

An Enhanced Approach for Human Computer Interface

Vikas Chahar
Research Scholar, NIMS University, Jaipur (Rajasthan)
vikas.chahar@gmail.com

Abstract

In this paper here will discuss biometric approach [1] that are used to create such kind of interface between human being and computer that are more reliable, fast, efficient, robust and produce usable and safe system as well as functional system.

Keywords: HCI, Biometric, Analytical Approach.

Introduction

As we know that interface is the way of communication between two things that is not only between machines but also between living being. In computer science interface is create a relationship between two devices by using software or any other medium.

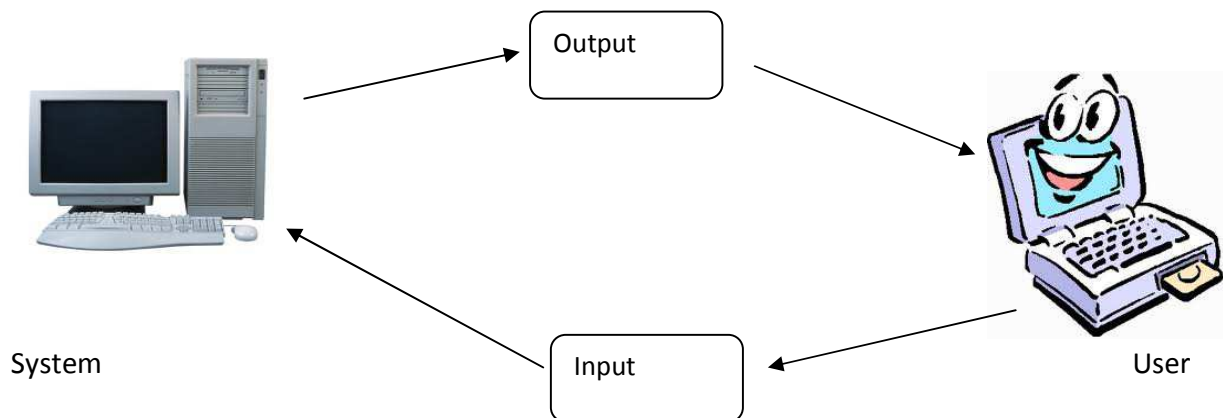
Generally computer interface takes place between hardware and software, through which human and computer could communicate or perform operation to

achieve desired goal. However, effective interface that will discover the newest technology such as cyber space's, animation, multimedia, finger print and speech recognition etc...

Common things that are used for HCI [2] are computer mouse, touch screen, icon, pull down menu, dialog box, check box, radio button etc...

It is an art of interaction between human and computer for direct manipulation to get immediate feedback, proper affordances, judicious use of sound and animation, protection from accidental mistakes, gentle error message and so on....

It will explore how human beings interact with computational devices.



Traditional Diagram for Interconnection between Human and Computer

Language interface designs are text, speech, and hypermedia. These are one of popular approach that will cover the interconnection between human and computer using language either typed, clicked on (with a mouse) or spoken.

HCI help us to understand what is going on in the interconnection between user and system. They address the translation between what the users wants and what the system does.

- It is a joint performance tasks that is takes place by human and machines.
- It is a structure communication between human and machine
- It is an algorithmic and programming approach of interface itself
- It will creates a way human efficiently and effective use machines
- An engineering concerns, that arise in designing and building interfaces

Thus HCI is a science, engineering and design aspects.

There are nine different kind of rule that is used to design HCI:

1. First rule is to, strive for consistence
 - i. Make consistent sequence of action that should be required in similar situation
 - ii. Use identical technology that should be used in prompts, menus and help screen
 - iii. Use consistent color, layout, capabilities, fonts and so on employed throughout
2. Second rule is, enable frequent users to use the shortcuts
 - i. To increase the piece of interaction use abbreviation, special key, hidden commands and macros
3. Third rule is, to offer information feedback
 - i. For every user action, system should responds in same way
4. Forth rule is, to design dialogs to yields closure
 - i. Make a sequence of action that is organized into groups with a beginning module and ends. The informative feedback at the completion of a group of actions shows the user their activity has completed successfully
5. Fifth rule is, to offers error prevention and simple error handling
 - i. To design the form, due to this users cannot make a serious errors

- ii. If any how user make errors (such a entering data into database or file that can be alphabetic, alphanumeric, numeric or decimal number) , instruction should be written to detect the error and offer simple, constructive and specific instruction for recovery
- b. To segment the long forms, sends section separately, so that the users is not panelized by having to fill the form again
6. Sixth rule is, to permit easy reversal of action
7. Seventh rule is, to support internal locus of control
 - i. Experience uses want to be change
8. Eight rule is, to reduce short terms memory load
9. Last rule is, to prevent error, whenever possible.

Biometric approach for HCI

Biometric technique [3] currently used or under research, we found that most of them explore characteristics extracted from: face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice point, DNA, palm part, body odor, key stroke dynamic, ear shape, finger nail bed, hand written signature etc.....

These system have been applied to a broad range of application, such as forensic science, financial and trade security, information system security, custom and immigration, national identification cards, driver license, RC of vehicle, smart cards etc...

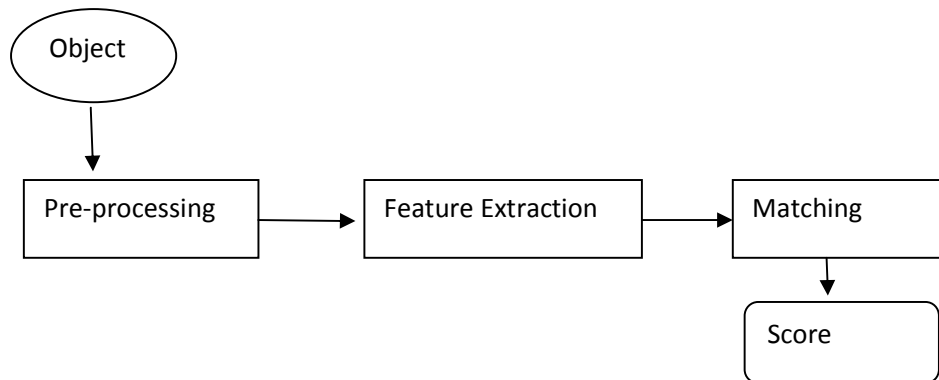
Biometric technique can be categorized direct or indirect HCI

1. **Direct HCI Biometric:** it is based on ability, style, performance, knowledge or strategy used by people while working on computer. This directly interact with computer by using input devices, mouse [4-8] / keyboard [4, 9], knowledge or skill exhibited by the user during interaction with different software. It will measure advanced human behavior. E.g knowledge or skill, email behavior [10, 11], programming style [12-14], utilize on-line game strategy [15-17], biometric sketch [18, 19], command line lexicon [20-23].
 - i. Human interact with input devices such as keyboard or mouse
 - ii. Key stroke: typing pattern by users
 - iii. Mouse: moving all mouse actions, that include drag and drop, print or click and stillness
 - iv. Haptic system: are computer input and output devices which can provide us information about direction, pressure, force, angel, speed, position of the users interaction

2. **Indirect Biometric:** is a type behavioral biometric which will measure advance human strategies. That will be monitoring user's behavior via observable low level actions of computer software. For example audit logs, system call tracers, storage activities, call stack analysis, audit logs GUI interaction registry access and system call [24, 25].
 Based upon above categorization there is a algorithm that will create effective algorithm to create interface between human beings and computer.

ALGORITHM Direct-Indirect-Biometric (number of parameter based on biometric)

1. Pick a type of HCI behavior
2. Break up behavior into components actions
3. Determine the frequencies of component actions for each users
4. Combine the results into a feature vector profile



'Analysis of Biometric Model'

Base upon above model here we will represent a algorithm that will create effective interface between human being and machine to get exact solution of problem even though if we will provide little bit of information related to task.

ALGORITHM Biometric-HCI (number of parameter used for creating interface & existing values)

INPUT: Direct/Indirect HCI

OUTPUT: Verified Results with the threshold

1. Feature extraction based on parameter passed
 - i. Feature extraction based on existing value
2. Chromosome representation & Initialization pitfall P
3. Compute fitness value for each hypothesis in P

5. Apply similarity measure function to the stored template and current behavior
6. Experimentally determine a threshold values
7. Verify or reject user, based on the similarity score comparison to the threshold values

Generally biometric technique divided into two broad classes:

1. **Physiological biometric technique**
 Physiological biometric technique related to shape of body, including finger print, face recognition, DNA, palm print, hand geometry, iris recognition etc...
2. **Behavioral biometric technique**
 Behavioral biometric technique related to the behavior of person such as typing rhythm, gait and voice, signature verification, vein analysis, speech recognition etc...

4. If satisfy termination condition
 - i. If yes then go to step 5
 - ii. Otherwise go to step 3 by selection, crossover and mutation to generate new population P_n
5. If maximum fitness values is greater than threshold value
 - i. If yes then go to step 6 otherwise
 - ii. Go to step 7
6. Match the result and stop
7. Not match result and exit

Conclusion

The biometric systems are more reliable, secure, and robust and create very interface between human being and machine. By using Biometric-HCI algorithm, computation time can be reduced by using

more powerful computers and parallel computation on an appropriate hardware

References

- [1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst., Vol. 14.*, pp. 4-20, Video Technol, 2004.
- [2] R. V. Yampolskiy, "Human Computer Interaction Based Intrusion Detection," 4th International Conference on Information Technology: New Generations (ITNG 2007), Las Vegas, Nevada, USA, April 2-4, 2007.
- [3] M. Curtin, C. C. Tappert, M. Villani, G. Ngo, J. Simone, H. S. Fort, and S. Cha, "Keystroke Biometric Recognition on Long-Text Input: A Feasibility Study," *Proc. Int. Workshop Sci Comp/Comp Stat (IWSCCS 2006)*, Hong Kong, June 2006.
- [4] M. Pusara and C. E. Brodley, "User re-authentication via mouse movements," *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, Washington DC, USA, 2004.
- [5] A. A. E. Ahmed and I. Traore, "Detecting Computer Intrusions Using Behavioral Biometrics," Third Annual conference on Privacy, Security and Trust, St. Andrews, New Brunswick, Canada, October, 2005.
- [6] A. A. E. Ahmed and I. Traore, "Anomaly Intrusion Detection based on Biometrics," *Workshop on Information Assurance*, United States Military Academy, West Point, NY, June 2005.
- [7] H. Gamboa and V.-. A. Fred., 2004., "A Behavioral Biometric System Based on Human Computer Interaction," In *Proceedings of SPIE*, 2004.
- [8] H. Gamboa and A. Fred, "An identity authentication system based on human computer interaction behaviour," *Proc. of the 3rd Intl. Workshop on Pattern Recognition in Information Systems*, 2003.
- [9] G. Bartolacci, M. Curtin, M. Katzenberg, N. Nwana, S.-H. Cha, and C. C. Tappert, "Long-Text Keystroke Biometric Applications over the Internet," *MLMTA*, 2005.
- [10] S. J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern, and C.-W. Hu, "A Behavior-based Approach to Securing Email Systems," *Mathematical Methods, Models and Architectures for Computer Networks Security*, Sept. 2003.
- [11] S. J. Stolfo, C.-W. Hu, W.-J. Li, S. Hershkop, K. Wang, and O. Nimeskern, "Combining Behavior Models to Secure Email Systems," *CU Tech Report*, Available at: www1.cs.columbia.edu/ids/publications/EMT-weijen.pdf, April 2003.
- [12] E. H. Spafford and S. A. Weeber., "Software Forensics: Can We Track Code to its Authors?" 15th National Computer security Conference, Oct 1992.
- [13] A. Gray, P. Sallis, and S. MacDonell, "Software Forensics: Extending Authorship Analysis Techniques to Computer Programs," In *Proc. 3rd Biannual Conf. Int. Assoc. of Forensic Linguists (IAFL'97)*, 1997.
- [14] G. Frantzeskou, S. Gritzalis, and S. MacDonell, "Source Code Authorship Analysis for Supporting the Cybercrime Investigation Process," 1st International Conference on eBusiness and Telecommunication Networks - Security and Reliability in Information Systems and Networks Track, Setubal Portugal, August 2004.
- [15] R. V. Yampolskiy, "Behavior Based Identification of Network Intruders," 19th Annual CSE Graduate Conference (Grad-Conf2006), Buffalo, NY, February 24, 2006.
- [16] R. V. Yampolskiy and V. Govindaraju, "Use of Behavioral Biometrics in Intrusion Detection and Online Gaming," *Biometric Technology for Human Identification III. SPIE Defense and Security Symposium*, Orlando, Florida, 17-22 April 2006.
- [17] J. Ramon and N. Jacobs, "Opponent modeling by analysing play," *Proceedings of the Computers and Games workshop on Agents in Computer Games*, Edmonton, Alberta, Canada, 2002.
- [18] A. Brömme and S. Al-Zubi, "Multifactor Biometric Sketch Authentication," In A. Brömme and C. Busch, editors, *Proceedings of the BIOSIG 2003*, Darmstadt, Germany, 24. July 2003.
- [19] S. Al-Zubi, A. Brömme, and K. Tönnies, "Using an Active Shape Structural Model for Biometric Sketch Recognition," In *Proceedings of DAGM*, Magdeburg, Germany, 10.-12. September 2003.
- [20] D. Y. Yeung and Y. Ding, "Host-based intrusion detection using dynamic and static behavioral models," *Pattern Recognition*, vol. 36, pp. 229-243.
- [21] J. Marin, D. Ragsdale, and J. Surdu, "A hybrid approach to the profile creation and intrusion detection," *DARPA Information Survivability Conference and Exposition (DISCEX II'01)*, 2001.
- [22] T. Lane and C. E. Brodley, "An Application of Machine Learning to Anomaly Detection," 20th Annual National Information Systems Security Conference, 1997.
- [23] T. Lane and C. E. Brodley, "Detecting the Abnormal: Machine Learning in Computer Security," *Department of Electrical and Computer Engineering, Purdue University Technical Report ECE-97-1*, West Lafayette, January 1997
- [24] M. Pusara and C. E. Brodley, "User re-authentication via mouse movements," *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, Washington DC, USA, 2004.
- [25] M. O. Trujillo, I. Shakra, and A. E. Saddik, "Haptic: the new biometrics-embedded media to recognizing and quantifying human patterns," *MULTIMEDIA '05: Proceedings of the 13th annual ACM international conference on Multimedia*, Hilton, Singapore, 2005.