Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.622 – 634

RESEARCH ARTICLE

USER AUTHENTICATION BASED ON TOUCH DYNAMICS OF PATTERN UNLOCK

HIBA MOHAMMED WAJEEH[1], Sarab M. Hameed[2]

[1,2]Dept. of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

[1] hibamwalshamma@yahoo.com; [2] sarab_majeed@yahoo.com

Abstract*— This paper introduces the proposed User Authentication based on Unlock Pattern Touch Dynamics approach (coined as UA-UPTD) to improve the security of android unlock pattern by adding the behavioral biometrics namely touch dynamics in addition to the shape of unlock pattern. When the user draws the shape on the unlock pattern of android screen, the touch dynamics features namely "timing, finger pressure and area of finger pressure" are extracted. These features are analyzed by the Singular Value Decomposition (SVD) algorithm to reveal basis vector for authorized users. Three patterns (coined as pattern 1, pattern 2 and pattern 3) with different lengths and shapes are used to show the applicability of the proposed UA-UPTD approach. Results show that the pattern's length and complexity of shape on unlock pattern impact on UPTD-UA's performance. Also, the results show the effectiveness of the proposed UA-UPTD approach when compared with Naïve Bayes classifier.

***Keywords*— Android Mobile, Graphical Passwords, Touch Dynamics, Unlock Pattern, User Authentication**

I. INTRODUCTION

Mobile phone is an integral part of people's lives makes it the perfect device to hold the user's digital identity and play a role in the strong authentication system. This stimulates the user to undergo a more secure and scalable authentication for use in a mobile environment [1]. The authentication methods can be widely divided into three main areas [2], token based authentication such as smart cards, passports and physical keys [3], biometric based authentication: is the study of automated methods for uniquely recognizing humans based upon one or more substantial physical or behavioral attributes [4]. There are two types of biometrics: Physical biometrics such as fingerprint and behavioral biometrics, which are the biometric characteristics, related to person's behavioral characteristics such as signature, gait, voice, mouse dynamics, keystroke dynamics and touch dynamics [5]. Knowledge based authentication is based on "Something You Know" to identify a user, such as a Personal Identification Number (PIN), password or pass phrase. Knowledge based techniques are the most extensively used authentication techniques and include both *text based password* and *picture based password (graphical password).* People who use android/windows and other devices that have introduced a lot of applications of security locks that ask a user to open the device every time he/she wants to use it [6]. The graphical passwords are authentication mechanisms where users enter a shared secret as evidence of their identity. It improves the prominence of password and thus eases of use it, while at the same time improving strength against attackers [7]. Touchscreen and mobile devices (*such as Android mobiles*) are graphically orientated and therefore are more suitable for graphical input rather than text input [8]. The android operating system uses a graphical password (*such as unlock pattern*) to unlock touchscreen devices. Unlock pattern authentication mechanism is aim to prevent unauthorized access to android devices [7]. Since the smartphones nowadays are moving from devices used to make call to more personalization

level in term of the captures of highly sensitive information about the owner. There are problems and facts threaten the security of smartphones, these are as follows:

- Users don't tend to use sophisticated patterns to lock the smartphone due to the fact that smartphone is locked and need to be unlocked frequently; this behavior expose the smartphone to attackers who know the pattern.
- Users tend to use their fingers to enter the shape on the unlock pattern rather than using other input devices (i.e., touch screen pens).

Therefore, the aim of this study is to investigate the methodology of building behavioral unlock pattern authentication for android mobiles. The intended investigation is conducted by selecting certain features that characterize the user behavior and to be analyzed by SVD algorithm. The objectives of the methodology are to

- Determine the features through which users' behavior in interacting unlock pattern can be modeled. Features are output measures of sensors integrated within the android mobile.
- Promote current unlock screen beyond the pattern shape to a higher level of personalization; in this level, android mobile should be able to identify unauthorized users even when they know the shape on the unlock pattern.
- Reach out a robust personalization mechanism that can filter authorized users of the unauthorized based on their behaviors in entering the shape on the unlock pattern.

II. RELATED WORK

Several researchers have studied touch dynamics interaction finger on smartphone screen with widely features (Timing, Finger pressure, Area of Finger Pressure, etc.), these are:

In [9], the behavioral manners of users are presented by choosing the finger pressure feature when users interact with a touch screen. The result has shown that the finger pressure gives the discriminative and accurate information more than keystroke dynamics with the k-nearest neighbor (KNN) analytical method.

In [10], the two-factor authentication for the smart device was presented by adding the biometric information to lock patterns that enhance the security. A low Equal Error Rate (EER) of 10.39% was achieved by analyzing the data from 32 individuals using a Random Forest Classifier (RFC) when combining the three different lock patterns.

In [11], the biometric identification method based on Bayesian Non-Parametrics (BNP) was designed. BNP is a pattern recognition method that uses the Least Squares Method (LSM) for intelligent mobile devices by analyzing the user's input patterns, such as a finger's touch duration, pressure level and the touching width of the finger on the touch screen. The testing results show that this method effectively identifies users with near a 100% rate of accuracy.

In [12], the dynamic time warping (DTW) was used to analyze the input data. The results of this study provided possibility to distinguish users and to improve the security of password patterns with near the accuracy rate of 77%, False Rejection Rate (FRR) of 19% and False Acceptance Rate (FAR) of 21%. The results also show that by increasing the password length, positive effects on accuracies might be observed. However, this would come at the costs of decreased usability and memorability.

In [13], KNN classifier and a Gaussian Radial Basis Function (RBF) kernel which is a popular kernel function were used in a Support Vector Machine (SVM) to train the user profiles based on vertical and horizontal strokes. A data acquisition experiment was designed to collect natural touch behavior of 41 subjects. The classification framework has extracted 30 different behavioral features from the raw touch screen interaction data. The results of classifiers have achieved robust authentication results with EER (0% - 4%).

In [14], Naive Bayes classifier for authentication among users using the behavior of touch screen on smartphones was presented. The touch events are collected over 14,000 users who played a quiz game. The extracted features are, mean hold time and pressure. The result of choosing five users randomly is correctly identifying a user with a probability of about 80% after just the touch of ten buttons.

In [15], the user authentication scheme was presented by comparing several of machine learning classifiers. The results show that a Neural Network Classifier (NNC) is suitable for authentication of different users with an Average Error Rate (AER) of about 7.8% for the selected features. Finally, optimized NNC by using Particle Swarm Optimization (PSO) to deal with differences in usage patterns of users. The results show that the AER of the optimized scheme is only about 3%, which are achieved through the analysis of touch behavior of users on the android phone. The results show that the optimized Particle Swarm Optimization-Radial Basis Function Neural Network (PSO-RBFN) classifier significantly reduces the AER down to 2.92%, FAR of 2.5% and FRR of 3.34%.

In [16], the model was established to silently verify the user with high confidence that uses the SVM model to verify whether the current user was legitimate owner of the smartphone based on the behavioral biometrics, including touch behaviors and walking patterns. The accuracy was over 99%, FAR and FRR could be as low as < 1% after only collecting about 10 actions.

III. THE PROPOSED UNLOCK PATTERN USER AUTHENTICATION

The proposed (UA-UPTD) approach enriches the security of unlock pattern by adding behavioral biometrics namely touch dynamics in addition to the shape of unlock pattern. In other words, UA-UPTD approach is a two-factor authentication mechanism based on the shape of the unlock pattern and individuals behavior in drawing the shape on the unlock pattern.

UA-UPTD approach consists of four phases, which are touch dataset collection phase, feature extraction phase, analysis phase and authentication phase. These phases are conducted in two separate devices. The first one is an android mobile in which the android application is installed to collect users' input patterns (i.e. the shapes on the unlock pattern) by presenting unlock pattern screen and reading touch screen sensors while entering the shape on the unlock pattern. The second one is a high computation device (i.e., a PC with multiple core processor) that is used to analyze the collected data.

The Samsung galaxy SII android mobile with targeted android version Jellybean 4.2.2 and Application Programming Interface (API) 18 is used to build the android unlock pattern screen for entering the shape on the unlock pattern. Then, it is delivered through Universal Serial Bus (USB) cable to backend of the system (i.e., the backend here is a high computation device).

A. Touch Dataset Collection Phase

The acquisition of data from the touch screen is an essential part in the touch dynamic system. The touch screen of smartphones is sensitive to finger touch through the user interacts with the smartphone. Essentially, the proposed UA-UPTD approach is a smart authentication system for individuals based on their behaviors in drawing the shape on the unlock pattern.

The unlock pattern screen of the android mobile is designed in android application and is composed of nine visual nodes to:

1. Present the unlock pattern screen.
2. Ask the user to enter his/her pattern.
3. Acquire user input vectors and save them into a local database.
4. Build user profile and register every user in a local database.

Unlock pattern screen grid has itself a potential to personalize users where paths can be detected when moving from cell to cell over the unlock pattern. These paths hold users' behaviors. After registering, users can move on in entering their trials by asking users to re-enter the shape on the unlock pattern many times. Users are asked to not act abnormally and try to keep their behavior as normal as possible.

The android unlock pattern screen is divided into frames that would hold the grid visual nodes and to capture users' event when these visual events touched. Android developing environment provides an excellent notification when screen touched; this by broadcasting touch screen event to system queue, which can be retrieved by the applications by calling context methods. Two datasets are collected; the first dataset is dedicated for authorized users while the second one is for unauthorized users.

1) *Authorized users dataset*: data collected from authorized users is dedicated to reveal the basis vector of them. One important note that needs to be clarified: the smartphone is a device with a high level of personality. This means that the number of users who are to be allowed logging into the system should be as less as possible, but for research purposes the data for many authorized users is collected to prove that there is a separation basis even with increasing the attacking probability. Eight authorized users were chosen according to the following properties:

    A. Age groups (20-64 years old).
    B. Gender (4 female and 4 male).
    C. Different level of experience of using the android mobile.

Dataset of authorized users contains a data of finger pressure, area of finger pressure and time on each node in the unlock pattern of screen and this was conducted over a period of two months. Different lengths and shapes of users' patterns are considered (i.e., three patterns of four, six and seven nodes coined as pattern1, pattern2 and pattern3 respectively) and entries for each authorized user are collected and indexed. The authorized users are asked to enter his/her pattern twenty-five times (i.e. twenty-five patterns). The user draws the shape at different times to avoid an increase in his/her drawing speed while drawing the same path continuously.

2) *Unauthorized users dataset:* data of unauthorized users are collected to verify the revealed basis for authorized users. Twenty-two unauthorized users were eleven female and eleven male, from 20-60 years old, students and employees interacting with designed unlock pattern screen. Unauthorized users are asked to enter his/her pattern for testing. This was conducted over one day.

Users' profiles are kept in a SQLite database created in the storage of the android mobile and context of each user is loaded at the start point of capturing users' pattern. Databases are kept in "ilb" formats and can be transferred to the backend compute for the analysis phase.

B. Feature Extraction Phase

Features extraction from collected data is an important part in UA-UPTD approach. Several features can be extracted for each touch data. However, three touch dynamics features including finger pressure(P), area of finger pressure (A) and timing ($\mathfrak{T}$)are chosen to distinguish user's behavior representation.

Each vector of users' patterns in the database contains the data of finger pressure, area of finger pressure and sequence of time information which represent the time at each node on the unlock pattern screen. The finger pressure (P_i), the area of finger pressure (A_i) and the time (T_i) of node (i) on the unlock pattern screen while the user drawing the shape. The timing $\mathfrak{T}_i$ touch dynamics feature can be extracted from user pattern by equation (1):

$$\mathfrak{T}_i = T_{i+1} - T_i \tag{1}$$

Where

T_i**:** is the time at node (i) on the unlock pattern screen.
T_{i+1}**:** is the time at the next node $(i+1)$ on the unlock pattern screen.

After the timing features of pattern nodes are extracted, the mean of timing is calculated using equation (2):

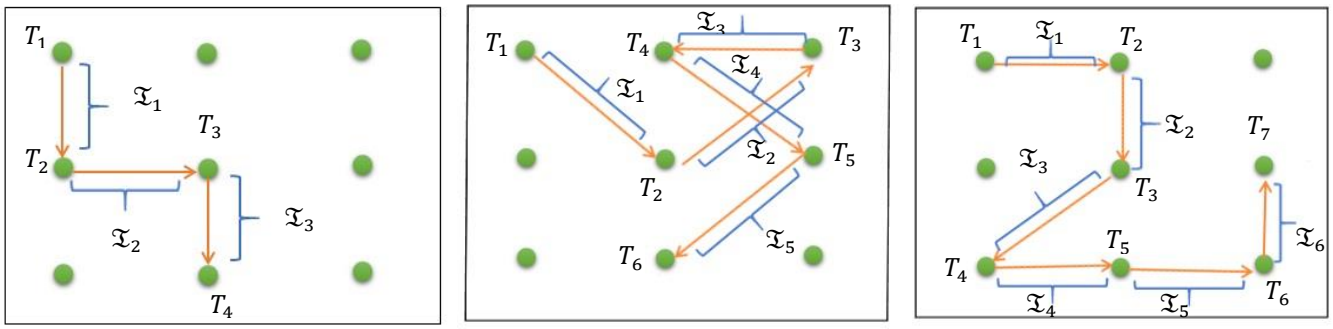
$$M_{\mathfrak{T}} = \frac{\sum_{i=1}^{P_l-1} \mathfrak{T}_i}{P_l-1} \tag{2}$$

The mean of finger pressure and the area of finger pressure (size) features are calculated as in equations (3) and (4) respectively.

$$M_P = \frac{1}{P_l}\sum_{i=1}^{P_l} P_i \tag{3}$$

$$M_A = \frac{1}{P_l}\sum_{i=1}^{P_l} A_i \tag{4}$$

Figure (1) depicts the computation of timing feature for three patterns length (P_l) (i.e. 4, 6 and 7 nodes) while the user drawing the shape.



(a) Timing Feature Representation of Pattern (4) (b) Timing Feature Representation of Pattern (6) (c) Timing Feature Representation of Pattern (7)

Fig.1 Computation of Timing Feature for Three Patterns Length

C. Analysis Phase

The analysis phase of UA-UPTD approach is dedicated to investigate the separation among users based on their behavior in entering the shape on the unlock pattern. The investigation is accomplished by applying SVD algorithm to decompose the matrix of authorized users' vectors (A_U) which is constructed in feature extraction phase. SVD algorithm analyzes touch data to reveal the most effecting vector (i.e., Basis Vector). SVD representation for authorized users is depicted in figure (2).

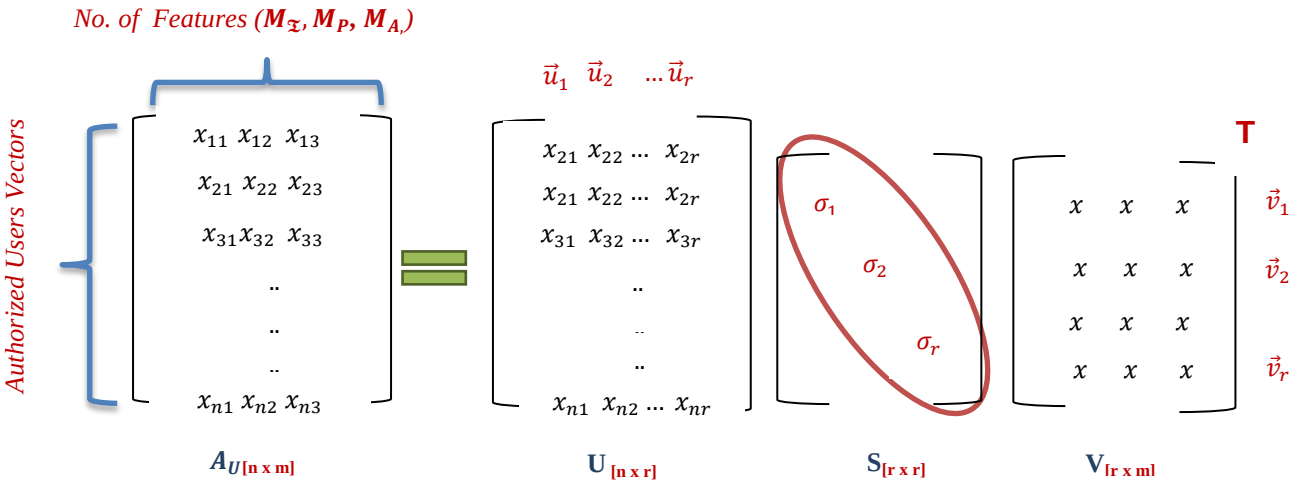


Fig.2 SVD Representation

The variation in the dataset of authorized users is modeled using basis vector. (A_U) is decomposed into its principal components to compute basis vector using the SVD as shown in equation (5)[17].

$$A_{U\,nxm} = U_{nxr}\ S_{rxr}\ V^T{}_{rxm} \tag{5}$$

Where

U, V: are orthogonal matrices

S: is a diagonal matrix which contains the square root of eigenvalues (λ) from U or V matrix.
n: Number of authorized users' vectors
m: Number of features
r : Rank of A_U

In other words, (A_U) can be computed as in equation (6)

$$A_U = \sum_{i=1}^{r} u_i \sigma_i v_i^T \tag{6}$$

Where σ: is the singular values in a matrix S and it is calculated as in equation (7) [17].

$$\sigma = \sqrt{\lambda}. \tag{7}$$

U, V matrices are orthogonal when $U^T U = I, V^T V = I$. This means the result of multiplying any matrix by the transpose of the same matrix is equal the identity matrix. The columns of U are orthonormal eigenvectors of $A_U {A_U}^T$ and the columns of V are orthonormal eigenvectors of ${A_U}^T A_U$. $A_U {A_U}^T$ is computed to obtain U matrix as shown in figure (3).

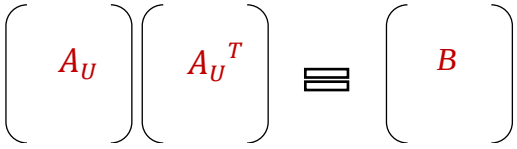


Fig.3 Computation of $A_U {A_U}^T$

Then, the result (i.e. B matrix) is taken to find the eigenvalues and the corresponding eigenvectors as shown in figure (4):

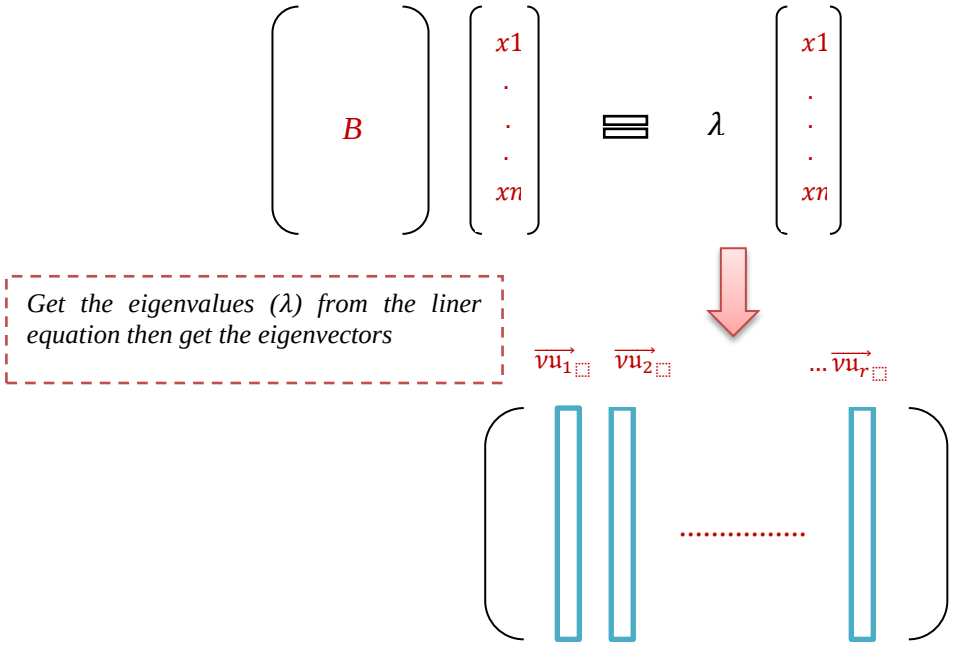


Fig.4 Eigenvalues and Eigenvectors

These eigenvectors are the column vectors in a matrix and ordered by the eigenvector of the largest eigenvalue in the first column and so on until the eigenvector of the smallest eigenvalue in the last column. This matrix is converted to orthogonal matrix (i.e. convert the set of vectors ($\overrightarrow{vu_1}, \dots, \overrightarrow{vu_r}$) to a set of orthonormal vectors), by normalizing $\overrightarrow{vu_1}$ to get the first vector of U matrix, as formulated in equation (8) [17].

$$\vec{u}_1 = \frac{\overrightarrow{vu_1}}{|\overrightarrow{vu_1}|} \tag{8}$$

Then, all vectors of U matrix are computed according to equations (9) and (10) respectively [17].

$$\vec{w}_{i+1} = \overrightarrow{vu}_{i+1} - \sum_{i=1}^{r-1} \vec{u}_i \cdot \overrightarrow{vu}_{i+1} \times \vec{u}_i \tag{9}$$

$$\vec{u}_{i+1} = \frac{\vec{w}_{i+1}}{|w_{i+1}|} \tag{10}$$

The V matrix calculation is similar to U matrix but V matrix depends on ${A_U}^T A_U$ calculation. The first raw vector of V matrix ($\vec{v}_1$) is representing the maximum variance among the users' vectors. The vector that causes maximum variance is called Basis Vector **($\mathfrak{B}v$)**, which represented in equation (11):

$$\mathfrak{B}v = \vec{v}_1 \times S \times U \tag{11}$$

Where

$\vec{v}_1$: The first raw vector of V matrix

D. Authentication Phase

This phase is dedicated for testing and evaluating UA-UPTD approach. Phase three (i.e. analysis phase) has ended with reaching out the basis vector for all authorized users. Thus, in this phase, this basis vector is validated in terms of evaluating its capability to discriminate authorized of the unauthorized users.

In this phase, the user is asked to enter his/her pattern in order to prove his/her identity for the android mobile. Then, the input vector of users trying to login the android mobile ($\overrightarrow{U_L}$) is normalized by calculatingthe relative weight of each feature to

the total length of the vector. Each feature in terms of its participation in the capacity of the vector, there is a common mathematical technique to have the values of vectors' features relative to each other's and to the total capacity of the vector.

The normalization process is crucial due to the relative weighting of users' input vectors. SVD cannot provide much information about the users' behaviors without normalizing input patterns where covariance matrix reached out by the SVD would provide misleading information with absolute values due to the fact that SVD measures linear independents based on measuring the effects of changing values for the matrix.

Each user input vector is tested with the basis vector of users to know if the input vector is authorized or unauthorized user. The testing is done by using the dot product, which is the multiplication of vectors (i.e. multiplying each component in first vector by the component in second vector in the same position and adding them all together to get the scalar value), as in equation (12)

$$U_{\mathfrak{B}} = \sum_{i=1}^{m} U_{L_i} \mathfrak{B} v_i \tag{12}$$

Where

The similarity measure will be calculated as the projection in a space of the new pattern vector and the directional vector of V matrix. The similarity between two vectors is measured as in equation (13).

$$\theta = \cos^{-1} \frac{U_{\mathfrak{B}}}{|U_L||\mathfrak{B}v|} \tag{13}$$

If the angle between two vectors is less than or equal to the threshold then the system allowed user to enter into android mobile as a legal user. If the angle is more than the threshold then the system rejects the user to enter into android mobile and is considered as unauthorized user. This is formulated as in equations (14) and (15) respectively.

$$\theta \leq t \rightarrow U_L \equiv authorized\ User \tag{14}$$

$$\theta > t \rightarrow U_L \equiv Unauthorized\ User \tag{15}$$

Where

t : Threshold value for expected separation line.

IV. RESULTS AND DISCUSSION

This section is dedicated to evaluate the capability of the proposed UA-UPTD approach to discriminate between authorized and unauthorized users.

A. Impact Features within Different Patterns

This study is dedicated to investigate the separation among users according to their behavior in entering the shape on the unlock pattern. For each user, a vector of three features is constructed and stored in a database. The basis vector is a characterization pattern for the authorized users. The basis vector for pattern1 is different from that of pattern 2. This due to the difference in behavior for the same user in entering the shape on the unlock pattern. This is also the same for pattern 3. Table (1) demonstrates the basis vector for the three patterns.

TABLE 1
Basis Vector for Authorized User

Pattern	Basis Vector		
	Timing	Pressure	Area of Pressure
1	1.264	0.244	1.014
2	3.252	7.099	8.187
3	4.256	13.213	8.854

Each user has a behavior in drawing the shape on the unlock pattern screen that distinguish him/her from the other. However, the probability of recognizing specific user based on his/her behavior in entering the shape on the unlock pattern becomes unique when his/her behavior is stable in a different circumstances. The three features *(timing, finger pressure* and *area of finger pressure*) are weighted according to its variance along the data collected with specific pattern length.

In pattern 1, the timing feature has highest impact than the area of pressure and pressure features because it has short and easy pattern's shape. However, in pattern 2 and pattern 3, the pressure and the area of pressure features have the highest impact than the timing because the pattern 2 and 3 have longer length and more complex of pattern shape than pattern 1

B. Impact of Threshold on UA-UPTD's Performance

Intuitively, increasing or decreasing threshold value (t) (i.e. separation line among all users) affects UA-UPTD's performance. In the authentication phase, all users are examined to validate their authorization status for each pattern. The authorization is done when the angle between the user input vector and basis vector is less than that threshold. The accuracy of UA-UPTD approach is examined with different threshold values to get the acceptable accuracy for authorized users that must be balanced with unauthorized user's accuracy over the same threshold values. In other words, we want to balance between the required level of security (FAR) and usability (FRR).

To reveal the best threshold value (i.e. find out the best threshold overall users), different values are taken by fine tuning the threshold value on both sides. The validating is done for the three patterns and it is clear that each pattern has different threshold values; this is due to the different behavior pattern for the same users and the different basis revealed for their data. Table (2) presents the resultant test values for all users with different threshold values. The best accuracy of authorized users is (86) and the best accuracy of unauthorized users is (81.8) over the threshold value of (34.70) (i.e., that threshold is the best threshold value that gives the best overall accuracy).

TABLE 2
Accuracy of Participants in Pattern 1

t	$Acc\%$	
	Authorized Users	**Unauthorized Users**
34.699	77.5	81.8
34.70	86	81.8
34.701	91.5	63.6
34.702	93	54.5

Table (3) clarifies the accuracy of UA-UPTD approach for all participants in pattern 2 with different threshold values. The best accuracy of authorized users is (92) and the best accuracy of unauthorized users is (81.8) over the threshold value of (14.964) (i.e., that threshold is the best threshold value that gives the best overall accuracy).

TABLE 3
Accuracy of Participants in Pattern 2

t	$Acc\%$	
	Authorized Users	**Unauthorized Users**
14.960	78	90
14.961	83.5	86.3
14.962	85.5	81.8
14.963	88	81.8
14.964	92	81.8
14.965	94	68.1

Table (4) presents the accuracy result for all users with different threshold values. The best accuracy of authorized users is (93) and the best accuracy of unauthorized users is (86.3) over the threshold value of (13.731) (i.e., that threshold is the best threshold value that gives the best overall accuracy).

TABLE 4
Accuracy of Participants in Pattern 3

t	$Acc\%$	
	Authorized Users	**Unauthorized Users**
13.729	89	95
13.730	90	95
13.731	93	86.3
13.732	94	81.8
13.733	97.5	81.8

Figure (5) depicts the accuracies of all authorized users in three patterns. The results indicate that the proposed UA-UPDT approach is capable of recognizing authorized users in pattern 2 and 3 with the higher accuracies than pattern 1 up to 100%.

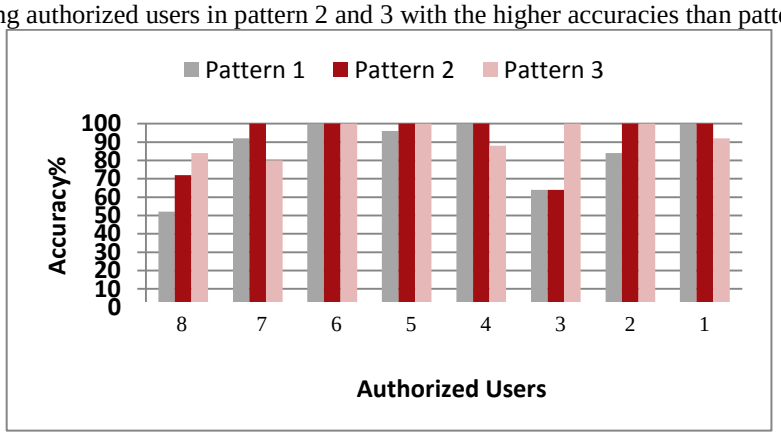


Fig.5 Accuracies of Authorized Users

Table (5) clarifies validating UA-UPTD approach capabilities in detecting authorized users and unauthorized users in terms of FAR, FRR and overall accuracy. Figures (6), (7) and (8) depict FAR, FRR and the overall accuracy of UA-UPTD approach in three patterns.

TABLE 5
Measurement of UA-UPTD's Performance

Pattern	FAR	FRR	**Overall** $Acc\%$
1	0.18	0.135	85.5
2	0.18	0.08	90.9
3	0.136	0.07	92.3

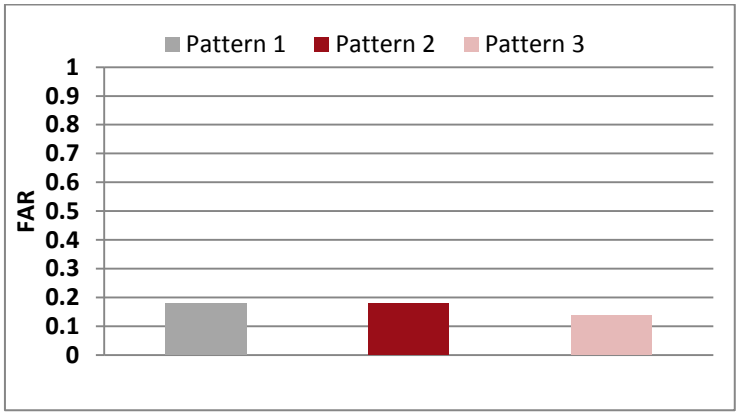


Fig.6 FAR of UA-UPTD approach in three patterns

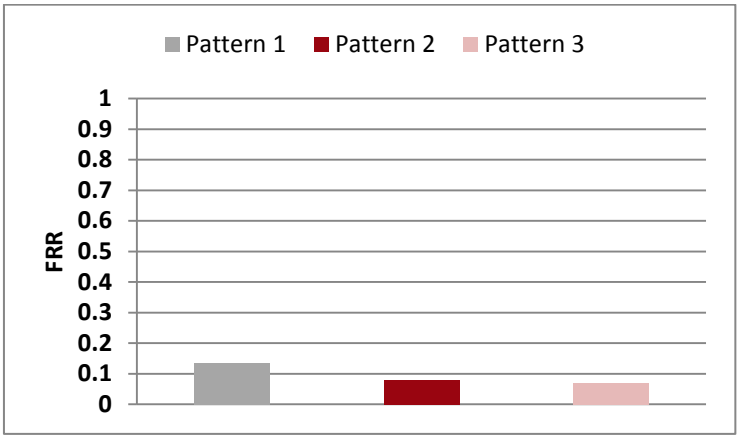


Fig.7 FRR of UA-UPTD Approach in three patterns

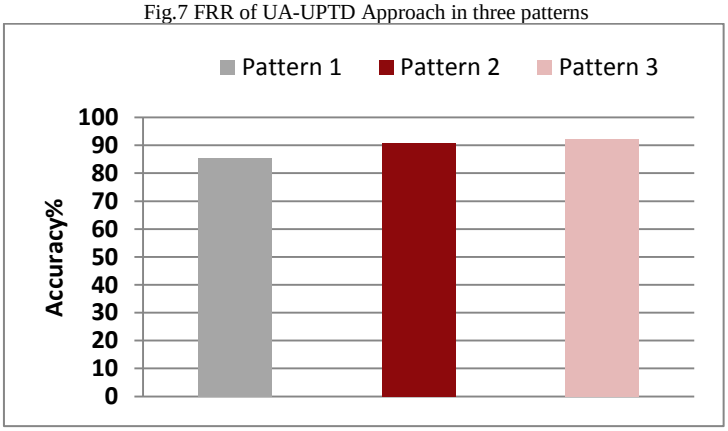


Fig.8 Overall Accuracy of UA-UPTD Approach in three patterns

The results reveal that UA-UPTD approach with pattern 3 provides high usability (low FRR) and more security (low FAR) than pattern 2 and pattern 1. This is due to the fact that pattern 1 has short and easy pattern's shape therefore it gives less discrimination for users as compared to patterns 2 and 3. Moreover, pattern2 has amid length and shape so it gives less discrimination for users compared to pattern 3. In other words, pattern 3 has the longest length and the pattern shape is more complex as compared to patterns 1 and 2. This means that the shape and length of pattern affect the performance of UA-UPTD approach.

C. Impact of Exposing of User's Pattern

UA-UPTD approach is a two factors authentication. This means that the security of UA-UPTD approach depends on the shape of the unlock pattern and users behaviors in drawing the unlock pattern. In this study, two scenarios are considered.

In first scenario, the unauthorized user exposes the shape of unlock pattern, while in the second, the unauthorized user does not know the shape of unlock pattern (i.e. only authorized users know it). The first scenario discusses the acceptance of entrance to the mobile system when the unauthorized user knows the shape on the unlock patterns 1, 2, and 3. The probability of acceptance the unauthorized user that knows pattern 1, 2 and 3 is given by the value of FARas shown in figure (7.a) (i.e. FAR for pattern 1 is $FAR_1 = 0.18$, FAR for pattern 2 is $FAR_2 = 0.18$ and FAR for pattern 3 is $FAR_3 = 0.13$)

In the second scenario, only the authorized users know the shape of the unlock patterns (i.e. pattern1, pattern 2 and pattern 3). Therefore, the unauthorized user has a little chance to a success full entrance to the mobile system. Since the android unlock pattern has nine visual nodes, then the combinations of pattern 1, 2 and 3 are 1624, 26016and 72912 respectively. The probability of the unauthorized user to enter the correct shape of unlock pattern 1, 2, and 3on the first trail is computed as follows:

$$P\ (Pattern\ 1) = \frac{1}{1624} = 0.000616$$

$$P(Pattern\ 2) = \frac{1}{26016} = 0.000038$$

$$P\ (Pattern\ 3) = \frac{1}{72912} = 0.000013$$

Thus, the probability of occurrence of these two independent events is computed for three patterns according to equation (16).

$$P\ (Pattern\ \text{ and } FAR) = P(pattern) \times P(FAR) \quad (16)$$

The obtained results from equation (16) are as follows:

$$P\ (Pattern\ 1\ \text{and} FAR_1) = 0.00011$$
$$P(Pattern\ 2\ \text{and} FAR_2) = 0.0000069$$
$$P\ (Pattern\ 3\ \text{and} FAR_3) = 0.0000018$$

The results show that UA-UPTD approach enhances the security of unlock patterns in which the probability of an unauthorized user with an unknown pattern would be allowed to pass in the mobile system is 0.00011, 0.0000069 and 0.0000018 for pattern 1, 2, and 3 respectively. This comes from the fact that UA-UPTD approach considers two factors to authenticate a user, namely the shape of the unlock pattern and user behaviors in drawing the unlock pattern.

D. UA-UPTD Approach against Naïve Bayes

A comparison with some other related work should be performed to evaluate the performance of UA-UPTD approach. In this study, the proposed of [15] is used for comparison. The sipina package [18], which is a free program for machine learning classifiers, is utilized to use the Naïve Bayes classifier. The collected data of authorized and unauthorized users for this research is separated into two parts (training set and testing set). The training set is used in the training phase of Naïve Bayes and it consists of 15 trials for each authorized user (i.e., fifteen trials for eight authorized users) and 11 unauthorized users. While, the testing set is used to evaluate the performance of Naïve Bayes classifier, which contain the remaining of 10 trials for each authorized user (i.e., ten trails for eight authorized users) and 11 unauthorized users. Table (6) clarifies the performance of Naïve Bayes classifier in terms of FAR, FRR and accuracy.

TABLE 6
Naïve Bayes Performance Evaluation

Pattern	FAR	FRR	$Acc\%$
1	0.54	0	93.4
2	0.27	0.31	69.2
3	0.54	0.31	65.9

Figures (9), (10) and (11) depict the performance comparison between UA-UPTD approach and Naïve Bayes classifier in terms of FAR, FRR and accuracy respectively.

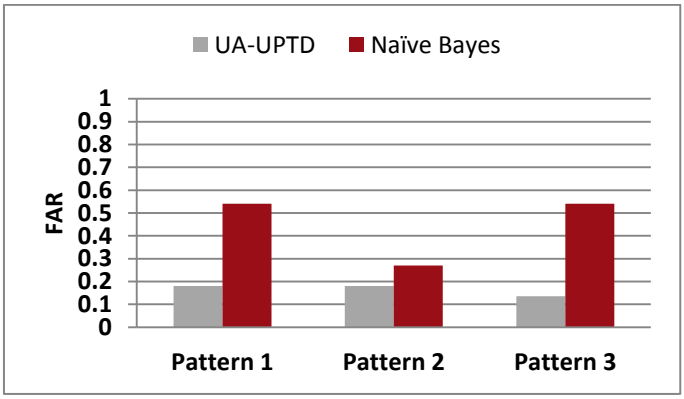


Fig.9 FAR of UA-UPTD and Naïve Bayes

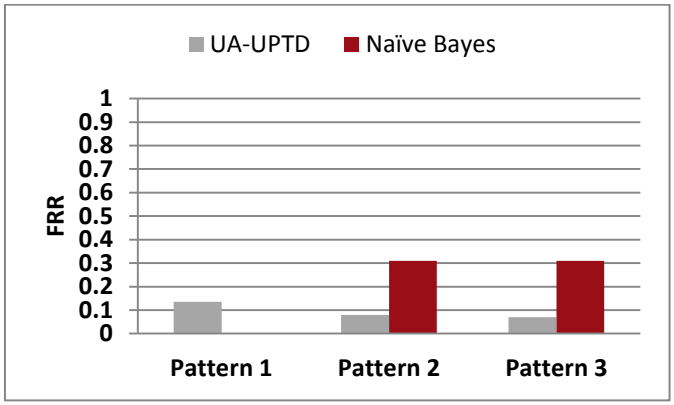


Fig.10 FRR of UA-UPTD and Naïve Bayes

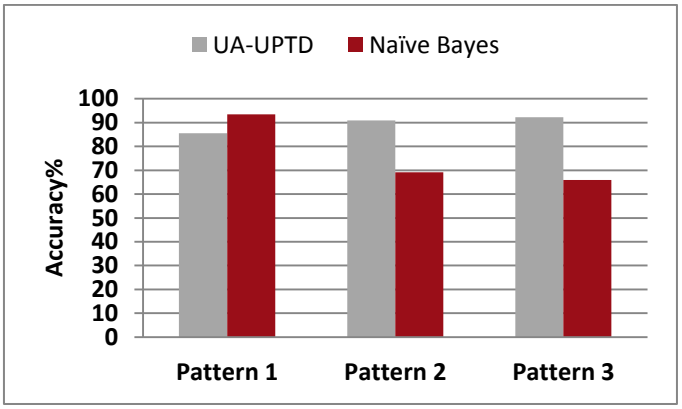


Fig.11 Accuracy of UA-UPTD and Naïve Bayes

The result illustrates that the performance of UA-UPTD approach is better than Naïve Bayes performance in all terms for all patterns except in pattern 1 in which the accuracy and FRR of Naïve Bayes classifier are better than UA-UPTD approach. These results reflect the ability of Naïve Bayes classifier to be bias towards maximizing accuracy and minimizing FRR at the expense of FAR in pattern1.

Moreover, one can observe that FAR of UA-UPTD approach is better than Naïve Bayes classifier for all patterns. This is due to the existence of balance between the required level of security and usability in UA-UPTD approach and the absence of this balance in Naïve Bayes classifier. In general, UA-UPTD approach results are the best when compared to the Naïve Bayes classifier.

V. CONCLUSIONS

The investigation of the results obtained from the proposed UA-UPTD approach has led to that the SVD is a candidate algorithm to reveal hidden relationships among input features; these relationships introduce new dimensions for correlating users to their input vectors. The results confirm that the three extracted features (timing, finger pressure and area of finger pressure) are candidate to discriminate between authorized and unauthorized users. Also, each user has a basis vector of three features, which characterizes the pattern of the authorized users. That features give discriminated values in three patterns. The results show that the Increasing or decreasing threshold value affects UA-UPTD's performance. Each pattern has different threshold values; this is due to the different behavior pattern for the same users and the different basis revealed for their data. The results show that the pattern length and complexity of pattern shapes have an impact of the ability of UA-UPTD approach in discriminate among users. The results of accuracies of the three patterns indicate that the proposed UA-UPDT approach is able to recognize the user in pattern 2 and 3 better than the approach of pattern 1. This study has shown that the UA-UPDT accuracy with pattern1, pattern2 and pattern 3 is 85.5%, 90.9% and 92.3% respectively.UA-UPTD approach with pattern 3 provides high usability and more security than pattern 2 and pattern 1. This is indicated by metrics FAR and FRR. UA-UPTD FAR with pattern 1, pattern 2 and pattern 3 is 0.18, 0.18 and 0.136 respectively and UA-UPTD FRR is 0.135, 0.08 and 0.07 for

pattern 1, pattern 2 and pattern 3 respectively. The results show that the UA-UPTD approach enhances the security of unlock pattern in which the probability that an unauthorized user with an unknown pattern enters in the android mobile is $0.00011, 0.0000069$ and 0.0000018 for pattern 1, pattern 2 and pattern 3 respectively. The result of comparison of the UA-UPTD approach with Naïve Bayes classifier shows that the UA-UPTD approach is better than Naïve Bayes classifier.

REFERENCES

[1] A. Andrade, "Strong Mobile Authentication in Single Sign-On System," M.Sc. Thesis, Aalto University, Department of Computer Science and Engineering, Espoo, Finland, 2011.

[2] P.P. Ray, "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices," *Journal of Information Engineering and Applications*, Vol. 2, No. 2, pp. 1-11, 2012.

[3] H.Z.U. Khan, "Comparative Study of Authentication Techniques," *International Journal of Video & Image Processing and Network Security - International Journals of Engineering & Sciences (IJVIPNS-IJENS)*, Vol. 10, No. 4, pp. 9-13, 2010.

[4] K.l. Patil and J.A. Shimpi, "Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, Vol. 2, No. 4, pp. 155-157, 2013.

[5] M.O. Derawi, "Smartphones and Biometrics - Gait and Activity Recognition," Ph.D. Thesis, Gjøvik University College, Department of Computer Science and Media Technology, Gjøvik, Norway, 2012.

[6] B. Farooq, U.F. Ansari, and N.Z. Bawany, "Usability and Comparisons of Passwords," *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, Vol. 3, PP. 94-101, 2013.

[7] R. Biddle, S. Chiasson, and P.C.V. Oorschot, "Graphical Passwords: Learning From The First Twelve Years," *ACM Computing Surveys (CSUR)*, Vol. 44, No. 4, pp. 1-41, 2012.

[8] S. Shahzada, "Touch Interaction for User Authentication," M.Sc. Thesis, Carleton University, Human-Computer Interaction, Ottawa, Canada, 2014.

[9] H. Saevanee, P. Bhatarakosol, H. Saevanee, and P. Bhatarakosol, "User Authentication using Combination of Behavioral Biometrics over the Touchpad acting like Touch screen of Mobile Device," in *Proc. ICCEE*, 2008, pp.82-86.

[10] J. Angulo and E. Wästlund, "Exploring Touch-screen Biometrics for User Identification on Smart Phones," *IFIP Advances in Information and Communication Technology*, Vol. 375, pp. 130-143, 2012.

[11] H. Seo, E. Kim, and H.K. Kim, "A Novel Biometric Identification Based on a User's Input Pattern Analysis for Intelligent Mobile Devices," *International Journal of Advanced Robotic Systems (InTech)*, Vol. 9, Special Issue, pp. 1-10, 2012.

[12] A.D. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know it's you! Implicit Authentication Based on Touch Screen," in Proc. SIGCHI, 2012, pp. 987-996.

[13] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song "Touchalytics: on the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 1, pp. 136-148, 2012.

[14] S.M. Kolly, R. Wattenhofer, and S. Welten, "A Personal Touch-Recognizing Users Based on Touch Screen Behavior," in Proc. IWSAMP, 2012, pp. 1-5.

[15] Y. Meng, D.S. Wong, R. Schlegel, and L.F. Kwok, "Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones," *Information Security and Cryptology Lecture Notes in Computer Science*, Vol. 7763, pp. 331-350, 2013.

[16] C. Bo, L. Zhang, and X.Y. Li, "SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics," in Proc. AICMCN, 2013, pp 187-190.

[17] O.N. Osmanli, "A singular Value Decomposition Approach for Recommendation Systems," M.Sc. Thesis, Middle East Technical University, Computer Engineering Department, Ankara, Turkey, 2010.

[18] (2015) SIPINA website. Available: http://eric.univ-lyon2.fr/

