UDC 004.056
Preliminary Communication

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

Zoran Ćosić *zoran.cosic@statheros.hr*
"STATHEROS",d.o.o.
Kaštel Stari, Split, Croatia

Jasmin Ćosić *jascosic@bih.net.ba*
Ministry of the Interior of Una-sana canton
ICT Section of Police Administration, Bihać,B&H

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

Abstract

Biometric systems play an important role in digital investigation process as a important factor of authentication and verification applications, since they are strongly linked to the holder of a biometric traits and possible suspect. Thus it is important that biometric systems can be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as energy plants, access to borders at airports, e-commerce etc. Biometric recognition either raises important legal issues of remediation, authority, and 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 is growing, with some key cases going back decades and other more recent cases having raised serious questions about the admissibility of biometric evidence in court. In this paper authors is about to explain influence of reliability of biometric system on general acceptance of digital evidence in Court of Justice process. Through paper authors are also about to propose vulnerability assessment of biometric system as improvement factor of reliability of existing methodology for preserving chain of custody of digital evidence called DEMF (Digital Evidence Management Framework). Improvement proposal is presented as an introduction of phase of biometric vulnerability evaluation methodology within proposed framework called APDEMF (Admissibility procedure of DEMF). Using UML (Universal Modeling Language) modeling methodology authors are about to represent a APDEMF framework which will describe essential phases of the same process.

Keywords: biometrics, traits, characteristics, system digital evidence, chain of custody of digital evidence, chain of custody, digital forensic

1. Introduction

Digital investigation [15] [4] is a complex process usually conducted with a large number of protagonists and equipment. Instead a physical investigation a digital investigation is a process to answer in general to questions about digital states and events. Digital states and events can be a data-base that contain certain information about identity of an individual. Biometric systems are such systems that contain information about identification parameters

of an individual who can be potential suspect in certain legal processes. But biometric systems are also real systems, which can be affected by large number of possible vulnerabilities.

Thus vulnerabilities without assessment can seriously compromise confidence in a proper and secure function of biometric system as a source of digital evidence.
By definition biometrics [16] [20] is the automated recognition of individuals based on their behavioral and biological characteristic of human individuals. It is a method for establishing confidence that one is dealing with individuals who are already known or not known and consequently that they belong to a group with certain rights or to a group to be denied certain privileges.

It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways. Biometric systems are often used as a source of digital evidence during digital forensic investigation process. In this paper we are about to define role of a generic biometric system within the process of digital forensic investigation aimed to improve admissibility in Court of Justice for the digital evidence with biometric system provenience. General representation of biometric system, according to Waymann [34] [27], consists of splitting whole system in a number of subsystems like:

A. collecting data
B. data transfer
C. data analysis
D. database
E. decision process match
F. decision process non match

Figure 1 represents a simplification of biometric system function taking into account principal groups of generalized processes.

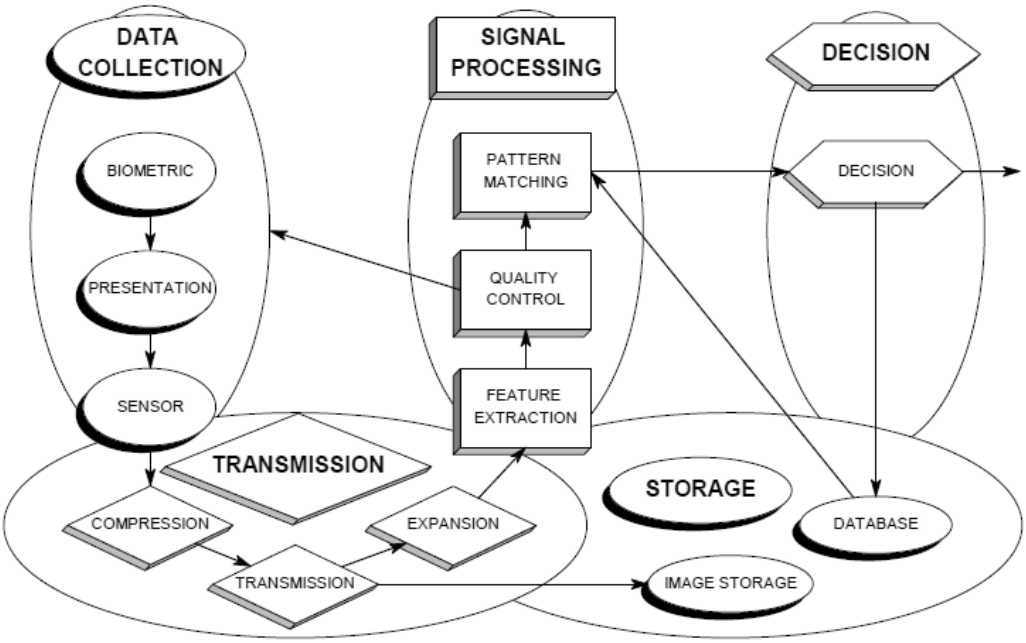

Figure 1. Basic operations of a generalized biometric system. [34] [21]

Biometric systems [28] 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..

The motivations for using biometrics are diverse and often overlap, and include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security.

Questions persist, however, about the effectiveness [21] 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.

1.1 Biometrics and legislation

Whilst the use of biometrics has a long history it is, however, only fairly recently that it has come to be defined and deployed as an important security technology by various international organizations. When the U.S. Army's biometrics [21] programs started, its main focus was to determine how to use biometrics as a way to secure access to military networks. After the events of 11 September 2001 biometric technology then began to be deployed as a solution to various threats to security. Most notably, biometrics was quickly deployed as a new and much needed anti-terrorist technology.

Biometrics was introduced at a number of U.S. ports of entry, notably in airports, to establish the true identity of foreigners wanting to enter the U.S. That the use of biometrics as a security and defense technology was new is also evident if we look at how research projects carried out at the U.S. Army War College began to engage questions aimed at identifying the role that the Department of Defense and its Biometric Management Office should play in the emerging Homeland Defense organization.

In European Union there is a number of activities according to the enhancements of a security and safety at national security levels such Schengen information system II generation operative since 2013 and EURODAC database consists in over 70 mil. fingerprint data's.

Furthermore European [13] Commission founded in 2011 a Biometric Evaluation and Testing (BEAT) Project under the seventh framework programs called Evaluation of identification technologies, including Biometrics (SEC-2011.5.1-1). The goal of BEAT is to propose a framework of standard operational evaluations for biometric technologies. This will be achieved by (1) developing an online and open platform to transparently and independently evaluate biometric systems against validated benchmarks, (2) designing protocols and tools for vulnerability analysis, and (3) developing standardization documents for Common Criteria evaluations.

2. Biometric system vulnerability considerations

Vulnerability considerations include security [13] [25] 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 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.

The information security community is extensive and has long experience with some of the challenges raised by biometric systems, which gives it a real opportunity for fruitful and constructive interaction with the biometrics community. Biometric systems pose two kinds of security challenges.

The first is the use of biometrics to protect-provide security for other information intensive systems. For what types of applications and in which domains is an approach incorporating biometric technologies most appropriate? This is a question for the broader information security community as well as the biometrics community and requires that we understand the goals and needs of an application to ascertain whether biometrics based approach is useful.

Assuming [13] 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 [14] 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.

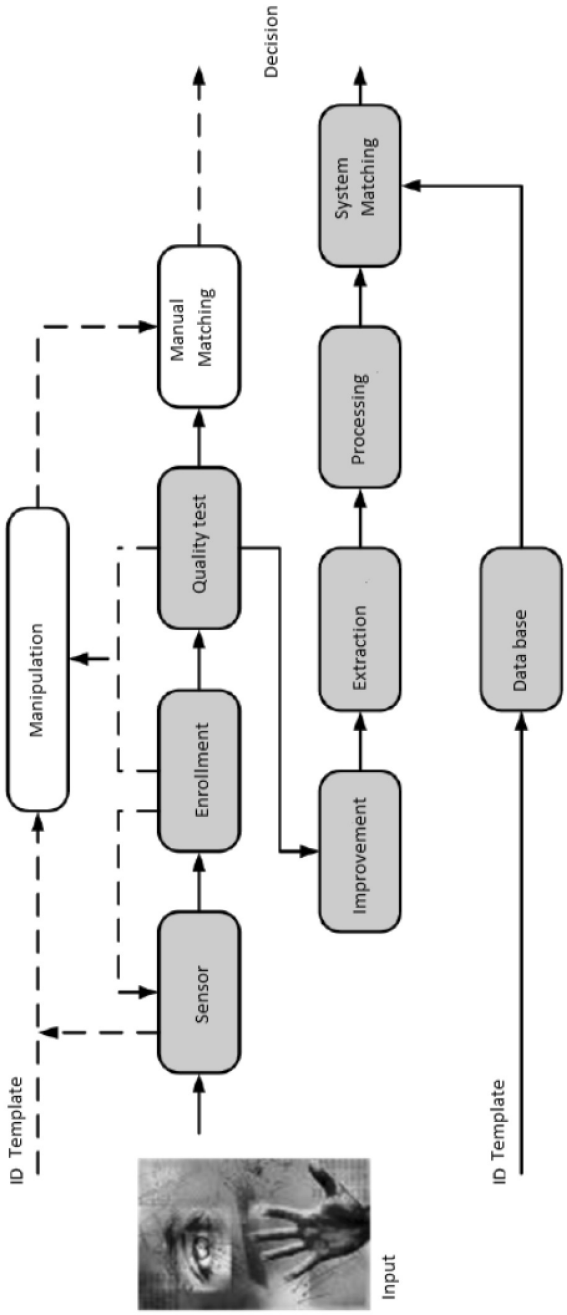

Figure 2. Matching and decisional process of a biometric system [28]

Conventional security analysis of component design and system integration involves developing a threat model and analyzing potential vulnerabilities that is, where one might attack the system. As described above, any assessment of the effectiveness of a biometric system, including security considerations [22], requires some sense of the impostor base rate. To estimate the impostor base rate, one should develop a threat model appropriate to the settings of a system. Biometric systems are often deployed in contexts meant to provide some form of security [17], and any system aimed at security requires a well-considered threat model. Before deploying any such system, especially on a large scale, it is important to have a realistic threat model that articulates expected attacks on the system along with what sorts of resources attackers are likely to be able to apply. Of course, a thorough security analysis,

however, is not a guarantee that a system is safe from attack or misuse. Threat modeling [2] for appropriate functionality of biometric system, is rather difficult.

Results often depend on the security expertise of the individuals doing the modeling, but the absence of such analysis often leads to weak systems. As in all systems [23], it is important to consider the potential for a malicious actor to subvert proper operation of the system. Examples of such subversion include modifications to sensors, causing fraudulent data to be introduced; attacks on the computing systems at the client or matching engine, causing improper operation; attacks on communication paths between clients and the matching engine; or attacks on the database that alter the biometric or non-biometric data associated with a sample.

A key element of threat modeling [25] in this context is an understanding of the motivations and capabilities of three classes of users: clients, imposters, and identity concealers. Clients are those who should be recognized by the biometric system. Impostors are those who should not be recognized but will attempt to be recognized anyway.

Identity concealers are those who should be recognized but are attempting to evade recognition. Important in understanding motivation is to envision oneself as the impostor or identity concealer.

2.1 Attacks typologies

Figure 3 represents general scheme [13] of possible attacks deployment over a general biometric identification and verification systems

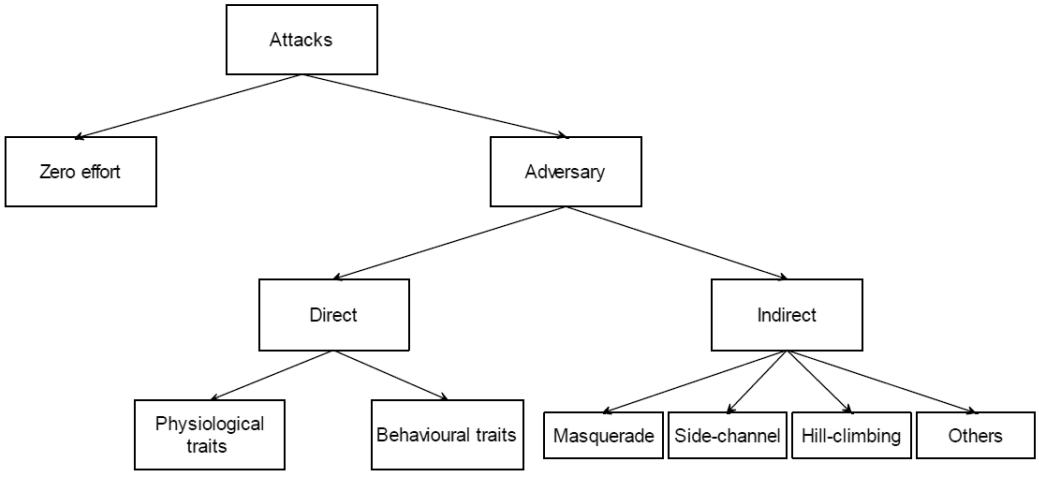

Figure 3. Biometric system attacks deployment [13]

The attacks that can compromise the security provided by a biometric system may be categorized into two basic types as follows:

Zero-effort attacks: also known as intrinsic failure is impossible to prevent and is present in all biometric systems, is derived from the fact that there is always a non-zero probability that two biometric samples coming from two different subjects are sufficiently alike to produce a positive match.

Adversary attacks: this refers to the possibility that a malicious subject (attacker), enrolled or not to the application, tries to bypass the system interacting with it in a way for which it was not thought.

Adversary attacks have been systematically categorized in 10 classes by depending on the point to which they are directed. The total 10 points of attack are depicted in Figure 4.

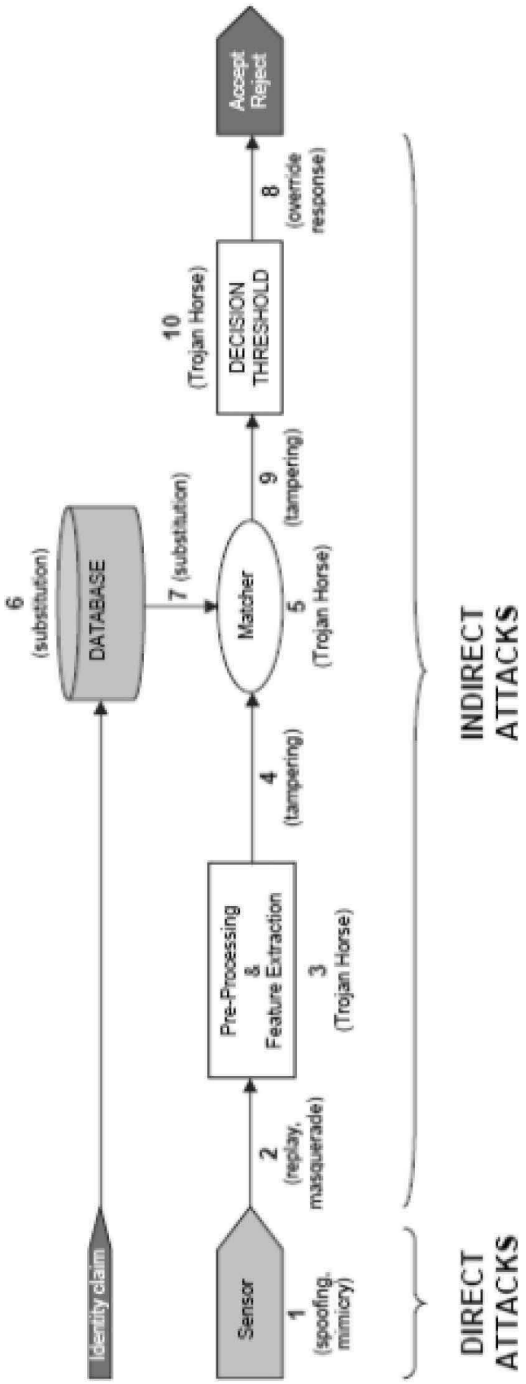

Figure 4. Adversary attacks specification into phases [14] [13]

Above representation [17] include description general attacks classes as an overture in vulnerability analysis and possible metrics definition.

1. Attack [25] [14] on the biometric sensor with mockups or dummies. A reproduction of a biometric trait is presented as input to the system. In addition to the risk of data

loss, it has also been pointed out that human agency brings about another possibility of misuse, namely the risk of 'spoofing'. Spoofing refers [22] to the process by which individuals introduce a fake biometric sample (e.g. a fake fingerprint) to illegitimately bypass a biometric system. Such spoofing attacks undermine the integrity and security of a biometric system by introducing fake biometric data into the system. An example of spoofing would be the use of a fake biometric to fool a system into allowing access to 'secure space' by, say, presenting it with a copy of the fingerprint of a person who is allowed access. A worst-case scenario could be if a person on a watch list used the fake fingerprint of a person from a 'safe passenger' list to gain access, for example, to an airport. Experts have stressed that it is a misconception that fooling biometric systems in this way is almost impossible (and therefore needn't receive much attention). Thus when a biometric is forged this process in itself entails a serious risk of illegitimate access to the very systems and spaces that the technology is believed to make 'safer' by presumably eliminating unwarranted access. Crucially, this risk not only compromises the security of the system but also that of the individual. If a person's fingerprint is spoofed this creates serious problems for the implicated person who cannot simply cancel his or her stolen digital trait. Referring to this point, critics have argued that the risk of having one's biometric feature(s) spoof

2. Replay attack. [25] [14] A recorded signal (containing a previously intercepted signal) is replayed to the system, bypassing the biometric sensor.
3. Attack [25] [14] on the feature extractor. The feature extractor is forced, e.g., by Trojan horse, to oppress single features of a biometric trait, or to produce altered values than those read by the biometric sensor.
4. Tampered feature representation. Features [25] [14] extracted from the sensor input are replaced by a different (fraudulent) feature set. The stages of feature extraction and matching are often inseparable, and the attack is complex. However, if the extracted feature set is sent to a remote matcher, e.g., over the Internet, the threat is real.
5. Attack on the matcher [25] [14]. The matcher is forced, e.g., by Trojan horse, to produce high or low matching score, in order to allow or deny access to an individual.
6. Attack on stored biometric templates [25] [14]. Templates stored in a biometric database (local, remote, distributed) are added, modified or deleted. Another important risk is that of data loss. This risk is often disregarded although numerous cases of the loss of sensitive digitalized data have already occurred. As one example amongst many, the Information Commissioner's Office (ICO) in Wales recently evaluated an incident where "five laptops and four memory sticks containing sensitive information have been lost by local [Welsh] authorities" – stressing that this is most regrettable given the risk that such data could end up "falling into the wrong hands" .Hence human agency and the risk of data loss need to be taken seriously when deciding to deploy biometrics to advance security if not, the effects might be extremely damaging for the individuals whose biometric data has been lost
7. Substitution of the template representation [25] [14].See 4.
8. Also 9. and 10. Attack [25] [14] on the decision end point. If the final matching decision is manipulated by the attacker, the authentication system is disabled. By overriding the final matching decision, the biometric system is rendered useless and the biometric data irrelevant.

2.2 Vulnerabilities metrics definitions

The objective evaluation [2] [14] of the performance of an attack (i.e., danger or risk posed to a system) is a very difficult and challenging problem as it depends on multiple non-independent factors. Here is to represent a number of general metrics, common to any type of attack that should be considered in order to compare the vulnerability of a given biometric system to different indirect attacks.

Figure 6 represents general division into separate groups of general aspects of vulnerability types.

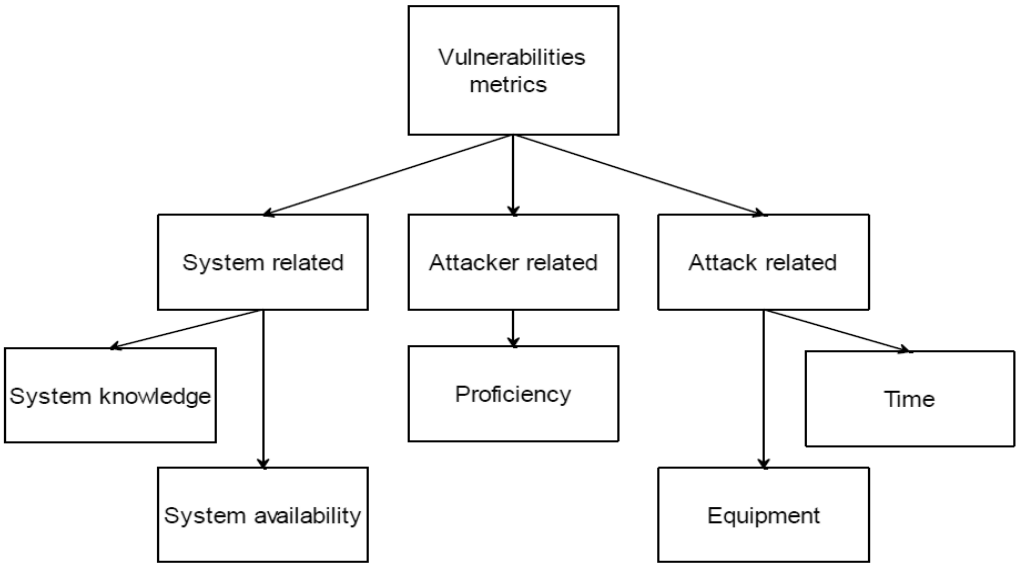

Figure 5. Vulnerabilities metrics representation

System-related metrics [2] [14]

System knowledge required. This metric refers to the amount of knowledge of the biometric system required to perform the attack. Example of metrics:

- Public: information which is fairly easy to obtain (e.g., on the web).
- Restricted: information which is only shared by the developer and organizations which are using the system, usually under a non-disclosure agreement.
- Confidential: information which is only available within the organization that develops the system and is in no case shared outside it.

System availability. This metric takes into account how easy/difficult it would be for an eventual attacker to acquire or to have access to a copy of the biometric system in order to prepare, develop, or carry out the attack. A suggested rating for this metric is:

- Public: The system is publicly available (e.g., on-line) and may be installed in your own facilities (e.g., a biometric SDK).
- Restricted: The system is accessible for the public but it is very difficult to get or to take with you (e.g., an ATM with a biometric system installed).
- Private: The system is only accessible to certain authorized people (e.g., access control to a restricted area of a company).

Attacker-related metrics [2] [14]

Proficiency. This metric refers to the level of proficiency required by the attacker and the general knowledge that he possesses, not specific of the system being attacked. A suggested rating for this metric is:

- Layman: no real expertise needed, any person with a regular level of education is capable of performing the attack.
- Proficient: some advanced knowledge in certain specific topics (e.g., optimization algorithms) is required. Good knowledge of the state-of-the-art of attacks. The person is capable of adapting known algorithms to his needs.
- Expert: a specific preparation in multiple areas such as pattern recognition, computer vision or optimization is needed in order to carry out the attack. The person is capable of generating his own new attacking algorithms.
- Multiple experts: the attack needs the collaboration of several people with high level of expertise in different fields (e.g., electronics, cryptanalysis, physics, etc.)

Attack-related metrics [2] [14]

*Time***.** Amount of time needed by the attack (including its preparation and execution) to break the system. This metric is strongly related to the Efficiency and to the countermeasures that the system may have integrated (see knowledge required in Sect. 3.2). For the rating of this particular metric it may be useful to distinguish between the identification and the exploitation of an attack. A suggested rating for this metric is:

- Low: less than one day.
- Medium: less than one week.
- Large: more than one week.

It should be noted that certain attacks may be considered to be unfeasible (i.e., the system is resistant to them) if the amount of time required to carry them out is too large.

*Equipment***.** This refers to the type of equipment required to perform the attack. This includes the biometric databases used (if any). A suggested rating for this metric is:

- Standard: equipment which is affordable, easy to obtain and simple to operate (e.g., computer, video cameras or mobile phones). In the case of biometric databases it would refer to publicly available ones (or datasets generated synthetically).
- Specialized: this refers to fairly expensive equipment, not available in standard markets and which require of some specific formation to be used (e.g., spectrum analyzer). In the case of biometric databases it would refer to datasets with restricted and limited access or which are specifically captured by the attacker.
- Multiple specialized: in this case more than one specialized equipment is required to perform different parts of the attack.

2.3 Vulnerabilities Evaluation Protocol definition

The evaluation protocol [2] [14] of biometric system vulnerabilities should include a set of guidelines for the security assessment of biometric systems and for reporting the results of the evaluation [21] in a useful and meaningful manner. In particular, the protocol is divided into two separate stages (performance and security evaluations) with a number of different steps to be followed. Figure 6 is a graphical representation of a vulnerabilities protocol definition.

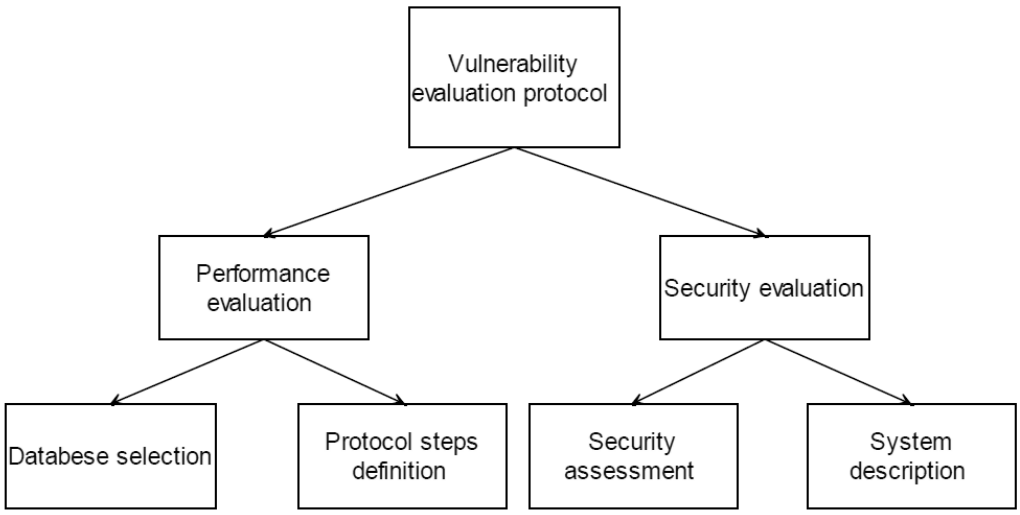

Figure 6. Vulnerability evaluation protocol definition.

Performance evaluation. Regardless of the error rates claimed by the vendor (usually computed on small self-acquired datasets), an independent performance evaluation in the Normal Operation Scenario (NOS) should always be the starting point for a posterior security assessment of the system.

However, we may highlight here two key factors to any performance [21] evaluation:

1. Database selection. A number of useful biometric databases for the different modalities should be chosen.

2. Protocol definition. It should be clearly stated the genuine and impostor access attempts carried out during the performance evaluation in order to reach the reported error rates. In general it is better to followed protocols.

Security evaluation. [21]

1. Description of the biometric system that will be evaluated.
2. Description of the attack for which we want to determine the vulnerability of the biometric system. This description must contain the parts of the system that are targeted by the attacker (e.g., template, algorithm, matching score...) and the goal of the attack.
3. Description of the equipment required to perform it.
4. Description of the attacker proficiency.
5. Description of the knowledge about the system under evaluation required by the attacker.
6. Execution of the vulnerability evaluation in the defined operating points (in the previously executed performance evaluation), paying special attention to the computation of the Success Rate and Efficiency of the attack (defined in Sect. 3).
7. Account for the time required to perform the attack (after a certain time, an attack can be considered as not feasible).

3. Chain of custody of digital evidence

3.1 Legal aspects of use of biometric systems as a source of digital evidence

Because a biometric [21] system recognizes the body, its applications may assume and embed particular Western notions of individuality and personal identity namely, that the individual acts in self-interest and has autonomy over his or her actions. However in some non-Western contexts there are different views on the primacy of the individual, and more collectivist views of identity prevail. In these contexts agency and authority are not presumed to reside with individuals and autonomous action is not assumed. An individual's identity, in such cases, cannot easily be separated from that of the larger group of which the individual is a member. This undermines the assumptions of biometric systems whose design expects that the actor is the individual (for example, accessing a bank account, doing a job, or making political decisions). Biometric systems are used to recognize individuals, but depending on the application and the cultural context, the broader system integrating biometric technologies may also need to recognize the position of individuals within the family, workplace, or community. That is, an understanding of the relational dimensions of individual action whereby a person or group acts on behalf of another may be required. For example, within a workplace context an assistant may be required to take action on behalf another to check in for a flight or post personnel evaluations or in a community context a neighbor may be enlisted to pick up prescription medication for someone unable to do so.

Some recognition systems [21] may function at a distance, making it possible to associate actions or data with a person without that person's explicit participation. Such tracking and collection of data has privacy implications not only for the person involved, but for society as a whole. If these capabilities were to be broadly deployed, with their existence becoming broadly known and concern about their use becoming common, there would be potential distrust of the institutions that had deployed the technology. Even if knowledge of a capability is not widespread, the power that flows to those who control it may have unanticipated effects. To date, widespread use of covert identification appears to be confined to movie plots. Contrary to popular belief, for example, the surveillance cameras used to investigate the 2005 London bombings did not perform biometric recognition as described in this report, because the cameras produced video searched by humans, not by machine. Nonetheless, several programs now pursuing recognition at a distance presage such applications. While concerns about choice to participate are often dismissed by the biometrics industry, they must be addressed to take into account the target community's cultural values in order to gain acceptance and become broadly effective, especially as such systems become more pervasive or if covert biometric surveillance systems mature and become widely deployed.

3.2 Digital forensic chain of custody & integrity

Digital investigation process known also as Digital Forensic may be defined through one of many definitions [26] is „digital forensic can be defined as the application of science and engineering to the legal problem of digital evidence“. According to Pollit and Whiteledge „digital forensic is the science of collecting, preserving, examining, analyzing and presenting relevant digital evidence [19] for use in judicial proceedings“.

Digital forensics [18] requires collection of digital evidences from physical and logical resources like hardware, media, database and files where the ‘crime’ is suspected to have taken place or originated. These resources are seized and searched for digital evidences and proper custodial measures are needed. Here it must be noted that al evidences that are collected should be done in a fool proof manner according to the standards prescribed for maintaining it, so that it doesn’t breach the principle of integrity of data in the first place.

Biometric traits as digital image remain often a very useful starting point of a investigation process in a digital forensics. Digital forensics is no longer associated only to a laboratory in police and security agencies, but it is also used outside that area. Some areas where digital forensic play important role are: insurance companies, banks and corporate. Digital evidence is defined as any data stored or transmitted using a computer that support of refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi. The definition proposed by the Standard Working Group on Digital Evidence (SWGDE) is any information of probative value that is either stored or transmitted in a digital form [30]. Another definition proposed by the International Organization of Computer Evidence - IOCE is „...information stored or transmitted in binary form that may be relied upon in court“ [9]. According to multiple definitions of it digital investigation process can be represent as in Figure 7.

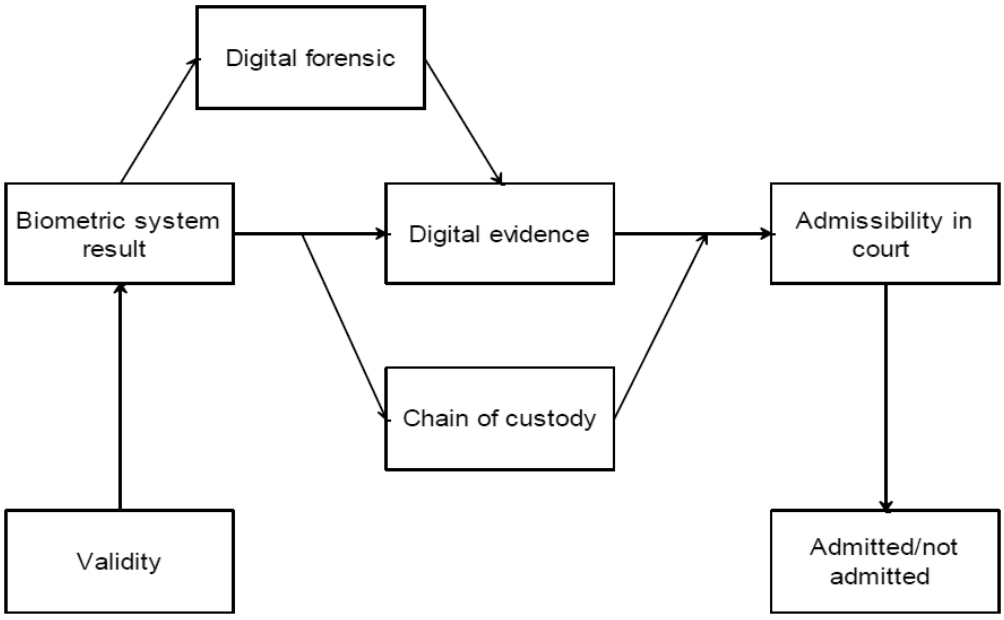

Figure 7. General representation of a digital investigation process

Digital investigation process is requiring a scientific approach [32] in the phase definition. Authors has chosen an UML modeling method to describe process of digital investigation process.

Using UML [1] modeling methodology through sequence diagram annotations we can describe digital investigation process, divided into six phases, as in Figure 8.

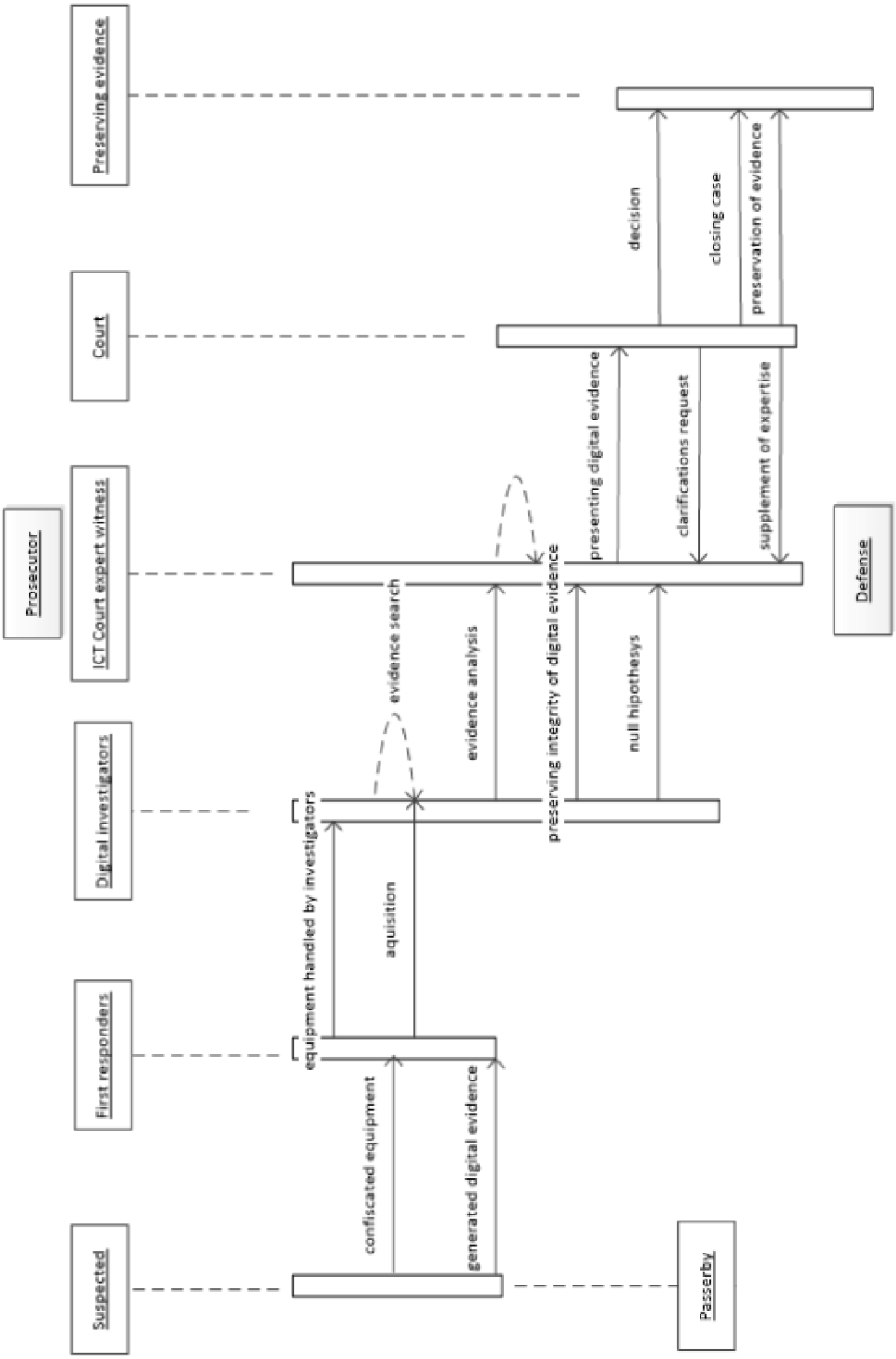

Figure 8. UML sequence diagram representation of digital investigation process

In all phases of forensic investigation, digital evidence is susceptible to external influences and coming into contact with many factors, which can easily exclude relevance of the same digital evidence. Legal admissibility of digital evidence is the ability of that evidence to be accepted as evidence in a court of law.

The evidential weight of digital evidence can only be safeguarded if it can be proven that the records are accurate i.e. by whom they were created and when and that no alteration has occurred. In order for the evidence to be accepted by the court as valid, chain of custody for digital evidence must be kept, or it must be *known who exactly, when and where and why* came into contact with evidence in each stage of the investigation. In this case very important role has digital evidence integrity, that must be kept during the process of digital forensic investigation.

According to Vanstone [33] digital integrity is "the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source".

Scientific Working Group of Imaging Technology define that "The integrity of digital evidence ensures that the information presented is complete and unaltered from the time of acquiring until its final disposition" [8]. Investigator or other personnel, who will eventually present his/her investigation hypothesis to the court, must be able to accurately describe not only those who handle the evidence, but when and where, and what happened regarding this. If he/she is not able to explain and prove that, the court will not accept evidence and the whole investigation is in vain. In order for the evidence to be accepted by the court as valid, chain of custody for digital evidence must be kept, or it must be known who exactly, when and where came into contact with evidence in each stage of the investigation [5].

The phrase "chain of custody" refers to the accurate operation sequence auditing control of original evidence material that could potentially be used for legal purposes. The purpose of testimony concerning chain of custody is to prove that evidence has not been altered or changed through all phases, and must include documentation on how evidence is gathered, how is transported, analyzed and presented. To prove the chain of custody, we must know all the details on how the evidence was handled every step of the way [6]. Today it is very often the case that some of the digital evidence, and the piece of evidence, contained some of the biometric characteristics of a person and must be presented to the Court in order to prove an offense.

According to FBI data, digital evidence appearing in over 85 % of leading by this organization, and even in 65% of these investigations are crucial evidence[1] . Very often we have a situation where video cameras captured the particular person who may be linked to some crime, video was not good enough in quality for several reasons: low-resolution camera, low-light area, camera angles, etc., and therefore was not possible to identify a person. One way to identify a person is one of its biometric features (walking pace, height , length of arms, legs , the characteristic points on the face and head , etc.) In other cases performed audio - recording of the suspect for a criminal offense and is necessary to identify the recorded voice which in most cases is not enough of good quality so it is necessary to perform additional filtering and treatment of voice in order to be useful and to be able to identify the person. In all of these cases is crucial to identify the certain knowledge of biometrics, the use of the necessary tools, and it's combination to digital forensics.

[1] Federal Bureau of Investigation (www.fbi.gov).

4. Improving admissibility in court of digital evidence

4.1 Admissibility of digital evidence in court

The concept of admissibility of a digital evidence means that the Court ultimately accepts digital evidence as such and that during the trial it will be treated equally with other materials and evidences. Court is that who ultimately accept and / or reject digital evidence and decisions, and the responsibility for this lies within the judge figure who leads the case. Here an expert witnesses, play an important role that as friends of the court independently, professionally and scientifically explain the court the evidence. Digital evidence must comply to the certain requirements in order to be acceptable.

Today there are very few published papers on the subject of admissibility of digital evidence [12]. Many years used "Frye test," was replaced by Daubert's principle and according to it, it's more and more science and the scientific method as required for evaluation and presentation of digital evidence [3]. The Court could accept only those evidences that meet certain conditions:

-The procedures are repeatable, the error rate of applied procedures is known, the procedures are published in recognized journals with peer review,

-The procedures are scientifically accepted.

By the application of Daubert's principles number of exclusions of witness and quasi-judicial expert has rapidly increased, but according to some research it also disturbed equilibrium of parties in the process. The reliability of biometric recognition has received considerable attention for many years. Numerous scholarly articles discuss whether particular forms of biometric evidence, such as DNA or fingerprints, are admissible in court and whether they should be.

A recent NRC report took [7] a broad look at forensics, not just biometric evidence, and concluded that "a body of research is required to establish the limits and measures of performance and to address the impact of sources of variability and potential bias.

After the misidentification and arrest of Brandon Mayfield in connection with the Madrid train bombings of 2004, courts appear to be taking a cautious approach to biometric recognition, even though the error was ultimately attributed to human experts and the Department of Justice report does not fault the automated matching portion of the system.

The reverse perception may set excessively high standards; that is, if the assumption is that all evidence must be up to the standards implied by certain popular culture phenomena, then cases in which resources were not available to meet those standards may face challenges. It is important to note that such biometric evidence may or may not be forensic evidence (for example, latent fingerprints)

4.2 Improving of chain of custody as a important factor for increasing admissibility

4.2.1 Chain of custody parameterization according DEMF[2]

According to Vanstone [33], digital integrity is "the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by

[2] DEMF is a Digital Evidence Management Framework (Cosic&Baca).

an authorized source" and there are several adapted methods for digital signing a evidence in order to improve its integrity: CRC (Cyclic Redundancy Check), hash function, digital signature, timestamp, encryption and watermarking.

All process is presented on Figure 9.

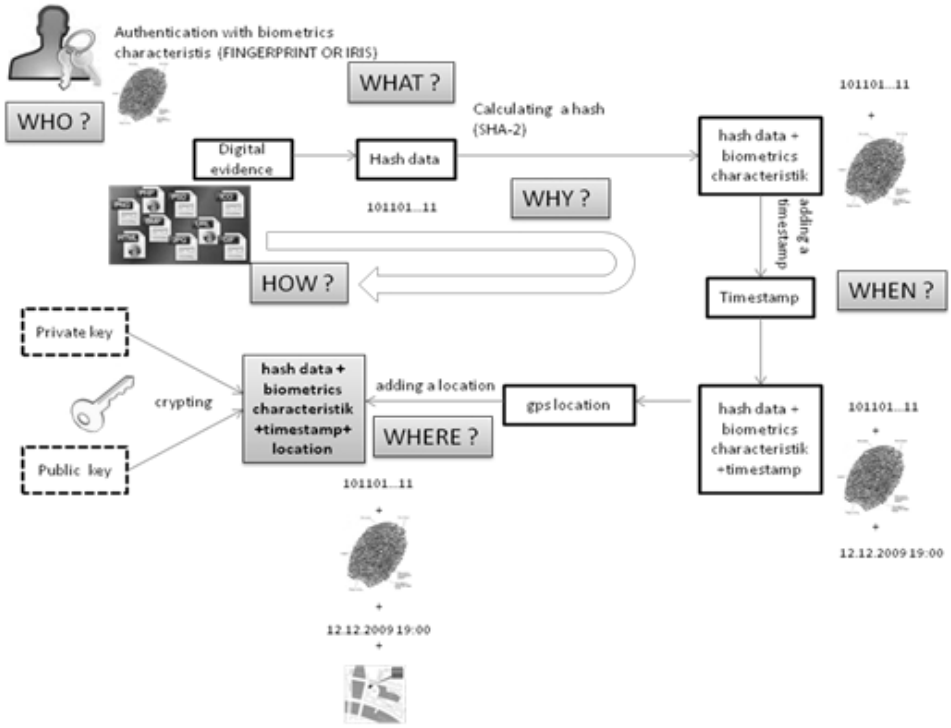

Figure 9. Process of chain of custody [33]

Authors proposed to use a SHA-2 function for fingerprint of evidence, a biometrics characteristic to authentication and identification for digital signing (Who), trusted time stamping for adding a time (When), use some of web services (GPS coordinate and google maps) or some RFID device for geo location (Where) and asymmetric encryption for securing digital evidence. DEMF ("Digital Evidence Management Framework") can be presented as a function for secure management that consist of this factors defined as DEMF [31]:

(DEMF) = f { fingerprint _of _file, *//what*
biometrics_characteristic, *//who*
time_stamp, *//when*
gps_location, *//where*
reason, *//why*
set_of_procedures}; *//how*

Use of all these factors in the right way provide safe and secure chain of custody [35] [29], to ensure that digital evidence will be accepted by the court. For this purpose the good method is use a biometric characteristics of a person who is manipulating data. It can be a fingerprint, iris image or face image. With this method can be done authentication and identification process of a person who handle with digital evidence. Prerequisite for this is that we must have a template database of all person who handled with evidence. It must include followed person:

- First responders
- Forensic investigators

- Court expert witness
- Law enforcement personnel
- Police officers (crime inspectors)

4.2.2 Chain of custody (DEMF) improvement possibility

As we see in section (2) biometrics could be a starting point or container of a possible digital evidence for a purpose of an digital investigation process.

Each of particular phase in such process can be consider as a step or component of a same process and consequently, a lack in each of them can result as compromising factor of validity of a digital evidence and can influence it's admissibility in court.

According to actually proposed Digital Evidence Management Framework (DEMF) , it does not consider vulnerability assessment of a biometric system as a source of possible digital evidence as a biometric trait of a possible suspect. Biometric trait can be also subject of some kind of manipulation as described in a section 2. Analysis of possible situation acting manipulation can be, for sure, reinforcement point of major acceptability grade of presented digital evidence.

Technically we can describe all process of collecting digital evidence as a chain made of components which describes particular phases of a same process
Thus we can suppose so called serial dependency of components of this process of collecting and manipulating digital evidence. 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:

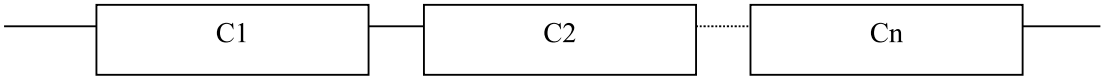

Figure 10. Components in serial dependence relationship

Considering overwhelming serial dependence between components during investigation process, is very important to rise level of reliability of results for every precedent step or component.

Generally, probability of failure during execution of certain task [28] of any components in serial dependence relationship can be described with formula:

$$R = 1 - P(A_1 \cup A_2 \cup A_3 \cup \ldots\ldots A_n) = Q \quad (1)$$

Where is:
R- reliability of component
P- probability of failure
A- failure event of any component
Q- probability of non-failure of the system

A Chain of Custody of a Digital Evidence, is assumed to be a system composed of C components [29], of respective failure rates λ_i, i = 1, . . . , C.

The system behavior with respect to the execution process is modeled through a Markov chain with the following parameters:
S = number of the states of the chain, a state being defined by the components under execution
$1/\gamma_i$, = 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:

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

A system failure 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:

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

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 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 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 of digital evidence source. Reliability of digital evidence source is a result of a vulnerability assessment process subject of some kind of vulnerability assessment protocol.

Figure 12 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.

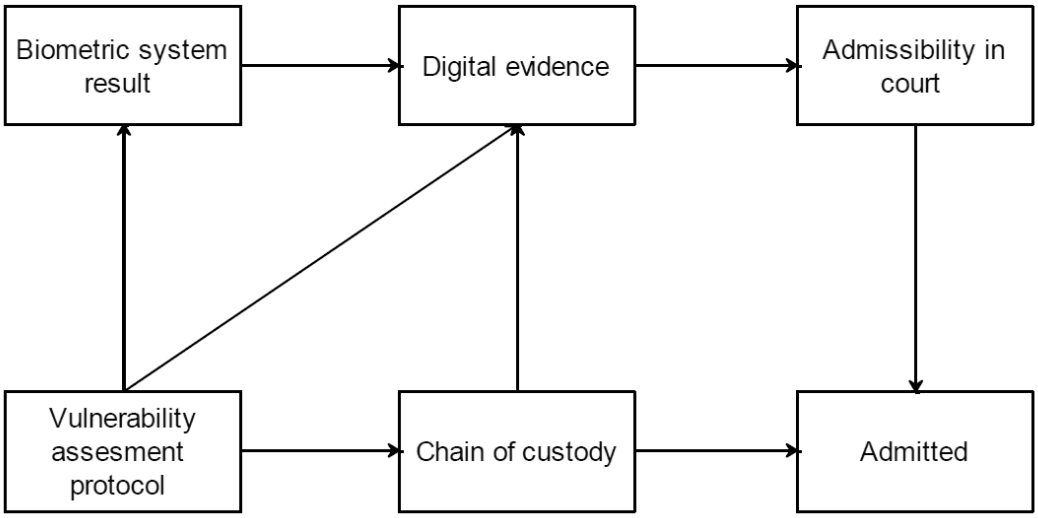

Figure 11. General representation of improvement of DEMF

With UML modeling methodology authors propose Class diagram model to introduce digital evidence source vulnerability assessment as shown in a Figure 12:

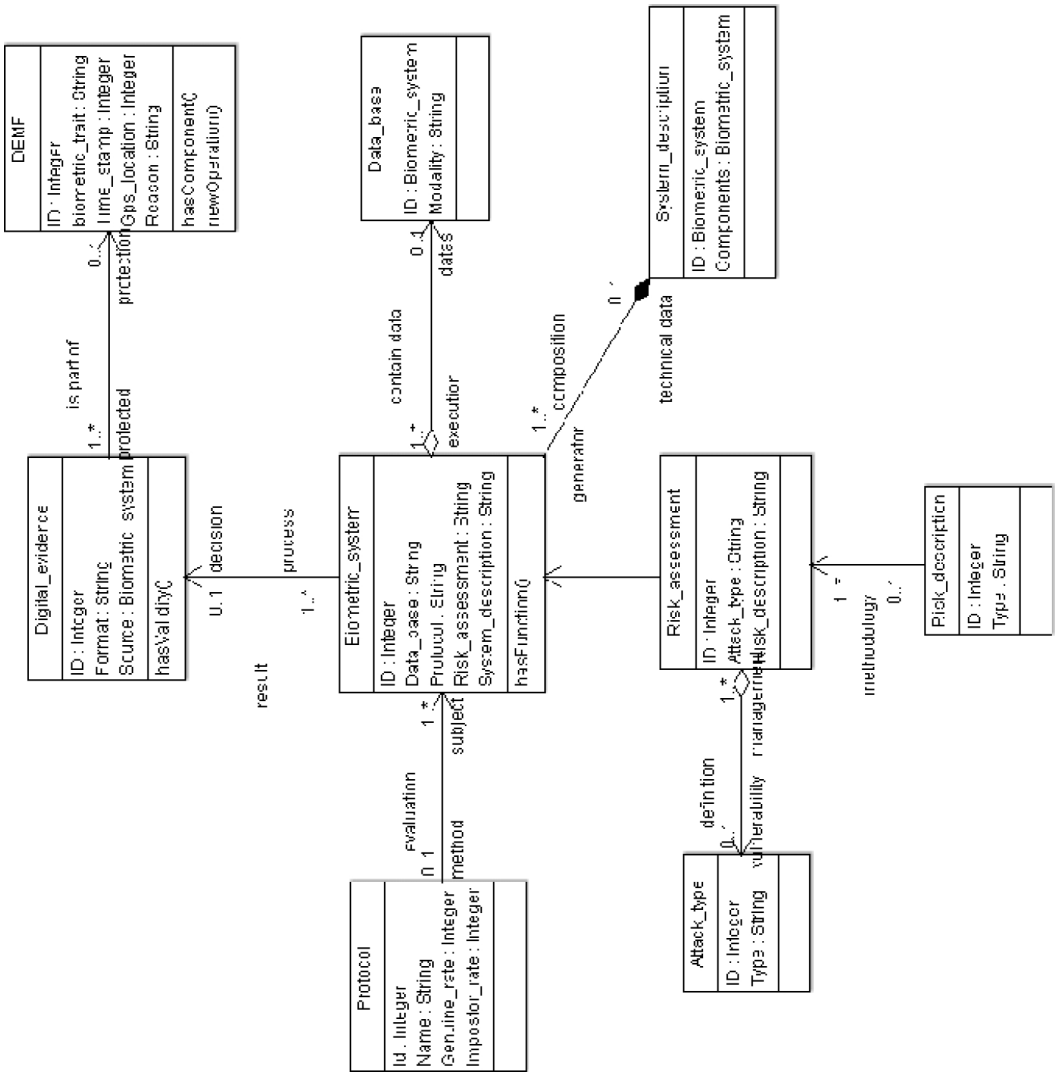

Figure 12. An improvement proposal for digital evidence chain of custody DEMF

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 procedure as defined in chapter 2.3 considering following validation factors concerning biometric system as a structure of potential vulnerability assessment protocol:

1. Performance evaluation
    - database analysis
      In this phase is necessary to define integrity level of database within future digital evidence is contained. If integrity is compromised also compromised should be the digital evidence.
    - acquisition steps analysis
      Analysis of a functional phases of acquiring process of a digital evidence and considering eventual malfunctions or other social, legal or other aspect.
2. Security evaluation
    - system evaluation
      Biometric system evaluation considering users, technology, environment and usability aspects of a system.
    - security assessment

Assessment of risks and security issues of a system with risk analysis and risk treatments programs.

4.2.3 Digital evidence management framework (DEMF) improvement proposal

DEMF methodology acknowledge existence of digital evidence as a starting point of digital investigation process. As described in precedent chapter , inclusion of vulnerability analysis of biometric system within a procedure of DEMF would improve reliability of whole process and influence in a higher level of acceptance of digital evidence in Court of Justice.
Considering conclusions in a precedent chapter authors are about to propose an open framework methodology for admissibility in court assessment which can be described as follows:
(Admissibility procedure DEMF [31] - APDEMF):

APDEMF = f {biometric_system_vulnerability,
Investigation performance evaluation,
investigation security evaluation
gps_location,
time_stamp}

Considering expression (1) we can explicate dependency function amongst phases of a digital investigation process:

$$R_{DE} = \prod_{i=1}^{n} R_i \quad (4)$$

Where:
-Rde is a reliability function of Digital evidence
-Ri is a reliability of each phase of digital investigation process.

Each of proposed parameters should be metrically defined and acceptability level of results should be described. In addition for implementation facilitation process should be defined automated procedure for framework proposal.
APDEMF as open framework is about to be developed as ontology [34] with reasoning procedure ,implemented in SWRL[3] language [35] for testing confidence rate in validity of digital evidence. Improvement of existing chain of custody method can be realized by an introduction of component of evaluation of biometric system vulnerability as described above. Improvement of a confidence in source of the digital evidence , according to a model above, would influence whole chain of custody confidence by increasing reliability knowledge of each phase.
Realization of automatized procedure for testing such process on the very beginning of digital investigation would facilitate confidence consideration of a digital evidence in a Court of Justice.

5. Conclusion remarks and further research

For the improvement of a level of confidence of digital evidence certainly digital investigators do need an information about, the vulnerability analysis of biometrics, reliability analysis of a performance of biometrics, distinctiveness and stability of various biometric traits under a variety of collection processes within a variety of environments where to be applied and across a wide population of possible users.

The individuality of biometric traits, their long- and short-term physiological and pathological variability, and their relationship to the providing population's genetic makeup, health, and other private attributes all merit research attention, which will require extensive data

[3] Semantic Web Rule Language; available online : http://www.w3.org/Submission/SWRL/ seen 17.10.2013 at 19:12

collection. The privacy protections to be afforded participants in such data collection need to be clearly outlined. The reliability of biometric recognition is very important and rather is often 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 this prospective during 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. Some of these threats, as we described, can affect very beginning of a digital investigation process. The goal of this document is to propose enlargement of considerations about possible weaknesses that can have a consequence of acceptance process and define a life cycle of digital evidence.

Proposed considerations about vulnerabilities of a Chain of Custody methodology consisting in the first phase weakness definitions and countermeasures propositions for reinforcement of the same, considering questions related to it's reliability.

Further research will be focused on a problem how to implement a framework to secure and maintain certain digital evidence relevant through chain of custody of digital evidence reinforced methodology using Ontology modeling method as a implementation environment and realization of theoretical basis of automatized procedure for testing rate of confidence in a digital evidence. Such procedure will help investigators to safely handle evidence and enhance admissibility process in the court.

6. Acknowledgements

The presented research and results came out form the research supported by the Center for biometrics - Faculty of Organization and Information Science Varaždin, University of Zagreb

References

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

[2] Bhattacharyya, D. ; Ranjan, R. F. A. A. and Choi, M. "Biometric Authentication : A Review," *Int. J. Serv. Sci. Technol.*, vol. 2, no. 3, pp. 13–28, 2009.

[3] Calhoun, M. "Scientific evidence in court: Daubert or Frye,15 years later, Legal Backgrounder," 2008.

[4] Carrier, B. and Spafford, E. H. "Getting Physical with the Digital Investigation Process," *Int. J. Digit. Evid.*, vol. 2, no. 2, 2003.

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

[6] Ćosić, J. and Bača, M. "Chain of digital evidence based model of digital forensic

investigation process," *IJCSIS- Int. J. Comput. Sci. Inf. Secur.*, vol. 9, no. 7, 2011.

[7] Ćosić, J. and Bača, M. "A Framework to (Im)Prove „Chain of Custody" in Digital Investigation Process," in *CECIIS2010 - Central European Conference on Information and Intelligent Systems - University of Zagreb – Croatia*, 2010.

[8] 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. .

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

[10] Fernandez, M. ;Gomez-p, A. and Juristo, N. "METHONTOLOGY : From Ontological Art Towards Ontological Engineering," *AAAI Tech. Rep. SS-97-06*, vol. SS-97–06, pp. 33–40, 1997.

[11] Finin, T. ;Reddivari, P. ;Cost, R. S. and Sachs, J. "Swoogle : A Search and Metadata Engine for the Semantic Web," in *ACM conference on Information and knowledge management*, 2004, pp. 652–659.

[12] Frowen, A. "Computer Forensics In The Courtroom: Is An IT Literate Judge And Jury Necessary For A Fair Trial," 2009.

[13] 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.

[14] Galbally, J. (UAM) ;Fierrez, A. (IDIAP) ;Anjos, S. (IDIAP) ;Marcel, N. (UNIS) ;Poh, C. C. (UNIS) HO, and J. (MORPHO) Bringer, "Biometrics Evaluation and Testing," Bruxelles, 2012.

[15] Gayed, T. F. ;Lounis, H. and Bari, M. "Cyber Forensics : Representing and (Im) Proving the Chain of Custody Using the Semantic web," in *COGNITIVE 2012 : The Fourth International Conference on Advanced Cognitive Technologies and Applications*, 2012, no. Im, pp. 19–23.

[16] Gomez-Barrero, M. ;Galbally, J. ;Morales, A. ;Ferrer, M. a. ,Fierrez, J. and Ortega-Garcia, J. "A novel hand reconstruction approach and its application to vulnerability assessment," *Inf. Sci. (Ny).*, vol. 268, pp. 103–121, Jun. 2014.

[17] Gomez-Barrero, M. ;Galbally, J. and Fierrez, J."Efficient software attack to multimodal biometric systems and its application to face and iris fusion," *Pattern Recognit. Lett.*, vol. 36, pp. 243–253, Jan. 2014.

[18] Hesh, N. I. T., K. N. A. N. Dh, A. K. Um, U. Al, A. G. Arw, and F. A. L. H, "Use of AFF4 ' Chain of Custody ' - Methodology for Foolproof Computer Forensics Operation," *Int. J. Commun. Netw. Syst.*, vol. 01, no. June, pp. 49–57, 2012.

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

[20] Moore, A.M. "Biometric technologies -- an introduction," *Biometric Technol. Today*, vol. 15, no. 1, pp. 6–7, 2007.

[21] Pato, J. N. ;Millett, L. I. and Street, F. "Biometric Recognition Challenges and opportunities," The National Academies Press; 500 Fifth Street, N.W. Washington D.C. 20001, Washington D.C., 2010.

[22] Pereira, T. D. F. and De Martino, M. "Can face anti-spoofing countermeasures work in a real world scenario ?," in *Biometrics (ICB), 2013 International Conference on Biometrics Compendium, IEEE*, 2013, pp. 1–8.

[23] Poh, N. ,Kittler, J. and Motivation, A. "A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures," *Pattern Anal. Mach. Intell. IEE Trans. Biometric Compend. IEEE*, vol. 34, no. 1, pp. 1–14, 2012.

[24] Pollit, M. and Whiteledge, A. "Exploring big Haystack,Data Mining and Knowledge ManagementNo Title," *Adv. Digit. forensic II IFIP*, 2006.

[25] Rattani, A. and Poh, N. "Biometric System Design Under Zero and Non-Zero Effort Attacks," in *Biometrics (ICB), 2013 International Conference on Biometrics Compendium, IEEE*, 2013, pp. 1–8.

[26] Sammes, A. and Jankinson, B. "Forensic Computing: A Practitioner's Guide (Practitioner Series)," *Springer-Verlag New York*, 2000.

[27] Schatten, M. ;Bača, M. and Čubrilo, M. "Towards a General Definition of Biometric Systems," *IJCSI Int. J. Comput. Sci. Issues*, vol. 7, no. 4, p. 1, 2010.

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

[29] Schatz, B. ;Mohay, G. and Clark, A. "A correlation method for establishing the provenance of time stamps in digital evidence," *Digit. Investig.*, vol. 3, pp. 98–107, 2006.

[30] 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. .

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

[32] Uchenna, P. D. A. "A Framework for Evidence Integrity Preservation in Virtualized nvironment: A Digital Forensic Approach.," 2012.

[33] Vanstone, S. ; Oorschot, P. and Menezes, A. *Handbook of Applied Cryptography*. 1997.

[34] Wayman, J. L. "A generalized biometric identification system model," in *Conference Record of the ThirtyFirst Asilomar Conference on Signals Systems and Computers Cat No97CB36136*, 1997, vol. 1, pp. 291–295.

[35] Wilassen, S. "Hypothesis based investigation of Digital Time stamps," *Adv. Digit. Forensics IV IFIP — Int. Fed. Inf. Process.*, vol. 285, pp. 75–86, 2008.