ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Mobile Waving Android Based System for Girls Safety

A.Joshi #[1], M.Pravesha Ramesh#[2], Ramya.R #[3], A.Sherly #[4]

Professor and Head of The Department , Dept. of IT, Panimalar Institute of Technology, Tamil Nadu, Chennai, India[1]

B. Tech Student, Dept. of IT, Panimalar Institute of Technology, Chennai, Tamil Nadu, India[2]

B. Tech Student, Dept. of IT, Panimalar Institute of Technology, Chennai, Tamil Nadu, India[3]

B. Tech Student, Dept. of IT, Panimalar Institute of Technology, Tamil Nadu, Chennai, India[4]

ABSTRACT: The Internet Of Things that refers to the ever growing network of physical objects that feature an IPaddress for communication and internet connectivity that occurs in between these systems and objects and other Internet devices. The existing approaches does not support smart phones well due to the issues such as high cost ,efficiency of security , and poor usability. In the proposed system Android app is developed in which user's Hand Waving Pattern repeat& record the above actions for many times until the Application registers user's pattern. Here we use SVM algorithm for identifying the user. Modification of the project is that the waving pattern can be used for Girls Security. If any inappropriate situations happen to girls, they can send a notification to the Guardian and to the Authorities through the Hand Waving pattern. Once the pattern is recognized then automatically the Global Positioning System is triggered and location details are sent to the Guardian and Police authorities as URL Links along with Voice clip that is recorded and sent as a SMS Link.

KEYWORDS: Authentication, Smart phone,Ipaddress,Security.

I. INTRODUCTION

Smart phones are no longer the devices that are not only used to text or call others. They became prevalent with more functions. As pocket PCs, smart phones are used to deal with difficult tasks such as receiving /sending e-mails, mobile payment etc. Screen lockers are the fundamental utilities for smart phones for preventing the devices from inappropriate use. (1)Slide-to-Unlock. (2) PIN, the most commonly used method in traditional digital device, is also adopted on smart phones for unlocking them. (3) The user can have a pre-defined graphical password, like connecting at least three circles shown in the screen. The biometric measures are grouped into two categories: behavior biometrics and physiological biometrics .Physiological biometrics uses the physiological features of human beings for identifying the user, including Voice, fingerprints, recognition of face, ear and so on. The behavior biometrics is the another classification of biometric techniques, which identifies the user based on their behavioral features, such as gesture, typing, mouse movement, tapping or stepping.. (More discussions related with these works are shown in Section 5).In this paper, we realize that different users wave their smart phones in different ways. For example, some people wave their smart phones drastically while some others wave their phones in a gentle manner. This makes the frequency and waving speed totally different among users. Also, the way of wrist twisting and waving range are also different between users. These patterns are derived from user's habits and physical features. For example, the users with longer arms wave wider and faster than those with shorter arms. Some persons are habituated to end their waving action with a twisting of wrist while some others like to start with a wrist twisting. Moreover, the gender, occupation and age also heavily affect the feature of waving action. On the other hand, we also observe that when a user waves his smart phone, he also shakes it in a similar way. This is because, without any intentional changes, a specific person tends to follow his habits. Based on the above observations, we use a hand waving biometric approach, called Open Sesame, to unlock the smart phones. When comparing with the existing methods, there are two main advantages of our approach.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

II. LITERATURE SURVEY

UNLOCKING SMART PHONES THROUGH HANDWAVING BIOMETRICS :
Screen locking/unlocking is important for modern smart phones to avoid the unintentional operations and secure the personal stuff. The existing unlocking approaches can be categorized into four groups: motion, password, pattern, and fingerprint. We collect 200 users' hand waving actions with their smart phones. The waving pattern of a person is kind of unique. In this paper, we propose Open Sesame, which employs the users' waving patterns for locking/unlocking

A LARGE SCALE STUDY OF WEB PASSWORD HABBITS :
A client component on users' machines recorded a variety of password strength, usage and frequency metrics. This allows us to measure or estimate such quantities as the average number of passwords and average number of accounts each user has, how many passwords she types per day ect. We get extremely detailed data on password strength, the types and lengths of passwords chosen, and how they vary by site.

SECURING MOBILE CLOUDE USING FINGER PRINT AUTHENTICATION:
The combination of cloud computing and mobile computing introduces mobile cloud computing. Which also present new issues of security threats such as unauthorized access to resources exist in mobile cloud. Protecting mobile cloud computing from illegitimate access becomes an important concern to mobile users. This paper proposes and implements a new user authentication mechanism of mobile cloud computing using fingerprint recognition system. Fingerprint images of mobile users can be captured and processed using mobile phone camera to access mobile cloud computing .

III. WAVING CHARACTERIZATION

In this section, we present the sensor which is used for real trace collection, wave sensing and analyzing the data.

A. WAVING SENSING:

For brief characterization, selecting appropriate sensors and user's waving actions is necessary. Due to the tremendous growth of MEMS technology, there are many sensors equipped in our smart phones today, such as microphone, camera, accelerometer, proximity sensor magnetic sensor and gyroscope etc. In this system, the selected sensor should be able to detect the hand waving pattern. In addition, it should be stable, energy-efficient, cheap, and compatible for a wide deployment in many kinds of smart phones. Obviously, the first three sensors cannot get the phone's motion pattern. The gyroscope sensor is very attractive because it is designed and developed for maintaining or measuring purposes, based on the principles of angular momentum .But, this kind of sensors are not the standard equipment in most of the smart phones due to its high price. The magnetic sensor is used for compass, but it can to be interfered by the mental objects under specific environments, like subway or inside the car.

B. DATA COLLECTION :

For detecting the uniqueness of hand waving, we collect the waving action information from 200 different smart phone users. Each specific user is asked to shake their smart phones for more than 10 seconds and repeat the same for three times. Note that there are no special restrictions on user's waving actions. He/she can shake the smart phone arbitrarily in each trial. Main focus is at perception of the hand waving action and not the motion pattern. the data collection is processed in two sampling modes: fast and normal modes . In fast mode, accelerometer transitive every 10 to 20 milliseconds, which corresponds to the acceleration value change rate. Trails are collected for 100 users easily using this mode. In the normal mode, the transitive interval YANG ET AL: UNLOCKING SMART PHONE THROUGH HANDWAVIG BIOMETRICS 1045 is 200 milliseconds. 100 users trails are sampled using normal sampling mode of accelerometer some data are lost, but this conserves energy. We shall compare these two modes in the appraising selection. The raw waving action is recorded as the sequence of tuples which is represented as (x_t,y_t,z_t) , where x, y, z which donates the accelerations along the x-axis, y-axis and z-axis respectively, and t which specifies the time. As a result, we collect totally 600 files containing 389; 373 raw tuples.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

C. WAVING MEASUREMENT:

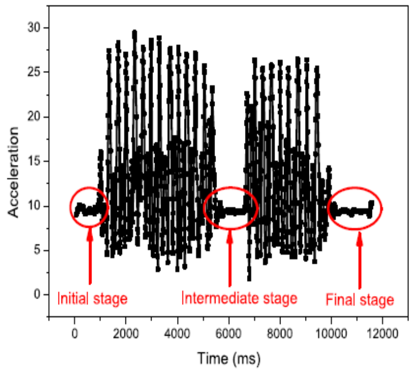
On purpose, we shall define the waving function for the measurement of the global geometric properties of the waving shapes, which is formally specified as the : f=S(A)where A={(xt0,yt0,zt0),(xt1,yt1,zt1),…(xtn,ytn,ztn)}.A is a set of raw waving tuples are collected during t0 and tn.The wave function considers A as input and outputs to a feature of vector f. A perfect waving function should enhance the following properties i.e., Efficiency. Since shape function shall be performed in the smart phone, as it should be simple to enable fast and efficient functionality Invariance. In recent trends, the smart phones are working in the mobile platforms. The waving function should be irresponsible to the position and the direction of variation of smart phones robustness. Even though the waving data generated by one person is the same, there always exist many noises and the sampling time is variable. The waving function should always be robust to noise, blur, cracks, and dust in the waving.

IV. OPEN SESAME

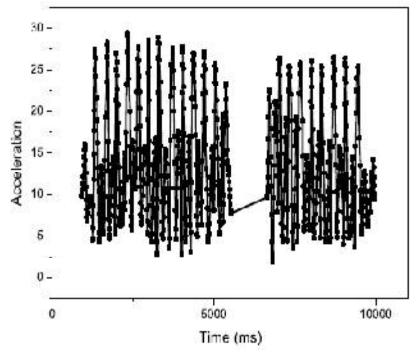
In this part it outlines about the present unlocking method for smart phone devices called Open Sesame.

A. OVERVIEW:

Open Sesame involves of five key components: sensing, filter, fetcher, classifier, and matcher Sensing: This unique device has a straightforward use to record the user's hand waving pattern data. Filter: In this device, we conclude that there exist some of the silent periods when there is no waving or very low level sensing data is detected and fetched. For better enhancements, we enable the use of filter components to wipe out the silent period. Fetcher: The filtered raw tuple is inserted into fetcher components in which four waving functions are implemented to fetch the wave features Classifier: The support vector machine (svm) is employed in our system for discriminating the authorized users and unauthorized users Matcher: In final component, the deduced feature is used in determining whether patterns are matched the predefined one.



(a) Before filtering



(b) After filtering

Fig. 4. Comparing the features before and after filtering.

Fig. 4a explains12 seconds of data acquiring. We are able to find three explicit periods in which the wave values are too low to get detected. We can define such a period as silent periods. These silent periods exist at the beginning stage very before the person shakes his or her smart device, or in the ending stage after the waving is done. These periods may be noticed in the intermediate stage where an unexpected member pause occurs. This silent period will affect the accuracy of Open Sesame module; we should filter those data acquired during these periods. The Ith raw tuple with the composed acceleration value Ai is transceiver out if the equation is satisfied.

$$\sum_{x=i-b}^{i+b}\left(A_x - \sum_{y=i-b}^{i+b}\frac{A_y}{2b+1}\right)^2 < \alpha,$$

Where B is the tolerant static period, which represents the amount of acceleration points to be used to determine the stability feature of the acceleration point. Where A is the threshold which filters the silent point. Based on the algorithm

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

framed, the filtered data is illustrated in the Fig. 4b.

V. IMPLEMENTATION

In this part, we contain the overview of the implementations of Open- Sesame and to evaluate its performance characteristics.

A. IMPLIMENTATION APP:

The Open Sesame has the implementations in the Android-based smart phones. The versions of the Android system are 2.3.3. This app is implemented based on Android-SDK using Java SE. Fig. 5 modularizes the GUI of the application. Containing this app, the user's hand waving pattern is collected and analyzed by the smart phones. Specifically, those interfaces which are shown in Figs. 5b and 5c are used to notify whether the unlocking pattern is successful or not. We hereby use the open source library tool, LIBSVM [16], to classify the SVM. LIBSVM is an integrated software tool for the support vector classifications. The version we used is LIBSVM-3.12. In our experiment, we used the default kernel function (Gaussian Radial Basis Function) and found the best setting of parameters Cost and g for the kernel function via the cross-validation when generating the training model.

B. METRICS:

We evaluate Open Sesame in terms of the authentication accuracy. The authentication accuracy is measured via the following metrics: False negative rate. The probability that an authorized user is treated as an unauthorized user. This rate is indeed the ratio of the number of incorrect authentications conducted by an authorized user to the number of his authentication attempts. True positive rate (TPR). The probability that an authorized user is successfully verified. This rate derived from the ratio of correct authentication times of an authorized user to the number of his authentication. False positive rate, Which is the probability that an unauthorized user is treated as an authorized user. This rate is obtained from the ratio of the incorrect authentication times of an unauthorized user to the number of his authentication attempts. Note that FNR and TPR are related to the convenience of users when they use our system, where the authorized user can successfully unlock the smart phone by a single try. The FPR reflects the security of the Open Sesame, where the unauthorized user should be denied to unlock the smart phone.

C.EXPERIMENT SETUP:

For analyzing the uniqueness of hand waving, we collect the waving action data from 200 distinct smart phone users. The subjects producing these data sets are selected randomly in different public places, including railway station, university library, and stadtpark. When collecting the waving action data, three smart phones from different brands are used. For collecting each specific users hand waving data, he is asked to act with the following instruction: The user first randomly selects one of the three smart phones we provided, and holds this smart phone, which is running our data collection app, in his accustomed way. Then he pushes the button of 'start′ on the screen and begins to wave the smart phone until the hint sound is played by the smart phone. This waving process lasts for more than 10seconds. The user has to repeat the above action for three times to terminate the data collection. Note that there is no special restriction on users waving actions. He can wave the smart phone arbitrarily in each trail. Indeed, we aim at taking insight into the handshaking action but not the motion pattern. Overall, 389,373 raw tuples are captured from 200 distinct users, with an average 1,947 raw tuples per user. Each user performs the hand waving for three trails while each trail persists 10 _ 20 seconds. For each user, the training data will be extracted from the first two trails, while the testing data will be retrieved from the last one. Therefore, there is no overlap between the training data and testing data. The classification is based on self and non-self discrimination. For a given user, the training data is composed of negative samples belonging to this user, and an equal number of positive ones from others.

C. IMPACT OF WAVING FUNCTIONS:

There are mainly four waving functions to parameterize the A Space representation of hand waving pattern. In this

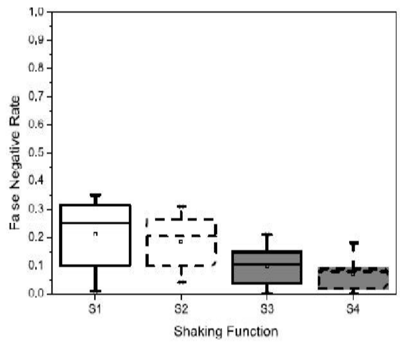
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

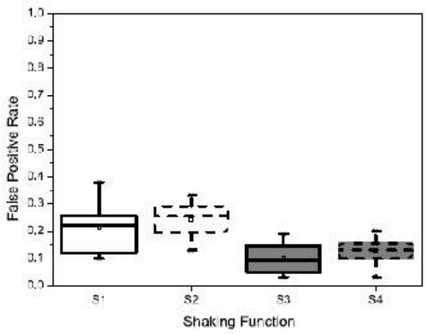
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

process, we



(a) False Negative Rate

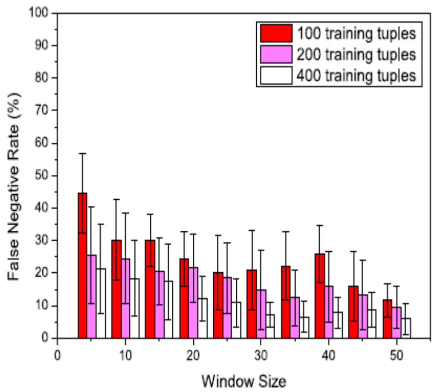


(b) False Positive Rate

Choose 30 user's hand waving pattern and maintain the window size as 50 tuples. Fig. 6 plots the FPR and FNR for the four waving functions, which are taken into account. From the Fig. a, we analyze that the average FNR using S1 and S2 are around 20 percent while the values are below 10 percent using S3 and S4. The similar observation is obtained on FPR, as shown in Fig.6b. This shows that the distance-based waving functions perform better than the angle-based ones. We further focus on the distance-based waving functions. S3 and S4 have close FNRs and FPRs. However, the variance of S4 is smaller than that of S3, which means S4 is more stable than S3.

E.IMPACT OF SVM:

Window size is an important factor. For capturing enough windows, we require the users to shake their phones in an acceptable time period. A large window size will prolong the waving time period for unlocking and seriously affect user experiences. But a small window size will influence the identification accuracy. We change the windows size from 5 to 50 with the increment of 5 and employ S4 for testing. The result is shown in Fig. 7. The average FPR reduces from 42 to 18 percent and average FNR decreases from 20 to 8 percent as the window size increases. This shows that the larger windows help improve the accuracy. This is due to the more number of raw tuples that are extracted in a larger window and the user ' s hand waving is better characterized. The number of training tuples also affects the accuracy. As illustrated in Fig. 7, FNR is approximately reduced by 50 percent, i.e. from 15 to 8 percent, when window size is50.This reduction is even obvious with small window size.



(a) False Negative Rate

On the other hand, when the window size is 50 the average FPR only reduces from 20 to 15 percent taking 5 percent off. This shows that, to the number of training tuples the FPR is less sensitive.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

VI. CONCLUSION

In this paper, we propose a novel behavioral biometric-based authentication approach called Open Sesame for smart phone. We design four waving functions to fetch the unique pattern of user′s hand waving actions. The smart phone can accurately verify the authorized user with the hand waving action by applying the SVM classifier. Experiment results based on 200 distinct user's hand waving actions show that the Open Sesame reaches high level of security and robustness, and achieve good user's experience.

VII. FUTURE ENHANCEMENT

In the proposed system Android app is developed in which user's Hand Waving Pattern record & repeat the above actions for many times until the Application registers user's pattern. Here we use SVM algorithm for identifying the user.

REFERENCES

[1] Mell, P., and Grance, T., "The NIST definition of cloud computing (draft)," NIST Special Publication, vol. 800, p. 145, 2011.
[2] De Capitani di Vimercati, S., Foresti, S., and Samarati, P., "Managing and accessing data in the cloud: Privacy risks and approaches," in Proc. 7thInt. Conf. Risk Security Internet Syst., 2012,pp. 1–9.1272 IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 5, MAY 2015.
[3] Williams, P., Sion, R., and Carbunar, B., "Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage," in Proc. 15th ACM Conf. Comput.Commun. Security, 2008, pp. 139–148.
[4] Paillier, P., "Public key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. Cryptographic Techn., 1999, pp. 223–238.
[5] Samanthula, B. K., Elmehdwi, Y., and Jiang, W., "k-nearest neighbor classification over semantically secure encrypted relational data, 'eprintarXiv:1403.5001, 2014.
[6] Gentry, C., "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Sympos. Theory Comput., 2009, pp. 169–178.
[7] Gentry, C., and Halevi, S., "Implementing gentry′s fully-homomorphic encryption scheme," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Techn.: Adv. Cryptol., 2011, pp. 129–148.
[8] Shamir, A., "How to share a secret," Commun.ACM, vol. 22, pp. 612–613, 1979.