A. M. Heinecke, H. Paul (Hrsg.): Mensch & Computer 2006: Mensch und Computer im Struktur*Wandel*.
München, Oldenbourg Verlag, 2006, S. 339-347

Biometrical Signatures in Practice: A challenge for improving Human-Computer Interaction in Clinical Workflows

Andreas Holzinger, Regina Geierhofer, Gig Searle

Institute for Medical Informatics, Statistics & Documentation, Medical University Graz

Abstract

Experience shows that within the sensitive area of documentation in a clinical centre, there are problems involved in acquiring the end user's acceptance of authentication solutions based on smart cards, passwords, finger prints or digital signatures. The individual signature is still the most accepted method of certifying medical documents in hospitals and other health care sectors.

This paper presents some solutions to the problem of using the biometric signature for certifying Diagnostic Finding Reports (DFRs) within a traditional clinical workflow. For this purpose, the authors implemented a framework application in C# and .NET on a Tablet-PC. A usability study was carried out to gain insight into the acceptance and usability of the biometric signature. Good end user acceptance and usability can only be obtained by providing simple operation (good user guidance), very short response times and, where possible, low rejection rates. In order to make an application successful, a clear increase in value must be immediately apparent to the end user.

1 Introduction

The law in Austria demands that all Medical Doctor's certificates (Diagnostics Findings Report, DFR) are authenticated ("vidiert" in German, from lat. videre = to check visually). The interpretation of the KALG (Styrian Hospital Law paragraph 31, section 2, which refers to paragraph 13 section 2) does not specifically state that this must take the form of a handwritten or personal signature; however, the importance of determining the signatory and the possibility of tracing this person is made clear. No Doctor's certificates may be sent out without this authentication.

The medical profession is traditionally accustomed to providing this authentication by means of a hand written signature, which has always been accepted as a very safe method of identification. Every other procedure rapidly incurs rejection: Passwords can be forgotten, ID cards can be lost, fingerprints are impractical within the clinical workflow (gloves), retina scan and iris scan are unusual and digital signatures are laborious.

2 Initial Situation

At the Pathology Department of the University Hospital in Graz, a Medical Doctor (MD) controls and signs up to 30 certificates at a time, several times a day.

The present solution consists of a reiterated input of the doctor's username and password. However, this is an unsatisfactory solution from the point of view of both Medical Doctors and Lawyers. In addition, the continual signing of papers represents an enormous expenditure of effort on the part of the MD's. Furthermore, when the system later converts to electronically transmitted documents, the establishment of an electronic signature will become inevitable and make the printing of the document, together with the extra work of forwarding it by post, unnecessary while retaining the individual signature as the method of authentication.

The Pathology attaches importance to the fact that their referrers still receive a controllable and recognizable signature on their electronic diagnoses report. Furthermore, this identification must also remain verifiable for many years. Therefore, the method utilized is crucial in ensuring the simplification of the conversion while increasing usability. Special attention must also be placed on the psychological factors; only a method which the MD's accept and are willing to use can be integrated into any routine practice, while the visual examination of the document and signature play an important role in the referrer's acceptance, which must not be underestimated.

3 Identification Possibilities

Generally, we can differentiate between various possibilities of identification, which can be arranged in a four-quadrant field: Objects versus Biometrics and passive physical (bodily) characteristics versus active behavioural characteristics (see figure 1) (Guptaa et al. 2004).

Biometrics generally refers to the identification (or verification) of an individual by using certain physiological or behavioural characteristics or traits associated with the person (Jain et al. 1999). The term biometrics designates extremely diverse applications of mathematical statistics. However, by using biometrics it is possible to establish an identity based on *who you are,* rather than by *what you possess* (e.g. ID card) or *what you remember* (e.g. a password) (Jain and Ross 2004).

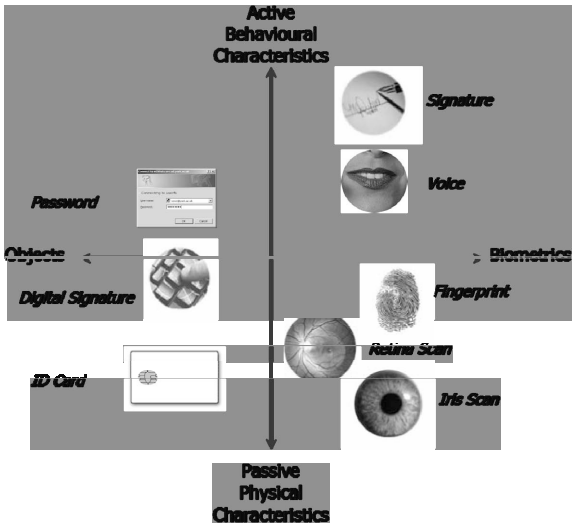

Figure 1: View of different identification possibilities

Biometric characteristics are a component of the users' personality. These characteristics are generally available, impractical to steal and can only be falsified with difficulty. Besides bolstering security, biometric systems enhance user convenience (Jain and Ross 2004). Some attributes of biometric characteristics include:

- Universality: everyone has a biometric characteristic;
- Singularity: the attributes of a biometric characteristic differ from person to person;
- Permanence: the biometric characteristics are durable;
- Measurability: biometric characteristics are mathematically, quantitatively easily detectable;
- Performance: with regard to accuracy, speed and robustness of a procedure;
- Acceptance: a biometric procedure is accepted by the end users;
- Security: a biometric system is relative secure against falsification.

How and where, which biometric system will be applied will depend most often on performance. However, the final decision about putting a specific identification possibility to work depends almost entirely on the application's purpose (Phillips et al. 2000).

4 Biometric Signature

Technically, the classical signature is referred to by the term *biometric electronic signature* or *biometric signature.* In comparison to other technologies, hand written signatures have some general advantages (Guptaa et al. 2004), (Jain et al. 2002):

- The signature can be automatically authenticated by analyzing dynamical parameters including the shape, speed, acceleration, stroke, pen pressure, pen removal, writing angle and timing information during the act of signing;
- Whereas recognition of iris, retina or fingerprints requires special and relatively expensive hardware to capture the image, a signature is respectively easy to confirm;
- Signatures are generally accepted by the general public as a common method of identity verification.

Since the evaluation of dynamic parameters represents the identification of a living person, the security against falsification is fairly high and the high error rate experienced recently by our users. In this connection, positive experiences have been made in the clinical centre at Ingolstadt (Germany), (Kleemann 2004).

At the time of writing of this paper, the most common method of entering signatures is by the use of a commercial graphic tablet or signature pad. However, in order to take full advantage of state-of-the-art mobile computing technology, we implemented special software for a Tablet PC.

5 Our Implementation

The electronic forms interface, similar in layout to the currently used printouts, was developed for signature using Microsoft® InfoPath 2003. On completion of the examination data input, an XML file containing the diagnostic data was created and placed before the physicians for control and signature.

Decisive for choosing this method was that an application to convert the doctors certificates to XML format, for the electronic document transmission, had already been developed and implemented within the clinics. This solution makes both the correction of the data possible and takes advantage of the implementation of the Soft Pro SignDoc® for InfoPath, which already exists, to make the input and control of the signature possible. The authentication of the signature is achieved by comparison with the physician's registered signature (Dimauro et al. 2004).

The development of a framework application was unavoidable in order to embed these solutions into our questionnaire. C# and .NET were chosen to enable and promote a synergy with other projects. These languages were used for the presentation, control and transfer of the Diagnostic Findings Report (DFR) certificate. The InfoPath form was developed from the current printed form, whereby the basic rules of good usability (for instance: minimal scrolling) were applied. Two solutions were substantialized, whereby, after controlling the docu-

ment, the Medical Doctor was given the choice of returning this for correction or signing and releasing the document. However, the solutions differ only in the *method of signing the documents.*

6 The Usability Study

6.1 Experimental Setting

During the current *on paper* signing process, the Medical Doctors work through a pile of printed DFRs, page for page, either signing and releasing the reports or correcting them by hand and returning them for retyping. The electronic solution, in which the users identify themselves by means of an account name and password, corresponds to the general methods currently used for identification in IT systems and/or user interfaces with authentication by means of digital signature. This process is known as *electronic signature.* Our solution, in which the physicians sign by means of a biometric signature, corresponds, to a large extent, to the natural, print and sign, process. This process is called: *biometric signature.* The two processes were compared to the *on paper* signing process and tested for usability (see section 7) in a real-life situation at the end-users workplaces (figure 2).

6.2 Participants, Methods and Tasks

For usability evaluations, five participants are usually sufficient to get reliable results (Virzi 1992), (Nielsen 1993), (Holzinger 2005). Subsequently, five selected Medical Doctors from the Department of Pathology were presented with fifteen examination reports to be controlled and released: five were printed on paper; five were on a Tablet PC in an application for *biometric signature* and five on a Tablet PC in an application *electronic signature.* The end users received a numerical password, similar to those used by cash card systems and digital signatures. All tests were filmed on video and timed with a stop watch.

After each of the 15 sessions, we asked the participants to answer a questionnaire asking what they liked and disliked most, what they would wish to be added, their opinion on signing DFRs in batches and how they found the handling of the Tablet PC. One week later, the tests were repeated and the pathologists interviewed.

The videos were examined by using INTERACT 7.0 analysis software; thus we were able to compare our observations and to determine the congruence between the individual analysis sessions.

Efficiency is one of the major aspects of the usability of a new software application. During our experiments, we concentrated particularly on the *time required to perform a specific task,* which is still the most important factor to measure the efficiency of an software application (Stary et al. 1997), (Stary and Peschl 1998).

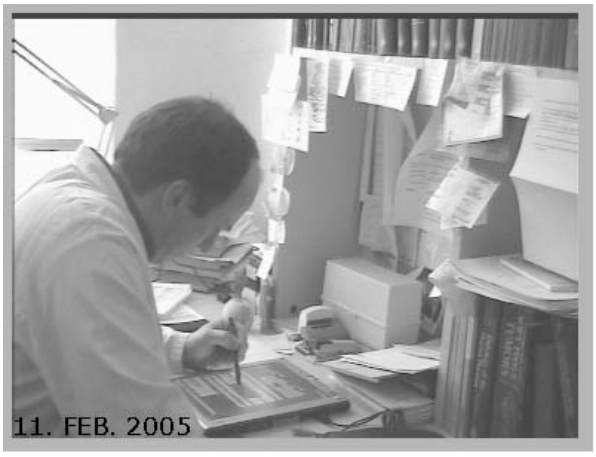

Figure 2: A Pathologist during a usability test session with our solution on a Tablet PC

6.3 Application Flow

To begin the procedure, the InfoPath form can either be started directly from a directory listing of the pathological reports or by use of the Launcher Program, which enables all the forms to be automatically displayed on the screen (see figure 3). This program observes the activity in the directory listings relevant to the pathological reports. Changes (such as a file transfer) can immediately be observed in the respective column. The forms can be opened separately with a double mouse click within the Launcher window. In this manner, it is possible to control the processed forms, for example, for a visual control of the signature. The form at the top of the directory list can be opened by pressing the button "Nächsten Befund öffnen" (open next document).

Within each form, it is possible to initiate a transfer of the form on closure, either to the signed and released directory or to a return for correction directory, the Launcher reacts to this process by starting the next report waiting for completion from the list on the screen. This procedure can be repeated until all reports have been controlled and transferred to another directory or until the program is terminated by the user. The root directory is C:\public\Befunde and the *Unsigned, Signed and To be Completed* directories direct subdirectories.

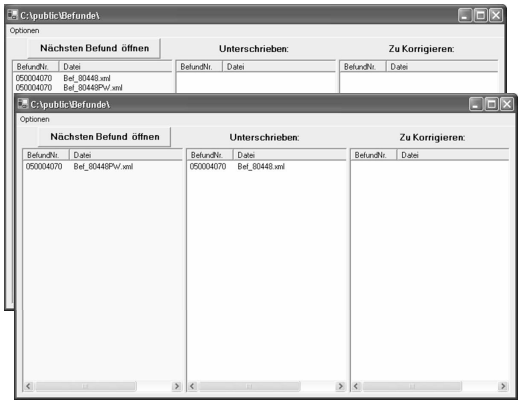

Figure 3: A view of the Launcher

In order to present both procedures (signing with a biometric signature and signing with username and password) rapidly, it was necessary to install two different form templates on the Tablet PC with two corresponding sets of test data. The forms and the test data were swapped by the use of batch jobs.

7 Findings & Discussions

From the experiments, a total of 150 measurements were taken. The results of the measurements can be seen in figure 4. The mean time necessary for the paper based workflow was slightly less at the second trial, one week later, which is definitely within variance, whereas the mean time of the electronic version was significantly less. Consequently the learnability of our software was satisfying. Although the mean time to perform the task was higher when using the electronic system, the participants liked the system generally.

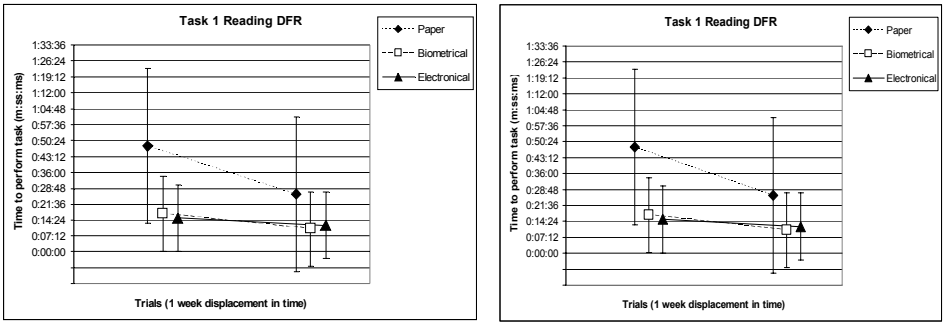

Figure 4: Reading and Signing DFR Trials

The biometric signature was perceived as natural by all participants. The greatest disadvantage with the password was the effort to memorize it and the unwieldy handling of the input. After the second trial, the software was subjectively felt to be slower by 3 participants although the response times were the same as in the first trial. A possible cause being that the novelty having worn off, natural impatience took over.

The arrangement of the fields was conform to the format of the electronic exchange interface used for the DFRs, not however to the print format which the MDs usually signed. This was felt to be disturbing and slowed the process down. In the same way, the switch from keyboard to stylus was disturbing. The waiting time between the appearance of the reports on the screen was too long, both from the developer's and the user's point of view.

Activating the mouse's *Double-Click* function caused difficulty for four of the five end users taking part in the test. The single mouse click caused less difficulty but was not completely problem free either. The *right mouse button* function, which was integrated into the stylus, was unintentionally activated by three of the five end users, despite previous warnings. Three end users were decidedly in favor of a separate keyboard to enter the password, since they found the Tablet PC's screen keyboard unpleasant to use.

Three end users considered the display quality bad; only one end user tilted the Tablet PC in an attempt to influence the light reflection factor. The end users were completely unaccustomed to handling Tablet PCs.

Four end users endorsed a batch signing process; one end user was against this on the grounds of protecting the direct connection between the DFR and the corresponding patient. He wished to avoid the de-personalization of a production line. Only one end user wanted to see the document after signing it, he considered this form of the signature positive.

The sequential report control workflow varied for printed and electronic forms; the focus of the pathologist remained on the paper in front of him. This meant that, while his hand was placing the signed copy on the *completed* pile, his eyes were already on the next report. With both electronic variations, the focus could only be on the screen. One end user conscientiously signed only a few reports during the first trial, due to finding medically incorrect formulations. He returned these for correction, despite being informed that the reports used in the test had already been signed and forwarded to the referrers. Two end users wanted to make alterations directly on the Tablet PC. Two end users wanted to know whether it would be possible to retain signed reports, rather that sending them off directly. This is interesting, because one of the main benefits of this system is exactly this method of immediate forwarding of the reports to the referrer. Several end users expressed concern as to whether the printed reports were to be forwarded by post after signing. This could be due to a strong identification with the classical signature procedure. Interesting in this context is the fact that none of the end users were concerned as to the reliability of forwarding the electronic reports to the referrers after signature.

8 Conclusion and Future Work

This study explored the extent to which the MD's were supported in their workflow by the implementation of the biometric signature together with the electronic report and to what extent an appropriate solution can increase the worth of this support. A new method must not involve a greater expenditure of time for learning, perception or execution than the previously employed method of the handwritten signature on documents. On the contrary, efficiency should be increased by the application of time-saving innovations, such as grouping (a number of documents are controlled and marked for signing) so that the single signature validates all documents. In this manner, it is possible for the MD to sign a number of examination reports with one signature, which is a definite increase in efficiency and a time-saver for the physician. Further investigations into the security and efficiency aspects of biometric signatures will require the enlargement of the application to include every aspect involved with biometric signatures. Here, Usability Engineering methods will be essential.

References

Dimauro, G.; Impedovo, S.; Lucchese, M. G.; Modugno, R.; Pirlo, G. (2004): *Recent Advancements in Automatic Signature Verification.* Paper presented at the Ninth International Workshop on Frontiers in Handwriting Recognition (IWFHR'04) Tokyo, 179-184.

Guptaa, A.; Tung, Y. A.; Marsden, J. R. (2004): Digital signature: use and modification to achieve success in next generation e-business processes. *Information & Management,* 41, 561-575.

Holzinger, A. (2005) Usability Engineering for Software Developers. *Communications of the ACM,* 48, 1, 71-74.

Jain, A. K.; Bolle, R.; Pankanti, S. (Eds.) (1999): *Biometrics: Personal Identification in a Networked Society,* Dordrecht (The Netherlands), Kluwer.

Jain, A. K.; Griess, F. D.; Connell, S. D. (2002): On-line signature verification. *Pattern Recognition,* 35, 12, 2963-2972.

Jain, A. K.; Ross, A. (2004): Multimodal interfaces that flex, adapt, and persist. *Communications of the ACM,* 47, 1, 34-40.

Kleemann, T. (2004): Hospital Increases Productivity with Integrated Desktop Tools to Automate Workflow.

Nielsen, J. (1993): *Usability Engineering,* San Francisco, Morgan Kaufmann.

Phillips, P. J.; Martin, A.; Wilson, C. L.; Przybocki, M. (2000): An introduction to evaluating biometric systems *IEEE Computer,* 33, 2, 56-63.

Stary, C.; Peschl, M. F. (1998): Representation Still Matters – Cognitive Engineering and Task-Based User Interface Development. *Behavior and Information Technology,* 17, 6, 338-360.

Stary, C.; Vidakis, N.; Mohacsi, S.; Nagelholz, M. (1997): *Workflow-Oriented Prototyping for the Development of Interactive Software.* Paper presented at the IEEE COMPSAC 1997, 530-535.

Virzi, R. A. (1992) Refining the test phase of usability evaluation: how many subjects is enough?. *Human Factors,* 34, 4, 457-468.