Biometric system reliability as a important factor of influence on Chain of Custody of Digital Evidence

Zoran Ćosić
Director
“STATHEROS” d.o.o
Kaštel Stari, Split, Croatia
zoran.cosic@statheros.hr

Jasmin Ćosić
IT Section of Police Administration
Ministry of Interior of Una-sana canton
502.V.bbr br.2, Bihać, B&H
jasmin.cosic@mupusk.gov.ba

Miroslav Bača
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
miroslav.baca@foi.hr

Abstract. *Biometric recognition in a nowadays uses, raises important legal issues such as: remediation, authority, reliability, and, of course, privacy. The standard assumptions of the technologists who design new techniques, capabilities, and systems are very different from those embedded in the legal system. Legal precedent on the use of biometric technology for identification or verification of individuals, is growing, with some key cases going back decades and other more recent cases having raised serious questions about the admissibility of biometric (digital) evidence in court. In this paper authors is about to propose analysis of existing methodology for preserving chain of custody by an introduction of biometric vulnerability evaluation methodology as important factor of influence for integrity and acceptability in Court of Justice of presented Digital Evidence through preservation of Chain of Custody (CoC). Using UML modeling methodology authors are about to represent a framework which will describe essential phases for evaluation of admissibility process of digital evidence including a vulnerability assessment process of biometric system exposing issues on reliability of biometric system that can have influence on reliability of CoC.*

Keywords. biometrics, traits, characteristics, system digital evidence, chain of custody of digital evidence, chain of custody, digital evidence

1 Introduction

Biometric systems [1] are used increasingly to recognize individuals and/or regulate access to physical spaces, information, services, and to other rights or benefits, including the ability to cross international borders, usage of different consumers electronic applications such toys, kitchen equipment, doors and windows opening controls, pens with pattern writing recognition etc. Questions persist, however, about the effectiveness [2] of biometric systems as security or surveillance mechanisms, their usability and manageability, appropriateness in widely varying contexts, social impacts, effects on privacy, and legal and policy implications. The risk that even a flawless biometric technology might be misused necessarily represents rather a limitation to wide deployment of biometric systems. Various critics have pointed to a number of important risks regarding usability of biometric systems such as data base of biometrical samples, where is an undeniable risk of unauthorized access to this biometric data. One of possible countermeasure about this risk is a cancellable biometrics application. A crucial point about this risk is that it might translate into insecurity for those individuals whose data can now be accessed and used for purposes that would neither have predicted nor agreed to.

2 Biometric system reliability considerations through its vulnerabilities

Biometric system vulnerability considerations are including security [3] [2] considerations and assessment, which are critical to the design of any complex technical system, and biometric systems are no exception. In seeking process to understand the security issues of biometric systems, two security-relevant processes are of interest: (1) the determination that an observed trait belongs to a living human who is present and is acting intentionally and (2) the proper matching (or non-matching) of the observed trait to the reference data maintained in the system. In many applications, biometric systems are one component of an overarching security policy and architecture. Biometric systems pose also two kinds of security challenges. The first is the use of biometrics to protect-provide security for other information intensive systems. Assuming [4] that a biometrics system is a part of another complex system, the challenge also is the analysis and assessment of security, integrity, and reliability of the system itself. Information security research is needed that addresses the unique problems of biometric systems, such as preventing attacks based on the presentation of fake biometrics, the replay of previously captured biometric samples, and the concealment of biometric traits. Developing techniques for protecting biometric reference information databases to avoid their use as a source of fake biometrics is another area for such research. Decision analysis and threat modeling are other critical areas requiring research advances that will allow employing biometric systems more fully across a range of applications. Security challenges for biometric systems can be seen as stemming from two different views of such systems:(1) the use of biometric systems as a security mechanism to protect information systems or other resources and (2) vulnerabilities of the biometric system itself. First, it is necessary to determine if a biometric system [2] is an appropriate component for the application at hand at all. One needs to specify the problem to be solved by a particular biometric system in order to adequately assess its effectiveness and deal with the consequences of deployment. Conducting a threat analysis and developing threat models for the system that incorporates analysis of feasibility of threats against the resource being protected and against the system doing the protecting is an important component of understanding the problem. Decisions about whether and how to incorporate biometric approaches should consider their appropriateness and proportionality given the problem to be solved and the merits and risks of biometrics relative to other solutions and need to be considered by the broader information security community as well as within the biometrics community. Second, biometric systems are themselves vulnerable to attacks aimed at undermining their integrity and reliability. For password or token-based systems, a breach can usually be remediated by issuing a new password or token. Example of biometric system function in the matching and decisional process as described in section 1 can be shown as in Figure 1.

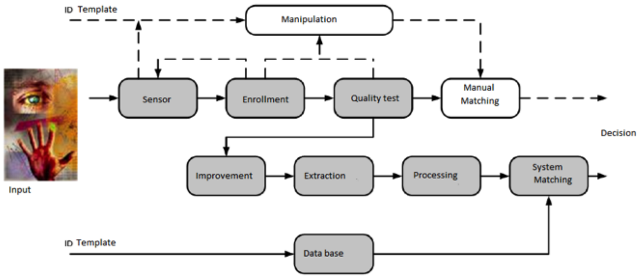


Figure 1. Matching and decisional process of a biometric system [4]

3 Biometric system reliability considerations

Biometric system, in a common usage, could be a source or container of a possible digital evidence [5] for a digital investigation process [6] [7] [8]. Each of particular phase in a digital investigation process can be consider as a step or component of the same, and lack in each of them can result as compromising factor of validity of a digital evidence and can heavily influence it's admissibility in court. Thus we can suppose ,so called, serial dependency of components of CoC DE [9]. Such dependency can be mathematically described as a serial dependence of components. Serial dependence of components of chain of custody of digital evidence can be depicted as follows:

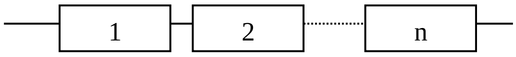


Figure 2. Components in serial dependence relationship

Where:
1,2,3… n – represents components or phases of digital investigation process.
Considering overwhelming serial dependence between phases, or components in investigation phase is very important to rise level of reliability in results of every precedent component.

Probability of failure [10] of any components in serial dependence relationship can be described with formula [11]:

$$R = 1 - P(\bar{A}_1 \cup \bar{A}_2 \cup \bar{A}_3 \cup \ldots\ldots \bar{A}_n) = Q \qquad (1)$$

Where is:
R- reliability [12]of component
P- probability of failure
$\bar{A}$- failure event of any component
Q- probability of non-failure of the system

A Chain of Custody is assumed to be a system composed of C components [13], of respective failure rates λ_i, i = 1, . . . , C. The system behavior with respect

to the execution process is modeled through a Markov chain [14] with the following parameters:
S = number of the states of the chain, a state being defined by the components under execution. Every next state depend only of the precedent state in the space of states within the chain of states.
$1/\gamma_j$, = mean sojourn time in state j; j = 1, . . . , S
q_{jk}, = P{system makes a transition from state j to state k ; start or end of execution of one or several components},
j = 1. . . . , S , k = 1: . . . ,S, with:

$$\sum_{k=1}^{S} q_{jk} = 1 \qquad (2)$$

A system failure [15] is provoked by the failure of any of its components. The system failure rate ξ_j in state j is thus the sum of the failure rates of the components under execution in this state:

$$\xi_j = \sum_{i=1}^{C} \delta_{i,j}\lambda_i \text{ ; j = 1, . . . , S} \qquad (3)$$

where $\delta_{i,j}$ is equal to 1 if component a is under execution in state j ; otherwise it is equal to 0.
The system failure behavior [16] may be modeled by a Markov chain with S + 1 states, where the system delivers correct service in the first S states (components are under execution without failure occurrence); state S + 1 is the failure state, which is an absorbing state.
In very beginning of investigation process after [17] Court order for an exemption of possible digital evidence is of a crucial significance to have high rate of confidence in matter of source of digital evidence. High rate of confidence we shall denominate as Reliability [18] of digital evidence source. Figure 3 represents a proposal of inclusion of vulnerability assessment protocol against biometric system result (digital version of a biometric trait) which can be used as digital evidence in a legal process in a Court [19].

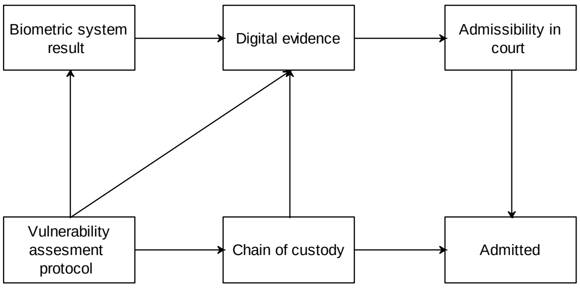


Figure 3 General representation of influence of Biometric system reliability on CoC DE

Biometric system results as a biometric trait supposedly used as digital evidence should be object of kind of validation process. Vulnerability of biometric system result is of crucial importance for validity of digital evidence and is a starting point of whole process.
With UML [20] modeling methodology authors propose Class diagram model to introduce digital evidence source vulnerability assessment as shown in a Figure 4:

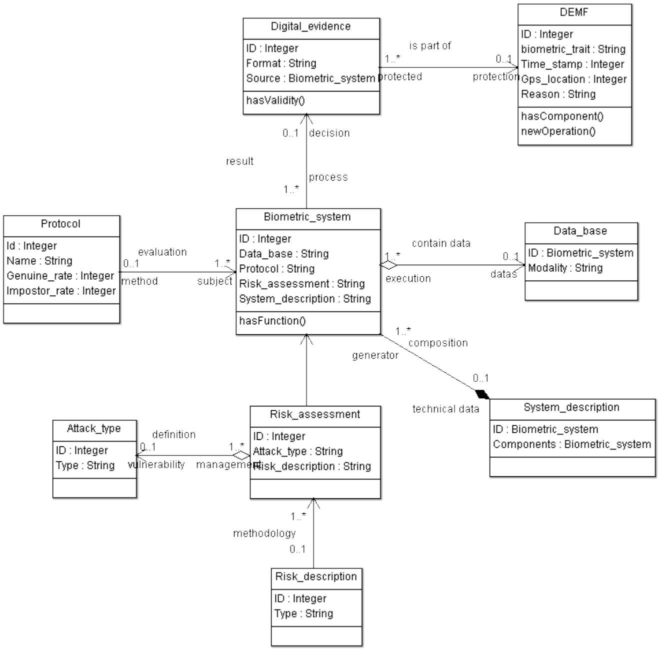


Figure 4 : UML representation of influence of Biometric system reliability on CoC DE

Validation process is proposed to include in reinforcement of validity of chain of custody during presenting digital evidence in legal process within the Court of Justice. Biometric system result validation consists in executing specific vulnerability assessment procedure and considering following validation factors concerning biometric system:

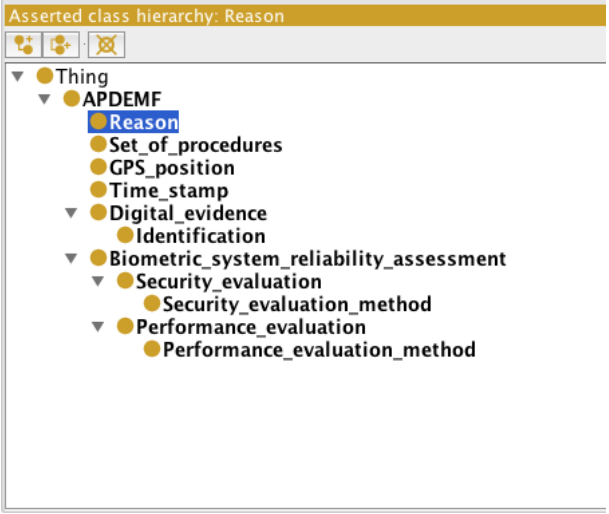
1. Performance evaluation of a biometric system considering it's function and position
2. Security evaluation of a biometric system considering context of it's activity and purpose of use.

Described methodology are including existence of digital evidence contained as digital data within a certain biometric system as a source or starting point of digital investigation process. Existing DEMF [17] (digital evidence management framework) methodology as described by authors Cosic,Cosic, Bača, can be reinforced by introduction of a concept described in precedent chapter. Inclusion of a biometric system reliability assessment before of using a digital evidence within digital investigation process can be an important contribution for it's admissibility in court of justice.
Authors are about to propose an open framework methodology for admissibility in court assessment which can be realized using Ontology methodology with following structure:
(Admissibility procedure of digital evidence management framework-APDEMF):
APDEMF = f { Biometric system performance evaluation,
Biometric system security evaluation,

digital_evidence,
biometrics_characteristics,
gps_location,
time_stamp
reason,
set of procedures}

Where :
Function f represents serial dependence function among listed parameters. Serial dependence function influences, as described in precedent chapter, reliability of whole chain of custody and for consequence influence also acceptability in Court of Justice of a digital evidence.

Using Ontology methodology for systematic representation of specified domain will simplify approach to define such context. Authors are using tool Protégé' [21] [22] developed at Stanford University for realization of APDEMF open framework. Initial taxonomy diagram accordingly to figure 4. UML representation is shown in figure 5.


Asserted class hierarchy: Reason

- Thing
  - APDEMF
    - Reason
    - Set_of_procedures
    - GPS_position
    - Time_stamp
    - Digital_evidence
      - Identification
    - Biometric_system_reliability_assessment
      - Security_evaluation
        - Security_evaluation_method
      - Performance_evaluation
        - Performance_evaluation_method

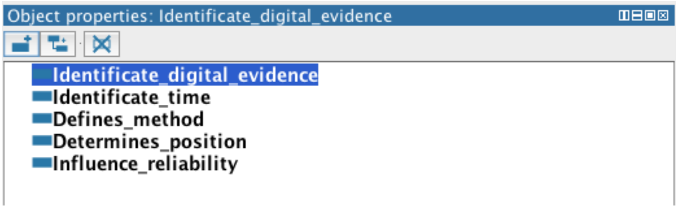
Figure 5 APDEMF taxonomy definition in Protégé'

Representation of APDEMF concepts/classes can be also realized using Manchester notation as follows:

```
Class: Reason
   SubClassOf:
      APDEMF
Class: Identification
   SubClassOf:
      Digital_evidence
Class: Set_of_procedures
   SubClassOf:
      APDEMF
Class: GPS_position
   SubClassOf:
      APDEMF
Class: Time_stamp
   SubClassOf:
      APDEMF
Class: Digital_evidence
   SubClassOf:
      APDEMF
Class: Identification
   SubClassOf:
      Digital_evidence
Class: Biometric_system_reliability_assessment

   SubClassOf:
      APDEMF
Class: Security_evaluation
   SubClassOf:
      Biometric_system_reliability_assessment
Class: Security_evaluation_method
   SubClassOf:
      Security_evaluation
Class: Performance_evaluation
   SubClassOf:
      Biometric_system_reliability_assessment
Class: Performance_evaluation_method
   SubClassOf:
      Performance_evaluation
```

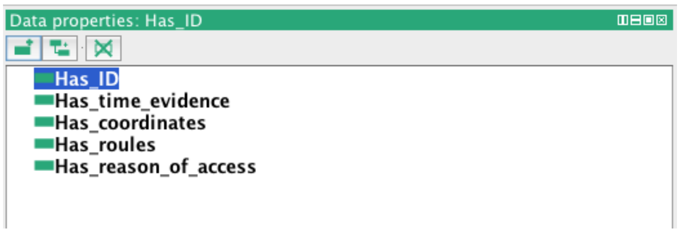
Figure 5 depicts defines object properties of concept/classes in APDEMF.


Object properties: Identificate_digital_evidence

- Identificate_digital_evidence
- Identificate_time
- Defines_method
- Determines_position
- Influence_reliability

Figure 5 APDEMF object properties definition in Protégé'

Figure 6 depicts defines data properties of concept/classes in APDEMF.


Data properties: Has_ID

- Has_ID
- Has_time_evidence
- Has_coordinates
- Has_roules
- Has_reason_of_access

Figure 6 APDEMF data properties definition in Protégé'

Object and data properties defines main relations among defined concepts within the framework. Framework represent conceptualization of methodology for digital evidence chain of custody enriched by the evaluation of biometric system reliability at the very beginning of lifecycle of Chain of custody.

Development and implementation reasoning rules using SWRL language [23] will facilitate a realization of automatized procedure/s for testing such process on the very beginning of digital investigation and would improve confidence of digital in Court of Justice.

4 Conclusion and Further Research

Biometric systems perform well in many existing applications, but biometric capabilities and limitations are not yet well understood in very large scale applications involving tens of millions of users. Questions remain about whether today's biometric systems are sufficiently robust, able to handle errors when the consequences are severe. Although fingerprinting technology has been applied on a large scale for decades in law enforcement, human experts are available in this application to help process noisy or difficult samples. Even so, there have been a few high-profile misidentifications with serious ramifications. It remains to be seen if fully automatic biometric systems can meet performance requirements as the number and scale of deployments increase. As mentioned above, a scientific basis is needed for the vulnerability analysis , reliability of performance and distinctiveness and stability of various biometric traits under a variety of collection processes and environments and across a wide population over decades. The reliability of biometric recognition is clouded by the presumption of near-infallibility promoted by popular culture. Such presumptions could make contesting improper identifications excessively difficult. Conversely, if all evidence must be up to the standards implied by certain popular culture phenomena, unreasonable difficulties could be faced in cases lacking sufficient resources or evidence to meet those standards. The courts have sometimes taken the view that an individual's expectation of privacy is related to the ubiquity of a technical means, which implies that the legal status of challenges to biometric technologies could be affected by the commonality of their use. In all phases of forensic investigation, different profiles of personnel come into contact with digital evidence. Through the entire lifecycle of digital evidence, there are threats that can affect its integrity and thus in the end, the court's decision. The goal of this document is to show weaknesses that are a consequence and to define a life cycle of digital evidence with improvement in the very beginning of the process. Further research will be focused on problem how to implement a framework, through development of rules in SWRL language which will facilitate reasoning about reliability issues, to secure and maintain digital evidence and chain of custody of digital evidence using ontology method as implementation environment and realization of theoretical basis of automatized procedure for testing rate of confidence in digital evidence. Such procedure will help investigators to safely handle evidence and enhance admissibility process in the court.

References

[1] M. Schatten, "Zasnivanje otvorene ontologije odabranih segmenata biometrijske znanosti," FOI (Varaždin), 2007.

[2] B. (Tuvit) J. (UAM). Galbally, J. (UAM) Fierrez, A. (IDIAP) Merle, A. (CEA-Leti) Merrien, L. (Morpho) Leidner, "Biometrics Evaluation and Testing D3 . 3 : Description of Metrics For the Evaluation of Biometric Performance," Bruxelles, 2012.

[3] K. L. Jacobsen, "Biometric as security technology : Expansion amidst fallibility," Vesterkopi AS, Strandgade 56, DK-1401 Copenhagen, Denmark, 2012.

[4] M. Theofanos, B. Stanton, and C. A. Wolfson, "Usability & Biometrics: Ensuring Successful Biometric Systems," National Institute of Standards & Technology Information Access Division Information Technology Lab, Gaithersburg, MD 20899, 2008.

[5] J. Ćosić and M. Bača, "(Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp," in *MIPRO2010*, 2010, no. Im.

[6] FBI, "Best Practices for Maintaining the Integrity of Digital Images and Digital Video," *[Online](Available:http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2008/standards/2008_04_standards01.htm)*, 2007. .

[7] S. W. G. on D. E. (SWGDE), I.O, and D. E. (IOCE), "Digital Evidence: Standards and Principles," *[Online] (Available: http://www.fbi.gov/about-us/lab/forensic-science-)*, 1999. .

[8] FBI, "IOCE Princips and Definition," *[Online] (Available: http://www.ioce.org/core.php?ID=5)*, 1999. .

[9] J. Ćosić and M. Bača, "Chain of digital evidence based model of digital forensic investigation process," *IJCSIS- Int. J. Comput. Sci. Inf. Secur.*, vol. 9, no. 7, 2011.

[10] A. Schottl, *A reliability model of a system with dependent components*, vol. 45, no. 2. 1996, pp. 267–271.

[11] Z. Ćosić, “Sustav dinamičko modeliranje tehničkog sustava brodskog kompresora,” 2007.

[12] Z. Cosic, J. Cosic, and M. Baca, “Additive model of reliability of biometric systems with exponential distribution of failure probability,” *IJCSI Int. J. Comput. Sci. Issues*, vol. 9, no. 6, pp. 1–4, 2011.

[13] J. C. Laprie and K. Kanoun, “X-ware reliability and availability modeling,” in *IEEE Transactions on Software Engineering*, 1992, vol. 18, no. 2, pp. 130–147.

[14] H. Ý. Singh, V. Þ. Cortellessa, B. Þ. Cukic, E. Ý. Gunel, and V. Þ. Bharadwaj, “A Bayesian Approach to Reliability Prediction and Assessment of Component Based Systems £ Ý Department of Statistics,” in *Proceedings of the 12th International Symposium on Software Reliability Engineering (ISSRE□01)*, 2001.

[15] J. L. Horowitz and E. Mammen, “Nonparametric Estimation of an Additive Model With a Link Function,” *Ann. Stat.*, vol. 32, no. 6, pp. 2412–2443, 2005.

[16] S. Yacoub, B. Cukic, and H. H. Ammar, “A scenario-based reliability analysis approach for component-based software,” in *Ieee Transactions On Reliability*, 2004, vol. 53, no. 4, pp. 465–480.

[17] J. Ćosić, Z. Ćosić, and M. Bača, “An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence,” *J. Inf. Organ. Sci.*, vol. 35, no. 1, pp. 1–13, 2011.

[18] Z. Cosic, J. Cosic, and M. Baca, “Recovery function of Components of Additive Model of Biometric System Reliability in UML,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 9 No.7, no. ISSN 1947–5500, pp. 1–4, 2011.

[19] Z. Ćosić, J. Ćosić, and M. Bača, “Biometric System Vulnerability as a Compromising Factor for Integrity of Chain of Custody and Admissibility of Digital Evidence in Court of Justice: Analysis and Improvement Proposal,” *J. Inf. Organ. Sci. - JIOS*, vol. 38, no. 1, pp. 11–33, 2014.

[20] M. Bača, M. Schatten, and B. Golenja, “Modeling Biometric Systems in UML,” in *18TH INTERNATIONAL CONFERENCE INFORMATION AND INTELLIGENT SYSTEMS*, 2007.

[21] N. F. Noy, A. Chugh, W. Liu, and M. A. Musen, “A Framework for Ontology Evolution in Collaborative Environments,” in *ISWC’06 Proceedings of the 5th international conference on The Semantic Web*, 2006, pp. 544–558.

[22] N. F. Noy and D. L. Mcguinness, “Ontology Development 101 : A Guide to Creating Your First Ontology,” 2001.

[23] I. Horrocks, N. Inference, P. F. Patel-schneider, L. Technologies, H. Boley, S. Tabet, B. Grosof, M. Dean, and I. R. Notices, “SWRL : A Semantic Web Rule Language Combining OWL and RuleML,” in *W3C Member Submission 21 May 2004*, 2004, no. May.