A Novel Non-Intrusive User Authentication Method based on Touchscreen of Smartphones

Chien-Cheng Lin
Computer Science and Engineering
National Taiwan Ocean University
Keelung, Taiwan, R.O.C.
hammerlin@hotmail.com

Chin-Chun Chang
Computer Science and Engineering
National Taiwan Ocean University
Keelung, Taiwan, R.O.C.
cvml@mail.ntou.edu.tw

Deron Liang*
Computer Science and Information Engineering & Software Research Center
National Central University,
Taoyuan, Taiwan, R.O.C.
drliang@csie.ncu.edu.tw

***Abstract*—In recent years, the functionality of smartphones has been rapidly improved; then, the smartphones are not only used for telecommunication but also for various applications, such as email and social network accessing. These applications raise new security issues to smartphone users; however, the current protection mechanisms of smartphones are not sufficient due to convenience issue and shoulder-surfing issue. We therefore propose a non-intrusive authentication approach based on touchscreen of smartphones. To the best of our knowledge, this work is the first publicly reported study that adopts the histogram features of touchscreen to build an authentication model for smartphone users. Our empirical results for fifty-five participants show that the proposed approach is feasible. The performance of the proposed approach could be increased if users continuously operate their smartphone after a period of time. Finally, we further discuss the applications and limitations of the proposed approach.**

Keywords-Non-intrusive authentication; Smartphone; Touchscreen sensor; Histogram features.

I. INTRODUCTION

The performance and the features of smartphones are rapidly increased in recent decade. This enables to use such devices not only as a telecommunication tool but also as an endpoint device for various applications, such as accessing email or social network, on a regular basis. Several surveys reported that the smartphones are used more frequently for various applications other than telecommunication [16][17][28]. These new applications raise new security issues to smartphone users, including the client-side security when engaged in accessing sensitive information stored in the phone or stored on remote sites [5][6][9][13][26]. On the other hand, recent survey reports that the smartphone penetration has increased four times in five years (growth since 2007) [21]. This also increases the risk of being target of attacks.

The current protection mechanisms of these devices are usually based on PIN codes or passwords, and biometric-based methods such as fingerprints [25][39] or facial recognition [19][27][29]. Both fingerprints and password entry are intrusive in the sense that they require explicit action from the user, which is not convenient in a frequent use. According to recent surveys [34][36], 60% to 80% of users choose to turn these verification features off simply because of its inconvenience. On the other hand, accessing the sensitive information stored in remote sites are generally protected by the passwords, PINs, or security codes; however, the password-based authentication methods used on mobile devices have a shoulder-surfing issue [12][23][32][35]. In order to enhance the security level of the mobile devices, non-intrusive authentication mechanisms are desirable [5][6][13].

Non-intrusive authentication systems could be briefly divided into two types based on the applied features they exploit for verification. The first type is dynamics feature-based approach [11][24][30][31][33], which utilizes various features, such as distance, velocity, acceleration and angular speed of a movement. A dynamics-based authentication approach could authenticate users in a short period of time; however, its performance in general is limited due to the size of the obtained testing data. The second type is the behavior-based approach [1][4][15], which exploits the statistics of some predefined types of actions, such as a histogram of movement distributions. The performance of histogram-based approach could be improved by increasing the amount of testing data; however, the statistics of the behavior collected in a short period of time may be inaccurate.

Based on our analysis, a histogram-based authentication approach is especially feasible for the scenarios of using smartphones to access sensitive information since these operations are time-consuming. We therefore propose a histogram-based and non-intrusive authentication approach based touchscreen sensor of smartphones. To the best of our knowledge, this work is the first publicly reported study that adopts the touch-based features to build an authentication model for smartphone users. To validate the feasibility of the proposed approach, we then implemented an authentication model based on touchscreen of smartphones. To collect experimental data, an app has been implemented to collect

* Corresponding Author

978-0-7695-5010-7/13 $26.00 © 2013 IEEE
DOI 10.1109/ISBAST.2013.37

the biometrics of fifty-five participants when they operate the smartphones in their hands. For each smartphone user, a histogram-based authentication model is constructed based on the three combined features. To construct the authentication model, the feature score algorithm is used to weigh features for each participant and KL-Divergence algorithm is used to determine the divergence among smartphone users. Then, the weighted k-nearest neighbor (WkNN) is used as the classification algorithm. A commonly used strategy of cross-validation, namely leave-one-out [10], is used. Our empirical results for fifty-five participants show that the proposed approach has an equal error rate of about 4.6% to 5.7% when the number of flicks is thirty (about 5 minutes). Besides, the proposed approach has an equal error rate of about 2.9% to 3.6% when the number of flicks is sixty (about 10 minutes). Finally, we discuss the applications and limitations of the proposed approach.

II. Structural Modeling and Experiment

A. Touch-based Features

To determine the touch-based features, we observe the commonly used touch gestures of smartphones. The touch gestures are generally categorized as following types: Flick, Spread, Pinch, and Drag touch gestures. The flick touch gesture is used to move scrollbars of a smartphone apps, such as email and browser. The spread and pinch touch gestures are separately used to zoom-in and zoom-out on touchscreen. Finally, the drag touch gesture is used to move the location of icons, files, or folders. Based on our observation, flick is a frequently used touch gesture while operating smartphone apps. We therefore focus on using the flick touch gesture for authenticating purpose.

An example of raw flick data is shown in Table I. Each record consists of six fields: the type of action, the touch position of x-axis in pixels, the touch position of y-axis in pixels, the touch pressure, the touch size, and the timestamp. The type of action and timestamp were used to discriminate the start and the end of a flick action. After appending each pair of the touch positions (x-axis and y-axis), a trajectory of a flick action then could be determined.

Table I An example of raw flick data

type of motion	touch				timestamp
	x-axis	y-axis	pressure	size	
…	…	…	…	…	…
down	379.22	683.9117	0.6	0.1	1358839609887
move	344.36	626.8816	0.6	0.1	1358839609939
move	326.6	594.2988	0.6	0.1	1358839609962
move	304.81	558.8608	0.6	0.133333	1358839609981
move	280.37	525.4977	0.6	0.1	1358839610002
move	256.16	495.7088	0.6	0.1	1358839610025
move	204.88	435.0411	0.75	0.133333	1358839610053
move	162.93	397.9022	0.75	0.1	1358839610072
move	110.12	352.6057	0.75	0.133333	1358839610091
move	69.609	318.8223	0.4625	0.066667	1358839610107
up	69.609	318.8223	0.4625	0.066667	1358839610136
…	…	…	…	…	…
down	275	713.1718	0.141176	0.141176	1352280110963

To qualify the touch-position, we split the touchscreen (480x800 pixels) with a 12x20 grid to monitor the varying of touch-position referred to flick trajectories. The obtained values of the touch-pressure and the touch-size, which depict the strength and agility of flick actions, are normalized based on the smartphone manufactories. From such data, we were able to build flick behavioral models for discriminating smartphone users.

B. Data Collection

As presented in previous subsection, the flick action is by far the most commonly used touch gesture in all apps. We therefore design an app on HTC™ Sensation XL [20] with Android™ 2.3 [18] platform to collect user's behavioral biometrics of flick actions from the touchscreen. Two GUIs, namely up-down-flicks and left-right-flicks, were designed. The up-down-flicks is used to collect the operating behavior while a user conducts a vertical flick action of her/his finger. The left-right-flicks is used to collect the operating behavior while a user slides her/his finger over the screen horizontally. Once a user's finger touches the screen of the smartphone, the app continuously collects the touch-based readings at a sampling rate of 50 Hz until her/his finger does not touch the screen for a while.

To collect experimental data, all of our participants were asked to sit on the same chair. Based on our analysis, we found the obtained data of flick gestures have less contribution for authenticating purpose if the time of a flick action is less than 100ms (the time of a flick action is too short). We then use this strategy to abandon useless data in the noise reduction phase

C. Behavior Modeling

According to the characteristics of the features, various statistical packages can be used to generate a pattern characterizing user behavior. As indicated earlier, a flick touch gesture consists of the combination of three features: touch-position, touch-pressure, and touch-size. In the remainder of this subsection, we analyze each of these features and illustrate the modeling techniques used. Notice that each of the histograms was created using 450 flick actions.

1) Histogram of Touch-Position: To qualify the touch-position of a flick touch gesture, we have split the touchscreen with a 12x20 grid. Then, the histogram of the touch-position could illustrate the distribution of the touch positions performed by the users with flick actions. Based on our observation, this distribution in general differs from one user to another. Fig. 1 shows a comparison between two users. The bars of User 1 are distributed in five groups; 64 percent of his or her actions are within the range of 185-200. On the other hand, the bars of User 2 are distributed in nine groups and only 9.4 percent of his or her actions in the same range (185-200). The distributions of touch-position represent that User 1 and User 2 use different positions while they perform flick actions.

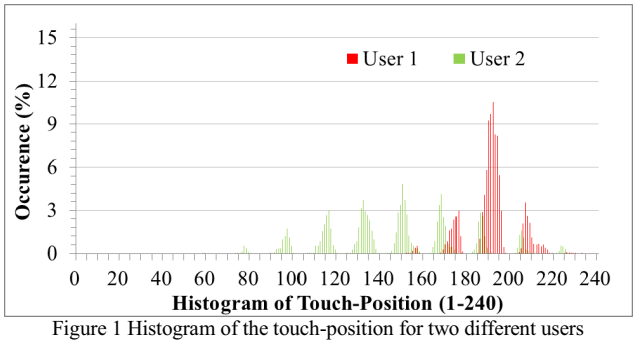

Figure 1 Histogram of the touch-position for two different users

2) Histogram of Touch-Pressure: The applied touch-pressure feature involves calculating the percentage of flick actions occurring in each of the two-hundred bins. The bins from one to two-hundred separately represent the touch-pressure from the lightest to the heaviest. Our pre-test results showed that the touch-pressure feature represented by the two-hundred bins could be added to model the flick actions of smartphone users.

3) Histogram of Touch-Size: Similar to the histogram of touch-pressure feature, the histogram of touch-size feature involves calculating the percentage of actions occurring in each of the twenty bins. The bins from one to twenty separately represent the touch-size from the smallest to the biggest. Another pre-test results showed the behavioral differences between two users can be easily detected via the distribution of the histogram.

D. System Modeling

To construct the proposed authentication model, we adopted the three touch-based features discussed in previous subsection. In the learning phase, the feature score algorithm is used to weigh applied features for each participant. Then, authentication models are trained by using the weighted features and the weighted k-nearest neighbor (WkNN) classifier, which classifies a query sample by the k training samples nearest to the query sample. In our experiments, the k nearest training examples around a query sample are determined by KL-Divergence algorithm. Finally, we applied leave-one-out cross-validation to compute the performance metrics of the proposed approach.

III. Results and Discussions

Fifty-five participants (37 male, 18 female) with varying smartphone experiences and ages ranging from 18 to 40 years, joined this experiment to generate two data sets: one is for the up-down flicks and the other is for the left-right flicks. These participants used the same smartphone to produce a total of 78,888 flick samples for the two data sets. The data collected were directly stored in the embedded storage of the smartphone. Each participant conducted about 2,000 up-down flick samples and 1,800 left-right flick samples. About 3.8 percent of collected data were abandoned due to the touch-based readings being determined as useless data for authentication. To perform our experiments, we firstly use a learning curve to determine the sample size of a training set. The pre-test result represented that a training model could gain better performance while the size of a training set is 450 flicks.

In our experiments, the accuracy rate, the false acceptance rate (FAR), and the false rejection rate (FRR) were estimated by the leave-one-out strategies based on the results of 5 runs. For each run, the training set contained 450 flicks was built a template histogram, and the test set had 810 histograms. In addition, the test set of genuine user had 270 histograms, and the test set of imposter user had 540 histograms. Each of the 54 imposter users contributed 10 histograms.

A. Experimental Results

To validate the proposed approach, we evaluate the performance of the proposed approach. Fig. 2 and Fig. 3 show the performance of the proposed approach with respect to the data sets of the up-down flicks and the left-right flicks, respectively, where the FAR and FRR with respect to different threshold limits. The experimental results have an equal error rate less than 5.5% while the number of flicks exceeds 30.

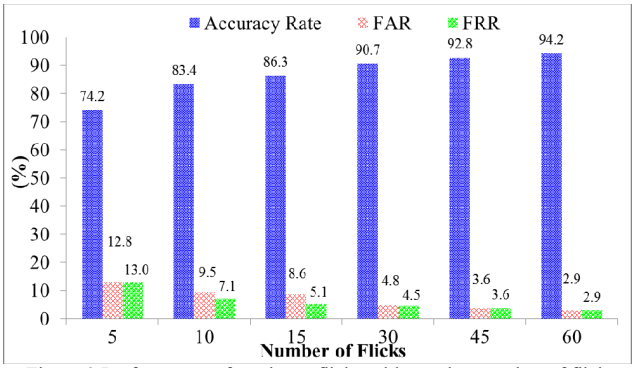

Figure 2 Performance of up-down-flicks with varying number of flick actions

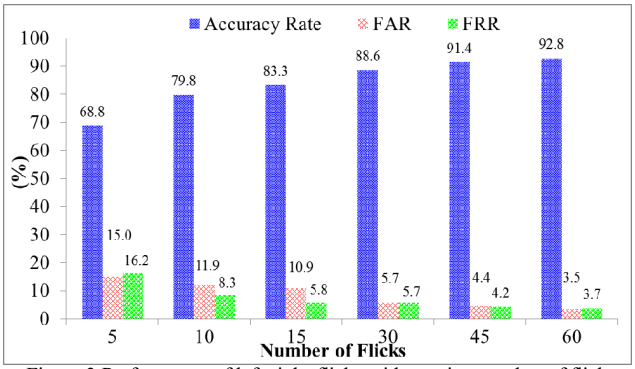

Figure 3 Performance of left-right-flicks with varying number of flick actions

The performance with flick numbers five, ten, fifty, forty-five, or sixty show similar trends. Notice that the proposed approach could has an equal error rate about 3.5 % with sixty flicks (about 10 minutes). The performance of the proposed approach is close to gait-based approach [7][14][37]. Followings are the brief summarization of

existing biometrics including both physiological ones as well as behavioral ones:

1) *Physiological biometrics:*
   - IRIS[27][29]: EER = 0.0259%
   - Fingerprint[25][38][39]: EER = 3.2%
   - Palmprint[29][38]: EER = 0.19%
   - Face[29]: FRR= 16%; FAR = 16%
   - Voice[29][37]: FRR = 7%; FAR = 7%
2) *Behavioral biometrics:*
   - Signature[22]: EER = 0.99%-1.07%
   - Keystroke[2][5]: FRR = 4%; FAR = 0.01%
   - Mouse[1][24][31]: FRR = 2.461%; FAR =2.464%
   - Gait[7][14][37]: EER = 5% to 9%

B. Discussion

1) Applications: The applications of the operation biometric can include authentication and access control. It has been reported that the physiological approaches typically show better performance than behavioral models [3][14]. It should be noted, however, that we do not propose this approach as a replacement or sole mechanism of authentication but rather as a complementary mechanism that can be used to improve security in hand-held devices. The proposed approach could be implemented as an individual non-intrusive authentication mechanism or be used as a complementary mechanism of intrusive authentication mechanisms, such as password or fingerprints.

2) Limitations: Based on our analysis, the proposed approach still has several limitations (e.g. mimic issue, regular behavior issue, and posture issue). The ideal situation is that the person holds and operates the smartphone in a similar style all the time. We did not address the mimic issue in this paper. It is important to verify if impersonation attack can be improved by training of the hostile users; are there such users whose hold-and-operate style is relatively easy to mimic? Are there such attackers who can easily mimic other people? In Doddington et al. [8] terms, whether there are any "lambs" or "wolves" users in hold-and-operate mimicking.

IV. Conclusions

In this work, we have proposed a novel non-intrusive authentication approach based on touchscreen of smartphones. The proposed approach adopted three features, which are transformed from the readings of the touchscreen. To the best of our knowledge, this work is the first publicly reported study that adopts the histogram features of touchscreen to build an authentication model for smartphone users. To collect the applied features, we have implemented an app. The experimental results show that the proposed approach is feasible since its performance is close to gait-based approach. We further discuss the applications and the limitations of the proposed approach.

Acknowledgment

This work was partially supported by the National Science Council of R.O.C. under Contract Nos. 101-2218-E-008-001 and 101-2218-E-008-002 and Software Research Center of National Central University.

References

[1] A.A.E. Ahmed, and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," IEEE Trans. on Dependable and Secure Computing, vol. 4, no. 3, pp. 165-179, 2007.

[2] F. Bergadano, D. Guneti, and C. Picardi, "User Authentication through Keystroke Dynamics," ACM Trans. Information and System Security, vol. 5, no. 4, pp. 367-397, 2002.

[3] R. Bolle, J.H. Connell, and N.K. Ratha, "Biometric perils and patches," Pattern Recognition, vol. 35, pp. 2727-2738, 2002.

[4] K.T. Chen, H.K. Pao, and H.C. Chang, "Game Bot Identification Based on Manifold Learning", 7th Workshop on Network and Systems Support for Games (NetGames), Worcester, Massachusetts, USA, Oct. 2008, pp. 21-22.

[5] N. Clarke, and S. Furnell, "Authenticating mobile phone users using keystroke analysis," Int. J. Inf. Secur., vol. 6, pp.1-14, 2007.

[6] N. Clarke, S. Karatzouni, and S. Furnell, "Flexible and transparent user authentication for mobile devices," IFIP Advances in Information and Communication Technology, 297/2009, 1-12, 2009.

[7] M.O. Derawi, P. Bours, and K. Holien, "Improved Cycle Detection for Accelerometer Based Gait Authentication," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. pp. 312-317, 2010.

[8] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation," in 5th International Conference on Spoken Language Processing, 1998.

[9] M.N. Doja, and N. Kumar, "User authentication schemes for mobile and handheld devices," INFOCOMP Journal of Computer Science, vol. 7, no. 4, pp.38-47, 2008.

[10] B. Efron, and R. Tibshirani, "Improvements on cross-validation: The .632 + Bootstrap Method," Journal of the American Statistical Association, vol. 92, no. 438, pp. 548–560, June 1997.

[11] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunary, Y. Jiangz and N. Nguyen, "Continuous Mobile Authentication using Touchscreen Gestures", To appear in the 12th IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, November 2012.

[12] A. Forget, S. Chiasson, and R. Biddle, Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2010), April 10 – 15, 2010, Atlanta, Georgia, USA. pp. 1107-1110.

[13] S. Furnell, N. Clarke, and S. Karatzouni, "Beyound the PIN: Enhancing user authentication for mobile devices," Computer Fraud & Security, pp. 12-17, August2008

[14] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric Gait Authentication Using Accelerometer Sensor," Journal of Computers, vol. 1, pp.51-59, October/November 2006.

[15] H. Gamboa, and A. Fred, "A User Authentication Technic Using a Web Interaction Monitoring System", Lecture Notes in Computer Science (Pattern Recognition and Image Analysis), vol. 2652, pp. 246-254, 2003.

[16] Gartner Inc. "Gartner Says Number of mobile payment users worldwide to Increase 70 percent in 2009." May 28, 2009 Press Releases. available from: http://www.gartner.com/it/page.jsp?id=995812 (2011/11/11).

[17] Gartner Inc. "Gartner identifies the top 10 consumer mobile applications for 2012." November 18, 2009 Press Releases. available from: http://www.gartner.com/it/page.jsp?id=1230413 (2011/11/11).

[18] Google Inc. Android™ Platform. available from: http://www.android.com/, and http://developer.android.com/index.html (2011/11/11).

[19] Google Inc. Face Recognition on Android™. available from: https://sites.google.com/site/androidfacerecognition/Home (2011/11/11).

[20] HTC. Smartphone. available from: http://www.htc.com/us/products (2011/11/28).

[21] L. Kamp, Mobility Trends that Will Define the Next Decade, Mobile World Congress 2012, Accenture Mobility, available from: http://www.slideshare.net/scapecast/accenture-mobility-mwc-2012-bubble-over-barcelona-lars-kamp (2012/2/29 published).

[22] A. Kholmatov, and B. Yanikoglu, "Identity authentication using improved online signature verification method," Pattern Recognition Letters, vol. 26, no. 15, pp. 2400–2408, 2005.

[23] S. Komanduri, and D.R. Hutchings, Order and Entropy in Picture Passwords, Proceeding GI'08 Proceedings of graphics interface 2008, May 28-30, Windsor, Ontario, Canada. pp. 115-122.

[24] C.C. Lin, C.C. Chang, and D. Liang, "A New Non-intrusive Authentication Approach for Data Protection Based on Mouse Dynamics," International Symposium on Biometrics and Security Technologies, Taipei, Taiwan, March 26-19, pp. 9-14, 2012.

[25] D. Maio, D. Maltoni, R. Capelli, J.L. Wayman, and A.K. Jain, "FVC2000: Fingerprint Verification Competition," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 3, pp. 402-412, Mar. 2002.

[26] O. Mazhelis, J. Markuula, and J. Veijalainen, "An integrated identity verification system for mobile terminals," Information Management & Computer Security, vol. 13, no. 5, pp. 367-378, 2005.

[27] D.M. Monro, S. Rakshit, and D. Zhang, "DCT-Based iris recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 586-595, 2007.

[28] O2 News Centre, Making calls has become fifth most frequent use for a Smartphone for newly-networked generation of users, http://news.o2.co.uk/Press-Releases/Making-calls-has-become-fifth-most-frequent-use-for-a-Smartphone-for-newly-networked-generation-of-users-390.aspx (2012/6/29)

[29] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2021-2040, Dec. 2003.

[30] S.B.E. Raj, and A.T. Santhosh, "A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics", International Journal of Computer Science and Network Security (IJCSNS), vol.9, no.4, pp. 370-377, April 2009.

[31] K. Revett, H. Jahankhani, S. Magalhães, and H. Santos, "A survey of user authentication based on mouse dynamics," Communications in Computer and Information Science (Global E-Security), vol. 12, pp. 210-219, 2008.

[32] V. Roth, K. Richter, and R. Freidinger, A PINEntry Method Resilient Against Shoulder Surfing, Proceedings of the 11th ACM conference on Computer and communications security, October 25-29, 2004, Washington, DC, USA. pp. 236-245

[33] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong , "SenGuard: Passive User Identification on Smartphones Using Multiple Sensors." 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Shanghai, China. pp. 141-148, 2011.

[34] Smart Credit. "Consumer Reports survey on mobile phones and security." 2011 Press. available from: http://www.smartcredit.com/blog/2011/09/02/consumer-reports-survey-on-mobile-phones-and-security/ (2011/11/15).

[35] F. Tari, A.A. Ozok, and S.H. Holden, A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords, Symposium on Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006, Pittsburgh, PA, USA. pp. 56-66.

[36] C. Theriault, "Survey says 70% don't password-protect mobiles." 2011 Press. available from: http://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/ (2011/11/11).

[37] E. Vildjiounaite, S.M. Makela, M. Lindholm, V. Kyllonen, H. Ailisto, "Increasing Security of Mobile Devices by Decreasing User Effort in Verification," Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on, Cap Esterel, 25-31 Aug. 2007, pp.80-80.

[38] X. Wu, K. Wang, and D. Zhang, "Palmprint texture analysis using derivative of gaussian filters," in: Proceedings of 2006 International Conferenceon Computational Intelligence and Security, pp.751–754, 2006.

[39] Y.L. Zhang, J. Yang, and H.T. Wu, "Sweep fingerprint sequence reconstruction for portable devices", Electronics Letters, vol. 42, no. 4, pp. 204-205, 2006.