CIMSA 2007 - IEEE International Conference on
Computational Intelligence for Measurement Systems and Applications
Ostuni, Italy, 27-29 June 2007

# Ensuring the identity of a user in time: a multi-modal fuzzy approach

Antonia Azzini, Ernesto Damiani, Stefania Marrara

Università degli Studi di Milano
Dipartimento di Tecnologie dell'Informazione
via Bramante 65 26013 Crema (CR), Italy
{azzini, damiani, marrara}@dti.unimi.it.

***Abstract –*** *This work proposes a fuzzy multimodal technique capable of guaranteeing the desired level of security while keeping under control the high costs typically associated to some biometric authentication devices. Specifically we describe a fuzzy controller choosing within a palette of authentication techniques to continuously check and confirm its trust in the identity of a user.*

## I. INTRODUCTION

The effectiveness of access control systems rests on one important assumption, proper user identification [1]. This condition has been traditionally guaranteed by authentication engines checking the user's credentials before granting access to a computer system. For our purposes, authentication techniques can be divided into two main classes: *weak* and *strong* authentication methods.

- Weak authentication methods include traditional cryptosystems that do not identify the user as such. The authentication is based on *knowledge*, such as a password, or on a *token*, such as a key, magnetic or chip card. The basic problem is that passwords can often be guessed or searched by an attacker and a long, randomly changing password is difficult to remember. For this reason *smart cards* have been introduced which include tamper-resistant packaging and special hardware that disables the card if it is tampered with or if the number of failed authentication attempts exceeds a chosen threshold. Unfortunately, these devices can be lost, stolen, forgotten or disclosed.
- Strong authentication methods have been developed to address drawbacks of traditional techniques. They include biometric systems (also called *ID-based* authenticators) answering the question: "Who are you?". Common physical biometrics include fingerprints, hand or palm geometry and retina, iris or facial characteristics. Behavioral features include signature, voice (which has also a physical component), keystroke pattern and gait. Biometric characteristics are essentially permanent and unchangeable and users cannot pass them to other users as easily as they do with cards or passwords. Furthermore these techniques are based on features that cannot be lost or forgotten. A biometric authentication system is also fast. The authentication of an user in a fingerprint reader system can take under two seconds, whereas finding a key ring, locating the right key and using it can take as long as ten seconds.

Some issues related to strong authentication methods are still unsolved. In some cases, if the input sample quality is not sufficient for further processing, the system must reacquire data, and the resulting system might be more complicated or more expensive. Furthermore some biometric sensors, particularly those having contact with users, have a limited lifetime. In highly sensitive environments, such as military facilities, it may be necessary to perform strong authentication many times (e.g., at random intervals) to prevent identity substitution after the initial authentication step. In such a scenario, the authentication system must distinguish between the initial step, in which it uses strong authentication to identify the user, and the following authentication steps in which the system decides if its trust in user's identity is high enough to allow the user to continue to perform the activity she is doing. *Multi-modal* biometric systems integrate multiple authentication techniques. Multi-modality will be important for many security applications, including checking the digital passports of the future, incorporating biometric data that will be probably different from country to country[1]. In this paper, we propose a multi-modal authentication system that combines face authentication known for its acceptability with conventional password-based techniques providing high accuracy. In our approach, different trust levels are set for different methods of authentication. When a user gains access to a protected facility, our system continuously checks whether the users' authentication data can be trusted, e.g. enough to satisfy the required security clearance level. If trust is sufficiently high, no action is taken. When trust gets too low, the system chooses a suitable authentication technique, gets the corresponding biometric data, and decides whether the new information satisfies the required security level. In this way, users are kept under a continuous authentication process and security clearance levels can be rigorously maintained. The paper is organized as follows: Sect.II contains a brief description of advantages and disadvantages of the main authentication techniques available today, Sect.III details and motivates the choices made in terms of adopted

[1] While a portrait image will remain a shared element of passports around the world, the U.S. adopted fingerprint data while the European Union may still opt for iris data for its passports.

technologies and system architecture, Sect.IV briefly reviews Mamdami and Takagi-Sugeno-Kang inference methodologies and motivates the approach adopted in our system, Sect.V describes the architecture of the fuzzy based system used to continuously check the identity of the user, Sect.VI reviews the prototype simulation data and describes the most important results obtained and, finally, Sect.VII reports the conclusions and outlines some future work.

### A. Related Work

In the last few years, there has been increasing awareness that multi-modal authentication (i.e., techniques more than one form of credential to identify a user) is generally stronger than any single-mode authentication method. In multi-modal systems "redundancy" is used to tolerate possible failures of authentication devices, including those due to users anomalies (e.g., eye diseases which may prevent iris recognition systems from capturing an appropriate image of the user's eye, or skin diseases which may prevent fingerprint acquisition). In this context, the multi-modal approach was originally introduced in order to alleviate the drawbacks of each individual technique. The work [10] presents a multi-biometric verification system that combines speaker verification, fingerprint verification with face identification. The authors use a fuzzy decision support system in order to take into account the external conditions that can affect verification performances. They show how the fusion of the three techniques reduces the error rates of $48\%$ w.r.t. the speaker verification alone. Another interesting work is [11] that improves security by using *typing biometric* to reinforce password authentication mechanism. Also this methodology employs fuzzy logic to measure the user's typing biometrics. About face recognition, [13] presents a face template matching algorithm based on a 3D head model created from a single frontal face image. In this way the matching is robust across variations in pose, expression and illuminations conditions. This work was extended in [14] where authors describe a method for tracking a face on a video sequence, by recovering the full-motion and the expression deformation of the face using 3D expressive facial model. From some characteristic face points given on the first frame, an approximated 3D model of the face is re-constructed. Using a steepest descent image approach, the algorithm is able to extract simultaneously the parameters related to the face expression and to the 3D posture. Industrial researchers at Hitachi (`http://www.sdl.hitachi.co.jp`) developed a fully-fledged multi-modal system capable of choosing the "right" authentication technique depending on the required security clearance level. However, to the best of our knowledge [12] is the first paper where multi-modality is applied to the problem of checking continuously user identity during a working session to avoid malicious behavior such as identity substitution.

TABLE I
BASIC USER AUTHENTICATION ATTRIBUTES.

| Attributes | User Authentication | | |
|---|---|---|---|
| | Knowledge Based | Token Based | ID based |
| Identification | Password, Secret | Token | Biometric |
| Supports | Secrecy or obscurity | Possession | Uniqueness and personalization |
| Security Defence | Closely kept | Closely held | Forge resistant |
| Security Drawback | Less secret | Lost, stolen | Difficult to replace |
| Examples | Combinational lock, password | Metal key, smart card | Fingerprint, face |

## II. ADVANTAGES AND DRAWBACKS OF AUTHENTICATION TECHNIQUES

Different authentication techniques may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or database, environmental conditions, and other application specific parameters. Attributes of three categories of user authentication methods are compared in Table I.

The work [4] carried out a detailed comparison of authentication technologies, discussing potential attacks against each technique. Some issues related to defenses are listed below:

- Knowledge-based techniques, thanks to challenge-response password protocols, have proved robust against replay and transmission attacks. However, these techniques do not support compromise detection and do not offer much defense against repudiation.
- Token-based techniques provide for compromise detection and add protection against denial-of-service attacks. The two main shortcomings of token-based techniques are high cost, and vulnerability to theft. Token validation requires equipment whose cost is comparable to the one of (much more secure) biometric systems.
- Biometrics data are less easily lent or stolen than others. For this reason, biometric systems provide a much stronger defense against repudiation. Problems include limited lifetime of particular biometrics, and possible violations of the user privacy.

## III. CHOOSING MODALITIES

First of all, we must inquire which authentication devices commercially available can be used in our context. Since our system needs to continuously check the identity of the user while she is working, we want it to be the least intrusive as possible. Hence we will not consider devices such as retina, iris or voice recognition systems, because they would require the user to interrupt her activity for a while during the biometric acquisition process. Fingerprint, hand geometry and face recognition express matching between the acquisition and the stored template by a number $n \in [0, 1]$ that indicates the normalized number of features that perfectly match the template. This value is a suitable input for a fuzzy controller. In this

paper, we will not deal with fingerprint and hand geometry because these techniques require devices having a limited lifetime. More importantly, they hardly guarantee that the person who provides biometric data is the same that was authenticated originally. For example, suppose that university students sit their exams using a computer application without faculty supervision. In such a scenario, identity substitution could easily be performed after authentication, with the consent of the authenticated user, even if the authentication system keeps on requesting fingerprints. The original user could just stay available to provide fingerprints when required, while another student works on the examination paper. On the other hand, in the case of face recognition a digital camera can be installed on the top of the computer display, pointing in the direction of the user. The user does not know if the entire session is recorded or if the camera is used only for an automatic authentication, therefore malicious behavior is less likely. Of course, face recognition suffers of other drawbacks such as inconsistent presentation (i.e. different acquisitions may represent different poses of a face), irreproducible presentation (e.g. due to facial hair growth, a broken nose or wearing eyeglasses) and imperfect signal/representation acquisition (e.g. due to different illuminations). However it has been experimentally tested [4] that face recognition is affected by a experimentally determined FNMR (False NonMatch Rate) of $16\%$ and a FMR (False Match Rate) $= 16\%$. In our context these values can be decidedly reduced just by asking the user to check the illumination conditions of the room where she is working. In this paper, we shall use face recognition as our first (*Strong*) modality and standard UserId/Password authentication as our second (*Weak*) modality. Specifically, when the user tries to login, she initially inserts her UserId and Password. As we shall see, UserId will be used to select the template to which the system will try to match the face acquisition.

## IV. A FUZZY APPROACH TO MULTI-MODALITY

We are now ready to discuss which inference technique best fits our requirements. In this section we discuss applicability to multi-modality of two inference methodologies: Mamdami (MA) [5] and Takagi-Sugeno-Kang (TSK) [6]. A MA type fuzzy rule has the form $\texttt{IF}\ x_1\ \texttt{IS}\ A_1^j\ \texttt{AND}\ x_2\ \texttt{IS}\ A_2^j \ldots \texttt{AND}\ x_n\ \texttt{IS}\ A_n^j\ \texttt{THEN}\ y\ \texttt{IS}\ B_j$ with $j \in [1, M]$, where $x_i$, $i = 1 \ldots N$, are linguistic input variables (e.g. temperature), $A_i^j$ are input fuzzy sets (e.g., "medium", "high") while $y$ is the linguistic output variable (e.g., trustworthiness), $B_j$ is the output fuzzy set and $M$ is the number of fuzzy rules.

In a MA type inference rule the consequent of each rule is also composed of fuzzy sets which are represented as linguistic variables. For each firing fuzzy rule the output of the rule inference (implication) will be mapped to its corresponding output fuzzy set, i.e., the result is described in terms of membership in fuzzy sets. Finally, in order to compute a crisp output value, a process called *defuzzification* must be applied. Popular defuzzification techniques include *center of area*, *center of maxima* and *mean of maxima* (see [7] for a review). In the TSK fuzzy inference method, the antecedent block of each fuzzy rule remains the same as in the previous approach, but the consequent employs a simple equation which takes input variables into account. Fuzzy inference systems can also be modeled using fuzzy rules with singleton consequents. However ([8]), limited modeling capabilities of singleton type FIS result in more coarse grained results and thus affect the quality of the model. When applied to trust-based decision support systems [8], MA is a more intuitive approach since the output is modeled using linguistic variables rather than linear or quadratic equations. However, when using linguistic variables within the consequent block of fuzzy rules it becomes necessary to perform additional calculations in order to generate a crisp output. In this case, defuzzification requires more computational resources and can thus result in slower performance compared to TSK. This is especially true when the fuzzy inference engine contains a large set of rules. Furthermore, MA offers the flexibility of choosing the defuzzification method more suitable to the specific application. Finally, MA fuzzy inference engine is more suitable for analytic applications [8] where the decision process must be human-understandable and it is not necessary to process a large amount of data.

### A. A Fuzzy Controller for Multi-modal Authentication

We developed a fuzzy controller computing an output variable expressing trust in the user identification. Trust is well-expressed as a linguistic variable. Our controller follows the Mamdani approach with a *center of area* defuzzification. Experimental results confirm the goodness of our choice (see Sect. VI). The controller's operation is described in detail in Sect. V. Briefly, we suppose that, after the initial authentication in which the password is used to limit the biometric FNMR and FMR, trust in user identity is computed on the basis of *i)* biometric matching score and *ii)* password check (accept/reject). If the password is correct and the biometric score is higher than a pre-set threshold, the session starts with a certain trust value. Then, biometric and password trustworthiness start to decay and, after a certain time, a new trust value is computed. On the basis of this value the system may decide to close the session altogether, continue the session without asking for a new authentication or asking the user to authenticate again. If a new authentication is asked, a new trust value is computed and the session goes on. This cycle ends when the session is closed by the system, or ended by the user.

## V. ARCHITECTURE OF THE FUZZY SYSTEM

Our approach includes a trust evaluation process which continuously checks the identity of the user who is performing a certain activity. Figure 1 shows the basic steps of our process: after an initial authentication, the server can require further authentication steps based on two parameters 1) the level of trust previously computed and 2) the time passed from the last authentication. We suppose the first authentication to have been performed using both techniques. Indeed the userID is used to choose in the database the template to be used in the matching of the biometric acquisitions, because in a matching one-to-one

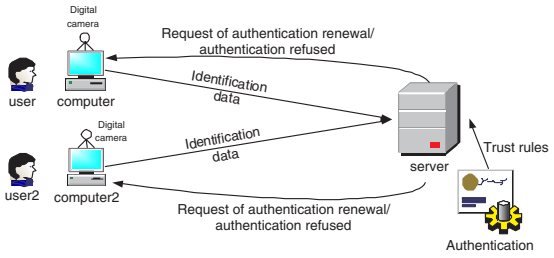


Fig. 1. Context for trust evaluation model

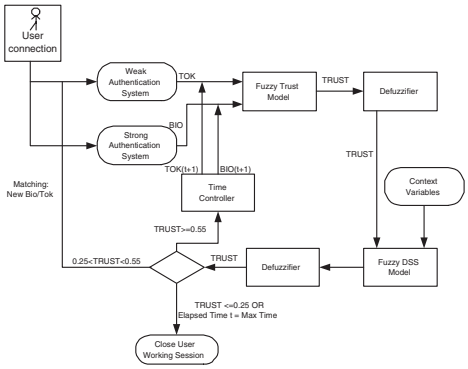


Fig. 2. Architecture of the Multi-modal Fuzzy Trust Model.

the error rates are significantly reduced. The following steps, instead, can be acquired by strong or weak techniques on the basis of the trust level.

### A. Trust Evaluation Parameters

In our model each user authentication can be performed using strong or weak authentication techniques. The *BIO* value represents how the biometric enrollment matches the user's template. In this approach *BIO* corresponds to the acceptance rate resulting from the matching phase of the face authentication process, normalized in the range $[0, 1]$. The second authentication parameter, *TOK*, corresponds to the boolean output (low/high) of the weak authentication system which supports the evaluation of the trust in the user's identity during the activity. In our prototype we used a UserId/password system. At the initial authentication step, the weak technique is involved to enforce the biometric acquisition and the parameter *TOK*, if the authentication successes, is set to *high*, i.e. equal to 1. Two *aging* parameters, respectively for the biometric and the token parameter values, are defined in order to measure how the system's trust in the identity of the user decays in time, by considering separately two straight lines for *BIO* and for *TOK*. The curves are shown in equations 1 and 2, where the values $M_{bio}$ and $M_{tok}$ represent respectively, the gradient that describes the measurement of the grade of the corresponding straight line; in this approach the gradient is obviously set to negative values, since the function has to be time-linearly decreasing. $Timeline$ corresponds to the $x$-axis of the timeliness function, that shows the time $t$ computed as $n * \Delta$ where $n = [1, \infty]$ is the number of trust evaluations performed by the system and $\Delta$ is the time interval between two consecutive trust evaluations. Its maximum value corresponds to the overall session duration. Finally, $BIO_{max}$ and $TOK_{max}$ represent, respectively, the initial values obtained at the initial authentication at time $t_0$. Then, when time is equal to 0, the $BIO_{max}$ and $TOK_{max}$ are equal to *BIO* and *TOK* values resulting from the weak and the biometric authentication systems. At run time, *BIO* and *TOK* will be set to the values of aging corresponding to the elapsed time $t$.

$$BIO_{Curve} = M_{bio} * timeline + BIO_{max} \quad (1)$$

$$TOK_{Curve} = M_{tok} * timeline + TOK_{max} \quad (2)$$

### B. Fuzzy Controller Operation

The entire process implemented in our approach is shown in Figure 2.

At the first step, the information obtained by the biometric engine, i.e. the value *BIO*, and the parameter *TOK* are fed into a fuzzy inference engine *Fuzzy Trust Model* in order to calculate a trust value *TRUST* that expresses the level of trust of the system in the user's identity after the initial authentication at time $t_0$. Of course, prior to processing of the inputs, it is necessary to define fuzzy membership functions which define the degree of membership of each input parameter in the context of the proposed model. Also, it is necessary to define the controller's fuzzy rules. We shall deal with these aspects in the next section.

At time $t_0$ *BIO* and *TOK* are initialized; at each time $t_i$ $(i > 0)$, the decay rate of these values will depend on the corresponding aging parameters. The *TRUST* value is then defuzzified through a *Defuzzifier* engine, using the standard centroid-of-area technique. The output is then fed to another fuzzy engine, *Fuzzy DSS Model*, to compute the final level of trust. This second engine takes as inputs, together with the trust defuzzified value, also external conditions, that may become useful in such a multi-modal authentication approach, that consider biometric authentication techniques. Acceptance rate may degrade when the lighting is too bright or too dark, or when the input facial image for matching is posed at an angle or carries an expression that differs from the enrollment images. In Table II these context variables are generally named *CONTEXT* and supposed, for simplicity, with possible fuzzy values "good" and "poor". The label *ALERT* represents an alert message that is displayed on the user's video asking the user to set the lighting conditions of the room before going on with the new authentication acquisition. The resulting trust of the Fuzzy DSS Model is defuzzified again with the standard centroid-of-area technique, and the output value is compared with the threshold of the membership functions of the Fuzzy DSS Model at each time $t_i$.

If the output trust is *low* the system asks for trust enforcement by going through the *Matching* phase. In this case the system asks for a user re-authentication, that can be biometric

TABLE II

SAMPLE FUZZY RULES DEFINED FOR EACH TRUST MODEL.

| Model | Fuzzy Rules |
|---|---|
| Start Trust Model | **IF** BIO is high **AND** TOK is high **THEN** TRUST is high |
| | **IF** BIO is high **AND** TOK is low **THEN** TRUST is low |
| | **IF** BIO is medium **AND** TOK is high **THEN** TRUST is medium |
| | **IF** BIO is medium **AND** TOK is low **THEN** TRUST is low |
| | **IF** BIO is low **AND** TOK is high **THEN** TRUST is low |
| | **IF** BIO is low **AND** TOK is low **THEN** TRUST is very low |
| Fuzzy DSS Model | **IF** TRUST is very low **THEN** Close User Working Session |
| | **IF** TRUST is low **AND** CONTEXT is good **THEN** Matching: New BIO/TOK |
| | **IF** TRUST is low **AND** CONTEXT is poor **THEN** ALERT **AND** Matching: New BIO/TOK |
| | **IF** TRUST is medium **THEN** Time Controller |
| | **IF** TRUST is high **THEN** Time Controller |

or knowledge-based, depending on the *BIO* and *TOK* values at that time $t_i$. In particular, the system re-acquires the parameter whose value at time $t_i$ is less than a corresponding minimum threshold, previously defined, while maintains the same value at time $t_i$ if it is more than the corresponding threshold. If the trust output is considered *medium* or *high* the system checks, through the *Time Controller* module, how the trust acquired at time $t_i$ has been affected by the decay rate of the *BIO* and *TOK* authentication timeless functions, giving the new, decreased, parameter values for *BIO* and *TOK* at time $t_{i+1}$. These values are fed into the *Fuzzy Trust Model* in order to obtain the new trust value at time $t_{i+1}$.

When the trust level decays to the value of *very low*, the user inserts two wrong passwords in the same weak authentication step, or when the maximum value of the examination time is reached, the execution step goes to the *Close User Working Session* and the process stops.

### C. Trust Model Rules

Each of the two fuzzy models presented in the previous section, has been implemented with different rules, in order to control the trust value at each time step $t_i$ with respect to different evolved parameters of *BIO* and *TOK*. The fuzzy rules defined for each fuzzy model are reported in Table II.

The Start Trust Model is carried out in order to give a trustworthy value depending on biometric and token based acceptance rates, acquired from the *Strong* and *Weak* authentication systems. The *TRUST* value defuzzified is then passed to the Fuzzy DSS Model, and the final resulting defuzzified trustworthy value is used to decide the next steps during the user permission checks.

## VI. PROTOTYPE EVALUATION

The Figure 3 shows the pseudocode of the algorithm implemented in order to test the performance of our approach.

Several experiments have been carried out by considering different values of *BIO* and *TOK* parameters, that result from the Strong and Weak Authentication Systems, and the information about parameter settings and outputs obtained from some

```
BIO = Biometric User Authentication
TOK = Weak User Authentication
while not not expired time do
  TrustA=FuzzyControllerA(BIO,TOK)
  Trustworthiness=FuzzyControllerB(TrustA)
  if Trustworthiness is very low then
    Access Deny
  else if Trustness is low then
    Matching: new BIO — new TOK
  else
    Time Control
    Biometric User Authentication
  end if
end while
Save history of multi-modal authentication process in time
```

Fig. 3. Pseudocode of the Multi-modal Fuzzy Approach.

TABLE III

EXPERIMENTS TABLE.

| Session Id | Biometric Acquisition Number | Password Acquisition Number | Workin Session Time |
|---|---|---|---|
| Id1 | 1 | 2 | 300 |
| Id2 | 2 | 2 | 275 |
| Id3 | 1 | 2 | 300 |
| Id4 | 1 | 3 | 300 |
| Id5 | 2 | 2 | 300 |
| Id6 | 1 | 1 | 183 |
| ... | ... | ... | ... |

of them are summarized in Table III. The global session time was fixed in all the simulations to 300 minutes.

Note that in two cases the working session time was less than the global session time. The Id2 session ended because the user inserted two consecutive wrong passwords, giving a *TOK* value equal to 0. In the other case, Id6 session, the *BIO* and *TOK* values decay to low values: with both values so low, the overall trustworthiness value become very low and the session was closed by the system.

The results of two of the experiments carried out are also shown in Figure 4 and Figure 6. In these figures the curves of the values acquired by the *BIO* (dashed line) and *TOK* (dotted line) parameters during the entire period of the user connection are shown, together with the curve of the *TRUST* values (solid line) obtained during the period of the right permission check implemented by the multi-modal fuzzy approach. Figure 5 shows the time curves of the two authentication techniques (bio and tok) used in the simulation shown in Figure 4. Note that it is obvious to suppose the weak authentication to decay faster than the biometric one.

Results show some interesting properties of the security system. We describe them on the basis of the simulation shown in Figure 4:

- the system requires to set the parameter $\Delta$ that regulates how often the TRUST parameter has to be evaluated. The value of this parameter is application dependent and obviously depends on the security level we want to obtain. Simulation results show that it is possible to obtain a good security ($\Delta = 1$ minute) without interrupting the user many times and consequently not disturbing her work sig-

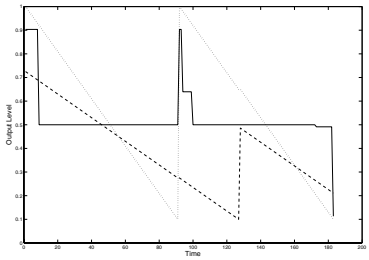


Fig. 4. Simulation of a session closed because TRUST value becomes very low.

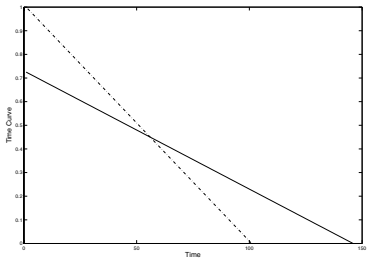


Fig. 5. Biometric and password time curves used in the simulation shown in Figure 4

nificantly. Indeed during a working session long about three hours the user was asked to re-authenticate only twice: for the first time with the password (after about 1 hour and half from the beginning of the session) and the second time by the face image (about 2 hours after the beginning of the session). During the image acquisition the user did not notice to be authenticated and continued to work;

- the system works well even if context variables (i.e. lighting in the room) or biometric acquisitions (due for example to the position of the user who continues to work and does not stay exactly in front of the digital camera) are not perfect. In the simulation shown in Figure 4 the first biometric acquisition takes matching score 0,725 due probably to the not perfect lighting conditions of the room and the second biometric acquisition takes score 0.4860 due to the not perfect position of the user face. Even with these drawbacks the system was able to evaluate a trust level enough high to allow the user to continue to work undisturbed.

## VII. CONCLUSION

In this paper we have studied the possibility of using a fuzzy control system to manage a multi-modal authentication system, with the aim of checking the identity of a user not only at login time but during the entire working session. Our results show that it is possible to obtain a good level of security during the session, without forcing the user to interrupt her work too many times. Also, the system can be used efficiently even if the context variables involved in the acquisition are not optimal. Future work will include techniques to prevent biometric attacks during the overall session time.

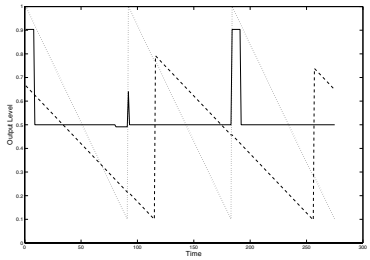


Fig. 6. Simulation of a session closed because the user inserted twice a wrong password.

## ACKNOWLEDGMENT

The authors wish to thank Nick Kasabov for his valuable comments on multi-modal authentication perspectives.

This work was partly funded by the Italian Ministry of Research Fund for Basic Research (FIRB) under projects RBAU01CLNB_001 "Knowledge Management for the Web Infrastructure" (KIWI). and RBNE01JRK8_003 "Metodologie Agili per la Produzione del Software" (MAPS).

[1] U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain, *Biometric Cryptosystems: issues and challenges*, Proceedings of the IEEE, vol. 92, num. 6, 948-960, June 2004

[2] C. Braz and J. Robert *Security and Usability: The Case of the User Authentication Methods* Proceedings of IHM 2006, 18th-21st April 2006, Montreal, Quebec.

[3] W.G. de Ru and J.H.P. Eloff *Enhanced Password Authentication through Fuzzy Logic*

[4] L. O'Gorman *Comparing Passwords, Tokens, and Biometrics for User Authentication.* Proceedings of the IEEE, vol. 91, no.12, 2021-2032, December 2003.

[5] E.H. Mamdani and S. Assilian. *An experiment in linguistic syntesis with a fuzzy logic controller.* International Journal Man-Machine Studies, 7:1-13,1975.

[6] T. Takagi and M. Sugeno. *Fuzzy identification of systems and its applications to modeling and control.* IEEE Transactions on Systems, Man, and Cybernetics, 15:116-132,1985.

[7] G.J. Klir and B. Yuan. *Fuzzy Sets and Fuzzy Logic: Theory and Applications* Prentice Hall, Upper Saddle River, NJ, 1995.

[8] S. Schmidt, R. Steele and T. Dillon *Towards Usage Policies for Fuzzy Inference Methodologies for Trust and QoS Assessment* Proceedings of Fuzzy Days 2006, Dortmund, Germany, September 2006.

[9] S. Krawczyk and A.K. Jain. *Securing Electronic Medical Records Using Biometric Authentication* Proceedings of AVBPA 2005, ed. Springer, pp.1110-1119.

[10] C.W. Lau, B. Ma, H. M. Meng, Y. S. Moon and Y. Yam *Fuzzy Logic Decision Fusion in a Multimodal Biometric System* Proceedings of the 8th International Conference on Spoken Languages Processing (ICSLP) Korea, October 2004.

[11] W. G. de Ru and J. H. P. Eloff. *Enhanced Password Authentication through Fuzzy Logic.* Journal of IEEE Expert Intelligent Systems & Their Applications, November/December 1997.

[12] Antonia Azzini and Stefania Marrara, *A Fuzzy Trust model proposal to ensure the identity of a user in time.* Proceedings of Fuzzy Days 2006, Dortmund, Germany, September 2006.

[13] M. Anisetti, V. Bellandi, E. Damiani and F. Beverina. *Facial identification problem: A tracking based approach.* Proceedings of the 1st International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2005, November 27 - December 1, 2005, Yaounde, Cameroon, pp. 28-35.

[14] M. Anisetti, V. Bellandi, E. Damiani and F. Beverina. *3D Expressive Face Model-based Tracking Algorithm.* Proceedings of the IASTED International Conference on Signal Processing, Pattern Recognition, and Applications, SPPRA 2006, February 15-17, 2006, Innsbruck, Austria, pp.111-116.