1

Reliability of Fingerprint Biometry (Weibull Approach)

Robert Brumnik[1], Iztok Podbregar[2] and Teodora Ivanuša[2]
[1]*Metra inženiring Ltd.*
[2]*University of Maribor,*
Faculty of Criminal Justice and Security
Slovenia

1. Introduction

Biometrics refers to the identification of a person on the basis of their physical and behavioural characteristics. Today we know a lot of biometric systems which are based on the identification of these, for everyone's unique identity. Some biometric systems include the characteristics of: fingerprints, hand geometry, voice, iris, etc., and can be used for identification. Most biometric systems are based on the collection and comparison of biometric characteristics which can provide identification. This study begins with a historical review of biometric and radio frequency identification (RFID) methods and research areas. The study continues in the direction of biometric methods based on fingerprints. The survey parameters of reliability, which may affect the results of the biometric system in use, prove the hypothesis. A summary of the results obtained the measured parameters of reliability and the efficiency of the biometric system we discussed.
Each biometric system includes the following three processes: registration, preparation of a sample, and readings of the sample. Finally the system provides a comparison of the measured sample with digitized samples stored in the database. Also in this chapter we show the optimization of a biometric system with neural networks resulting in multi-biometric or multimodal biometric systems. This procedure combines two or more biometric methods in the form of a more efficient and more secure biometric system.
During our research we carried out a »Weibull« mathematical model for determining the effectiveness of the fingerprint identification system. By means of ongoing research and development projects in this area, this study is aimed at confirming its effectiveness empirically. Efficiency and reliability are important factors in the reading and operation of biometric systems. The research focuses on the measurement of activity in the process of the fingerprint biometric system, and explains what is meant by the result achieved.
The research we refer to reviews relevant standards, which are necessary to determine the policy of biometric measures and security mechanisms, and to successfully implement a quality identification system.
The hypothesis, we have assumed in the thesis to the survey has been fully confirmed. Biometric methods based on research parameters are both more reliable and effective than RFID identification systems while enabling a greater flow of people.

2. Theoretical overview

Personal identification is a means of associating a particular individual with an identity. The term "biometrics" derives from Bio,(meaning "life" and metric being a "measurement". Variations of biometrics have long been in use in past history. Cave paintings were one of the earliest samples of a biometric form. A signature could presumably be decifered from the outline of a human hand in some of the paintings. In ancient China, thumb prints were found on clay seals. In the 14th century in China, biometrics was used to identify children to merchants (Daniel, 2006). The merchants would take ink and make an impression of the child's hand and footprint in order to distinguish between them. French police developed the first anthropometric system in 1883 to identify criminals by measuring the head and body widths and lengths. Fingerprints were used for business transactions in ancient Babylon, on clay tablets (Barnes, 2011).

Throughout history many other forms of biometrics, which include the fingerprint technique, were utilized to identify criminals and these are still in use today. The fingerprint method has been successfully used for many years in law enforcement and is now a very accurate and reliable method to determine an individual's identity in many security access systems.

The production logistics must ensure an effective flow of material, tools and services during the whole production process and between companies. Solutions for the traceability of products and people (identification and authentication) are very important parts of the production process. The entire production efficacy and final product quality depends on the organization and efficiency of the logistics process. The capability of a company to develop, exploit and retain its competitive position is the key to increasing company value (Polajnar, 2005). Globalization dictates to industrial management the need for an effective and lean manufacturing process, downsizing and outsourcing where appropriate. The requirements of modern times are the development and use of wireless technologies such as the mobile phone. The intent is to develop remote maintenance, remote servicing and remote diagnostics (Polajnar, 2003). With the increasing use of new identification technologies, it is necessary to explore their reliability and efficacy in the logistics process. With the evolution of microelectronics, new identification systems have been achieving rapid development during the last ten years thus enabling practical application in the branch of automation of logistics and production. It is necessary to research and justify every economic investment in these applications.

Biometrics is not really a new technology. With the evolution of computer science the consecutive manner in which we can now use these unique features with the aid of computers contemporaneousness. In the future, modern computers will aid biometric technology playing a critical role in our society to assist questions related to the identity of individuals in a global world.

"Who is this person?", "Is this the person he/she claims to be?", "Should this individual be given access to our system or building?", etc. These are examples of the every day questions asked by many organizations in the fields of telecommunication, financial services, health care, electronic commerce, governments and others all over the world.

The requirements and needs of quantity data and information processing are growing by the day. Also, people's global mobility is becoming an everyday matter as is the necessity to ensure modern and discreet identification systems from different real and virtual access points on a global basis.

3. Quality parameters of biometrics technologies (ER, FRR, FAR, SL, EC)

In order to adopt biometric technologies such as fingerprint, iris, face, hand geometry and voice etc., we will evaluate some factors including the ease of use, error rate and cost. When we evaluate the score for each of the biometric technologies, we find that there is a range between the upper and lower scores for each item evaluated. Therefore we have to recognize that there is no perfect biometric technology.
For example, if a biometric system uses fingerprint technology, we will determine several factors as follows:

a. What is the error rate (ER), as we use the False Acceptance Rate (FAR) or False Rejection Rate (FRR) that the system will allow?
b. False Acceptance Rate (FAR) is the probability that a biometrics verification device will fail to reject an impostor.
c. False Rejection Rate (FRR) is the probability that a biometrics verification device will fail to recognize the identity, or verify the claimed identity, of an enrolee.
d. What is the security level (SL) to protect privacy and fraud that the system will require?
e. Which environmental conditions (EC) for sensing fingerprints will be considered as dry or wet and dusty on the glass of a fingerprint scanner?

In the last ten years, new identification systems have been achieving extremely rapid development. The evolution of microelectronics has enabled practical application in the branch of automation of logistics and production. It is necessary to research and justify every economic investment in these applications. In this work the most important quantitative characteristics of reliability are explained. The authors also show the methodology for defining the reliability and efficacy of biometric identification systems in the process of identification and provide experimental research of personal identification systems[1] based upon reliability and efficacy parameters. Furthermore, a real identification system was upgraded based on automation and informatization.
In this article based on Biometric Identification Systems, we:

- show the availability and efficacy of analyses in the identification processes,
- extend reliability estimations of biometric identification systems based on significant reliability characteristics,
- provide a contribution to science by researching the biometric automated identification process to ensure optimal procedures.

A review of scientific databases shows that the area of assessing the reliability of identification systems in the process of production and logistics is not well explored. In modern production and logistics processes (automobile industry, aerospace industry, pharmacy, forensics, etc.) it is necessary to have fast and reliable control over the flow of people.

4. Defining the problem and research parameters

The availability of a production-logistic process is the probability that the system is functioning well at a given moment or is capable of functioning when used during certain

[1] Personal Identification Systems; Recent events have heightened interest in implementing more secure personal identification (ID) systems to improve confidence in verifying the identity of individuals seeking access to physical or virtual locations in the logistic process. A secure personal ID system must be designed to address government and business policy issues and individual privacy concerns. The ID system must be secure, provide fast and effective verification of an individual's identity, and protect the privacy of the individual's identity information.

circumstances. Reliability, by definition, is probability (capability) of the system to perform under the stated conditions defined by function and time (Hudoklin & Rozman, 2004). It is one of the most important characteristics of efficacy of identification systems and has an impact on safety and efficiency of the system. Military standard MIL HDBK 217 is also used to estimate the inherent reliability of electronic equipment and systems based on component failure data. It consists of two basic prediction methods: Parts-Count Analysis and Part-Stress Prediction. Increasing the system's reliability means less improper use, greater safety, fewer repair procedures and shorter identification times, consequently causing higher system availability. Implementing higher reliability in early development phases and its assurance during the use of the identification system, requires the knowledge of methods and techniques of reliability theory and their interactions.
Many different characteristics are used to measure the reliability of identification systems and their components. Some of them are connected to time functions others represent average time functions. Which of these characteristic are relevant in specified cases depends on the set goals, selected method of analysis, and the availability of data.
Characteristics of reliability are based on mean time intervals to the occurrence of failure. Time to failure is a random magnitude and we will mark it with the symbol "t_i". In this article we give definitions and statistical estimations of basic reliability characteristics. Reliability characteristics used in this research are:

- MTTF - mean time to failure
- MTBF - mean time between failures
- MTTR - mean time to repair
- F(t) - unreliability function
- λ(t)- failure rate
- β - shape parameter
  a. β<1 temporary failure frequency λ(t) decreases (early period, system implementation)
  b. β=1 temporary failure frequency λ(t) is constant (normal system operation)
  c. β >1 temporary failure frequency λ(t) increases (exploitation, ageing)

The shape parameter (β) changes the configuration of the temporal distribution of operational failures.

5. Quantitative reliability characteristics

The theory of reliability was obtained by the authors Hudoklin and Rozman (2004):
Unreliability function F(t) is defined by the equation:

$$F(t) = P(X \le t) \tag{1}$$

F(t) is therefore the probability of a system to become non-functional in the interval between 0 and t.
If we observe a number of systems, or system components, we can calculate the statistical estimation for the unreliability function by the equation:

$$\hat{F}(t) = \frac{N_0 - N(t)}{N_0} \tag{2}$$

N(t) - number of working/functional samples in the interval (0,t)

N0 - number of samples at the start of observation at t=0
Reliability function R(t) is complementary to the unreliability function. We can define it using the equation:

$$R(t) = 1 - F(t) = P(X > t) \tag{3}$$

R(t) is the probability that a system or component will become non-functional after a time period t. We can define a statistical estimation of the reliability function using the equation:

$$\widehat{R}(t) = \frac{N(t)}{N_0} \tag{4}$$

The product of the time to failure function and dt is the probability of the system or its component to become non-functional in the interval (t, t+Δt). We can calculate the function F(t) by differentiation of the unreliability function by time:

$$F(t) = \frac{dF(t)}{dt} \tag{5}$$

The statistical estimation for f(t) can be calculated with the equation:

$$\widehat{f}(t) = \frac{N(t) - N(t + \Delta t)}{N_0 \cdot \Delta t} \tag{6}$$

Where Δt is interval (t, t+Δt).
Product of Failure rate λ(t) and dt is the conditional probability of a system/part of a system to become non-functional in the interval (t, t+Δt).Momentary frequency of failure rate can be written as:

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{7}$$

The statistical estimation for λ(t) is defined with the equation:

$$\hat{\lambda}(t) = \frac{N(t) - N(t + \Delta t)}{N(t) \cdot \Delta t} \tag{8}$$

The mean time to failure (MTTF) of the system reliability is a characteristic and not a function of time, but the average value of the probability density function for the times to failure:

$$MTTF = \int_0^\infty t f(t) dt = \int_0^\infty R(t) dt \tag{9}$$

An estimate point for the mean time to failure (MTTF) is calculated for n times to failure with the estimator:

$$\widehat{MTTF} = \frac{1}{n} \sum_{i=1}^{n} t_i \tag{10}$$

During normal operation, the MTTF is equal to:

$$MTTF = \frac{1}{\lambda}. \tag{11}$$

For many systems, or system parts, the function λ(t) has a characteristic "bathtub" configuration (Figure 1.). The life cycle of systems can be divided into three periods: an early damaging period, a normal working period and an ageing or exploitation period. In the first period λ(t) decreases, in the second period λ(t) is constant, and in the third period λ(t) rises.

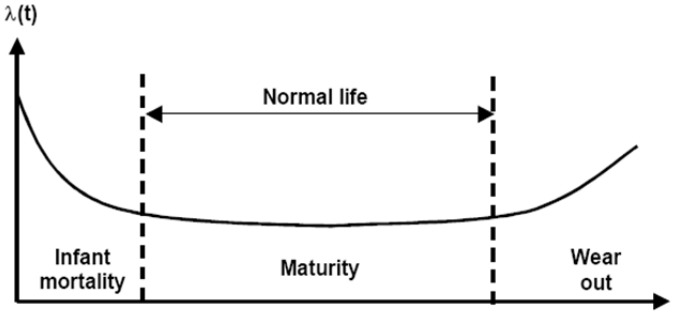

Fig. 1. "Bathtub" curve (FIDES, 2006).

5.1 Reliability of biometric identification systems

Definitions used in reliability calculation of biometric identification systems and terminology:

- FAR[2] is defined as the percentage of identification instances in which false acceptance occurs,
- FRR[3] is defined as the percentage of identification instances in which false rejection occurs,
- Mean time to failure (MTTF), mean time between failures (MTBF) and mean time to repair (MTTR),
- classification of failures,
- failures data bases.

In biometric methods, in contrast to the classic methods of identification, probability needs to be considered. All sensors are subject to noise and errors. The largest problem is the development and implementation of a safe crypto-algorithm. All limitations are summarized in the two terms: FRR and FAR. If a system is highly sensitive, the FAR value is low, but FRR is higher. In a system of low sensitivity the situation is reversed. Such a system is accepted by almost everyone (FAR>FRR). It is therefore necessary to make a compromise in the sensitivity of a system. It can also be regulated so that the FAR and FRR values are equal, the so-called EER (Equal Error Rate). Lower EER means a more accurate system. In an application where the speed of identification is more important than safety (e.g. hotel rooms), the high FAR value

[2] FAR (False Aceptance Rate); This can be expressed as a probability. For example, if FAR is 0.1 percent, it means that on average, one out of every 1000 impostors attempting to breach the system will be successful.
[3] FRR (False Recetion Rate); For example, if FRR is 0.05 percent, it means that on average, one out of every 2000 authorized persons attempting to access the system will not be recognized by that system.

can be allowed (Hicklin et al., 2005). Graphic presentation of both errors depending on the size of the error threshold of biometric system can be seen in Figure 2.

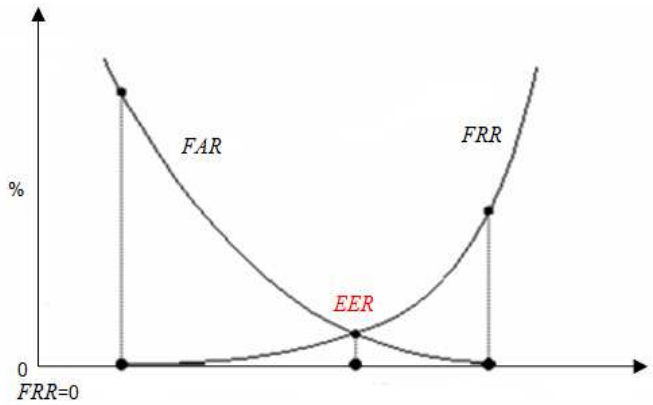

Fig. 2. Calculating EER from FAR – FRR intersection.

5.2 Usability and reliability characteristics of a biometric system reader

To fully understand user-centered design, it is essential to understand the features inherent in a usable system. Usability helps to ensure that systems and products are easy to learn, effective to use and enjoyable from the user's perspective. This is defined as: "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." (ISO 13407:1999). Additional attributes of usability that may also be considered include:

- effective to use (effectiveness),
- efficient to use (efficiency),
- enjoyable to use (satisfaction),
- easy to learn (learnability) and
- easy to remember (memorability).

The table on the next page lists each of these usability goals and provides a short description of each, along with a few questions for biometric system designers to consider. Usability testing not only provides insights into users' behaviour, but it also allows project teams to quantifiably measure the success of a system, including capturing metrics such as error rates, successful performance on tasks, time to complete a task, etc. (NIST, 2008). For quantitative testing, many teams use the Common Industry Format (CIF) (ISO/IEC 25062:2006) to document the performance of the system. The CIF provides a standard way for organizations to present and report quantitative data gathered in a usability test, so that it can later be compared to the results gathered in subsequent tests.

A review of the literature and standards for design and anthropometric measurements provided guidance on proper angles for fingers or palm placement. Standards focus on line of sight and reach envelopes including sloping control panels for cockpits or nuclear power stations (NISTIR 7504).

To determine the reliability characteristics, we used the Weibull model, which is useful in cases where $\lambda(t)$ cannot be illustrated by the constant function. For the resulting measurements we will take advantage of Weibull analysis, which provides a simple

graphical method. The analysis will be provided (with a reasonable error analysis) to obtain good estimates of parameters, despite the small sample size (in our case, thirty pieces of biometric modules). These solutions enable us to identify early signs of potential problems, so we can prevent more serious systemic failures and predict the maintenance cycle (increasing the availability of the system). The study was of a relatively small sample size also enabling cost-effective test curves. Testing is complete when the observed system fails (sudden failure) in each of the three groups (the first module of each series) biometric reader components and proceeds with the Weibull analysis.

Reliability of a biometric system depends on three factors (Chernomordik, 2002):

- uniqueness and repeatability, which means that the characteristic used should provide for different readings for different people, and the readings obtained for the same person at different times and under different conditions should be similar,
- reliability of the matching algorithm and
- quality of the reading device.

Failures, which we have taken into account in determining the characteristics of MTTF and MTTR of a biometric system (Table 1):

- failure of the software (the inability to read the sample),
- failure of hardware (biometric reader, PCBs) and
- errors due to sensor reading settings: FAR, FRR.

Ser. No.	Time to first failure (days)	Time to second failure (days)	Time to third failure (days)	Average value (days)
36365	53	89	88	88,8
36359	60	106	73	
36366	87	106	88	
36364	86	161	88	
36368	102	130	13	
36369	99	102	98	
36360	56	150	93	
36345	57	90	126	
36381	81	52	117	
36384	90	65	105	
Ser. No.	Time to first repair (days)	Time to second repair (days)	Time to third repair (days)	Average value (days)
36365	1	1	1	1,2
36359	0	1	0	
36366	1	3	2	
36364	1	0	1	
36368	1	3	1	
36369	2	1	1	
36360	2	1	1	
36345	3	1	1	
36381	2	1	1	
36384	2	0	1	

Ser. No.	Time to restart (days)	Time to restart (days)	Time to restart (days)	Average value (days)
36365	56	90	89	90,1
36359	60	105	73	
36366	88	107	90	
36364	85	161	89	
36368	103	133	16	
36369	101	103	99	
36360	58	151	96	
36345	60	91	127	
36381	83	53	118	
36384	92	65	106	

Table 1. Data for the MTTF, MTTR estimates determine for biometric system.

TIME TO FIRST FAILURE (days)										
i	1	2	3	4	5	6	7	8	9	10
t_i (days)	53	56	57	60	81	86	87	90	99	102
F_i	7	16	26	36	45	55	64	74	84	93
TIME TO SECOND FAILURE (days)										
i	1	2	3	4	5	6	7	8	9	10
t_i (days)	52	65	89	90	102	106	106	130	150	161
F_i	7	16	26	36	45	55	64	74	84	93
TIME TO THIRD FAILURE (days)										
i	1	2	3	4	5	6	7	8	9	10
t_i (days)	13	73	88	88	88	93	98	105	117	126
F_i	7	16	26	36	45	55	64	74	84	93

Table 2. The times to failure and the associated estimates points for F(t) of the biometric system.

TIME TO FIRST ACTIVE REPAIR (days)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	0	1	1	1	2	2	3	2	2
TIME TO SECOND ACTIVE REPAIR (days)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	1	3	0	3	1	1	1	1	0
TIME TO THIRD ACTIVE REPAIR (days)										
i	1	2	3	4	5	6	7	8	9	10
t_i	1	0	2	1	1	1	1	1	1	1

Table 3. The times of active repairs for the biometric module.

Assuming that the times to failure in Tables 2 are exponentially distributed couples (t_i, F_i). We join them together and rank them in Table 4 and estimate parameters β and η for a biometric system with the software Weibull++7.
Time to first failure is β = 4.6 and η = 72, while they are behind the times to failure of another parameter β = 3.23 and η = 117.2. For the third time to failure, the values of parameters β = 2 and η = 101. Table 4 shows the ranking values of times to failure of biometric systems (ti; i=1,2,3) and times to failure of the biometric identification system and the corresponding estimation point estimates of F(t).

biometric module		
i	t_i (days)	F_i
1	13	2,3
2	52	5,6
3	53	8,9
4	56	12,2
5	57	15,5
6	60	18,8
7	65	22,0
8	73	25,3
9	81	28,6
10	86	31,9
11	87	35,2
12	88	38,5
13	88	41,8
14	88	45,1
15	89	48,4
16	90	51,6
17	90	54,9
18	93	58,2
19	98	61,5
20	99	64,8
21	102	68,1
22	102	71,4
23	105	74,7
24	106	78,0
25	106	81,3
26	117	84,5
27	126	87,8
28	130	91,1
29	150	94,4
30	161	97,7

Table 4. Ranking times to failure for the biometric system and estimation point estimates of F(t).

For the biometrics module we provide an estimated point of the average time of repairs:

$$M\hat{T}TR = \frac{1}{r}\sum_{i=1}^{r} t_i = \frac{1}{30}(15+12+10) = \quad 1,2 \; days$$

Estimates point for the availability of a biometric module for the period of observation is:

$$\hat{A} = \frac{MTTF}{MTTF + MTTR} = \frac{88,8}{88,8+1,2} = 0,987$$

With the Weibull++7 analysing tool we modeled probability density for time to failure of a biometric system with a distribution law and with the Weibull parameters β and η (Figure 3). At 100% probability, a failure of a biometric system, appears at β = 2.8 and η = 101.7.

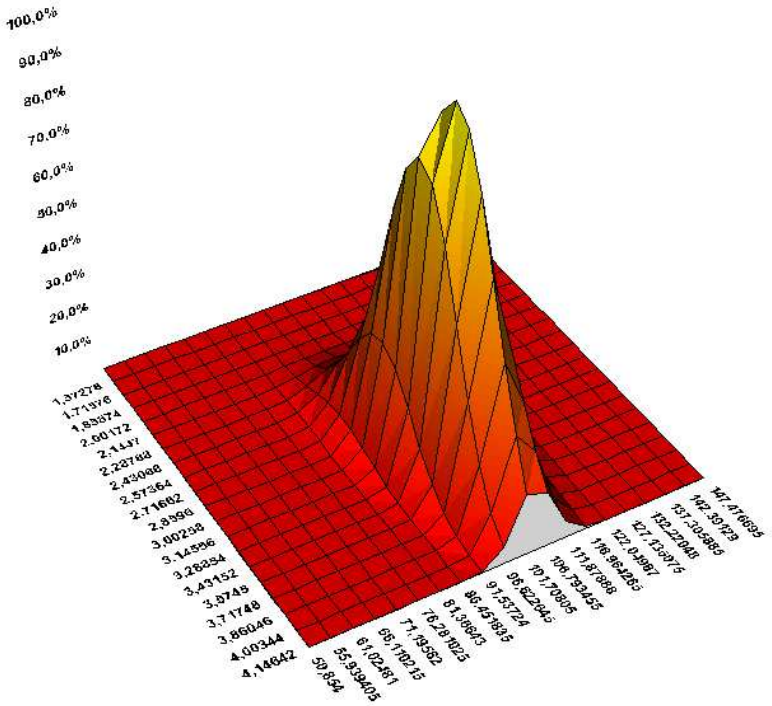

Fig. 3. Weibull model of failure appear for biometric system.

5.3 MTTF model calculation of system with two equivalent parts in parallel configuration

In practice, a request is made for the smooth functioning of the identification system, despite the likelihood of failure of a biometric card reader (airports, local government units, police stations, etc.). To increase the reliability of the biometric system and ensure the continuous operation despite the failure, we can associate two equivalent unit biometric module dynamic readings in the event of termination of the first reader to function by another

reader. We will show the probability graph for the biometric reader unit, which will be tied in parallel to achieve better reliability parameters of the identification system. Consider a system consisting of two equivalent units. From the failure rate λ of each dynamic reading module, the frequency of repairs and μ conclusions we can construct a corresponding probability graph for reliability (Figure 4) and availability (Figure 5) in the passive parallel configuration with an absolutely reliable switch.

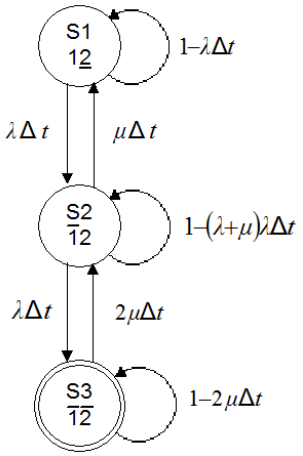

Fig. 4. Probability graph for the availability of two parallel biometric components.

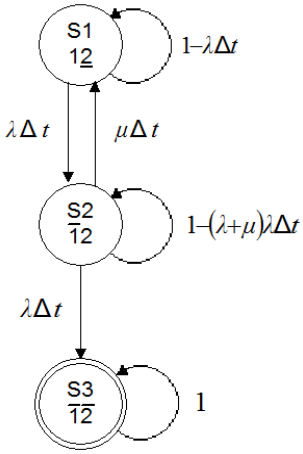

Fig. 5. Probability graph for the reliability of two parallel biometric components.

The probability graph for the availability of two parallel biometric components is shown in Figure 4. S3 state no longer abyss, the probability of transition from state S3 to state S2 is 2μΔt. The probability graph for the reliability of two parallel biometric components is shown in Figure 5.

6. Summary and future work

The reliability and availability of assessing identification systems is an area that is very important and essential in choosing an access control system. In this article we have used statistical methods for assessing the effectiveness of biometric access by assessing the reliability and availability of all parts of the identification system with the Weibull model. The Weibull function of two variables well describes the characteristics of reliability of biometric identification systems. Data visualization using graphs give a clear correlation between the measurements and the Weibull distribution. The greater the slope of the line, which means a higher Weibull parameter β, the greater the reliability of the products and also the lower the risk (with the same parameter η) that the identification system will terminate in shorter time. This is due to enhancing the value of the Weibull parameter leading to longer times to failure. In assessing the statistical parameters we must be aware that this appraisal is a deviation from actual values. It is clear that the expected interval of 30 data (with 90-percent confidence) for real values of the Weibull parameter allowing for a variation of about 10 percent of the calculated values of this parameter, while calculating the second parameter, the Weibull distribution is more reliable.

By calculating estimated times to failure and between failures of identification systems according to the Weibull methodology, we arrive at the following results for the assessment of the reliability and availability:

1. Estimated time to failure (reliability), of a biometric system by calculating the characteristics $MTTF_S$ = 88.8 days.
2. Estimated time to repair of a biometric system by calculating the characteristics $MTTR_S$ = 1.2 days.
3. Assessment of the availability of the biometric system by calculating the characteristics of A_S = 0.987.

During our research we carried out different models for estimating reliability and availability, which were designed using the Weibull approach. As a novelty in the field of design reliability estimates of the identification system, we also designed and applied a graphic Weibull model, which is independent of the calculated Weibull method and serves to check the calculations of the Weibull model. In the application model in the field of biometrics, we discussed the usefulness in a real domain.

The usefulness of biometric systems is shown in identification-logistic environments where personal identification is needed. From this research it is evident that the ageing period of biometric systems begins relatively quickly. The results also show that the availability of biometric identification systems is therefore lower and maintenance costs are higher. The functional and ergonomic advantages of biometry are clear because there is neither the need for cards nor any other elements of identification in the identification process. The use of biometric systems will make identification simple and at the same time increase reliability due to non-transferability of identification elements (e.g. fingerprints) and prevent improper use.

It can be expected that Slovenia will attain biometric technology despite the doubts expressed by some institutions (Office for Personal Data Protection). Many open ethical questions arise, mostly regarding human personality, privacy and control. However research such as this on reliability and availability show, unequivocally, that biometric technology has an advantage both in practical use and data safety. Not only do usability improvements lead to better, easier-to-use products, they also lead to improved user

performance and satisfaction as well as substantial cost savings. By designing a biometric system with usability in mind, development teams can enhance ease of use, reduce system complexity, improve user performance and satisfaction, and reduce support and training costs.

Personal responsibility and accuracy in fields such as legislation, regulation adjustment, and production and supply chain management in global technical operations are more easily controlled using automated identification. With the automation of identification there are also possibilities for merging and comparing current process data with that from integral information systems (ERP, MRII, etc.) or other business applications.

7. References

Barnes, J. G. (2011). History, *The Fingerprint Sourcebook*. Retrieved 09.01.2011 on: http://www.ncjrs.gov/pdffiles1/nij/225321.pdf

Daniel, G. (2006). *Biometrics - The Wave of the Future?* Retrieved 29.02.2011 on: http://www.infosecwriters.com/text_resources/pdf/Biometrics_GDaniel.pdf

Hicklin, A.; Watson, C. & Ulery, B. (2005). The Myth of Goats: How many people have fingerprints that are hard to match?, *NIST Interagency Report 7271*.

Hudoklin, A. & Rozman, V. (2004). *Reliability and availability of systems human-machine*. Publisher: Moderna organizacija, Kranj.

Polajnar, A. (2005). Excellence of toolmaking firms : supplier - buyer - Toolmaker, *Collection of Conference consultation*, Portorose, 11.-13. October 2005.

Polajnar, A. (2003) Exceed limits on new way : supplier - buyer – toolmaker, *Collection of Conference consultation*, Portorose, 14.-16. october 2003.

MIL-HDBK-217, *Reliability Prediction of Electronic Equipment*. U.S. Department of Defense. Retrieved 09.02.2011 on: http://www.itemuk.com/milhdbk217.html

FIDES (2006). *Nature of the Prediction*. Retrieved 29.01.2011 on: http://fides-reliability.org/Default.aspx?tabid=94

Chernomordik, (2002). *Biometrics: Fingerprint based systems*. Retrieved 24.01.2011 on: http://biometrica.ru/root/?Itemid=49&id=126&option=com_content&task=view&lang=en

ISO 13407 (1999). *Human-centred design processes for interactive systems*. Retrieved 24.01.2011 on: http://zonecours.hec.ca/documents/A2007-1-1395534.NormeISO13407.pdf

ISO/IEC 25062 (2006). *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability test reports*. Retrieved 22.01.2011 on: http://webstore.iec.ch/preview/info_isoiec25062%7Bed1.0%7Den.pdf

NIST (2008). Ensuring Successful Biometric Systems, *Usability & Biometrics*. Retrieved 22.01.2011 on: http://zing.ncsl.nist.gov/biousa/docs/Usability_and_Biometrics_final2.pdf

NISTIR 7504 (2008). *Usability Testing of Height and Angles of Ten-Print Fingerprint Capture*. Retrieved 18.02.2011 on: http://zing.ncsl.nist.gov/biousa/docs/NISTIR-7504%20height%20angle.pdf

Biometric Systems, Design and Applications

Edited by Mr Zahid Riaz

ISBN 978-953-307-542-6
Hard cover, 262 pages
Publisher InTech
Published online 21, October, 2011
Published in print edition October, 2011

Biometric authentication has been widely used for access control and security systems over the past few years. The purpose of this book is to provide the readers with life cycle of different biometric authentication systems from their design and development to qualification and final application. The major systems discussed in this book include fingerprint identification, face recognition, iris segmentation and classification, signature verification and other miscellaneous systems which describe management policies of biometrics, reliability measures, pressure based typing and signature verification, bio-chemical systems and behavioral characteristics. In summary, this book provides the students and the researchers with different approaches to develop biometric authentication systems and at the same time includes state-of-the-art approaches in their design and development. The approaches have been thoroughly tested on standard databases and in real world applications.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Robert Brumnik, Iztok Podbregar and Teodora Ivanuša (2011). Reliability of Fingerprint Biometry (Weibull Approach), Biometric Systems, Design and Applications, Mr Zahid Riaz (Ed.), ISBN: 978-953-307-542-6, InTech, Available from: http://www.intechopen.com/books/biometric-systems-design-and-applications/reliability-of-fingerprint-biometry-weibull-approach-

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821