A BIOMETRIC FUSION OF HAND AND FINGER VEIN APPROACH FOR AN EFFICIENT PERSONAL AUTHENTICATION IN HEALTH CARE

N S Priya[1], A Lenin Fred[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Lord Jeganaath College of Engineering, Nagercoil.

[2]Professor, Department of Computer Science and Engineering, Mar Ephraem College of Engineering.

Abstract

Manual mistakes are made in our healthcare systems more and more now a days because of the records being mixed up, medical charts are confused among patients; the wrong medication is given to the wrong patient. Healthcare biometrics refers to biometric applications in doctors' offices, hospitals, or for use in monitoring patients. It consists of access control, identification of patients and patient record storage. Biometrics has revolutionized the healthcare industry; devices can take unique information about you from your eye, your hand print, or your thumb print and use it to identify you. This information can be used to ensure that you are who you say you are, and you have permission to be working with the healthcare information you are trying to access. The proposed work focuses on analyzing the various Biometric approaches and algorithms and to generate an efficient Biometric fusion of hand and finger vein method to improve the performance such as time complexity, reducing missing and false minutiae from various sources in health care.

Keywords*: *Biometric security, biometrics, multi touch gestures, health care, patient record

INTRODUCTION

Biometrics is typically used for multi-factor authentication[1]. Multi-factor authentication combines at least two of the following: something you know (password), something you have (token) and something you are (fingerprint). Biometric authentication covers everything in that last category: finger vein approach, voiceprints, iris scans, handwritten signatures, and so on[2].

Most of the devices, so far can be combined with a biometric scanner such as a fingerprint scanner or an iris scanner[3]. Use of biometrics authenticate the user to the device rather than the authentication server. A positive biometric identification unlocks the device's functionality; the device still needs to generate some form of a cryptogram to prove the identity to the server[4]. For example a standard chip card reader comes with a numeric keypad which allows users to enter a PIN and authenticate themselves to the chip card before a cryptogram is generated. The PIN pad can be replaced with a more user friendly fingerprint scanner. While easy to use, futuristic and fashionable, biometric sensors are still relatively expensive and increase the cost of a two-factor authentication device[5].

Biometrics authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

The development of biometric multi-touch technology opens up an opportunity for new authentication techniques that go beyond text passwords. A biometric modality results from variations in movement characteristics of the fingertips. Multi-touch has allowed users to seamlessly communicate with devices using natural and fluid interaction. Although multi-touch interfaces are changing the manner in which the user can interact with computing devices[6].

One key advantage of biometric gesture based user authentication schemes compared to other well-known biometric modalities for user authentication is revocable. When a gesture is compromised or no longer effective, it can be replaced by another gesture. A gesture is defined as either a static palm gesture or dynamic palm gesture depending on whether or not a user's palm is moving while executing the gesture[7]. Second, a gesture is defined as parallel, close, open, or circular, depending on the movement pattern of the fingertips. Lastly, a gesture is defined as either all fingertips moving or a proper subset of fingertips moving depending on the set of fingertips being moved while executing the gesture[8].

SUBJECTS AND METHODS

Image Acquisition

The patient records are accessible by the use of biometric device. It is the straightforward and simple method, enabling faster authentication and access to patient records in times of emergency.

Pre-Processing

The biometric multi-touch gesture is a time series of the set of x-y coordinates of finger touch points captured as the gesture. Each set consists of multiple touch points, each from one fingertip. The system pre-process multi-touch gesture data by relabeling each and every touch point using simple polygon rule[9].

Feature Computation

A set of features is computed from the sorted set of touch points using pair-wise Euclidean distances between the points. The feature set is robust to translation and rotation caused by differences in a hand's position and orientation. The system derives rotation and translation invariant features to represent the gesture.

Distance Function

The distance between two biometric multi-touch gestures is computed using an elastic distance function, namely dynamic time warping (DTW). DTW is a well-known matching algorithm to measure similarity between two time series[10]. It may have different lengths and time deformations. Piece-wise linear mapping of the time axes to align the two sequences while minimizing cumulative warping cost.

Score Calculation

A dissimilarity score is finally calculated from these pairwise distances. At the end, the biometric multi-touch gesture is accepted if and only if the dissimilarity score is less than a pre-defined threshold.

RESULTS

Image Acquisition

In hospital, to capture the input image using biometric device. The biometric multi-touch gesture image is shown in figure 1.

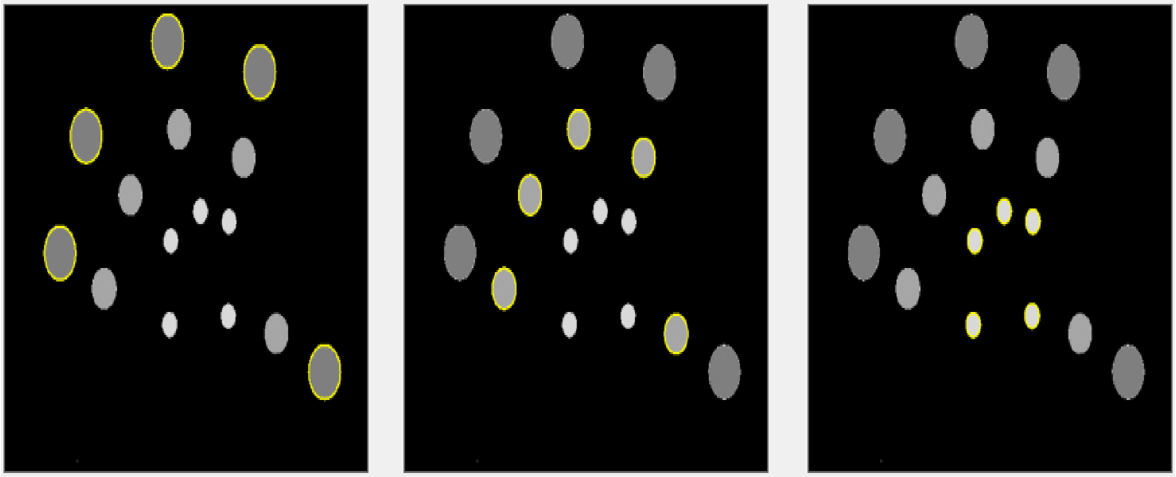
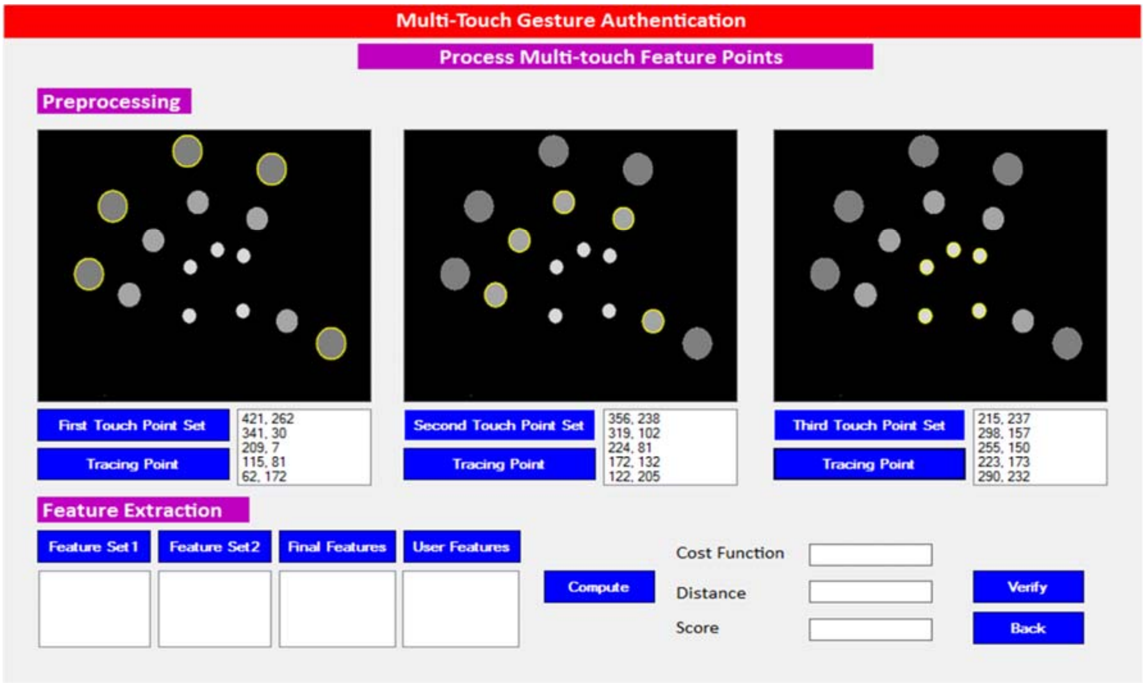


Figure1. Input Image

Pre-Processing

Each input set consists of multiple touch points, each from one fingertip. For the three touch point sets, initialization is done by sorting the touch point set, either the first set or the last set. Once the touch points are sorted, the highly visible points are traced. It is shown in figure2.



First Touch Point Set: 421, 262
341, 30
209, 7
115, 81
62, 172

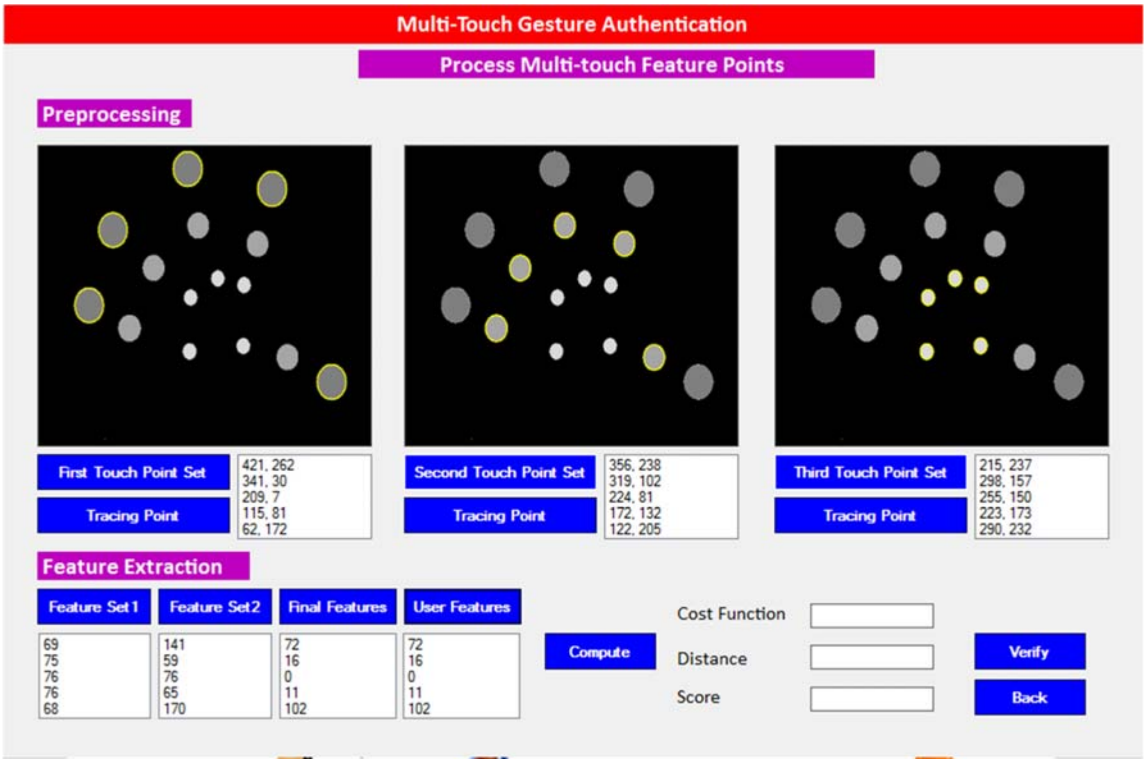
Second Touch Point Set: 356, 238
319, 102
224, 81
172, 132
122, 205

Third Touch Point Set: 215, 237
298, 157
255, 150
223, 173
290, 232

Figure 2. Preprocessing

Feature Computation

A set of features is computed from the sorted set of touch points using pair-wise Euclidean distances between the points. With the values of touch point set and tracing points, the feature sets and the final features are calculated. The final features are then computed with the user features which is shown in figure3.



First Touch Point Set: 421, 262
341, 30
209, 7
115, 81
62, 172

Second Touch Point Set: 356, 238
319, 102
224, 81
172, 132
122, 205

Third Touch Point Set: 215, 237
298, 157
255, 150
223, 173
290, 232

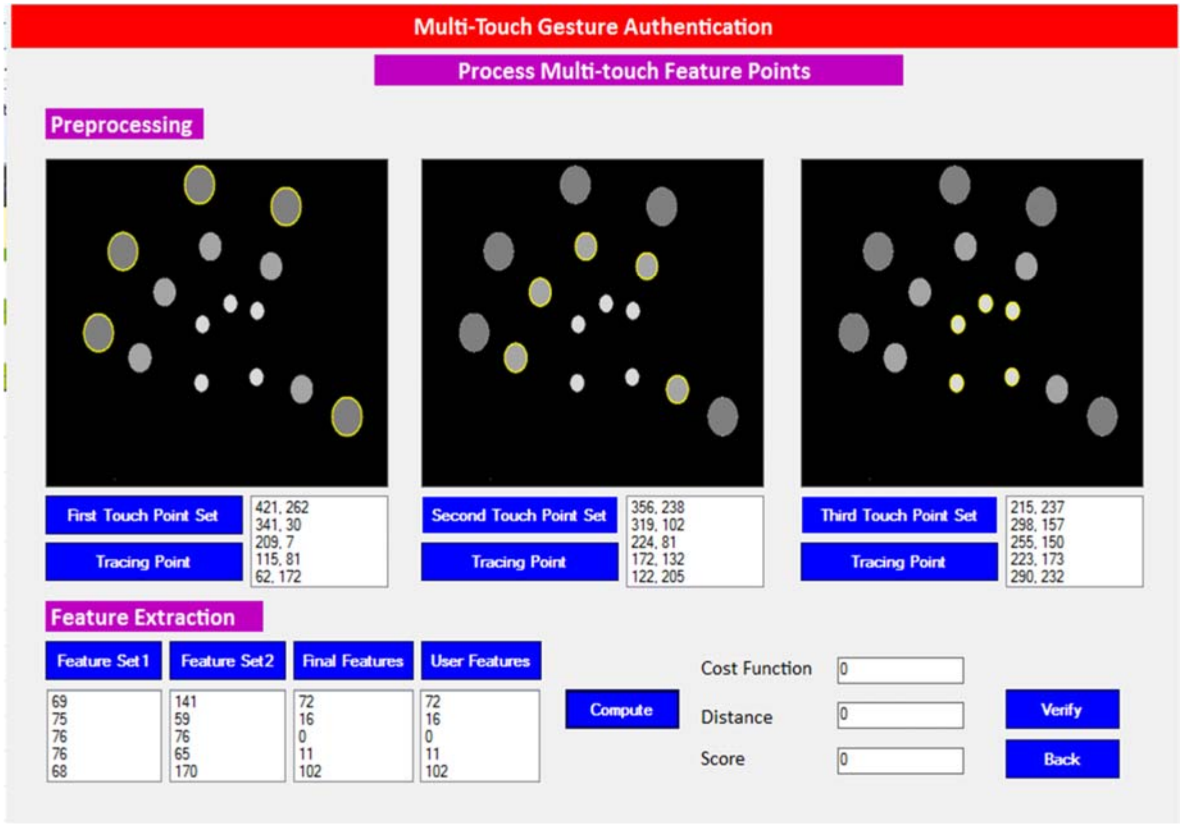
Feature Set1	Feature Set2	Final Features	User Features
69	141	72	72
75	59	16	16
76	76	0	0
76	65	11	11
68	170	102	102

Figure3. Feature Computation

Distance Function and Score Calculation

The distance between two biometric multi-touch gestures is computed using an elastic distance function, namely dynamic time warping. DTW is a well-known matching algorithm to measure similarity between two time series. It may have different lengths and time deformations. A dissimilarity score is finally calculated from these pairwise distances. At the end, the multi-touch gesture is accepted if and only if the dissimilarity score is less than a pre-defined threshold can be shown in figure4

.



First Touch Point Set:
421, 262
341, 30
209, 7
115, 81
62, 172

Second Touch Point Set:
356, 238
319, 102
224, 81
172, 132
122, 205

Third Touch Point Set:
215, 237
298, 157
255, 150
223, 173
290, 232

Feature Set1	Feature Set2	Final Features	User Features
69	141	72	72
75	59	16	16
76	76	0	0
76	65	11	11
68	170	102	102

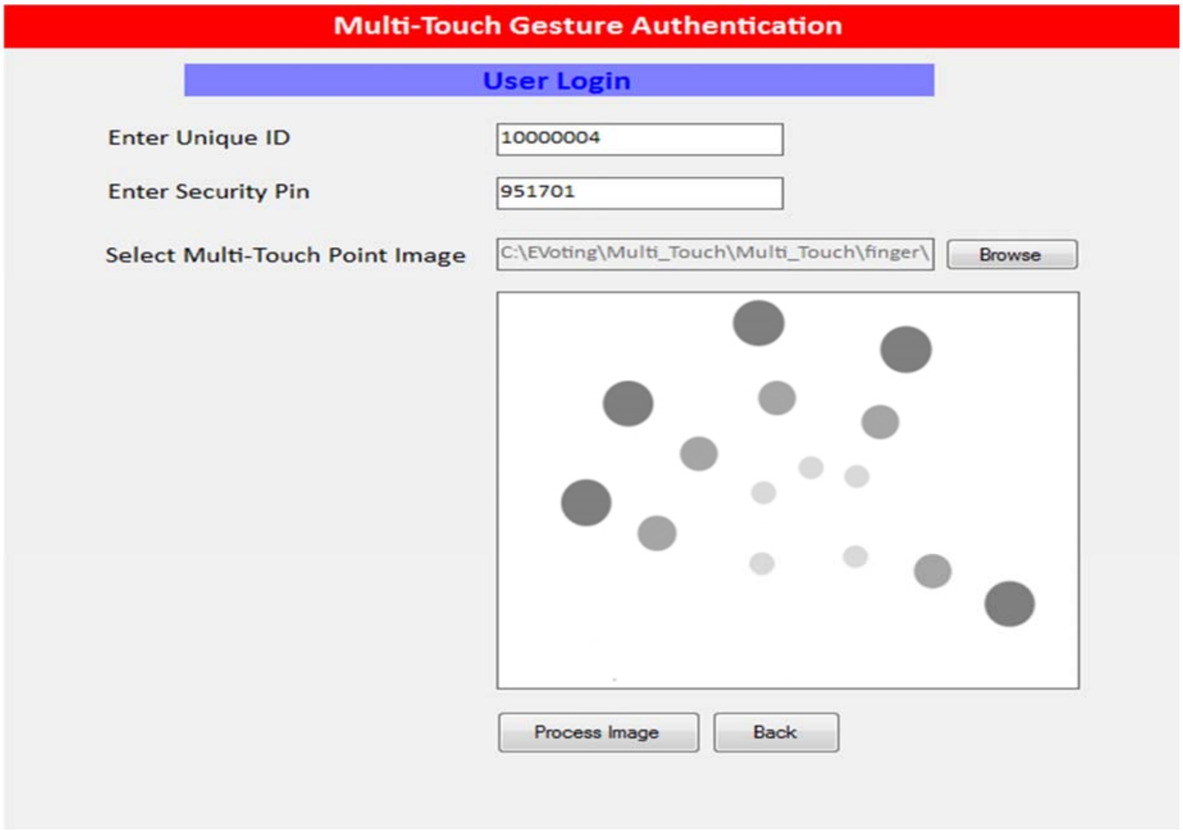
Cost Function: 0
Distance: 0
Score: 0

Figure4. Distance Function and Score Calculation

DISCUSSION

As biometric patient identification and authentication systems continue to improve, one can expect to see more multi-touch gesture authentication solutions that combine multiple modalities for patient identification such as hand and finger vein approach. This provides healthcare with additional tools to accurately identify patients in the event of injury or trauma.

In this phase of authentication, the user is requested to get the input such as unique id, security pin and fingertips. The biometric multi-touch gesture is accepted if and only if the dissimilarity score is less than a pre-defined threshold. Then click process image button an open the patient details which is shown in figure 5.



Multi-Touch Gesture Authentication

User Login

Enter Unique ID: 10000004

Enter Security Pin: 951701

Select Multi-Touch Point Image: C:\EVoting\Multi_Touch\Multi_Touch\finger\

Figure5. User Authentication

CONCLUSION

This article proposes and evaluates biometric multi-touch gestures for user authentication on touch devices. The results show that multi-touch gestures have the potential for developing new patient authentication techniques. In terms of usability, the results show strong correlation between positive user experience, in terms of ease of use, pleasure, and excitement, and biometric performance of the gestures. To improve privacy and security measures, to install biometric access controls to verify medical personnel's identities and increase efficiency. Due to password authentication process, hospital officials have difficulty accurately tracking access to its sensitive data networks. Passwords can be cumbersome and oftentimes personnel would stay logged in to avoid having to manually type a password each time they needed to access patient information thus, making it difficult to track who had accessed information. Biometric technologies are defined as automated methods of identifying or verifying the identity of a living person based on unique biological (anatomical or physiological) or behavioral characteristics. Biometrics can provide very secure and convenient verification or identification of an individual since they cannot be stolen or forgotten and are very difficult to forge.

ACKNOWLEDGEMENTS

The authors thank the supervisor, forum friends, project staff and research scholar for their contribution to the project. The authors also thank Mar Ephraem College of Engineering for assistance with equipment for the project.

Author Contributions

NS Priya conceived paper, oversaw data collection, conducted data analysis, written manuscript and approved final version. Dr A Lenin Fred revised manuscript and approved final version. The authors declare that they have no conflicts of interest.

REFERENCES

[1] K. Ahmed, K. Isbister, and N. Memon (2012) "Biometric-rich gestures: A novel approach to authentication on multi-touch devices" Proc. ACM Annu. Conf. Human Factors Comput. Syst., pp. 977–986.

[2] C.Battista Biggio, Giorgio Fumera, Fabio Roli (2013) "Security evaluation of pattern classifiers under attack" IEEE Transaction on

knowledge and data engineering. pp. 34-76

[3] S. Chiasson, P. van Oorschot, and R. Biddle (2007) "An Hmm-Based Behavior Modeling Approach For Continuous Mobile Authentication" Computer Security–ESORICS. Berlin, Germany: Springer-Verlag, pp.359–374.

[4] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu (Dec. 2008) "A Tap And Gesture Hybrid Method For Authenticating Smartphone Users" in Proc. Annu. Comput. Security Appl. Conf., pp. 121–129

[5] A. Jain, A. Ross, S. Pankanti (Jun. 2006) "Biometrics: A tool for information security" IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 125–143.

[6] D. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin (1999) "Motionauth: Motion-Based Authentication For Wrist Worn Smart Devices" Proc. 8th USENIX Security Symp., pp. 1–14.

[7] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, et al., (2010) "Multi-touch authentication on tabletops" Proc. SIGCHI Conf.Human Factors Comput.Syst., pp. 1093–1102.

[8] N. Memon, and K. Isbister (Sept2012) "Investigating multi-touch gestures as a novel biometric modality," Proc. IEEE 5th Int. Conf. Biometrics, Theory, Appl. Syst., pp. 156–161.

[9] I. Odinaka, P. Lai, A. Kaplan, J. O'Sullivan, E. Sirevaag, and J. Rohrbaugh (Dec. 2012) "Continuous Remote Mobile Identity Management Using Biometric Integrated Touch-Display" IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1812–1824.

[10] U. Park, R. R. Jillela, A. Ross, and A. K. Jain (Mar. 2011) "Continous Mobile Authentication Using Touch Screen Gesture" IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 96–106.