A Survey on Multimodal Biometrics Using Fingerprint Minutiae and Signature Verification

[1]B Meenakshi, [2]C Anuradha, [3]Dr. C Nalini
[1]PG Student, [2]Assistant Professor, [3]Professor
[1]Department of CSE, Bharath University,Chennai-73, [2]Department of CSE, Bharath University,Chennai-73,
[3] Department of CSE, Bharath University,Chennai-73
[1]meenakshi.08.87@gmail.com, [2]anuradha.ak23@gmail.com, [3]drnalinichidambaram@gmail.com

Abstract: **A secured system process is becoming a tough process to validate the online users. In an online process, normally user name and password is given for user registration. But since this alone is not sufficient for security, biometric identifier, fingerprint is used in registration step using a fingerprint device. In this paper, an additional security parameter, signature using mouse, that is, keystroke based or mouse based signature registration and verification is used, hence the concept of multimodal biometric authentication is used in this paper.**

Index Terms: **Secured System Process, Biometric Identifier, fingerprint, online user, online process, keystroke, and mouse based signature, multimodal biometric authentication.**

I. INTRODUCTION

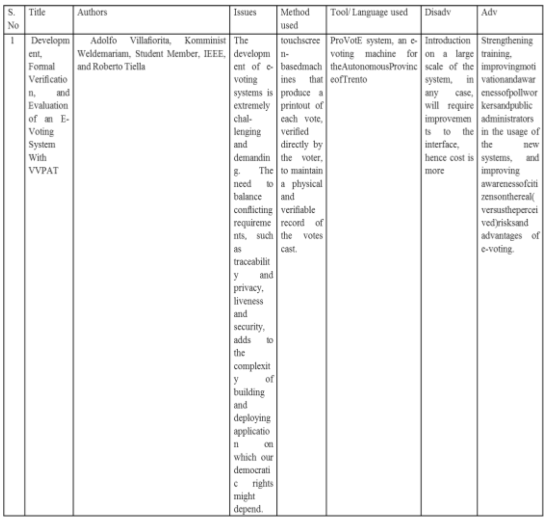
Biometrics is a term describing a characteristic or a process. As a Characteristic, it is measurable both anatomically as well as physiologically. As a Process, it encompasses automated methods of recognizing an individual based on measurable characteristics. There are two categories of biometrics, viz, unimodal biometric and multimodal biometric. Similar to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a “single shot” , providing user verification only during login phase when one or more biometric traits are required [1]. A single biometric or an unimodal biometric system has its disadvantages which is overcome by the multimodal biometric system. For instance, we consider this simple scenario: a user has already logged into a security- critical service, and then the user leaves the PC unattended trickier in the context of mobile devices, often used in public and crowded environments, where the device itself can be lost or forcibly stolen while the user session is active allowing impostors to impersonate the user and access strictly personal data [1]. In these scenarios, the services where the users are authenticated can be easily misused [1]. To overcome this disadvantage of misusing and prevent unauthorized user maliciously, the concept

The accuracy of a multimodal biometrics system is normally calculated in terms of image acquisition errors and matching errors [2]. Failure To Acquire (FTA) and Failure To Enroll (FTE) are the two types of image acquisition errors False Non Match Rate (FNMR) and False Match Rate (FMR) are the two classifications of Matching errors [2]. A higher level of assurance for an accurate match in verification and identification is also provided by a multimodal biometrics unlike an unimodal biometric which may result in false match. Another advantage of a multimodal biometric system is that by making use of multiple methods of identification, a system can preserve higher threshold recognition settings and a system administrator can make a decision on the level of security that is needed [2]. Also, a multimodal biometric system has the ability to avoid spoofing attacks. Hence, due to the above advantages of a multimodal biometric system, these are widely accepted by various users all over the world.

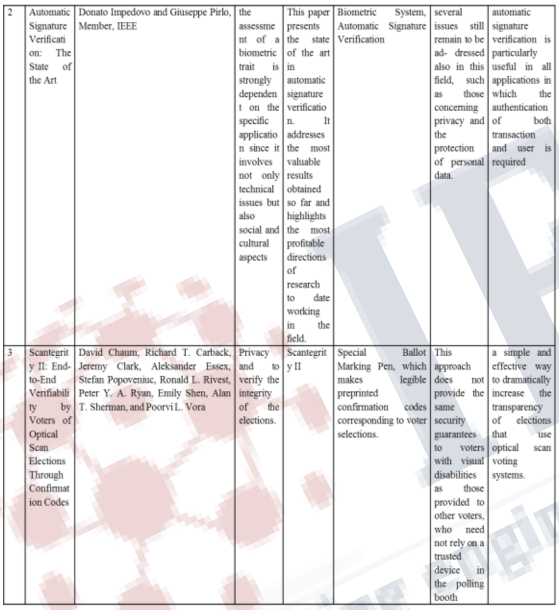
II. RELATED WORK

2.1 Literature Survey

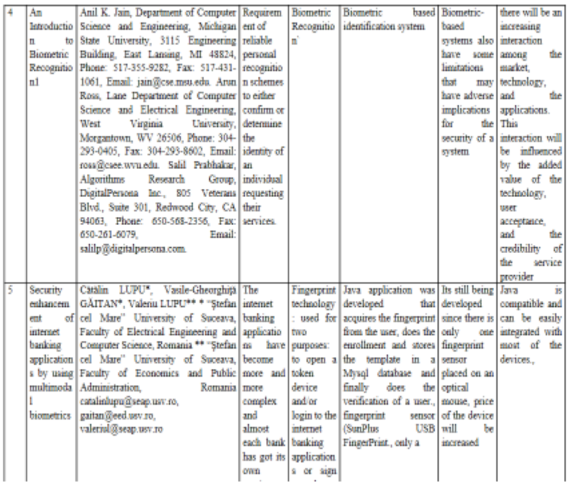
The below tabular columns gives the details of the literature survey made about multimodal biometrics system. The advantages and disadvantages of the referred paper are also tabulated.



S. No	Title	Authors	Issues	Method used	Tool/ Language used	Disadv	Adv
1	Development, Formal Verification, and Evaluation of an E-Voting System With VVPAT	Adolfo Villafiorita, Komminist Weldemariam, Student Member, IEEE, and Roberto Tiella	The development of e-voting systems is extremely challenging and demanding. The need to balance conflicting requirements, such as traceability and privacy, liveness and security, adds to the complexity of building and deploying application on which our democratic rights might depend.	touchscreen-basedmachines that produce a printout of each vote, verified directly by the voter, to maintain a physical and verifiable record of the votes cast.	ProVotE system, an e-voting machine for theAutonomousProvinceofTrento	Introduction on a large scale of the system, in any case, will require improvements to the interface, hence cost is more	Strengthening training, improvingmotivationandawarenessofpollworkersandpublic administrators in the usage of the new systems, and improving awarenessofcitizensonthereal(versustheperceived)risksand advantages of e-voting.



2	Automatic Signature Verification: The State of the Art	Donato Impedovo and Giuseppe Pirlo, Member, IEEE	the assessment of a biometric trait is strongly dependent on the specific application since it involves not only technical issues but also social and cultural aspects	This paper presents the state of the art in automatic signature verification. It addresses the most valuable results obtained so far and highlights the most profitable directions of research to date working in the field.	Biometric System, Automatic Signature Verification	several issues still remain to be addressed also in this field, such as those concerning privacy and the protection of personal data.	automatic signature verification is particularly useful in all applications in which the authentication of both transaction and user is required
3	Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes	David Chaum, Richard T. Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, Alan T. Sherman, and Poorvi L. Vora	Privacy and to verify the integrity of the elections.	Scantegrity II	Special Ballot Marking Pen, which makes legible preprinted confirmation codes corresponding to voter selections.	This approach does not provide the same security guarantees to voters with visual disabilities as those provided to other voters, who need not rely on a trusted device in the polling booth	a simple and effective way to dramatically increase the transparency of elections that use optical scan voting systems.



4	An Introduction to Biometric Recognition1	Anil K. Jain, Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI 48824, Phone: 517-355-9282, Fax: 517-431-1061, Email: jain@cse.msu.edu. Arun Ross, Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506, Phone: 304-293-0405, Fax: 304-293-8602, Email: ross@csee.wvu.edu. Salil Prabhakar, Algorithms Research Group, DigitalPersona Inc., 805 Veterans Blvd., Suite 301, Redwood City, CA 94063, Phone: 650-568-2356, Fax: 650-261-6079, Email: salilp@digitalpersona.com.	Requirement of reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services.	Biometric Recognition`	Biometric based identification system	Biometric-based systems also have some limitations that may have adverse implications for the security of a system	there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider
5	Security enhancement of internet banking applications by using multimodal biometrics	Cătălin LUPU*, Vasile-Gheorghiţă GĂITAN*, Valeriu LUPU** * "Ştefan cel Mare" University of Suceava, Faculty of Electrical Engineering and Computer Science, Romania ** "Ştefan cel Mare" University of Suceava, Faculty of Economics and Public Administration, Romania catalinlupu@seap.usv.ro, gaitan@eed.usv.ro, valerial@seap.usv.ro	The internet banking applications have become more and more complex and almost each bank has got its own	Fingerprint technology : used for two purposes: to open a token device and/or login to the internet banking applications or sign	Java application was developed that acquires the fingerprint from the user, does the enrollment and stores the template in a Mysql database and finally does the verification of a user., fingerprint sensor (SunPlus USB FingerPrint., only a	Its still being developed since there is only one fingerprint sensor placed on an optical mouse, price of the device will be increased	Java is compatible and can be easily integrated with most of the devices.,

2.2 System Architecture

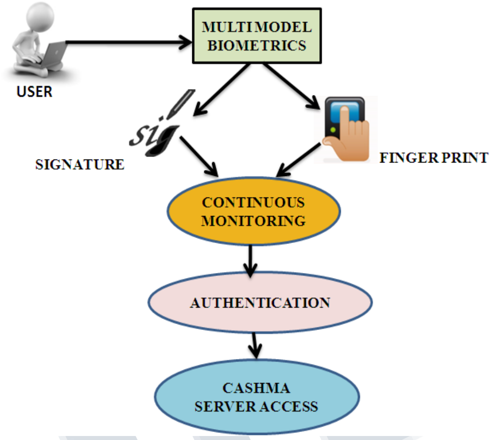


Figure 1: Architecture Diagram of a Multimodal Biometric System

The above figure shows the multimodal biometrics scheme, which uses the Fingerprint verification and the digital signature verification through a continuous monitoring and sent for authentication to a CASHMA Server Access. CASHMA stands for Context Aware Security by Hierarchical Multilevel Architectures, which operates securely with any kind of web service, including services with high security demands as online banking services and it is intended to be used by different from different client devices, e.g., smartphones, Desktop PCs or even biometric kiosks, placed at the entrance of secure areas [1]. Based upon the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it [1].

III. SYSTEM DESCRIPTION

3.1 User Registration

This is the first step process. Here, the client interacts with the application. To access the Application, the Client registers their details with the Application Server. The details include Name, Password, Date of Birth, Mobile Number etc. which are stored in the Application Server Database, thereby making the user to access the application only by their provided Interface.

3.2 Fingerprint Registration

Here, the system identifies the User's Finger using the Fingerprint device.

3.3 Signature Registration

Here, the system identifies the User's Signature using the mouse, viz, it's the registration using digital signature concept.

3.4 Fingerprint Recognition

Here, the server verifies the fingerprint provided by the user during login session with the fingerprint provided by the user. In case of mismatch of the fingerprint, user is not allowed to access the account.

3.5 Keystroke Based Signature Recognition

Here, the server verifies the signature provided by the user upon login with the signature provided by the user. In case of mismatch of the signature, user is not allowed to access the account.

3.6 Banking Authentication

Once the user provides both signature as well as fingerprint correctly, the Server will generate the Session Key using Secure Random Number Generation Algorithm and send it to User's email id. Once the session key received in the user's email id is verified by the server, the user is allowed to access the account.

IV. FINGERPRINT IDENTIFICATION AND FINGERPRINT MINUTIAE ALGORITHM

4.1 Fingerprint Identification

Fingerprint is one of the most well-known and important biometrics [3]. Fingerprints are considered as a biometric characteristic due to their uniqueness consistency over time.

The following advantages make fingerprints more popular:

(i)Ease in acquisition

(ii)Established use

(iii) Numerous sources (ten fingers) available for collection

And (iv) Collections by law enforcement and immigration. [3].

The following figure shows the image of a fingerprint and its various parts

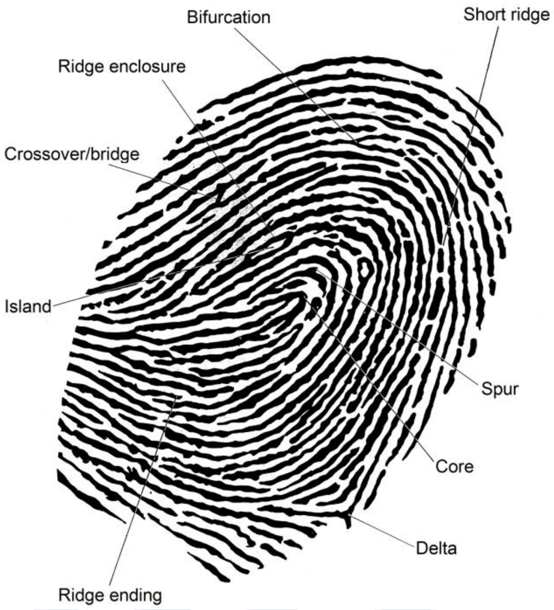


Figure 2: Fingerprint Image

4.2 Fingerprint Minutiae Algorithm

Fingerprint is the most critical step in both verification and identification problems [4]. As per the fingerprint minutiae algorithm, the two fingerprints are compared with each other and the output of the comparison is either a degree of similarity or a degree on non-similarity. The Fingerprint Minutiae Algorithm is a very useful and effective algorithm to check and compare two fingerprints given for comparison.

The algorithm mostly attempts to get the similarity degree between two minutiae fingerprint sets [6]. Two fingerprints are said to be *genuine* if they represent the same finger, and *impostor* if they are different [4]. There are various reasons which make fingerprint matching a challenging problem, viz, skin features, displacement, distortions, , image noise, etc. There are two categories in fingerprints:

1) Small inter-class variations- describe the similarity between two images from different fingers.
2) Large intra-class variations- describe the large variability in different impressions of the same finger.

Minutiae-based matching algorithm is the most widely and popularly used technique. The output of a minutiae extraction stage is, at least, a set of minutiae [4].

The formula to calculate the minutiae-based matching is as follows:

Matching_score=k/((n+m)/2)

V. KEYSTROKE BASED SIGNATURE VERFICATION OR MOUSE SIGNATURE VERIFICATION

Once the fingerprint verification is over, mouse signature is input by the user so that it will also be verified and based on the match or mismatch verification, the user will or will not be allowed to access the account. User has to train the system by registering his signature for about 20 times and mouse signature is used to validate the user.

The following are the steps for signature verification:

Step 1: Sign up or Register to get an account no. and pin no.

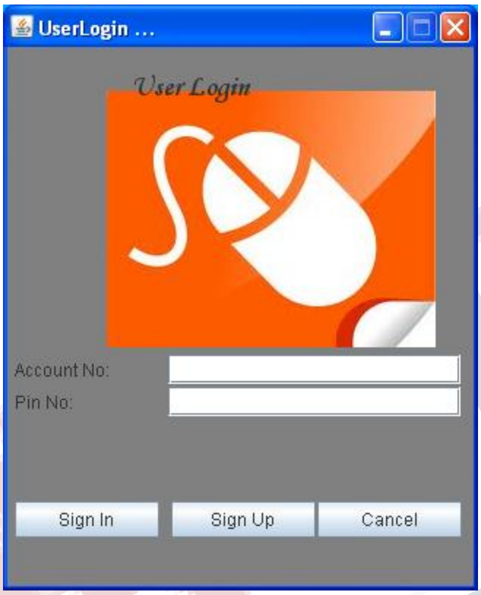


Figure 3: User Login

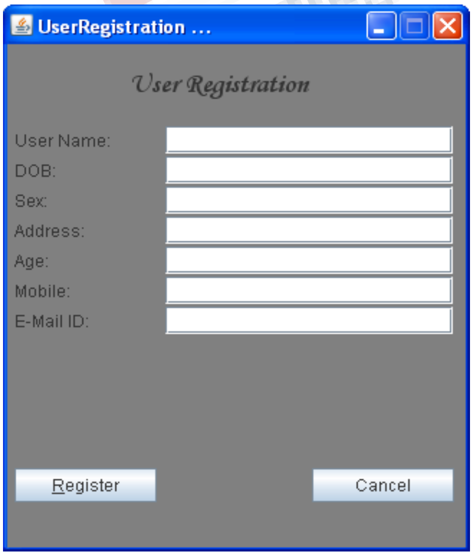
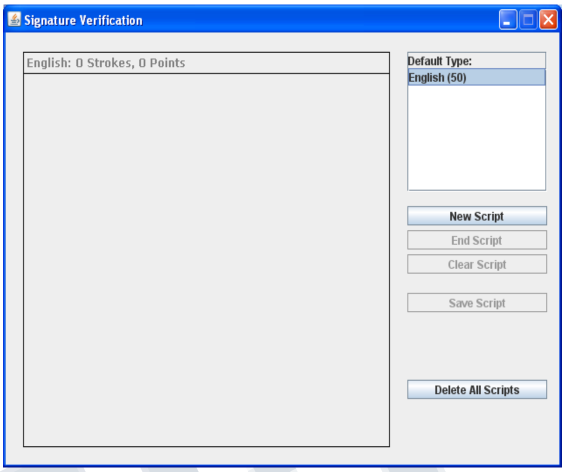


Figure 4: User Registration

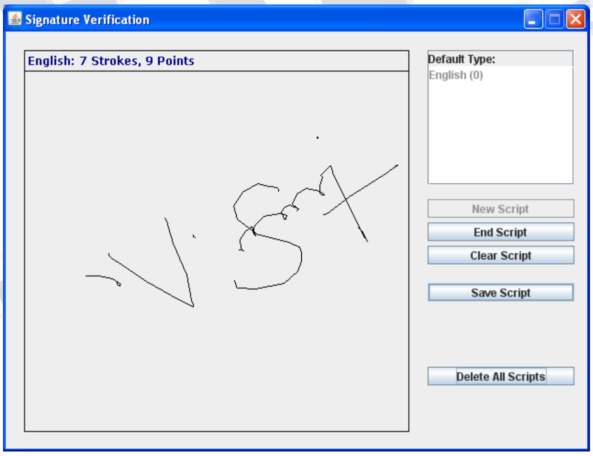
Step 2: Once Fingerprint registration and verification is completed, verify the signature as per the below screenshots:



English: 0 Strokes, 0 Points

Default Type: English (50)

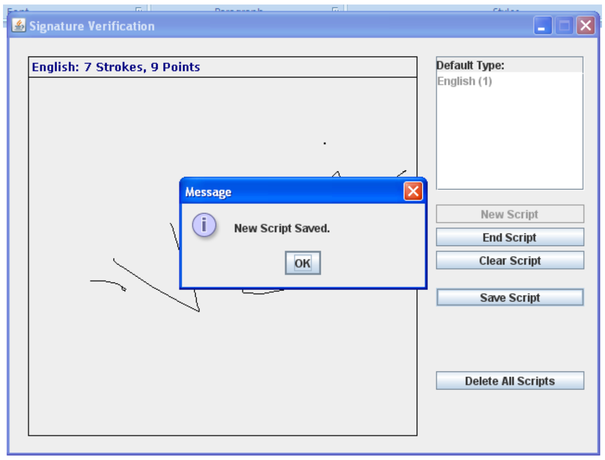
Figure 5: Signature Verification



English: 7 Strokes, 9 Points

Default Type: English (0)

Figure 6: Signature Verification with signature

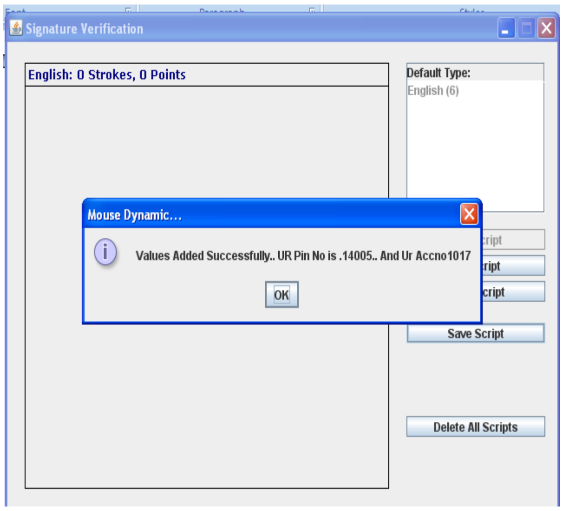


English: 7 Strokes, 9 Points

Default Type: English (1)

New Script Saved.

Figure 7: Signature Verification with saved script message



Values Added Successfully.. UR Pin No is .14005.. And Ur Accno1017

Figure 8: Signature Verification with registration completed message

CONCLUSION

In this paper, we described what a Biometrics is, the identifiable features of Biometrics using the Biometrics techniques, viz, Fingerprint and Signature Verification, and also about the User registration, User verification and about the Keystroke or Mouse based signature verification using a training system. In this paper, we also described about what a Multimodal Biometrics System is, and hence distinguished between an unimodal and a multimodal biometrics system. Even the advantages of a multimodal biometrics system are presented in this paper. We also explained about the Fingerprint Minutiae Algorithm highlighting the features of the algorithm.

REFERENCES

[1] “Continuous and Transparent user Identity Verification for Secure Internet Services”, IEEE Transactions on Dependable and Secure Computing, Vol. 12, No. 3, May/June 2015.

[2] blog.m2sys.com/important-biometric-terms-to-know/top-5-reasons-deploy-multimodal-biometrics/

[3] ”A Survey on Continuous User Identity Verification Using Biometric Traits for Secure Internet Services”, International Journal of Science and Research, Vol 3, Issue 12, December 2014.

[4] “A survey on fingerprint minutiae-based local matching for 4 verification and identification: Taxonomy and experimental 5 evaluation”, Information Science, INS 11514, April 2015.

[5] “Automatic Signature Verification: The State of the Art”, IEEE Transactions on Systems, Man and Cybernetics-Part C Applications and Reviews, Vol 38, No.5, September 2008.

[6] “A Minutiae-based Fingerprint Matching Algorithm Using Phase Correlation”, IEEE, 2007

[7] “Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances”, IEEE, 2007.

[8] “User Identity Verification Using Mouse Signature”, IOSR-JCE, Jul-Aug 2013.

[9] “Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition.”,

[10] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, “Quantitative Security Evaluation of a Multi-Biometric Authentication System,” Proc. Int’l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.

[11] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous Verification Using Multimodal Biometrics,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.

[12] Zach Jorgensen and Ting Yu, “On Mouse Dynamics as a Behavioral Biometric for Authentication”, ASIACCS’11, March 22-24, 2011.

[13] A. Altinok and M. Turk, “Temporal Integration for Continuous Multimodal Biometrics,” Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.

[14] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, “Using Continuous Biometric Verification to Protect Interactive Login Sessions,” Proc. 21st Ann. Computer Security Applications Conf. (ACSAC ’05), pp. 441-450, 2005.

[15] L. Hong, A. Jain, and S. Pankanti, “Can Multibiometrics Improve Performance?” Proc.Workshop on Automatic Identification Advances Technologies (AutoID ’99) Summit, pp. 59-64, 1999.