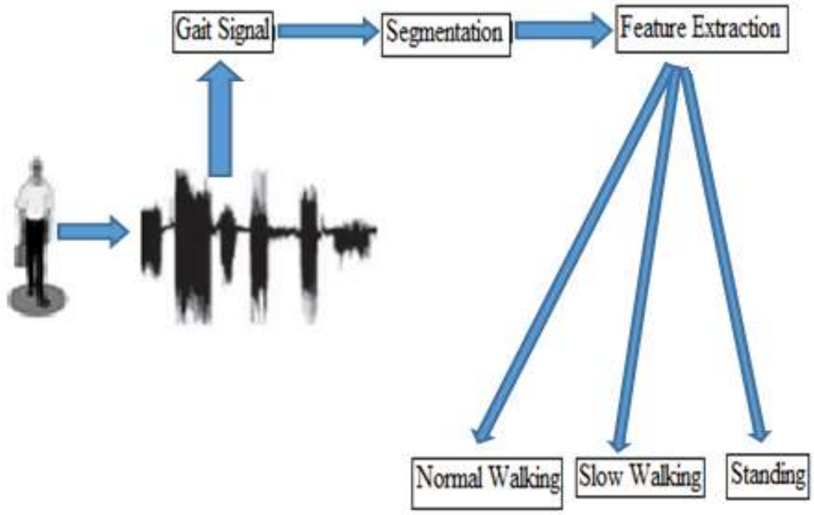


Figure 8: Sub-modules in Enrolment process.

After the gait data is generated for each sub-module it will then be stored in the phone separately and this stored data will be further used to authenticate the user.

5.2.2 Verification Input/Authentication Input

At the time of authentication the user can select any one of the sub-modules either Normal Walking or Slow Walking or Standing, and then the gait data will be provided by the user. The gait data will be stored and then it will be matched with the existing data which is stored in the phone at the time of enrolment. If there is a match then the user will be provided access or else the user won’t get access.

Chapter 6

RESULTS AND DISCUSSION

6.1 Analysis of data

The data sample for this system is collected with 4 different candidates. The value of accelerometer sensor depends upon three parameters.

- Height of the person
- Position of the mobile
- Gesture of a person (in which gesture is the candidate either standing or sitting)

The values on the three axes for each candidate are stored first and then analysed.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	87	0.0	9.595961	2.7102363
2.	87	0.0	9.969456	2.690352
3.	87	0.0	9.998186	0.0
4.	87	0.0	9.80665	0.0
5.	87	0.0	9.39848	0.0
6.	87	0.0	9.346964	0.0

Table 2: Sample data of candidate ‘A’ for Standing sub-module.

Table 2 of candidate ‘A’ displays the value in X, Y and Z axis. The initial 2 datas contains values in Z-axis and it means that the candidate is standing in different gesture and the rest of the values are taken when the candidate is standing at normal gesture.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	65	0.0	0.0	10.055647
2.	65	0.0	0.0	10.0748005
3.	72	0.0	3.0933087	9.77792
4.	72	0.0	2.0590134	10.237606
5.	62	0.0	0.0	9.892841
6.	62	0.0	2.2888567	9.825804

Table 3: Sample data of candidate ‘A’ for Sitting sub-module.

Table 3 shows the value when the candidate ‘A’ is sitting. The initial two data shows that the candidate is sitting in a normal gesture. The later values shows that the candidate is sitting with a different gestures.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	78	0.0	9.9790325	0.0
2.	78	0.0	9.950302	0.0
3.	78	0.0	9.509769	0.0
4.	78	0.0	9.902418	0.0
5.	78	0.0	9.404425	3.3806129
6.	78	0.0	9.720459	2.5378537

Table 4: Sample data of candidate ‘B’ for Standing sub-module.

Table 4 of candidate 'B' displays the value in X, Y and Z axis. The final 2 datas contains values in Z-axis and it means that the candidate is standing in different gesture and the rest of the values are taken when the candidate is standing at normal gesture.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	52	0.0	2.873042	9.662998
2.	52	0.0	2.9496565	9.672575
3.	61	0.0	2.3175871	9.998186
4.	61	0.0	0.0	10.055647
5.	56	0.0	3.1124623	9.528923
6.	56	0.0	2.920926	9.771305

Table 5: Sample data of candidate 'B' for Sitting sub-module.

Table 5 shows the value when the candidate 'B' is sitting. The initial two data shows that the candidate is sitting in a normal gesture. The later values shows that the candidate is sitting with a different gestures.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	90	0.0	9.787497	0.0
2.	90	0.0	9.911995	0.0
3.	90	0.0	9.32781	0.0
4.	90	0.0	9.279925	0.0
5.	90	0.0	9.787497	0.0

6.	90	0.0	9.730036	2.3558946

Table 6: Sample data of candidate ‘C’ for Standing sub-module.

Table 6 of candidate ‘C’ displays the value in X, Y and Z axis. The final data contains values in Z-axis and it means that the candidate is standing in different gesture and the rest of the values are taken when the candidate is standing at normal gesture.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	63	0.0	0.0	10.208876
2.	63	0.0	0.0	10.160992
3.	66	0.0	2.9783869	9.797073
4.	66	0.0	4.0414124	9.346964
5.	62	0.0	0.0	10.132261
6.	62	0.0	0.0	10.199299

Table 7: Sample data of candidate ‘C’ for Sitting sub-module.

Table 7 shows the value when the candidate ‘C’ is sitting. The initial two data shows that the candidate is sitting in a normal gesture. The later values shows that the candidate is sitting with a different gestures.

Sl. No.	Height (in cms)	X- axis	Y-axis	Z-axis
1.	83	0.0	9.873688	0.0
2.	83	0.0	9.902418	0.0
3.	83	0.0	9.902417	0.0

4.	83	0.0	9.931149	0.0
5.	83	0.0	9.595961	2.4899697
6.	83	0.0	9.768343	2.0111294

Table 8: Sample data of candidate ‘D’ for Standing sub-module.

Table 8 of candidate ‘D’ displays the value in X, Y and Z axis. The final 2 datas contains values in Z-axis and it means that the candidate is standing in different gesture and the rest of the values are taken when the candidate is standing at normal gesture.

Sl. No.	**Height (in cms)**	**X- axis**	**Y-axis**	**Z-axis**
1.	62	0.0	2.7964275	9.710882
2.	62	0.0	2.2984335	9.854534
3.	70	0.0	2.9017725	9.825804
4.	70	0.0	2.585738	9.988609
5.	60	0.0	2.231396	90720459
6.	60	0.0	2.1452048	9.653421

Table 9: Sample data of candidate ‘D’ for Sitting sub-module.

Table 9 shows the value when the candidate ‘D’ is sitting. The initial two data shows that the candidate is sitting in a normal gesture. The later values shows that the candidate is sitting with a different gestures.

As for each candidate the data values in all the axes do vary according to the gestures of the candidate. For candidate ‘A’ the data values are stored in the database and as there is variation in the values, so for authentication a range is defined for each and every candidate based on their enrolment values. The minimum value at the time of enrolment and the maximum value at the time of enrolment is considered for range for each and every candidate.

Range = [min. value of candidate (i), max. value of candidate (i)]

Now based on this range for each candidate the authentication process is evaluated and the results are described in the next section.

6.2 Results

System is tested with 10 different users and each user had undergone each sub-module of enrolment process and the final results generated by the system is given in table 2. It shows the FMR, FNMR and FTER of any candidate. For FTER the enrolment done for each individual was a minimum of 5 times. FMR is calculated with all the enrolment done by each candidates.

$$\text{FMR}= \frac{\text{No. of false match of candidate (i)}}{\text{Total no of enrolment done by each user – No of enrolment done by candidate (i)}} *100$$

$$\text{FNMR} = \frac{\text{No. of false non- match of candidate (i)}}{\text{No of enrolment done by candidate (i)}} *100$$

Candidate	FMR (%)	FNMR (%)	FTER (%)
A	6.67	20	0
B	11.11	40	0
C	13.33	60	0
D	2.22	20	0
E	4.44	20	0
F	15.56	40	0
G	13.33	60	0
H	4.44	40	0
I	11.11	40	0
J	6.67	20	0

Table 10: Results of final system.

6.3 Output Screenshots and their Descriptions

The snippets of the whole proposed system are as follows describing the final system.

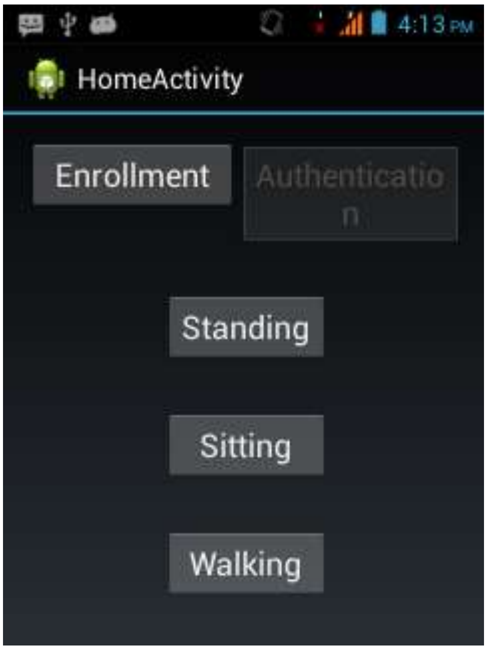
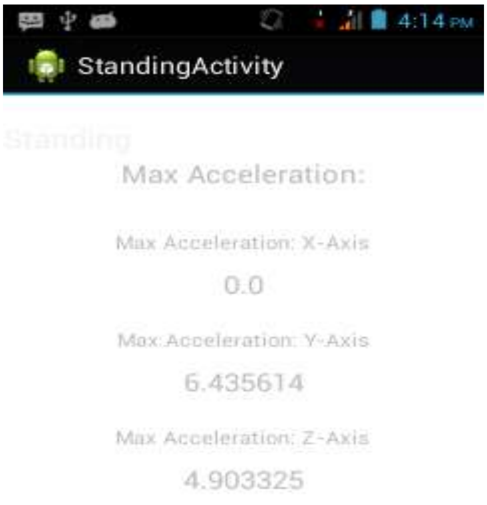


Figure 9: The Enrolment Input of the system.

This is the very first interface of the application developed for this system. As mentioned earlier in methodology part that this is the part where the user has to undergo enrolment for various sub-modules, and the accelerometer will collect the gait data of the user and which can be further used for authentication purpose.



Standing

Max Acceleration:

Max Acceleration: X-Axis

0.0

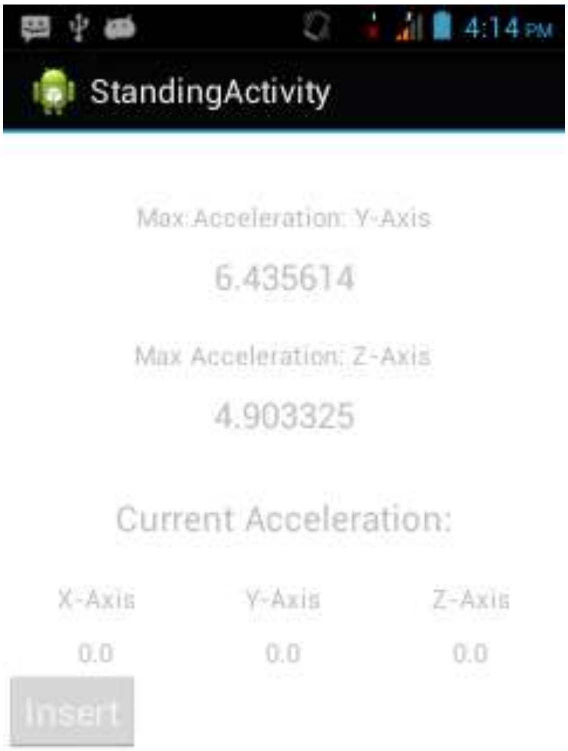
Max Acceleration: Y-Axis

6.435614

Max Acceleration: Z-Axis

4.903325

Figure 10 (a): Part of Standing sub-module in Enrolment system.



StandingActivity

Max Acceleration: Y-Axis

6.435614

Max Acceleration: Z-Axis

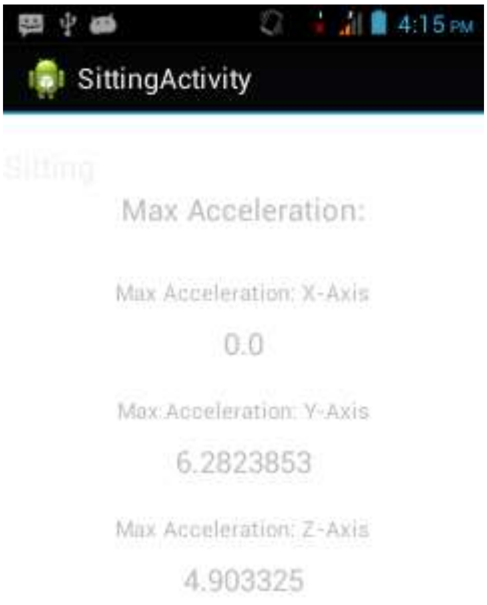
4.903325

Current Acceleration:

X-Axis	Y-Axis	Z-Axis
0.0	0.0	0.0

Figure 10 (b): Part of Standing sub-module in Enrolment system.

Figure 10 (a) & (b) shows the gathering of gait data via accelerometer. The maximum accelerated values in each axes is shown and these values are then stored in the phone so as it can be further used for authentication purposes. Although authentication process can only be accessed once all of the sub-modules inside the enrolment process is used atleast once.



SittingActivity

Sitting

Max Acceleration:

Max Acceleration: X-Axis

0.0

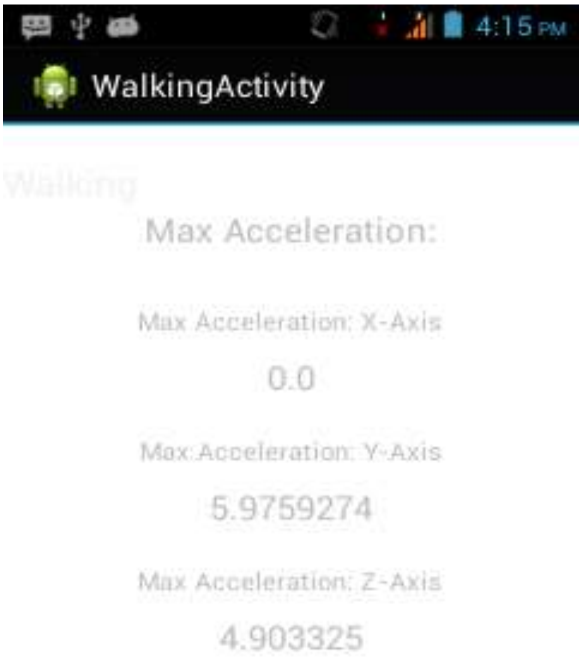
Max Acceleration: Y-Axis

6.2823853

Max Acceleration: Z-Axis

4.903325

Figure 11: Part of Sitting sub-module in Enrolment system.



Walking

Max Acceleration:

Max Acceleration: X-Axis

0.0

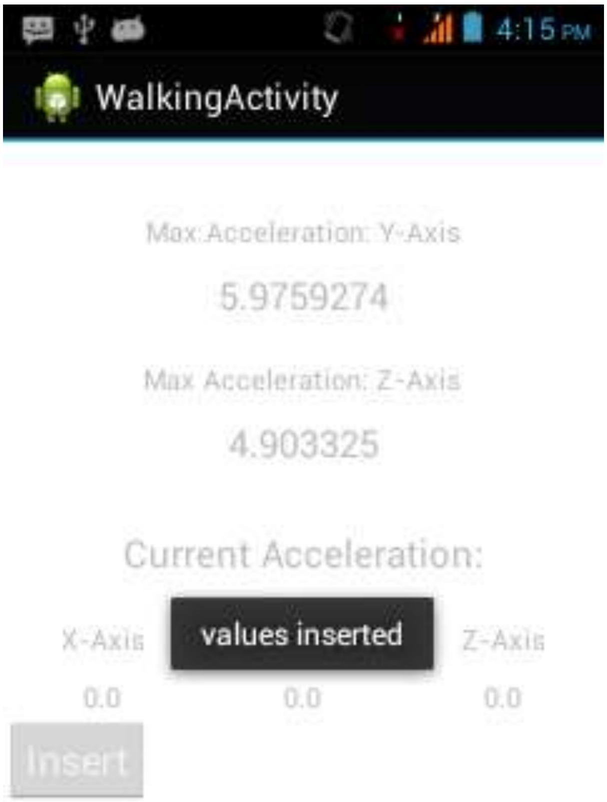
Max Acceleration: Y-Axis

5.9759274

Max Acceleration: Z-Axis

4.903325

Figure 12 (a): Part of Walking sub-module in Enrolment system.



Max Acceleration: Y-Axis

5.9759274

Max Acceleration: Z-Axis

4.903325

Current Acceleration:

X-Axis values inserted Z-Axis

0.0 0.0 0.0

Insert

Figure 12 (b): Part of Walking sub-module in Enrolment system.

Figure 11, 12 (a) & (b) describes the rest of the sub-modules in the enrolment process. As mentioned earlier that the user had to proceed with all three sub-modules at least once only then the authentication modules will be activated.

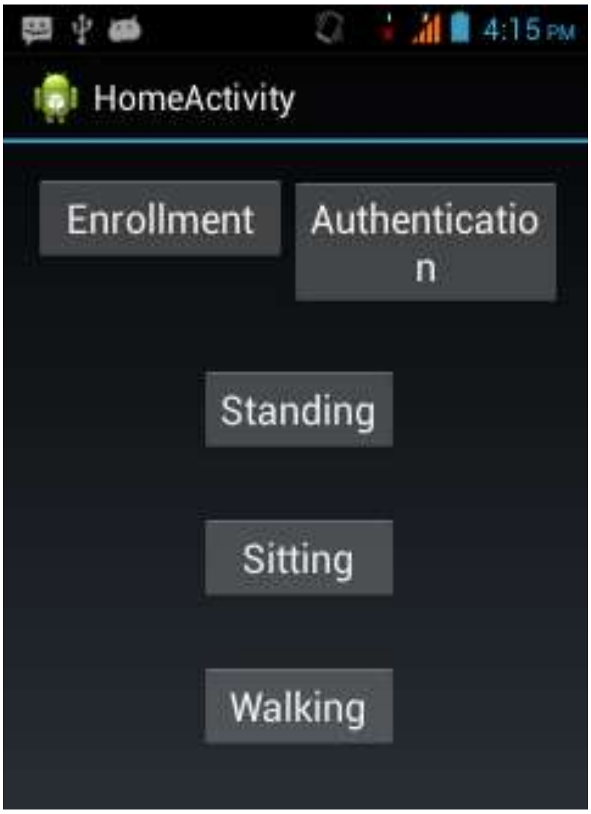
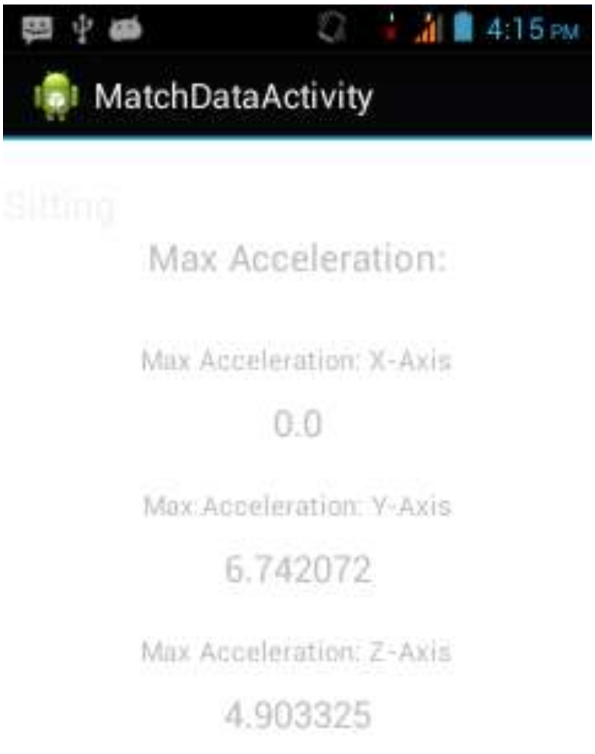


Figure 13: The Authentication process of this system.



Sitting

Max Acceleration:

Max Acceleration: X-Axis

0.0

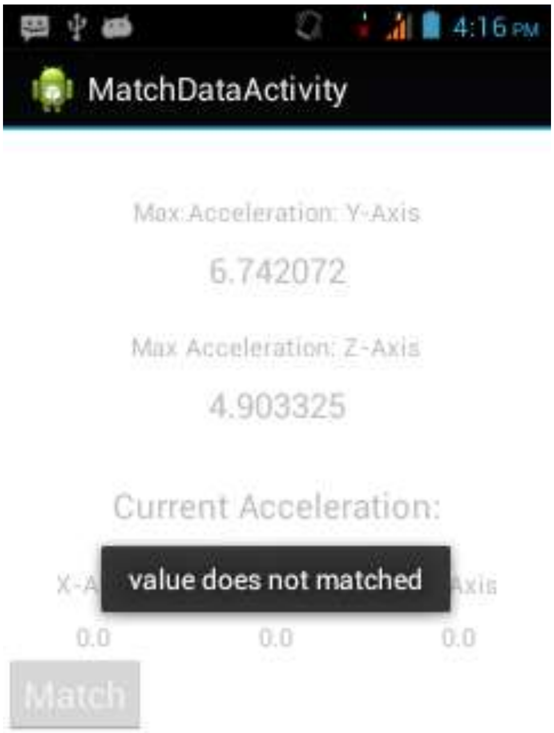
Max Acceleration: Y-Axis

6.742072

Max Acceleration: Z-Axis

4.903325

Figure 14 (a): Part of Authentication process.



MatchDataActivity

Max Acceleration: Y-Axis

6.742072

Max Acceleration: Z-Axis

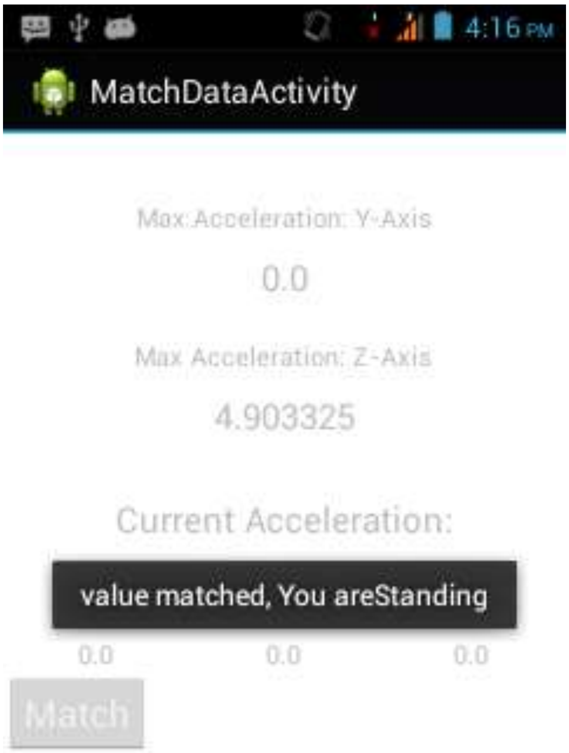
4.903325

Current Acceleration:

X-A value does not matched Axis

0.0 0.0 0.0

Figure 14 (b): The user did not get access.



MatchDataActivity

Max Acceleration: Y-Axis

0.0

Max Acceleration: Z-Axis

4.903325

Current Acceleration:

value matched, You areStanding

0.0 0.0 0.0

Figure 14 (c): The user did get access.

Figure 13 shows after the whole enrolment process is been carried out by the user atleast once, then the authentication module is activated.

Figure 14 (a) displays the match data activity where the user can proceed with either standing or sitting or walking to get authentication. The values will be displayed using the help of accelerometer and then these values will be matched with the values which were stored at the time of authentication.

Figure 14 (b) displays that the user didn't get access as the values do not match from the users enrolment values. Figure 14 (c) displays that a user gets access as the values did get match with the ones stored at the time of enrolment.

Chapter 7
CONCLUSION

Numerous techniques for gait recognition using accelerometer are discussed in this report but this work is different from those techniques. System proposed in this report allows a user to enrol in various sub-modules. Results in table 10 shows that the system works pretty decently. This system will help the users to access their smartphones without remembering tokens or passwords or pins of any kind. For future work this system lefts, problem to deal with fast walking and normal walking as the values for both these were unable to differentiate.

REFERENCES

A. Books:

[1] Nanavati, Samir; Thieme, Michael and Nanavati, Raj. (2008). *Biometrics: Identity Verification in a Networked World*. Wiley Publications 1st Edition, p. 3-41.

B. Research Papers:

[2] Bouchrika, Imed; Goffredo, Michaela; Carter, John and Nixon, Mark S. (2011, July), “On Using Gait in Forensic Biometrics”. J Forensic Sci, Volume-56, Issue-4, pp- 882889.

[3] Bouchrika, Imed and Nixon, Mark S. (2008). “Gait Recognition by Dynamic Cues”. Department of Electronics and Computer Science, University of Southampton, SO17 1BJ, UK, IEEE. pp- 1-4.

[4] Choudhary, Jitendra. (2012, Sept. – Oct), “Survey of Different Biometrics Techniques”. International Journal of Modern Engineering Research (IJMER), Volume-2, Issue-5, pp- 3150-3155.

[5] Cutting, J.E; Proffitt, D.R. and Kozlowski, L. T. (1978). “A biomechanical invariant for gait perception”. J Exp Psychol Hum Percept Perform. Volume-4, Issue-3, pp- 353– 372.

[6] Derawi, Mohammad and Bours, Patrick. (2013), “Gait and activity recognition using commercial phones”, Computers & Security 39, pp- 137-144.

[7] Gaba, Ira and Kaur, Paramjit. (2013, June). “A Novel Technique Used for Gait Recognition MDA, LDA and BPNN- A Review”. IJITEE. ISSN: 2278-3075, Volume-3, Issue-1, pp- 2278-3075.

[8] Gafurov, D. (2007). “A survey of Biometric Gait Recognition: Approaches, Security and Challenges”, NIK, pp- 19-21.

[9] Gafurov, Davrondzhon; Snekkenes, Einar and Bours, Patrick. (2007, September), “Spoof Attacks on Gait Authentication System”, IEEE Transactions on Information Forensics and Security, Volume-2, Issue-3, pp- 491-502.

[10] Goffredo, M; Bouchrika, Imed, Carter, John N. and Nixon, Mark S. (2009). “Self-calibrating view-invariant gait biometrics”. IEEE Tran. Syst., Man, Cybern. B, Volume40, Issue-4, pp 997-1008.

[11] Hadid, Abdenour; Ghahramani, Mohammad; Kellokumpu, Vili; Pietikainen, Matti; Bustard, John and Nixon, Mark. (2012, November), “Can Gait be spoofed?”, Institute of Electrical and Electronics Engineers, pp- 3280-3283.

[12] Hossain, Emdad; Chetty, Girija and Goecke, Roland. (2013). “Multi-view Multimodal Gait Based Human Identity Recognition from Surveillance Videos”. Volume7742, Springer, pp- 88-99.

[13] Jeong, Seungdo; Kim, Tai-hoon and Cho, Jungwon. (2013, March), “Gait recognition using description of shape synthesized by planar homography”, Volume-65, Issue-1, Springer, pp- 122-135.

[14] Kusakunniran, Worapan; Wu, Qiang; Zhang, Jian; Ma, Yi and Li, Hongdong. (2013), “A New View-Invariant Feature for Cross-View Gait Recognition”, IEEE transactions on information forensics and security, Volume-8, Issue-10, pp- 1642-1653.

[15] Lane; N.D., Miluzzo; E., Lu; H., Peebles; D., Choudhury; T. and Campbell; A.T. (2010, September). “A survey of mobile phone sensing.” Communications Magazine. 48(9):140e50.

[16] Lee, Tracey K. M.; Belkhatir, Mohammed and Sanei, Saeid. (2013, July). “A comprehensive review of past and present vision-based techniques for gait recognition”. Volume-72, Issue-3, Springer, pp 2833-2869.

[17] Nickel, C.; Derawi, M. O.; Bours, P. and Busch, C. (2011), “Scenario test of Accelerometer-based biometric gait recognition”, Security and Communication Networks (IWSCN).

[18] Pushparani, M. and Sasikala, D. (2012, May). “A Survey of Gait Recognition Approaches Using PCA & ICA”. Global Journal of Computer Science and Technology. Volume-12, Issue-10, pp- 975-1258.

[19] Wang, Jin; She, Mary; Nahavandi, Saeid and Kouzani, Abbas. (2010, December). “A Review of Vision-based Gait Recognition Methods for Human Identification”. IEEE, Piscataway, N.J., Volume-1, Issue-3, pp- 320-327.

[20] Witte, Heiko and Nickel, Claudia. (2010). “Modular Biometric Authentication Service System (MBASSy)”. Proceedings of the Special Interest Group on Biometrics and Electronics Signatures, pp- 115-120.

[21] Yang, Mingjing; Zheng, Huiru; Wang, Haiying; McClean, Sally; and Harris, Nigel; (2012) “Accessing the utility of smart mobile phones in gait pattern analysis”. Health Technol. February, DOI 10.1007/s12553-012-0021-8, pp- 81–88.

[22] Yu, Shiqi; Tan, Tieniu; Huang, Kaiqi; Jia, Kui and Wu, Xinyu. (2009, August). “A study on gait-based gender classification”. IEEE Trans Image Process. Volume-18, Issue8, pp- 1905–1910.

[23] Zijlstra W, Hof AL. (2003), “Assessment of spatio-temporal gait parameters from trunk accelerations during human walking.” Gait Posture. 18:1–10.

C. Websites:

[24] http://www.engineersgarage.com/sites/default/files/imagecache/Original/wysiwyg_imageupload/1/Biometric-working-diagram.gif

[25] http://en.wikipedia.org/wiki/Android_Lollipop

[26] http://en.wikipedia.org/wiki/Android_version_history

[27] http://en.wikipedia.org/wiki/Android_%28operating_system%29

[28] http://developer.android.com/guide/index.html

[29] http://developer.android.com/guide/practices/compatibility.html

[30] http://developer.android.com/guide/topics/security/permissions.html

[31] http://developer.android.com/guide/topics/sensors/sensors_overview.html

[32] http://developer.android.com/guide/topics/sensors/sensors_motion.html

[33] http://www.eclipse.org/platform

[34] https://dl-ssl.google.com/android/eclipse

APPENDIX

LIST OF ABBREVIATION

Keywords	Abbreviated Form	Page No.
ADT	Android Development Tools	20, 21
API	Application Programming Interface	19, 20, 21
ATM	Automatic Teller Machine	1
BPNN	Back Propagation Neural Network	6
DET	Decision Error Trade-off	4, 8
EER	Equal Error Rate	4
FAR	False Acceptance Rate	8
FMR	False Match Ratio	3, 4, 8, 29
FNMR	False Non-Match Rate	3, 4, 29
FRR	False Recognition Rate	8
FS-based	Floor Sensor-based	7
FTER	Failure-to-Enrol Rate	4, 29
GTI	Gait Texture Image	11, 16
IDE	Integrated Development Environment	20
LBP-TOP	Local Binary Patterns from Three Orthogonal Planes	12
LDA	Linear Discriminant Analysis	6

MBASSy	Modular Biometric Arithmetic Service System	**13, 16**
MDA	Multi-linear Discriminant Analysis	**7**
MR	Motion Reading Sensor	**7**
MV-based	Machine Vision-based	**7**
PCA	Principal Component Analysis	**6, 9**
PSA	Procrustes Shape Analysis	**11, 16**
RMS	Root Mean Square	**12, 16**
SDK	Software Development Kit	**20, 21**
TILT	Transform Invariant Low-rank Textures	**11**
UOULU	University of Oulu	**12, 16**
USOU	University of Southampton	**12, 16**
WS-based	Wearable Sensor-based	**7, 15, 16**
XML	Extensible Markup Language	**19**