JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Anti-theft Mobile Device Motion Pattern Identification Using LSTM

Ms. Ujwala Phere, Student, Department of Computer Engineering, TEC, Nerul
Mr. Ramesh V.Shahabade, Professor, Department of Computer Engineering, TEC, Nerul

***Abstract*-Currently Mobile anti-theft mechanisms are available for discovery of the particular theft occurrence. Locating lost phone, GPS, remotely wiping and locking device, locking the SIM card service provider is only anti-theft mechanisms for discovery of the actual occurrence. They cannot detect the stealing behavior. The anti-theft mechanism will determine if thephone is in the hands of thieves, which detect stealing behavior by using long short-term memory is classifier to enhance accuracy of reorganization. We detect ongoing unauthorized movement of device notify its motion pattern inherent to actual movement. We use the waveform of accelerometer provided in mobile devices to research the pattern.**

We apply Long short-term memory classifier is depending upon matching patterns. So LSTM requires the step cycles, which are stored in the database that is acceleration data. LSTM verify the unknown behavior, if the mobile device hand of a thief. Motion pattern to verify the identity of the person's possession of the device immediately whenever it has moved. We provide a device detection system for performing authentication whenever the mobile device is move. We use the accelerometer data, which monitors the device's acceleration because of human movement.

Long short-term memory requires when a user is sitting on adesk, the data is recorded by its accelerometer. Hence, we should always ignore this data instead of attempting process it into motion step cycles. However, we want to detect the start of a motion pattern during a timely fashion. We discovering out the accuracy using unauthorized movement within step cycles, which is test with some volunteers.

***Index Terms*- Mobile Society, Anti-theft, Motion pattern, Gait authentication.**

I. INTRODUCTION

Nowadays, mobile devices became personal and valuable itemin human life. Per report in 2014, 3.1 million people had their devices stolen, as a result, much private information is leaked to the final public soon defeat of mobile device theft, lots of anti- theft mechanism is means, for example, and Apple offers a free app called "Find my iPhone". It collects GPS information. Once users realize their devices are stolen, they will use the GPS information to remotely wipe and lock their devices. In anti-theft mechanisms having an example, which is required in SIM Cards Lock. The mobile user can call their service to lock the device by locating SIM cards. All of these methods require discovery of the unknown person before any security actions is formed. Although there are many device anti-theft mechanisms, all of them have one single limitation. In another word, all of these mechanisms cannot detect the stealing behavior. They need users' interaction to active these mechanisms. If users do not understand their devices are stolen, an attacker will have many times to full physical access to the device.

So, the mechanisms are detecting the stealing behavior that's ongoing movement of the device. Furthermore, we employ motion patterns to comparing with the unknown person's possession of the device immediately whenever it has moved.

We propose some way wherein we detect unauthorized movement of the device using its motion pattern. We use the waveform of accelerometer provided altogether mobile devices to analyze the motion pattern. Likewise, we apply long short term memory is a classifier to reinforce the accuracy of recognition. LSTMclassifier to classify where the step cycle belongs to the owner's or not and extract the normalized waveform of step cycles and match with the database of the owner's step cycle. We pass the waveform data to our algorithm to induce its features and apply one of all the next three classifier K-S statistical tests [10], statistical correlation and total variation distance. We use motion pattern identification to verify that the person position. User can be in walk or run condition. However, we use the accelerometer which monitor is the device's acceleration due to human movement compare with unauthorized movement.

The biggest challenge of our method is that our mechanism has to identify the user within a short amount of some time. After days of coaching process, the device has collected a huge amount of user's data. It needs some time to test with this user's data and so the database. If the comparing time is solely too long, a theft might need been escaped before the detection system notifies the owner. Thus, our method must reduce comparisons time with giving number of acceleration data as well as complexity. To manage that, we designed a pattern synchronization method to chop backthe size of user's database. We also designed a quick matching method to cut back comparison time.

We offer a detection system for performing authenticationwhenever the mobile device is moved. We use theaccelerometer, which monitors the device's acceleration due tohuman movement. Specifically, we have got also used the stepcycles for a behavior for improving accuracy and reduce Interval time.

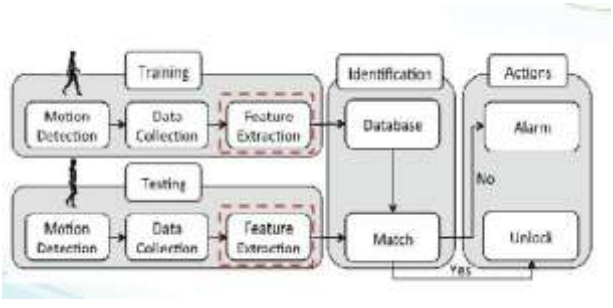

Fig 1: System Construction

Here is our system's construction. The Motion Detection component is accountable for distinguishing different states of the mobile device. Data collection component collects raw accelerometer data, which is deconstructed by the Feature Extraction component. The extracted features are stored into the database. The testing module has the identical three components

Because the training module. But it extracts features from this user's movement. These test features are compared with the owner's database within the Identification module. Finally, the choice made by the Matching component is shipped to the Action module as an Unlock action or an Alert action.

One-step cycle, within the feature extraction module, the Pattern synchronization method is employed to extract features. Here is an example of the features extracted from the two different people. The 2 persons' data are visibly different; of course, the step cycles extracted from person A are roughly 100 data points long, the step cycles from person B are around 50 data points long. Next, it will be able to show you the way our method extracts these step cycles Person A, Person B.

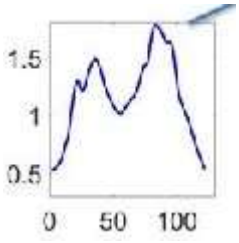

Fig 2. one step cycles

Through the development of an algorithm which compares only the repetitive walking pattern using elementary arithmetic which is using LSTM classifiers to discovering the patterns. We've got also created an identical algorithm to seekout and compare signature step cycle for a behavior. The matching phase compares unknown step cycles storing in the training database to spot unauthorized moves. We are using methods to check with unknown behavior cycles further as the user behavior.

II. LITERATURE SURVEY

The existing techniques specialize in other theft-reactant, authentication strengthening, and gait authentication work. Theft-reactant application currently available are supported combination of GPS, Wi-Fi positioning and cell tower triangulation to trace the location. As an example is Gadget track, is a popular anti-theft application implemented in both IOS system and android.

To detect and monitoring of theft or misplace mobile phones [1] develops a novel and efficient android application. The tracking application has the potential of SIM card detection, call monitoring, image capturing supported some predefined SMS. The applying installed are going to be running within the background and will not be shown within the task manager likewise. Once the portable is lost, this application enables the user to trace a mobile device and to receive notification via SMSto a predefined number. Some specified formatted messages willbe accustomed control the theft portable.

A sensible phone anti-theft solution [1][2] supported lockingSIM card of the itinerant is proposed. It also gives the structure of the anti-theft system in mobile devices, the most software functional blocks and the implementation flow chart of every module. The functions of locking and unlocking of the mobile and SIM card, anti-theft and short messaging service control are realized by adding locking SIM card setting module, locking SIM card control module and anti-theft processing module. By the utilization of software algorithm, users may findthe stolen portable and protect critical information. To some extent it can reduce the losses caused by the stolen phone.

In the group of strengthening authentication mechanism [3][4] behavioral and physiological biometrics are increasing in utilization

Our approach relies on gait analysis techniques on mobile devices. Some existing methods are during this field.

In Dynamic Time Warping (DTW) [8] is employed to extract the similar cycles as step data. The good thing about DTW is that it can compare two data patterns with different size.

In gait analysis techniques [7] like correlation andspectrographic analysis, respectively, to extract step cycles. We discover that those methods can only add ideal situation out of the presence of noise and without common irregular behavior. For identifying people from gait pattern [3][9] with accelerometers using other gait analytical techniques likecorrelation and spectrometry, respectively, to extract step cycles.We discover that those methods can only add ideal situation out of the presence of noise and without common irregular behavior. In gait verification of phones, it proposed a gait verificationmethod for mobile phones which extract the gait features byqualitative analysis.

Smartphone based gait recognition [9] from authentication to imitation. In this proposes another transportable-based gait authentication method using DTW [8] the smartphone based user verification leveraging gait recognition for mobile health care systems. It proposed user verification scheme. Their method uses correlation to extract human walking data and identifies this user's gait pattern. However, common to all or any is that it proposed user verification all gait features are stored and compared that the anti-theft mechanism must detect stealingbehavior in very short time. To solve all problems mentioned before, we design motion pattern authentication method.

III. MOTION PATTERN TECHNIQUES

Our system architecture figure [1] is shown the motion detection component is to blame for discovering that the device is currently experiencing normal motion pattern. The prevailing tools like Dynamic Time Wrapping [9] and K-S Test [7] compare between two motion patterns which can vary time or speed.

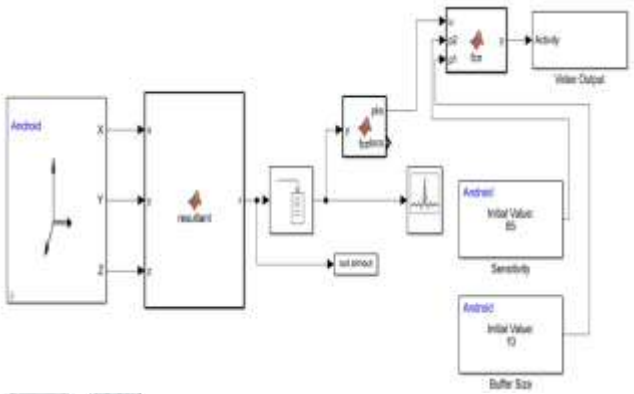

Figure3. Workflow diagram of proposed method

We first define a step cycle as data between two negative peaks accelerometer data that device observers an oversized downwards peak acceleration. We might not simply partition data into cycles supported local minima only, some minima are created accelerometer noise. However, we must select representative step cycle, which can use to divide the remainder of data in to the cycle. The 2 person's data are different of course the step cycles (12 steps) from person A are100 data points long, where the step cycles from person B are 50 data points long. Because the accelerometer collects data with roughly static frequency, this corresponds to 1.3 second for person A's pattern and 0.5 second for person B.

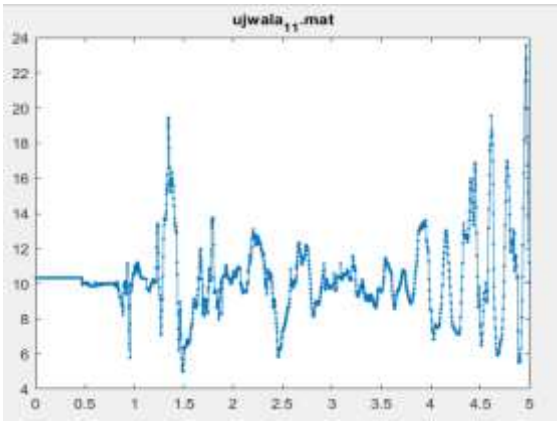

Figure4- Motion State.

The motion pattern techniques to detect the motion of unauthorized movement in any state so it may be rest operation state and actual motion state. However, in contrast to actual state an oversized acceleration is sensed when device is being moved by the user, which is represented by the dash-dot-line in the figure4.Hand movement differs because it is often just the once motion like finding out a tool from the desk or taking a tool out of pocket..

If the user is sitting on the desk or being operated by non- walking and being carried by a walking user respectively. The dash line represents device is sitting on a desk. There is no change of acceleration, which makes it easy to spot. The solid line represents the A onetime motion like studying a tool results in one large acceleration spike, therefore, we start data collection upon detection of acceleration change that's data is collected and if no cycles are detected the info is discarded device is being operated. A non-walking user are going to be standing or sitting so only a little random fluctuation is visible from fandom vibration of the hand.

Existing tools like K-S test and statistical correlation test [7] andLSTM are solutions to check between step cycles, which can vary in time or speed.

Consider figure 4 showing red, green and blue lines shows acceleration data readings in x, y and z direction and their resultant. On the proper side, the extraction of last full wave is defined accuracy between unauthorized user and it changes the directions.

However, there are some methods are to identify unknown step cycles which are comparable with stored in the database. All cycles, Random cycle subset,signature cycle subset.

1. All Cycles-: With n behaviors within the database, m cycles per behavior and k cycles within the unknown behavior, the overall number of comparisons is therefore nmk. This method should have the most effective end inaccuracy, because this provides the broadest view of the information. However, it also requires the biggest number of comparison calculations. Thus, it's not suitable for our quick detection cycles

2. Random Cycle-: We randomly select a subset from these cycles. Then we will only compare these cycle subsets to scale back the comparison time. As an example, we randomly choose q cycles from the extracted steps. And randomly choose p cycles in each behavior. The entire number of comparison is therefore p time's q time n. However, there is a controversy during this method. Some step cycles are most correlated with others, while someare consistent enough to be included within the behavior. In another word, these randomly chosen cycles are not the simplest cycles. The performance of this method is trusted the quantity ofrandomly chosen cycles. If p and q is greater enough, the result is the identical because the first method, but the comparison time is additionally high. If p and q are too small, although the comparison time is little, it is going to end in a coffee accuracy.

3. Signature cycle-: it is the littlest comparable and shortestdetection time. In addition, accuracy is not best for other methods.

Cycle Delimiter-: Our system having Training and testing component which receives accelerometer data detect the motion by thresholding greater than 2g to detect the owner's cycle which identifies the step cycle width. We partition data using step cycle width search by cycle delimiter and find matching methods. we pass or train extracted cycles and classify acquired cycle using LSTM, that's classifier to classify whether the step cycle belongs to the owner or not as mobile device could also beoriented in any direction using MS= √X2 + Y 2 + Z2, where X, Y and Z represent the values read from each axis [7].

Search representative cycle-: using window placement, endpointtest and search point reputation. This finds a step cycle length, which is able to split the acceleration data along the cycle start line.

However, Feature extraction component, which houses pattern techniques for processing the raw accelerated data into motionpattern for database, we identify step cycle width and partition the information using step cycle width use within the database,at the high end we discover local minima and pick start line Pseudo code and extended documentation on algorithm1.

Algorithm 1-:

Input = (*X, Y, Z*) ,*g* = 1 , *wSize* = 200 , *threshold* 1 = 0.8 , *threshold* 2 = 40, where (*X, Y, Z*) represents the values read from each axis,*g* represents the Acceleration of gravity,*wSize* represents the size of sliding windows and threshold *1*and *threshold* 2 represent the cycle comparison

//Remove the directional components
1 for all $i < sizeof(M)$, $i = 1$ do
2 $MS_i = X_i^2 + Y_i^2 + Z_i^2$
//Find all local minima
3 for all $i < sizeof(MS)$ *wSize* , *i* = *wSize* do
4 if $MS(i) < MS(i-1)$ &&$MS(i) < MS(i+1)$ then
5 *Local Minima*(*j*) = *MS*(*i*)
//Find al l downward peaks
6 for all $i < sizeof(local\ Minima)$, $i = 1$, j =1 do
7 if $LocalMinima(i) < g$ then
8 *DPeaks*(*j*)-*LocalMinima*(*i*)9 *j* ++
//Find all deli miters
10 for all $i < sizeof(DPeaks)-1$,$i = 1$, j =2 do
11 *empty*(*delimiters*) //Empty delimiters array
12 for all $k < wSize$, $k = 1$ do
13 *represent cycle*(*k*) = *MS*(*DPeaks*(*i*)+*k*-1)
14 for all $r < sizeof(DPeaks)$ 1 , *r* = 1 do
15 for all $k < wSize$, $k = 1$ do
16 *Windows* (*k*) = *MS*(*DPeaks*(*r*)+*k*-1)
17 *result* = *match*(*represent cycle*, *Windows*)
18 if *result* > *threshold* 1 then
19 *delimiter*(*j*) = *DPeaks*(*r*)20 *j* ++
21 *delimiter*(1) = *DPeaks*(*i*)
22 if *sizeof* (*delimiter*) 1 > *threshold* 2 then
23 *break*
24 for all $i < sizeof(delimiter)$ 1 , *i* = 1 do
25 *stepCycle*(*i*) = *MS*(*delimiter*: *delimiter*)

IV. PROBLEM STATEMENT

Currently available Mobile Anti-theft Mechanisms available are
1. Locating lost phone using GPS
2. Remotely wiping and locking the device
3. Locking the SIM by informing service providers

However, all these mechanisms discovery of the actual theft occurrence. We propose a method wherein we detect ongoing unauthorized movement of a device using its motion pattern.

We use the waveform of the accelerometer provided in all mobile devices to analyze the pattern. We extract normalized waveform of step cycles and match it with the database of the owner's step cycle. Ultimately, we apply LSTM classifier toclassify whether the step cycle belongs to the owner or not.

V. PROPOSED SYSTEM

Many approaches are proposed recently to enable motion pattern identifications. However, get the most effective accuracy, which is reducing the comparisons and shortest detection time. The system is detecting authorized movement of mobile devices and Detect ongoing unauthorized movement of a tool.Basic theory:

- The Accelerometer block has three outputs: X, Y, and Z. Each port outputs a single-precision scalar value.
- LSTM block use the matlab function having input size i.e sequence of data
- Buffer port
- Array plot
- LSTM function1
- Initialize sensitivity(99)
- Buffer value(10)

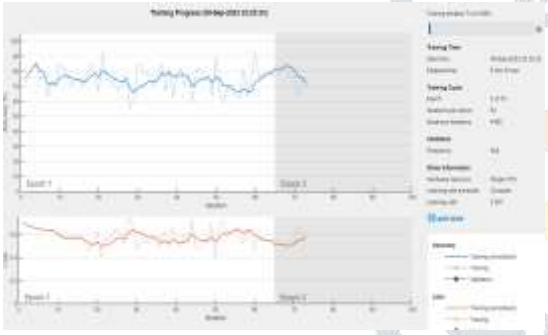

Fig 5. Training Progress of LSTM Analysis

We extract normalized wave type of step cycle and match it with the database of the owner's step cycle. We apply LSTM classifier to classify whether the step cycle belongs to owner or not. However, comparisons between existing tools gave best performance. We reduce the interval to its minimum. we've also compare LSTM step cycles for a behavior for improve accuracy and reduced time interval.

VICOMPARATIVE ANALYSIS

To analyze the performance of different tools we apply long short-term memory into our identification method. The performance of each comparison tool is depending on the systemResults show LSTM (long - term short memory) is best among all.Proposed method has Precision almost similar as Statistical and K-S statistical analysis however the Recall is lower.F1-score is usually more useful than accuracy.

Proposed method is compares step cycles, the database size is reduced from 15500 step cycles to 248 cycles, while 98.4% detection rate is promised.

Hence needs more improvement to compete with state-of-art methods.

Fig 6. Proposed method confusion matrix

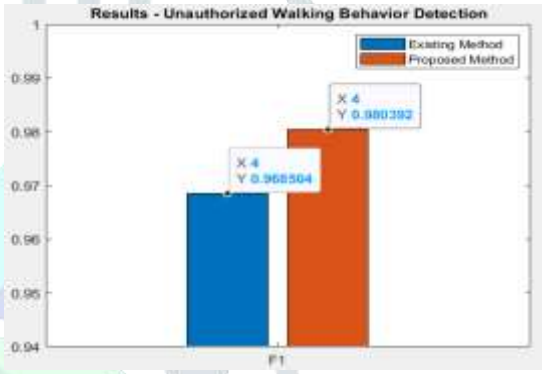

Fig7.F1 score comparision

Fig 8. Precision Comparision

TABLE 1
Comparison Tools Overview

	Statistical Test			K-S Test			LSTM		
	Method 1	Method 2	Method 3	Method1	Method 2	Method 3	Method 1	Method 2	Method 3
Detection	98.1%	95.2%	96.3%	97.5%	97.4%	96.4%	98.5%	95.5%	96.5%
Self-Identification	97.6%	95.4%	97.6%	97.8%	95.6%	97.8%	97.6%	95.4%	97.5%
Comparison times	36000	23000	220	62000	42000	240	66000	22000	220
Detection Time	1×10^{-1}	0.4×10^{-2}	0.5×10^{-4}	1×10^{-1}	0.5×10^{-2}	0.5×10^{-4}	1×10^{-1}	0.6×10^{-2}	0.8×10^{-4}

miss detection rate & detection time. According to ourexperiment, LSTM gave the best performance.

We compared the proposed method with existing Statistical correlation test and K-S test it shows the method 1 compares available. Method 2 applies the situation with 10 cycles randomly chosen behavior. Method 3 uses the result that gets from a training size of 1 signature step cycle and testing size of 10 signature step cycles.

So, the method 1 has better accuracy among all these methods. However, it has longest comparisons and detection time, whichis suitable for the proposed anti-theft identification system. As compared with existing tools, the performance of the proposed method has better in all the three motion matching methods in terms of detection accuracy is better and has a shorter detection time when using method 2and 3.

In our experiment, after two weeks of training, the ownerconverges to 22 behaviors and each behavior comprises 300 stepcycles. We used 10 extracted from unknown data forcomparisons. Thus, the number of comparisons is 66,000 for which we find an accuracy of 98.5%.

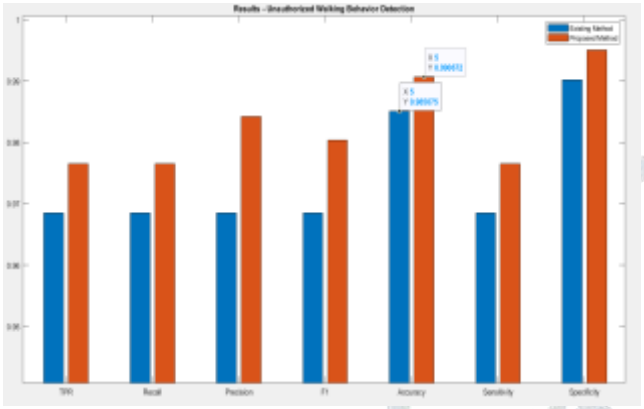

Fig 4: Accuracy Comparison

The main aim of figure 4 &5 shows the performance of method, which is having better accuracy. Thus, the LSTM gives better accuracy than both the methods in distinguishing the accelerometer patterns.

VI. CONCLUSION

We proposed a quick anti-theft system, which will detect authorized movement of mobile devices. We created motion synchronization techniques that may extract step cycles. We also created a representative matching algorithm to check the signature step cycles for a behavior rather than comparing all possible data. This report presents the existing work of anti- theft mechanism only discovered of actual theft occurrence. Here, we are not only discovering the theft but also improve the accuracy and reduced comparisons. This report presents existing work in the field of analyzing walking behavior pattern which has various application time series prediction, Human action recognisation,Text generation.

In proposed a quick anti-theft system, which will detect authorized movement of mobile devices.

This report presents existing work of anti- theft mechanism only discovered of actual theft occurrence. Here we aren't only discovering the theft but also improve the accuracy and reduced comparisons.

The most task of system we created some motion techniques that is LSTM that may extract the step cycles from the accelerometer data to enable comparisons between individuals

This paper provides a faster anti-theft system, which will detect authorized movement of mobile devices. The most task of systemwe created some motion techniques that are LSTM that may extract the step cycles from the accelerometer data to enable comparisons between individuals. Hence, we use waveform of accelerometer provided altogether mobile devices to research the pattern by using long short-term memory classifier to enhance the accuracy and successfully detect an unauthorized movement within interval.

REFERENCES

1. D.Dakun Shen, Ian Markwood, Dan Shen, Yao Liu,"Virtual safe: unauthorized walking Behavior Detection for mobile Devices," in IEEE Transaction on mobilecomputing,vol.18,no.3,pp.688-701,1March2019.
2. M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition: From authentication to imitation. IEEE Transactions on Mobile Computing, PP (99):1–1, 2017.
3. T. Y. Hubel and J. R. Usherwood. Children and adults minimise activated muscle volume by selecting gait parameters that balance gross mechanical power and work demands. Journal of Experimental Biology, 218(18):2830–2839, 2015.
4. ActiveTrak Inc. Gadgettrakios security. http://www.gadgettrak. om/products/iPhone/. [Online; accessed Feb.-2015].
5. E. T. Parker-Pope. The pedometer test: Americans takefewersteps.http://well.blogs.nytimes.com/2010/10
6. /19/ the- pedometer-test-americans-take-fewer\- steps/?r=0. [Online; accessed Mar-2015].
7. Y. Ren, Y. Chen, M. C. Chuah, and J. Yang. Smartphone based user verification leveraging gait recognition for mobile healthcare systems. In 2011 IEEE international Conference on Sensing, Communications and Networking (SECON), pages 149–157, June 2013.
8. P. Olofsson. Probability, Statistics, and Stochastic Processes 2nd edition. John Wiley, 2012.
9. H. M. Thang, V. Q. Viet, N. Dinh Thuc and D. Choi, "Gait identification using accelerometer on mobile phone", Proc. Int. Conf. Control Autom. Inf. Sci., pp. 344-348, Nov. 2012.
10. E. Keogh and C. A. Ratanamahatana, "Exact indexing of dynamic time warping", Knowl. Inf. Syst., vol. 7, no. 3, pp. 358-386, 2005.
11. J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. M. Makela and H. A. Ailisto, "Identifying users of portable devices from gait
12. pattern with accelerometers", Proc. IEEE Int. Conf. Acoustics Speech Signal Process., pp. ii/973-ii/976, Mar. 2005.
13. M. Hazewinkel, Correlation (in Statistics) Encyclopedia of Mathematics, Berlin, Germany: Springer,2002.
14. Y. Ren, Y. Chen, M. C. Chuah, and J. Yang. Smartphone based user verification leveraging gait recognition for mobile healthcare systems. In 2011 IEEE international Conference on Sensing, Communications and Networking (SECON), pages 149–157, June 2013.
15. P. Olofsson. Probability, Statistics, and Stochastic Processes 2nd edition. John Wiley, 2012.
16. H. M. Thang, V. Q. Viet, N. Dinh Thuc and D. Choi, "Gait identification using accelerometer on mobile phone", Proc. Int. Conf. Control Autom. Inf. Sci., pp. 344-348, Nov. 2012.
17. E. Keogh and C. A. Ratanamahatana, "Exact indexing of dynamic time warping", Knowl. Inf. Syst., vol. 7, no. 3, pp. 358-386, 2005.
18. J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. M. Makela and H. A. Ailisto, "Identifying users of portable devices from gait
19. pattern with accelerometers", Proc. IEEE Int. Conf. Acoustics Speech Signal Process., pp. ii/973-ii/976, Mar. 2005.
20. M. Hazewinkel, Correlation (in Statistics) Encyclopedia of Mathematics, Berlin, Germany: Springer,2002.