

INTERDISCIPLINARY DOCTORAL SCHOOL

Faculty: PRODUCT AND ENVIRONMENTAL DESIGN

DEPARTMENT OF PRODUCT DESIGN, MECHATRONIC AND ENVIRONMENT

Drd. Jr. Andra-Manuela BOTEZ (md. BEJINARU-MIHOC)

**THEORETICAL AND EXPERIMENTAL RESEARCH
ON THE DEVELOPMENT OF BIOMETRIC SYSTEMS**

ABSTRACT

Scientific leader

Prof.dr.ing., dr. marketing Angela REPANOVICI

BRASOV, 2018

Mr. (Mrs).....

**COMPOSITION OF
The Doctoral Commission**

Named by the Order of the Rector of Transylvania University from Brasov
Nr. 9615 of 05.11.2018

PRESIDENT: Prof.dr.ing. Codruța JALIU
Dean Faculty of Product and Environmental Design,
Transylvania University of Brasov

SCIENTIFIC LEADER: Prof.dr.ing.,dr.marketing Angela REPANOVICI
Transylvania University of Brasov

REFERENTS: Prof.dr.ing. Santiago Fernandiz BOU
Polytechnic University of Valencia
Prof.dr.ing. Mircea REGNEALĂ
University of Bucharest
Prof.dr.ing. Anca DRĂGHICI
Polytechnic University of Timisoara

Date, time and place of the public presentation of the PhD thesis: 14 December 2018, 12.00, Room E24 (Solar Cellar).

Possible appraisals or comments on the content of the paper will be submitted electronically, timely, at the address arepanovici@unitbv.ro

At the same time, we invite you to take part in the public hearing to support the PhD thesis.

Thank you.

CONTENTS

OVERVIEW	8	7
Figure list	16	
Table List.....	21	
CHAPTER 1		
GENERAL FRAMEWORK FOR THE SECURITY OF COLLECTIONS AND		
PERSONS IN LIBRARIES.....		
1.1 General concepts of security in libraries.....	22	13
1.1.1 Safety of users and staff	23	14
1.1.2 Problematic behavior	23	14
1.1.3 Children and young adults.....	24	14
1.1.4 Adult users	25	15
1.1.5 Uncomfortable or suspicious questions.....	25	15
1.1.6 Difficult visitors.....	25	15
1.1.7 Aggressive visitors.....	26	16
1.1.8 Intruders, bomb threats, hostage and weapon threats.....	27	16
1.1.9 Emergency escape: fire, tornado and bad weather.....	27	17
1.2. Protection of library staff	28	17
1.2.0 The staff.....	28	17
1.2.1 Other employees	29	18
1.3 Types of security systems used in libraries.....	29	18
1.3.1 Tattle-Tape security strips	30	18



1.3.2 RFID system	32	19
1.3.2.1 Components of an RFID system.....	32	19
1.3.2.2 Self-borrowing station.....	35	21
1.3.2.3 Automatic return station.....	35	21
1.4. Conclusions	36	22
CHAPTER 2		
THEORETICAL ASPECTS REGARDING FACIAL RECOGNITION SYSTEMS.....	37	23
2.1 Biometric recognition systems.....	37	23
2.2 Facial identification	40	25
2.2.1. Image capture	43	26
2.2.2 . Facial detection.....	43	27
2.2.3. Feature extraction.....	43	27
2.2.4. Comparing templates.....	44	27
2.2.5. Finding Pair Elements.....	44	27
2.3 Facial recognition algorithms	44	27
2.3.1. PCA (Principal Component Analysis).....	47	28
2.3.2. ICA (Independent component analysis).....	50	29
2.3.3. Haar classifier.....	52	29
2.3.4. LDA (Linear discriminant analysis).....	53	30
2.4 Difficulties and shortcomings in biometric verification systems	53	30
2.5 Community legal framework in the field of biometrics	55	31
2.6 Conclusions.....	56	31

CHAPTER 3

STATISTICAL RESEARCH REGARDING THE CONCERN OF LIBRARY MANAGERS AND LIBRARIANS FOR THE NEED TO IMPLEMENT A NEW SECURITY SYSTEM AND THE

EXISTING SYSTEMS IN LIBRARIES..... 5933

3.1 The description of tools used in statistical research..... 5933

3.1.1 Purpose and objectives underlying research.....59 33

3.1.2 Research hypotheses.....59 33

3.1.3 Material and method.....59 33

3.1.4 Description of the groups of subjects..... 60 34

3.2 Research results..... 6438

3.2.1 Results description 64 38

3.2.2 Hypothesis testing..... 75 45

3.3 Conclusions..... 7946

CHAPTER 4

OPTIMIZING THE LIBRARY SECURITY SYSTEM BY IMPLEMENTING A

FACIAL RECOGNITION SYSTEM.....8147

4.1 Introductive Notions8147

4.2 VisageCloud face recognition for authentication, quick verification,
and smart security (protection)..... 8547

4.2.1 Domain Model of VisageCloud.....85 47

4.2.2 Visage Cloud: The programming interface (API)88 49

4.3 VisageCloud: Face detection and recognition 12152

Step 1: Requesting an API key121 52



Step 2: Creating a collection.....	123	55
Step 3: Creating profiles for each person in the collection.....	126	57
Step 4: Face detection in photos	128	59
Step 5: Attaching each face detected to a profile	129	60
Step 6: Performing facial recognition.....	129	60
4.4 Facial Recognition experimental study.....	131	62
4.5 Conclusions.....	133	63
CHAPTER 5		
CONCLUSIONS.....	135	64
PERSONAL AND ORIGINAL CONTRIBUTIONS	138	67
A. Contributions with synthesis character.....	138	67
B. Contributions of theoretical and experimental character	138	67
C. Contributions of curricular nature.....	138	67
D. The novelty of the doctoral thesis.....	138	67
E. Usefulness of the research results	139	68
F. Valorisation and dissemination of the research results in the scientific academic environment.....	139	68
BIBLIOGRAPHY	141	70
APPENDIX 1	147
APPENDIX 2.....	152
THEORETICAL AND EXPERIMENTAL RESEARCH ON THE DEVELOPMENT OF BIOMETRIC SYSTEMS - Abstract.....		
	223	74
CURRICULUM VITAE - engleză.....	225	75

INTRODUCTION

Biometrics refers to the automatic identification of a person based on their own physiological or behavioral characteristics. This identification method is preferred over traditional methods involving passwords and personal identification numbers (PINs) for a variety of reasons including the person to be identified must be physically present at the identification point and / or identification based on biometric techniques avoids the need to remember any password or symbol. Different types of biometric systems are used for real-time identification. The most widespread is based on face recognition and fingerprint matching; other biometric systems use iris and retina scanning, speech, facial features and facial thermograms, and hand geometry.

Biometric technologies are defined as "**automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic.**"

There are two keywords in this definition: "**automated**" and "**person**". The word "automated" differentiates biometrics from the wider field of human identification science. Biometric authentication techniques are performed exclusively by the use of devices, generally a digital computer.

Benefits of biometrics: 1. Biometric features can not be lost or forgotten (while passwords can). 2. Biometric features are difficult to copy, share and distribute (passwords can be advertised in crackers sites). 3. They require the authenticated person to be present at the time and point of authentication.

In conclusion, it can be said that biometric authentication is a security process that relies on the unique biological characteristics of an individual to see if he is the one who says it is. Biometric authentication systems compare a biometric data capture with authenticated data, confirmed in a database. If both biometric data samples match, authentication is confirmed.

Biometrics provides high-level security management operations that have more advantages over traditional means and are now available at lower costs.

Biometric systems are based on several distinct processes: enrollment, real-time capture, templates extraction, and templates comparison. The purpose of enrollment is to collect and archive biometric samples and generate numerical templates for future comparisons. By archiving raw samples, new replacement templates can be generated if a new or an updated comparison algorithm is introduced into the system.

A distinction is made between real-time capture and enrollment as real-time sampling of "sample" biometric samples following an access or identification attempt and their comparison with a "gallery" of templates already entered.

Three important objectives are pursued during the present paper entitled **Theoretical and Experimental Research on the Development of Biometric Systems**:

1. determination of the general information system for the security of collections and persons in libraries.
2. identify security requirements for collections and individuals in libraries.
3. the realization of an experimental system based on facial recognition for the security of collections and persons in libraries.

General Objective: Establishing the general information system for the security of collections and individuals in libraries addresses the following **specific objectives**:

- a) Study on the general framework for the security of collections and persons in libraries.
- b) Study on the theoretical aspects of security of collections and persons in libraries.

The second general objective: The identification of security requirements for collections and persons in libraries contains the following **specific objectives**:

- a) Statistical research on the security of persons and collections in libraries.
- b) Analysis of statistical data and generation of security requirements in libraries.

The third general objective: The development of an experimental system based on facial recognition for the security of collections and persons in libraries is based on the following **specific objectives**:

- a) Developing the IT application for the security of people and collections in libraries.
- b) Developing the database with users.
- c) Experimental determination on the security of individuals and collections in libraries.

Regarding the type of approach, this paper focuses on:

1. **A formal approach** - Thus, the thesis consists of 5 (**five**) chapters, 2 annexes, 116 images and 15 tables;
2. A structural approach - In the first part of the paper some theoretical aspects are presented and the results of the current research are analyzed in depth.

The first chapter is titled **The General Framework of Security of Collections and People in Libraries**. This chapter addresses issues related to "security", a term that can have a variety of connotations in the library world. Internet security and library material security are both important aspects of the library service, but more important is the safety of users and staff..

In recent years, safety has become an issue of great importance in libraries. There are a number of procedures designed to protect users, employees and property. In the 21st century, this topic extends to the safety and security of the internet. Many libraries produce guides that contain provisions that provide detailed safety and security information.

There are at least four sub-topics to the general topic: (1) precautionary measures to protect users and staff from acts of violence; (2) protecting the collection materials against theft / vandalism; (3) procedural safeguards and response plans for natural and man-made disasters and (4) internet protection.

This chapter deals with subchapter 1. and 2. **personal safety** (for users and personnel): precautions against acts of violence, and in subchapter 3. **precautions to protect library collections against theft**, since these two aspects are the ones that directly influence customers.

Regarding subchapter 1, executives and staff of all types of libraries continue to be concerned about the actions of some clients who sometimes adversely affect the services of libraries, including homeless people, mental illness or consumers of prohibited substances.

Although it is difficult to confront users who ignore the rules of the library, threatening other clients or staff, otherwise creating discomfort or chaos, there are still ways and solutions that can be applied. Some of these solutions may require different approaches and partnerships with external groups such as law enforcement agencies, social services, mental health counselors and substance abuse, and even the human resources department.

Effective communication leads both to the increased convenience of library users and an increase in the morale of its staff, transforming the library into a space where everyone feels welcome.

Theoretical Aspects of Facial Recognition Systems is the title of Chapter 2, which aims at defining and presenting biometric recognition systems. Biometrics is the automatic recognition of people based on their behavioral and biological characteristics. It is an instrument that confirms that they are people who are already known (or unknown) - and therefore belong to a group with certain rights (or a group that is denied certain privileges). It is based on the assumption that individuals can be physically and behaviorally distinct in many ways. Biometric systems are increasingly used to recognize individuals and to regulate access to physical spaces, information, services and other rights or benefits, including the possibility of crossing international borders. Reasons for using biometrics include improving the convenience and efficiency of routine access transactions, reducing fraud and increasing public safety and national security.

A widespread theme in biometric research is face recognition in an image, which is covered in subchapter 2. The process of identifying or automatically checking people in frames or digital video images, based on the available database, is called face recognition. The objective of looking for faces in a source or video image is called face detection. Face Detection has become one of the most important research topics due to increased security concerns and many other applications (man-computer interaction, biometrics, person monitoring, etc.). The literature highlights numerous available techniques for detecting and recognizing face. Some techniques have led to effective solutions in obtaining the right precision and reducing processing time.

1. A large number of Face Detection and Face Recognition approaches are analyzed in terms of recognition precision and processing time.
2. An analysis of linear and nonlinear PCA face recognition techniques is presented.
3. There is a study on facial recognition methods for facial expression.

4. There are different face recognition techniques in which one approach is based on the problem of partial occlusion dilemma, where faces are processed to become unrecognizable to defeat the security system.

In this chapter we analyzed the most common image analysis methods used in practice, describing the standard for behavioral patterns that are formed in face detection and recognition. The advantages and disadvantages of face recognition techniques have been outlined.

Classification of face detection techniques has been performed, some of the facial recognition algorithms have been analyzed. The Core Component Analysis (PCA), Independent Component Analysis (ICA), Linear Discrimination Analysis (LDA) and Haar Classifier are the four facial recognition algorithms detailed in subchapter 3.

Difficulties and shortcomings in biometric verification systems have been mentioned in Chapter 2.

Librarians' concerns regarding the security of both staff (including both users and library employees) and the desire to meet the requirements of the institutions to optimize the security system have led to the development of high performance programs. In order to know the opinions of all users on this topic, a marketing research was initiated. As a result, **statistical research has been carried out to determine the views of library managers and librarians on the need to implement a new security system and the existing systems in libraries**, as described in Chapter 3.

The stage of qualitative research refers to the establishment of the problem, starting from the respondent's requirements. Quantitative research is a more complex process; allows for pertinent conclusions. Statistical research is based on the importance of objectively assessing security systems for collections and library staff, creating a facial recognition system to optimize this process.

The research is based on the hypothesis that librarians concerned with personal security want to implement a facial recognition system in their libraries, librarians for whom the most appropriate biometric recognition system to ensure the safety of collections and individuals is facial recognition, I agree with the implementation of such a system in the library, librarians who trust the facial recognition systems are in favor of implementing such a system in the library, librarians working in large libraries, agree to implement a facial recognition system, the higher the readiness of librarians, the more they are willing to implement a facial recognition system, senior management libraries are more likely to implement a facial recognition system in the library, the more the employee's work experience is, the more they are willing to implement a facial recognition system.

Conceiving the questionnaire, analyzing and interpreting the collected data are detailed in the chapter.

The 4th chapter, **Optimizing the security system in libraries by implementing a facial recognition system** is entirely dedicated to VisageCloud. The developed computer application monitors access to libraries and is designed to respond to the growing demand for an effective system to control access and presence in a location in the context of terrorism. The chapter begins by presenting some introductory notions needed to understand the operation of the practical application. The next subchapter shows the **VisageCloud Application Domain Model** and the **Programming Interface (API)** needed to complete the application itself. In software engineering, a domain model is a

conceptual model of the domain that incorporates both behavior and data. A domain model is a system of abstractions that describes aspects of a sphere of knowledge, influence or activity (domain). The domain model in the Unified Modeling Language (UML) is illustrated by a class diagram presented in subchapter. 4.2.1.

The VisageCloud API is a Cloud API REST (Representational State Transfer) API that can be used in applications to grant access to facial recognition and classification capabilities. The Cloud API is a type of API that allows the development of applications and services used to provide hardware, software and cloud platforms.

In subchapter 3, **VisageCloud: Face Detection and Recognition** are the steps required to run the application effectively: from getting the API key to access the application, creating a known profile collection (a profile is a person) to detect people in photos and to map them in profile and then, using that collection, to recognize people in new photos.

The 6 steps that need to be taken to obtain facial recognition of a person in a photo are described:

Step 1: Request an API key

In order to benefit from VisageCloud's facial recognition features, users can access the program at <https://visagecloud.com/>.

Step 2: The creation of a collection

For easier creation of a registered user in the system, it is necessary to create a collection (a set or a group of registered persons).

Step 3: Create profiles for each person in the collection

A profile is a person.

Step 4: Detect faces in photos

It consists in loading an image that may contain one or more faces

Step 5: Attach each face detected to a profile

You can associate a particular face from a photo with an existing profile.

Step 6: Make Facial Recognition

Once more profiles have been created and one or more facets have been mapped for each of them, the last step is to test the recognition operation.

The application can be particularly useful for intelligent surveillance, can be applied in libraries as well as in the hospitality industry (tourism), especially when one of the objectives is to identify and reward loyal users.

The final chapter **Final conclusions, own contributions (authentic)**. Summarize the research results by highlighting their own contributions and the original solutions that made it possible to achieve the objectives set in the paper.

Documentation has been done using both traditional and electronic bibliographic references.

This paper presents new aspects regarding the development of biometric systems, constitutes a useful utility element in the activity of librarians involved in the security process of collections and personnel and at the same time creates the premises for further research in this field.

CHAPTER 1

GENERAL FRAMEWORK FOR THE SECURITY OF COLLECTIONS AND PERSONS IN LIBRARIES

1.1. General concepts of security in libraries

The fact that security has become a key topic of criminological analysis of particular importance reflects the insecurity of the society of the twenty-first century.

In an attempt to understand the concept of security, Brooks (2009) noted that the exposure to terrorist attacks in many parts of the world (London, 2005, Jakarta, 2004, Spain, 2004, Bali, 2002 and New York, 2001) the level of social concern over the ability of governments to protect their citizens. [13] According to Zedner (2009), new crime prevention techniques and community safety initiatives combine to create a security concern among local authorities, partnerships between agencies, volunteer groups as well as private citizens.

Latuszek (2000) mentions that although many libraries are still in predominantly noise and crime quiet locations, there is no hard to notice a pervasive pattern of unrest in public and academic libraries.

Zedner (2009) considers that security is a promiscuous concept, being implemented in many areas (social security, financial security, environmental security, health and safety, human security, international relations and peacekeeping, etc.) Thus, security is the state of "being protected against threats" - either by neutralizing them, by avoiding, or by not risking them.

Maidabino and Zainab (2011) mention in their paper that the purpose of libraries is to provide access to information resources in both print and non-print formats. They believe that balancing access and security in libraries is difficult but at the same time a necessary task.

A number of studies have addressed the issue of collector security, as well as the personal security of visitors and library staff. Also, various studies have described how security breaches and incidents can affect the provision of library services to users. [35]

Latuszek made a review of articles describing incidents due to library visitors to highlight the importance of security plans. Through this article, the author wishes to outline an increased awareness of security in libraries, highlighting technological questions and policy concerns. [33]

Harris and Dimarco present a perspective on how Mansfield University in Pennsylvania addressed the issue of personal security, specifically in the library. The purpose of this article is to help libraries plan for the worst scenarios, covered issues including what self-locking is; planning, policies and procedures; physical security; the visitor's issue, secure places in the library, etc. [24]

Maidabino and Zainab (2012) proposed a tool to evaluate the implementation of collections security in university libraries. This tool incorporates five factors: the administration of collections security, operations and processes, people's issues, physical and technical aspects of collections security, and security culture in libraries. [35]

Westenkirchner offers in his article instructions for libraries wishing to acquire an integrated digital video surveillance system based on the experience of the Auburn University Library. The article includes the technical aspects of closed circuit television (CCTV) and Internet Protocol (IP) integrated video surveillance systems, providing a brief explanation of how the equipment works. [78]

1.1.1 Safety of users and staff

Libraries, museums and archives are considered to be safe places to visit, use and have a job. Unfortunately, there have been incidents in cultural institutions that have led to the wounding or kidnapping of certain individuals, as well as weapons or bomb threats. [29]

This PhD thesis addresses the safety of library users as well as employees. We want to encourage people to use and enjoy the vast resources of different libraries. It is therefore essential to take action and consolidate the idea that libraries are safe places to work on. [3]

The safety of users and staff is essential. In the first stage, the building should be examined, both outdoors and indoors, so that some users and staff can enter, use the unit, and get out without getting hurt, whether at night or during an emergency. Then, we need to consider the user's safety towards the employees as well as the employees towards the users. [29]

1.1.2 Problematic behavior

Kahn (2007), believes that library staff must establish and display policies that describe proper conduct in the building. Behaviors and practices that are not acceptable should be clearly defined. The author mentions that these policies should be applied uniformly, first with a warning and then with any restrictions or revocations of privileges published in the library policy. Warnings to stop inappropriate behavior are often given by senior staff, department chiefs and administrators. However, all staff members should be comfortable in making such comments. If the user does not follow policies after a warning, the security department or the head of department should be contacted if there are no policemen in the building.

1.1.3 Children and young adults

It is not uncommon for unattended children to be in the public library. They can be left alone both in the day and in the evening, while their parents are at work. Supervising children using libraries' collections is a concern. Thus, policies must be put in place to protect children from strangers and not get hurt. Not only does the library need to be aware that there are unattended children in the unit but

there are cases when they are noisy, disturbing or abused by other children. In this situation, it is possible to set a policy that limits the number of children who can work at a table or can create a room for group or noise activities. If there are adolescents who are visiting, set a limit on their number.

If the noise levels become intolerable, it is necessary to address security guards or a supervisor to warn the children to be quiet or to leave. It is important to have consistently posted and applied policies that are strengthened when the noise level is out of control. In addition to trying to control children and young adults, librarians and other staff members should be aware of what's going on in their library.

1.1.4 Adult users

If the institution is not a private organization, it can not limit who enters the building and uses collections. So, it is possible to have homeless, mentally deficient or traveling users in the midst of ordinary business people, students, and other community residents. There are several books describing how to deal with problem users [29].

1.1.5 Uncomfortable or suspicious questions

Kahn (2007), emphasizes in his paper that since 11 September 2001, librarians have become more aware of unusual reference questions. These questions could include addresses and photos of public officials, maps and drawings of public and government buildings, and designs for bombs and weapons. At the same time, one must be aware that some questions that may seem suspicious may be part of a project or homework theme for students.

1.1.6 Difficult Visitors

Libraries and archives (as well as historical societies and museums to a lesser extent, as they usually perceive an admission fee) are safe, warm and comfortable places for homeless people, mentally ill people and annoying people, unpleasant, or noisy; those who use obscene language; have unpleasant smell; sleep or sit at the computer all day and browse the internet. As long as these visitors do not bother anyone, no one can forbid them access to the library. Turner, however, talks about librarians and security staff who asked visitors who were nasty to come back after they washed out and cleaned their clothes. [29]

More problematic visitors are those who hide behind stacks and make inappropriate sexual advances to visitors and staff. Staff who arrange books are the most vulnerable to sexual advances, as well as members of reference staff who help users find the items they look for among the shelves. Installing convex mirrors to display stack areas outside the view area is a way to reduce inappropriate behavior and protect staff members from damage. In order to avoid these problems, written policies must be established to prohibit inappropriate sexual behaviors in the library. [2]

1.1.7 Aggressive Visitors

There are many reasons for visitors to look aggressive. They may be frustrated with their research project, with answers to questions addressed to staff members, they may also be disturbed or mentally ill. Sometimes library users are big or tall and they seem aggressive when they're just in your personal space. This can most often happen when staff members are at the information office. These visitors are not necessarily aggressive, they are just overwhelming. This aggression can be diminished by adjusting the personal space. [29]

From time to time, there is a user who is aggressive or upset when they reach the reference or information desk. To avoid conflict, Kahn (2007) proposes that the employee listens carefully to the complaint or problem and tries to respond without disturbing him. The staff member should try to defuse the situation by giving the visitor the opportunity to explain what is wrong, or why he is so upset. These forms of aggression can be resolved by looking ahead and without prejudices. [29]

Let's get to the abusive visitor. These are visitors who display abusive or inappropriate language and can be quite agitated. Again, staff members should try to calm users by listening carefully, trying not to assume a defensive or aggressive position. Thus, when the user is dissatisfied with his outstanding fines or missing books, the employee of the library must provide him with alternatives to solve the problem. [2]

1.1.8 Intruders, bomb threats, hostage and weapon threats

According to Kahn (2007), if someone in the staff gets a bomb threat, they have to ask the informant when the bomb explodes, what type of bomb is, where it is located, and other questions that show its interest. The staff member must maintain a calm voice and attitude. During the phone, he must make a sign to the nearest employee to call the police or security immediately. The staff member who responded to the phone should not put the informant on hold, but should try to get as much information as possible. If the danger appears to be imminent, or when the security department instructs employees, the building should be evacuated to a safe, remote location that should be the same as the disaster response plan. No one has to go back into the building until the firefighters or the bomb team authorizes it.

To ensure security, signs must be displayed to ban all types of weapons, including hidden weapons, in the building. You can make a list, which should include all types of firearms and knives of all shapes and sizes. If there are gunfire in the building, it must be evacuated as carefully as the visitors are sent out or in the tornado shelter. If there are gunfire in the immediate vicinity, you have to stretch on the floor, behind the furniture, or other solid protection, if possible. It is not advisable to move until the area is secured by the security department, the police officers, or the fire brigade. [3]

1.1.9 Emergency escape: fire, tornado and bad weather

Staff and users must leave the building immediately when the fire alarm sounds. The personnel should be gathered at the outside location, identified by the disaster response team or the security planning team. This gathering place is outside the building and easily accessible. [29]

In case the sirens of the air raid are heard, they usually indicate a tornado observation. In some communities, they indicate strong storms or hurricanes. Users must be transported to shelters for underground tornadoes or to a place inside the building that does not have windows. This shelter must not be left until the siren is clearly heard, or this is required by the security or public security officers. [2]

Some institutions use guard guards or departments to guide the users and the staff to an emergency exit or shelter. Before a disaster or an adverse weather alert, you should discuss how library staff will help wheelchair users reach a safe location. The library must collaborate with the security department and the fire department on this issue so that they are aware of the situation in which disability, fire or emergency personnel may be employees and disability staff. [3]

1.2. Protection of library staff

1.2.0 Staff

There is a wide range of views on protecting the safety of staff by visitors and other employees; ie interpersonal relationships. Shuman and Turner cover these issues in their publications. [29] A security policy must be established to protect the employee's physical security by asking him to notify someone or to get permission before being in the building. This is especially important if the building is cleaned and maintained after everyone returns home for the day. Not being alone in the building seems to be a matter of common sense, but this happens many times. [3]

There should never be one person to consolidate the building and work with the public. We know this is due to the fact that the staff is drastically reduced or because it is a weekend. Calendars should include a substitute or on-call staff member who can fill in when someone is ill. In addition, there should always be a high-level staff member during the hours when the institution is open, answer questions and respond to an emergency situation at the library or archive. [29]

For a good functioning of the institution, a member of the managerial staff, administrator or supervisor should be available by telephone if a problem arises. It is also important that whoever is the designated supervisor should know the policies of the institution and be able to make informed decisions. [29]

Another important factor for the proper functioning of a library is the staff perception of its own safety within the building. Not only should they feel safe during the day, in reference, information and circulation offices, but also in offices and workrooms. [29]

It is advisable to establish security and safety policies for staff members who work after hours so that they know who to call in an emergency, whether they are security guards, supervisors or the police. Phone numbers should be posted through office phones for easy access. [3]

1.2.1 Other employees

The Security Department should carry out a background check on maintenance personnel and cleaning staff, as well as on security agents. If the institution hires a company to handle these jobs, then the security department should carry out background checks on the company and ensure it is stable and secure. Security guards have to be on duty at any time when there are contractors or cleaning and maintenance staff in the building. Their role is to achieve the safety of these employees and contractors and to protect collections of theft and mutilation. [29]

1.3 Types of security systems used in libraries

Policies should be established to record the deliberate damage caused by visitors to collections, including common problems of breaking pages, images, or articles in journals and encyclopedias; removing pages from the covers; and the theft of audiovisual and digital materials. [29] These policies should be implemented by suspending privileges granted to library users and arrest for multiple and serious crimes.

However, there are still those visitors who are pulling books out of the covers or who do not get tired of returning them. [29]

It is essential that you have security agents to check that all visitors and staff who cease work to confirm that the materials have been checked and taught. It's also very effective to have security gates that detect electronic or magnetic targets inserted into books. Unfortunately, many small library systems can not afford the price of these security measures. In such cases, staff members must have their office near exit, so they can track who's leaving, what they have in their hands, but also in their baggage. If the library has an automatic material return system without security guards or verification devices, then staff members need to be extra vigilant and follow the habits and actions

1.3.1 Tattle-Tape security strips

Tattle-Tape security tapes and electronic or magnetic elements have been used for many years. Security strips are placed in the backs of hardcover books or between pages in the case of normal books; and the magnetic elements are usually put on the back cover of the book. These security devices trigger the alarm when a person passes through security gates with a book.

1.3.2 RFID system

Radio frequency identification is the most reliable way of identifying electronically, capturing data, controlling, tracking and inventory using RF communications. [31] This technology improves visibility and reduces running time and work requirements. [67]

An RFID target, called a label, is inserted into books and in the carcasses of audiovisual material, and can solve some of the issues of tracking and checking these materials. Costs for installing a device are one dollar, including both hardware and software. Libraries begin to put these devices in their collections, and museums use devices to mark and identify items at risk of theft in their collections. [29]

Libraries manage a considerable inventory of both printed and audiovisual material in their collections. Today, barcode technology is used by most libraries for their daily activities. [67]

Libraries use a bibliographic database to track traffic information about items in a collection. Each book, after being purchased by the library, has a unique number, usually called a barcode. [40]

Of course, there are some security issues that revolve around the privacy of visitors. The American Library Association (ALA) has published guidelines for the use of RFID in libraries, referring to intellectual freedom. [29]

Types of RFID systems

According to Kahn, 2007, RFID systems are divided into several categories:

- Electronic Article Surveillance (EAS) systems - have a small bit storage capacity that is sufficient to detect the presence or absence of an object.
- Portable Data Capture Systems - The portable terminal contains an RFID reader.
- Networking systems - The reader has a fixed position and is directly connected to a network management system.
- Positioning systems - The interrogation device is placed on a vehicle, connected to a board computer, and communicates data via radio frequencies to an information management system. f visitors when they leave the building. [29]

1.3.2.1 Components of an RFID system

RFID systems have more components than already mentioned RFID tags, just like barcode systems that include multiple elements, not just printed bars. A distinction is made between the following three components: RFID tags; RFID Readers; backend systems (ie middleware and applications) [27], [28]

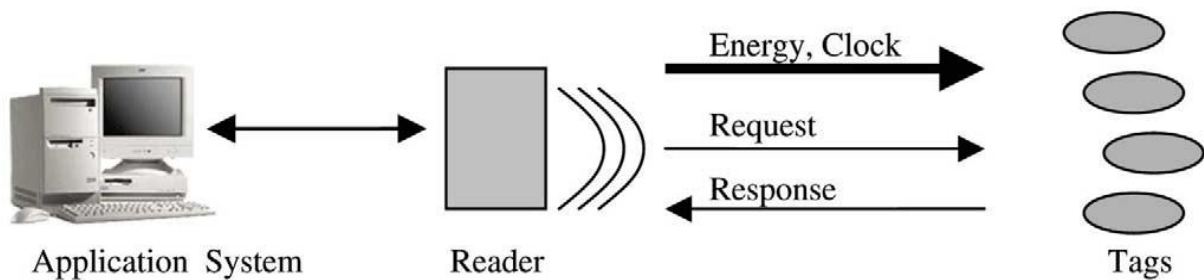


Fig. 1 Overview of an RFID system with passive labels [27]

In a typical RFID system, the tag and the reader communicate information to each other via radio waves. When a marked object enters the reading area of a reader, the reader signals the label to transmit the stored data. Once the data on the tag is received by the reader, the information is sent back to the computer through a network interface. [67]

RFID readers send and receive data to and from labels. The reader is the unit that supplies the RFID transponder with energy and triggers communication signals to force the transponder to execute the requested action. [31] Thus, they are made up of an antenna, the electronic communication needed, a microprocessor for device control, and an interface for transmitting data to the backend system. [28]

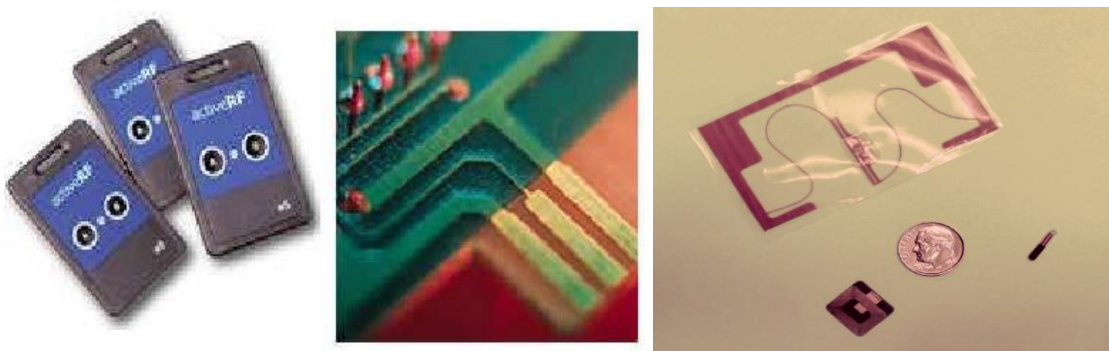


Fig. 2 Examples of labels

There are **two** completely different **types of labels** on power supply: passive and active.

Libraries' collections have always faced the danger of theft, damage and accidental loss. Many libraries have long relied on electromagnetic security gates to alert when they are triggered by magnetic tapes sensitized in books. Some systems now use RFID (radio frequency identification) or other technologies, alarming simply informing staff and visitor of possible theft.



Fig. 3 *RFID gates*

1.3.2.2 Self-borrowing station

Libraries with a self-borrowing system can offer users the ability to borrow their favorite items at any time and with extra privacy. Library users can be independent with access to their account and can handle the borrowed materials; users can access the option to pay fines and even receive a receipt for the amounts paid.



Fig. 4 *Self-borrowing station*



Fig. 5 *Auto return station*

1.3.2.3 Automatic return station

The automatic book return system is extremely useful because users are no longer conditioned by the time they want to return the borrowed materials. Using the RFID system, the user must access his / her account and be able to return the materials borrowed with a "real-time check".

1.4. Conclusions

University libraries are faced with a number of security challenges related to their collections (both printed and unprinted). Library collections provide the foundation for community services and serve as important assets in the library. As such, ensuring and protecting collections can help libraries provide an efficient service in response to the information requirements of the academic community.

Securing the collection implies the need for libraries to provide, maintain and protect their assets in order to ensure the longevity, accessibility and effective delivery of services to users. To achieve this goal, libraries need an effective strategy to assess the security of collections, the violations they face and to establish an acceptable level of implementation of security of collection.

RFID ensures fast and continuous tracking of goods with minimal human intervention. Increased visibility and precision contribute to a significant reduction in labor and inventory costs. In addition to these quantifiable cost factors, intangible benefits, including co-ordination of enhanced inter-organization and customer satisfaction, require advanced RFID investment analysis models. [67]

Summarizing the advantages of RFID systems with respect to other currently used identification systems and in particular the barcode: [31]

- No battery. Supply voltage derived from the RF field
- No communication line is required
- High operating and communication range
- The transponder memory read and write function
- High communication speed
- High data capacity (user memory)
- High data security
- Data encryption / authentication capability
- Multi-label scanning ability with 50-100 labels
- Durability and reliability
- Resistance to environmental influences
- Reusable transponder
- Handless operation
- Very low power.

Identity management systems that improve privacy can provide a higher level of transparency and control for the user.

CHAPTER 2

THEORETICAL ASPECTS REGARDING FACIAL RECOGNITION SYSTEMS

2.1 Biometric recognition systems

In the world of today, where technology is growing rapidly, there are still some issues related to authentication of people, problems to be solved in everyday life. Recognition of a person can be accomplished by various methods such as: what do we know? (based on knowledge, for example, a password, PIN), what do we have? (based on a thing / token, for example ATM card, credit card, smart card), and what are we? (based on biometric indicators, for example, front, speech, walk). The password or card can be distributed, forgotten, or stolen, but not biometric data. Acquiring biometric data is more complex than making combinations of numbers or card theft. Thus, biometrics is safer compared to other methods.

Biometrics is based on the principle of physiological measurement and behavioral characteristics such as fingerprint, facial features, voice patterns, or even the way a person moves. Each method has advantages and disadvantages; some being more reliable, safer, easier to capture, and less invasive than the others. [44]

In biometrics, the most common physiological factors are presented below.

- *Iris recognition* is a technique that uses color patterns and iris shape to confirm the identity of a person. [9]
- *Face recognition* is a technique that uses unique facial features to identify an individual. [9] However, there are problems with identifying people in poor lighting conditions and detecting the state of the individual's life, a prerequisite for ensuring a competitive level of security. [9], [44]
- *Voice recognition* is a technique that uses a voice pattern to analyze how a person says a particular word or a sequence of words unique to that individual. [9] This method has two major disadvantages: enrollment and security.
- *Fingerprint recognition* is a technique that uses the finger's distribution endings and bifurcations to confirm identity. [9] This technique has been considered a unique identifier of confidence. It also has some drawbacks: Fingerprint sensors do not always reliably read fingerprints. [44]
- *Ear traces*, ie based on the uniqueness of the "drawing" or the shape of the ear: the general shape of the pavilion, its size, its own characteristics, position, etc. [8],[45]
- *Lips traces* left on different objects. The following features of the lips are analyzed: shape, thickness and length. [8],[45]

- *DNA profiles* (deoxyribonucleic acid - nucleic acid formed from the most complex organic molecules). [8],[45]
- *Electronic signature* expressed by data in electronic form. In Romania, Law No 455/2001 establishes the legal regime for electronic signatures and electronic documents. [8],[45]

Each biometric technology has its own advantages and limitations. (Tab.1). [8]

Table 1. Comparisons on biometric technologies, after [1]

Biometric technology	Universality	Uniqueness	Continuously	Effectiveness	Acceptability
Face	H	W	A	W	H
Fingerprint	A	H	H	H	A
Hand geometry	A	A	A	A	A
Key pressing	W	W	W	W	A
Signature	W	W	W	W	H
The veins on the hand	A	A	A	A	A
Iris	H	H	H	H	W
DNA	H	H	H	H	W
Walk	A	W	W	W	H
Voice	A	W	W	W	H
Facial thermography	H	H	W	A	H
Retinal scan	H	H	A	H	W

Note: H – high; A – average; W – weak

Two ways have been identified systemically to measure the performance of biometric systems [8]:

1. false response rate, expressed as percentage of authorized persons rejected by the system;
2. rate of false acceptance, expressed by the percentage of unauthorized people accepted by the system.

There are two stages in the functioning of a biosystem [66]:

1. *verification*. After submitting the biometric signature in the system, the user, supports a certain identity through a PIN, login name, etc. In response, the recognition system validates or cancels the user request by comparing the current biometric signature with the enrollment associated with a private identity; [8]
2. *identification*. In this way, the system attempts to recognize the user by comparing the biometric signature presented with all the signatures entered into the database, making comparisons without requiring specific user identity. Identification is a crucial component in

negative recognition, if the user denies having a particular identity. In fact, negative recognition prevents a person from having more identities. [8]

The operating principles (stages) of biometric technologies are shown in Figure 6

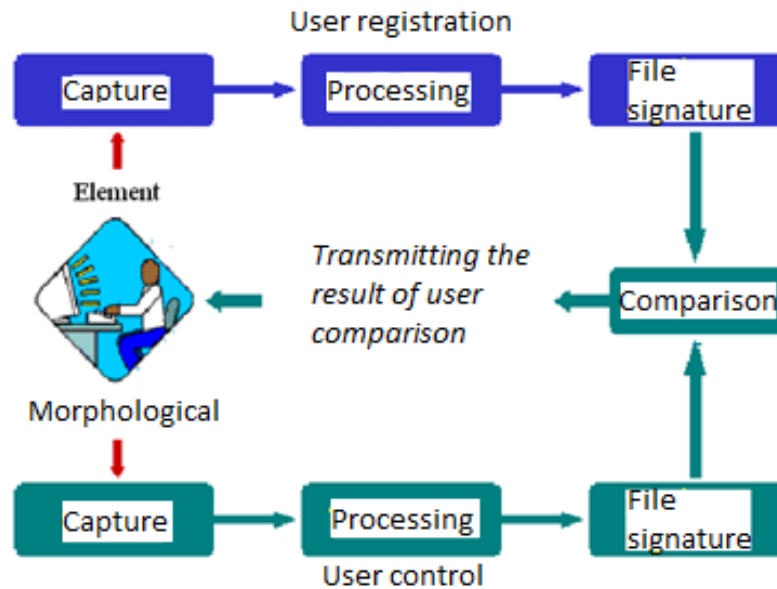


Fig.6 The structural scheme of the technology principle

2.2 Facial identification

One of the most important applications of image analysis is face recognition. It has been a real challenge to build an automated system that is able to identify, verify and classify the faces of people represented in digital images.

"The digital image is a coded representation of a two-dimensional image" [38]. The evolution of modern technologies has allowed easier facial recognition. One of these technologies is to replace the image in essence with a version that emphasizes the most relevant details for face identification; in the case of gradients (an arrow showing the light-to-dark flow across the image) it involves replacing each pixel with a representation of how the pixel brightness compares with the pixels around it.

Another proposal refers to the so-called "projection" of a 2D photo on a 3D model, such as a cylinder. Winding a face around a third dimension can often reveal forms of symmetry and distinctive features that are much harder to find in a flat and static image.

Once this image preparation has been completed, the system finally "encodes" the image or compresses its features and patterns in a smaller simplified file that exists only to cross-check with other encoded faces.

Always an image or video stream is the entry into a face recognition system. The result is an identification or verification of the subject or subjects that appear in the image or video. Some approaches define a face recognition system as a three-step process [34]: 1) facial detection; 2)

feature extraction; 3) facial recognition. According to this view, the face detection and extraction phases could work simultaneously.

- 1) **Face detection** is defined as the process of extracting faces from different frames. So, the system positively identifies a particular region of the image as a face.
- 2) The next step - **feature extraction** - involves obtaining the relevant facial features from the input data.
- 3) Finally, the system **recognizes the face**. With the objective of facial recognition, the system establishes an identity from a database. This phase involves a comparison method, a classification algorithm and a precision measurement of similarity.

Some systems detect and locate faces at the same time, others first apply a detection routine and then, if the results are positive, try to locate the face. Tracking algorithms may be required. Typically, face detection algorithms use the same general steps. First, a reduction in the data size is achieved to target an acceptable response time. The next stage involves extracting features or facial metrics. These will then be weighted, evaluated or compared to decide if there is a face and where it is. Finally, some algorithms apply a learning routine and introduce new data into existing models.

Techniques used for face detection are often used in facial recognition.

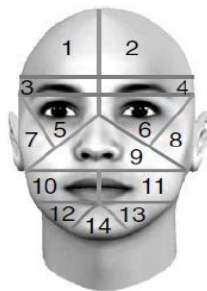
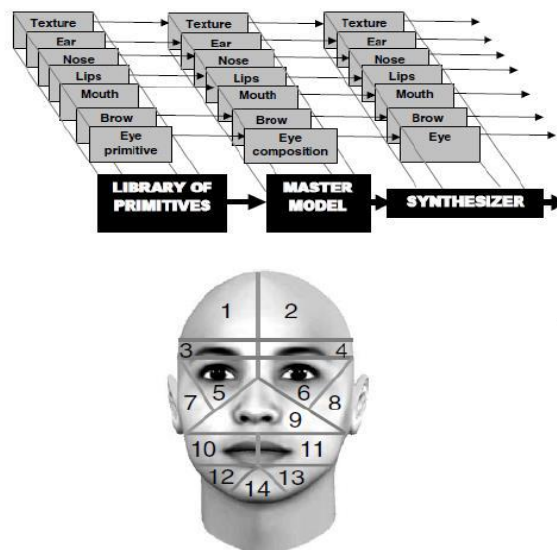


Fig. 7 Facial partitioning for facial analysis [38]

According to the literature, facial recognition is accomplished in a five-stage process: 1. capturing the image; 2. facial detection; 3. feature extraction; 4. comparing templates; 5. find the pair elements.

2.2.1. Image capturing

The first step in this process is to obtain the material for analysis, namely a face image. Facial recognition systems are divided into two general types: those that use static face images and those that analyze dynamic face images from a video.

2.2.2 . Face Detection

Face Detection is the second step and the location of all faces in the captured image is detected with the help of the software. Face detection is regarded as a particular case of object detection, called 'object-class detection'. " Object-class detection " aims to recognize and find interest categories in input images. [48], [79]

2.2.3. Feature extraction

In shape recognition and image processing, feature extraction is a special form of dimensional reduction. When the input data for an algorithm is too large to be processed, it will be converted into a reduced representation of a set of features. Extraction of features is accomplished by archiving information, reducing the size, extracting with relief, and cleaning image noise. Usually, after this step, a segment of the face is transformed into a fixed-size vector or a set of landmarks and their corresponding locations. Transforming input data into the feature set is called feature extraction. [9], [48] The result of the process is the generated template.

2.2.4. Comparing templates

Step four is to compare the template generated in the previous step with the features existing in a database of registered faces. In an identification application, this process produces scores that indicate how well the pattern matched with those registered in the database. In the verification application, the generated template is compared only to a template in the database, that of the claimed identity.[79]

2.2.5. Finding Pair Elements

The final step is to determine if the scores obtained in step four are large enough to declare a match between the generated and the registered template. The rules governing the level at which a match between the two templates can be declared are often configurable by the end-user so that it can determine the security level at which the system must work according to the utility.[79]

2.3 Facial recognition algorithms

A number of current face recognition algorithms use face representations found by uncontrolled statistical methods. Typically, these methods find a set of basic images and represent the faces as a linear combination of these images. Principal component analysis (PCA) is a very widespread example of such methods.

Yan, Kriegman and Ahuja have developed a classification that has been accepted by the specialists in the field. The methods are divided into four categories. These categories can overlap, so an algorithm might belong to two or more categories. Classification can be done as follows:

1. *Methods based on knowledge*

There are encoding methods based on the knowledge of the human faces, grounded by rules. They try to capture the knowledge about faces and translate them into a set of rules. It's easy to deduce some simple rules. As a rule, the face is composed of eyes, both of which are symmetrically disposed, the areas around the eyes being darker than the cheeks. Face features may be the distance between the eyes or the color difference between the eye area and the lower area.

2. *Methods based on invariant features*

The invariant method of the method is based on the extraction of the invariant features that exists even when the position from which the image is taken or the illumination conditions vary. The main drawback of this method is its poor performance in the presence of obstruction or noise. Face detection using skin color segmentation is the most common method based on this approach.

3. *Pattern matching methods*

Pattern matching methods try to define the face as a function. Looking to find a standard pattern for various types of faces. Defining distinct features is done independently. For example, the face is composed of the eyes, the contour of the face, the nose and the mouth. Also, a face model can be built by the edges (boundaries). But these methods are limited to faces that are frontal and unfocused. A face can also be represented as a silhouette.

4. *Methods based on appearance*

Patterns of appearance-based methods are learned from examples of images. Generally, appearance-based methods are based on statistical analysis and mechanical learning methods to find the key features of facial imagery. Some aspect-based methods work in a probabilistic network. An image or a function vector is a random variable that may or may not be part of a face. Another approach is to define a distinctive function between the two face and non-face classes. These methods are also used in extracting face recognition features.

2.3.1. *PCA (Principal Component Analysis)*

Principal component analysis (PCA) is the most widely used tool in multivariate analysis. PCA is a statistical technique that transforms a set of data with multiple variations of the interleaved variables into a new set of data consisting of uncorrelated linear combinations of the original variable. The PCA calculates the uncorrelated axes that calculate the maximum amount of variations in the image. [32]

PCA is an efficient technique when working with large volumes of data. Also, the method is useful for reducing the number of dimensions of the attribute space, but retaining the main features to minimize the loss of information.

Face recognition is a complex issue in the field of image analysis and computer vision. Information storage space is one of the most important challenges in designing the biometric system. Because of bandwidth and limited storage capacity, images must be compressed before storage and transmission. There are **two basic types of compression techniques**; lossless compression and

lossy compression. Loss compression is commonly used to compress audio, video, stop-frame data in applications such as streaming media. Conversely, lossless compression is required for texts and data files such as bank registers and text documents. In many cases, it is convenient to compile a lossless file that can be used to generate files for different purposes.

2.3.2. ICA (Independent Component Analysis)

Independent Component Analysis (ICA) is a statistical technique that reveals hidden factors that underlie sets of random variables or signals. Information describing a face can be included in both dependencies, whether linear or large, among pixels of the image. These large dependencies can be effectively captured through an ICA space representation. Independent Component Analysis (ICA) minimizes both second order and top-end dependencies in input data and tries to find the basis along which data (when projected on them) is statistically independent. [6] These coordinates are contained in the mixing matrix $A = W^{-1}$.

Bartlett et al. have provided two ICA architectures to perform the face recognition task [48]:

1. **Architecture I** - statistically independent image basis
2. **Architecture II** – representation of the factorial code.

Researchers who have approached this topic consider the ICA-induced metric to be superior to other methods in that it can provide a more robust display of noise effect such as light variations. [3]

2.3.3. The Haar Classifier

A Haar feature consists of two or more adjacent rectangular, vertical, or horizontal regions, and its value is the difference between the pixel sums within these rectangular regions.[42]

Contrast variations between pixel groups are used to determine dark areas and relative light areas. Two or three adjacent groups with a relative contrast variation from a Haar feature are used to detect an image. Haar functions can be scaled easily by increasing or decreasing the size of the pixel group being examined. This allows the use of various functions for detecting objects of various sizes.[48]

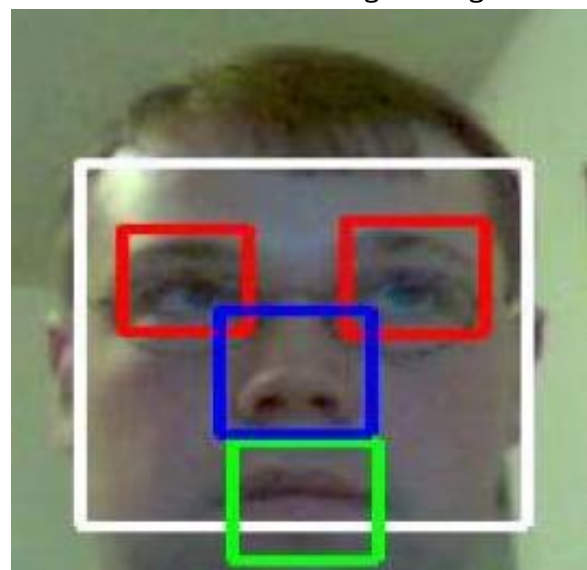


Fig. 13 Example of detection using Haar classifier [48]

2.3.4. LDA (*Linear discriminant analysis*)

Linear discriminant analysis (LDA) is a well-known method for reducing size in model recognition. It projects large original size data on a low dimensional space where all classes are well separated by maximizing the Raleigh coefficient. LDA creates a linear combination of independent features that produces the greatest difference between the desired classes. The basic idea in the case of LDA is to find a linear transformation so that the groups of characteristics can be separated after the transformation, which can be done by a dispersion matrix analysis.

2.4 Difficulties and shortcomings in biometric verification systems

- **Susceptibility of the biometric sensor to noisy or wrong data:** (a fingerprint image with a scratch or a cold-speckled voice sample are examples of noisy data). The captured biometric feature can be distorted due to imperfect purchasing conditions. This limitation can be seen in applications that use face recognition. The quality of captured facial images can be affected by illumination conditions and facial expressions. Noisy data may also appear from defective or inadequately maintained sensors
- **It may not be compatible with certain population groups.** Fingerprint images may not be properly captured for elderly and small children due to faded or incomplete digital prints.
- **"Intraclass" variations:** These variations are typically caused by a user who interacts incorrectly with the sensor (for example, it has an incorrect position on the face), or when the characteristics of a sensor are altered during authentication (for example, optical sensors to fingerprint sensors).
- **Within a large population, unimodal biometry is prone to inter-class similarities.** Face recognition may not work properly for identical twins, as the camera may not be able to distinguish between the two subjects. Erroneous matches may therefore occur.
- **Absence of universality:** The biometric system may not be able to acquire significant biometric data from a subset of users. For example, a fingerprint biometric system can extract incorrect features from fingerprints of some people due to the poor quality of papillary crests.
- **Cyber attacks:** unimodal biometric systems are quite vulnerable to cyber attacks in which data can be imitated or faked. It is mentioned of the creation of a fingerprint clone using Matsumoto's "gum fingers" technique or using latent traces of fingerprints from certain objects that have managed to "trick" the systems most often.

It should be noted that facial detection does not allow accurate results to be obtained for any of the commonly used techniques.

The main factors that can cause automatic face detection difficulties (in two-dimensional images):

- their position and orientation in the image (frontal, profile, angle, etc.) - some facial features (eyes, nose) may be partially or totally hidden; [74]

- the presence / absence of some structural components - some facial features such as beard, mustache, glasses may or may not be present and there is a great variability in shape, color or size;
- facial expression - face geometry being affected by it; [74]
- obturation - faces may be partially masked (covered) by other objects (including other faces);
- the conditions in which the photograph was taken - the illumination (spectrum, position and / or distribution of the source / sources of light, intensity) and camera characteristics (lenses, sensor) greatly affecting how a figure appears in the image. [74]

2.5 Community legal framework in the field of biometrics

A constant concern of the legislator, both national and communitary, was to regulate an adequate legal framework for the protection of personal data. This concern lies in the need to ensure the correct and legal use of the individual's personal data, subject to strict control that prevents any form of abuse of individuality and liberty. In the light of the fundamental principles governing individual social-human values, the legislator has set up a series of laws and directives both at national and European level that imperatively enshrine the rules on the protection of personal data.

At the same time, very rapid technological progress has forced the editing of legal norms able to prevent the misuse of personal data. In this regard, the legal norm comes to prevent this danger and provides protection for the individual.

In connection with the above, it has to be said that the facial recognition techniques have undergone a major improvement, which is both a technological success with real benefits and a potential threat to society.

The European personal data protection regulation is precisely such a new law, applicable to all Community states, which is based on the new realities.

2.6 Conclusions

Biometrics is a set of technologies (called biometric technologies) that exploits man physical or behavioral characteristics such as fingerprint, signature, iris, voice, face, walking, and hand gestures in order to differentiate the individuals. The abovementioned biometric parameters are unique to the individual, and there is little chance for others to replace these features, so that biometric technologies are considered the strongest in terms of security.

In conclusion:

- Biometrics is gradually becoming a part of our everyday life and is one of the major challenges for a safer world. The market for authentication and identification products is on the rise due to the growing need for personal security in the professional, public and private sector.

- Biometrics is increasingly used for identity cards, airports, prisons, access to secured premises, electronic voting, security of bank payments or Internet transactions.
- Biometrics is an alternative to passwords and other identifying elements that tries to eliminate any traces of doubt about identity. This makes it possible to verify that the user is the person who claims to be.

Facial identification is the subject addressed in the second subchapter of Chapter 2.

Compared to other biometric systems, such as fingerprints, iris measurements, facial detection does not work with extreme precision, but face analysis has several advantages. First, the face recognition system can use standard video cameras (as opposed to the cost and complexity of capturing fingerprints or iris images), and second, the human face is captured, even without any notice, and can be used for security systems.

The objective of such a system is to find the best fit in the sequence of images, captured by using a camera, with a given image. Using a set of image databases, the Face Recognition System should be able to identify or confirm one or more people in the scene. Before recognizing the face, the system must determine whether or not there is a face in a given image or in a video sequence of the images. Once the face detection has been performed, the face region must be isolated from the scene for face recognition. Face detection and extraction of facial features are often performed simultaneously.

Face extraction methods are the core (nucleus) of facial recognition algorithms, because the direct use of image pixels in the real-time system is not possible because of the large amount of data.

In most cases, in order to reduce data sets, the Principal component analysis (PCA) method is used, which describes data sets as coefficients that evaluate data variation. Other methods such as Independent component analysis (ICA), Linear discriminant analysis (LDA), and Haar Classifier are used to reduce data sets.

The last subchapter analyzes some of the problems and limitations faced by detection and facial recognition for better recognition and accuracy of recognition.

Although it offers many advantages, questions remain about the effectiveness of biometric systems as security or surveillance mechanisms, their degree of use and manageability, the opportunity in very different contexts, the social impact, the effects on privacy and the legal and political implications.

CHAPTER 3

STATISTICAL RESEARCH REGARDING THE CONCERN OF LIBRARY MANAGERS AND LIBRARIANS FOR THE NEED TO IMPLEMENT A NEW SECURITY SYSTEM AND THE EXISTING SYSTEMS IN LIBRARIES

3.1 The description of tools used in statistical research

3.1.1 Purpose and objectives underlying research

The study started from our desire to propose a complementary system permit entry library users based on facial recognition. The purpose of the research was to determine librarians' opinions, both with executive and management functions, on library security systems, as well as on the implementation of a system for facial recognition of users.

3.1.2 Research hypotheses

1. Librarians concerned with the security of individuals, in the context of terrorism, are eager to implement a facial recognition system in the library in which they operate.
2. Librarians who believe that the most appropriate biometric recognition system for security of collections and individuals is facial recognition, would agree to implement such a system in the library in which they operate.
3. Librarians who have confidence in facial recognition systems agree to implement such a system in the library in which they operate.
4. Librarians who work in large libraries agree to implement a facial recognition system.
5. The higher the level of education of librarians, the more they are willing to implement a facial recognition system in their library.
6. Librarians with a leading position are more likely to implement a facial recognition system in their library.
7. Librarians with work experience of more than 31 years are more likely to implement a facial recognition system in the library in which they work

3.1.3 Material and method

The working methodology used, relevant for identifying respondents' views on the security of collections and individuals, was the application of an online questionnaire, consisting of 16 questions. Respondents were notified before filling in the questionnaires on the confidentiality regime of the collected data. The questionnaire was designed on the basis of the concept's operationalization, starting from the definition of security in the library.

The survey comprised 177 respondents, both in Romania and abroad, and was conducted in February / March 2017. Data processing was performed using the SPSS (Statistical Package for Social Sciences) and the Excel program.

3.1.4 Description of the groups of subjects

In order to identify the librarians' opinion on the safety of collections and individuals, two groups of subjects were investigated. The questionnaires have been distributed in as many countries as possible for better representation.

The first batch comprises 145 respondents, of whom 93 are from Romania and 50 from Moldova.

Tabelul 2. Distribution of respondents from Romania and Moldova, depending on the country

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	România	93	64.1	65.0	65.0
	Moldova	50	34.5	35.0	100.0
	Total	143	98.6	100.0	
Missing	System	2	1.4		
Total		145	100.0		

Distribution of respondents from Romania and Moldova according to the country

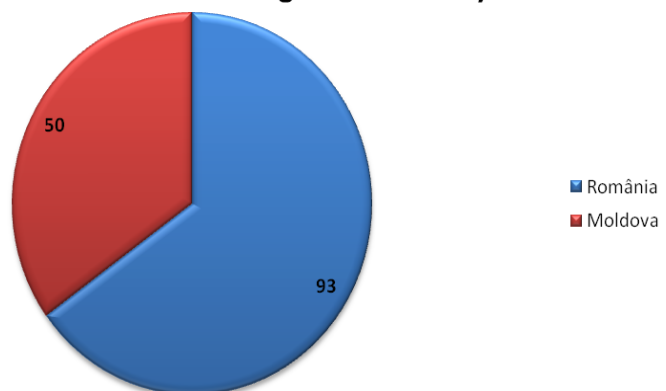


Fig. 16 *Distribution of respondents from Romania and Moldova, depending on the country*

As can be seen in the figure below (Figure 17), the level of education of the respondents is high. Of a total of 145 subjects in Romania and Moldova, 43.4% have university studies, 34.5% postgraduate and 15.9% doctoral.

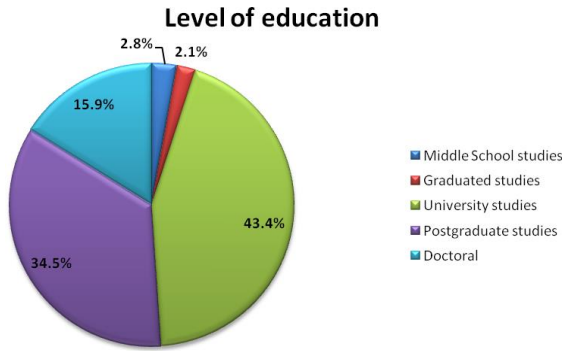


Fig. 17 *The level of education of the respondents in Romania and Moldova*

The questionnaires were distributed to both those with a leading position and executives. Thus, 30.3% represent those with leading positions and 66.2% are those with executive positions.

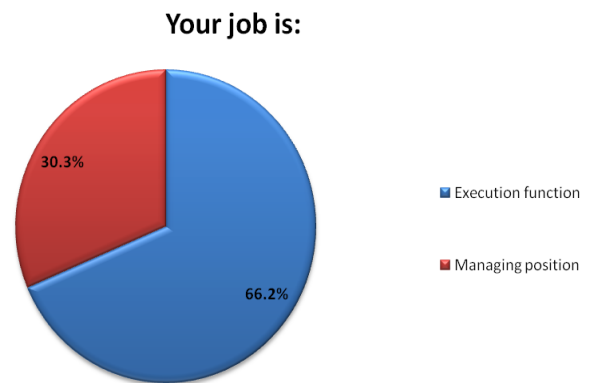


Fig. 18 *The function of the respondents in Romania and Moldova.*

Most of the respondents in Romania and Moldova, 44.1% have gained experience at work, with a workplace age of 21 to 30 years, 22.1% are between 11 and 20 years of work experience, 12.4% between 31 and 40 years, a smaller percentage of 10.3% have less experience, ranging from 5 and 10 years and only 5.5% have a work experience of over 40 years



Fig. 19 *Work experience of respondents in Romania and Moldova*

More than half of the first Lot of subjects work in a university library, 28.3% work in a school library, 5.5% in a public library, and 2.8% specialized libraries of the Academy, as well as other situations such as the National Military Library, Documentation and Information Center, limited access libraries.

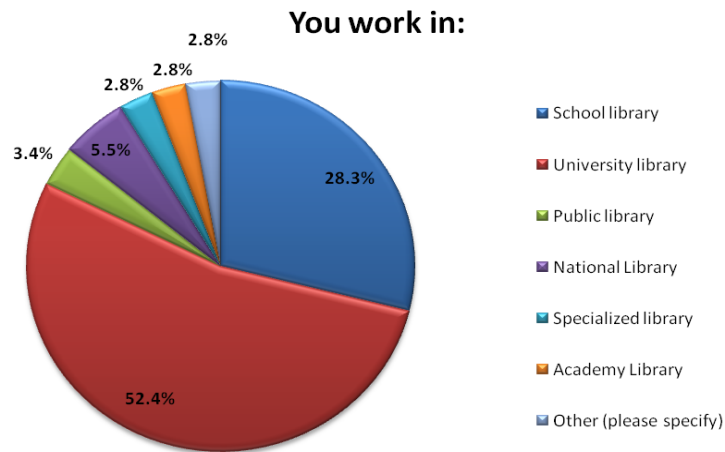


Fig. 20 Distribution of respondents from Romania and Moldova, depending on the library in which they work

Regarding the second group, it consists of 32 respondents, but this time abroad. We wanted to get the opinion of those outside the country about the project we want to implement, because the security of people in public places is a problem we are currently facing, with international terrorism being manifested anywhere in the world. Thus, the countries participating in the survey are: Albania, Armenia, Belarus, Bosnia and Herzegovina, Bulgaria, Greece, Ireland, Montenegro, Norway, the United Kingdom, Russia, Serbia, Turkey, Hungary. The questionnaire was translated into English, being a language of international circulation.

As with Romania, the level of education of respondents abroad is very high, all of them having more than average education. Most respondents, 34.4% graduate from postgraduate studies, 31.3% university graduates, and 25% graduate from a doctoral school.

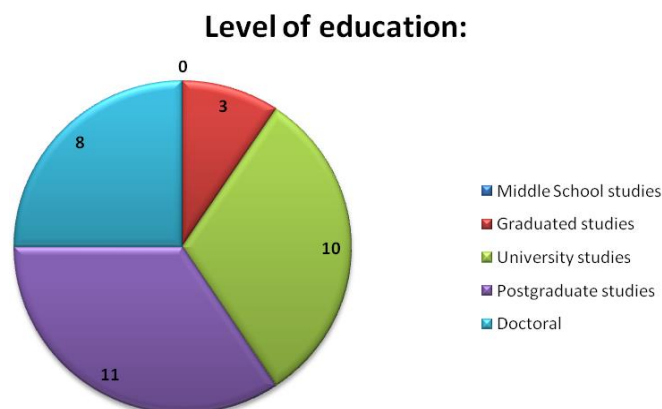


Fig. 21 The level of education of respondents in Lot 2

Most of those surveyed abroad have a staff management post, 28.1% represent the leading staff and only 21.9% have a job of execution.

Your job description: Response Percent

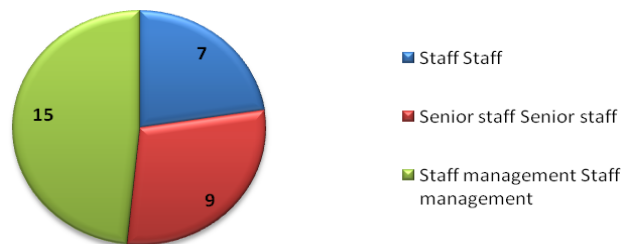


Fig. 22 Description of the work position of respondents in the Lot 2

Out of a total of 32 respondents from several countries, 4 have less than 5 years of experience in the workplace, 10 of those interviewed have experience between 5 and 10 years, 3 between 11 and 20 years, 9 between 21 and 30 years and 6 between 31 and 40 years.

Experience in the workplace:

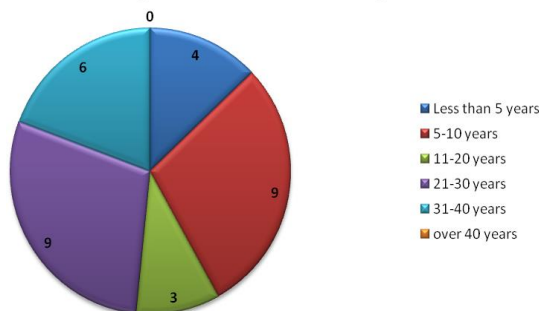


Fig. 23 Work experience of respondents in Lot 2

Most respondents in Lot 2 work in a university library, 5 in the Academy library, and 3 in specialized libraries.

You work in:

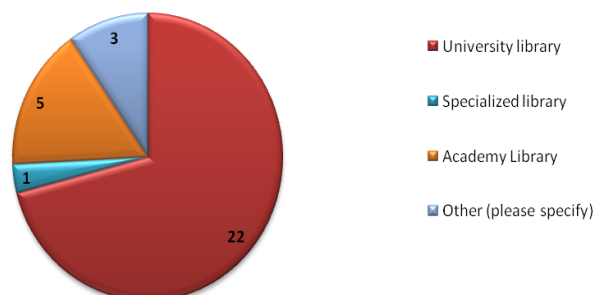


Fig. 24 Distribution of respondents in Lot 2, depending on the library in which they work

3.2 Research results

3.2.1 Results description

To the question "Overall, how satisfied are you with the security of library collections?" Most respondents in Romania and Moldova, 45.5%, are quite satisfied, 33.1% consider themselves quite dissatisfied about this, 8.3 % are very satisfied and 10.3% very dissatisfied.

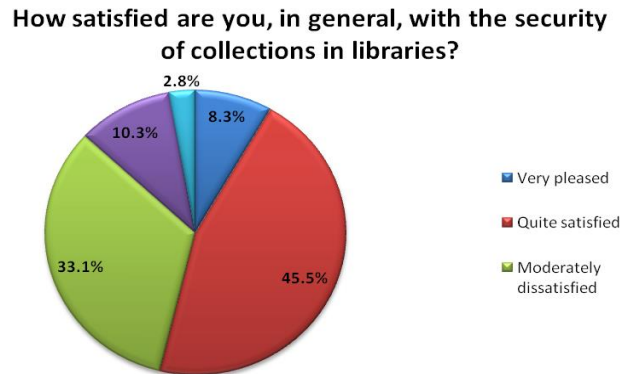


Fig. 25 Satisfaction of the librarians from Romania and Moldova on the security of library collections

Analyzing the answers of the librarians in Lot 2, we found that most are quite satisfied with the security of libraries' collections, but there are also 9 librarians, quite dissatisfied and 3 very dissatisfied with this issue.

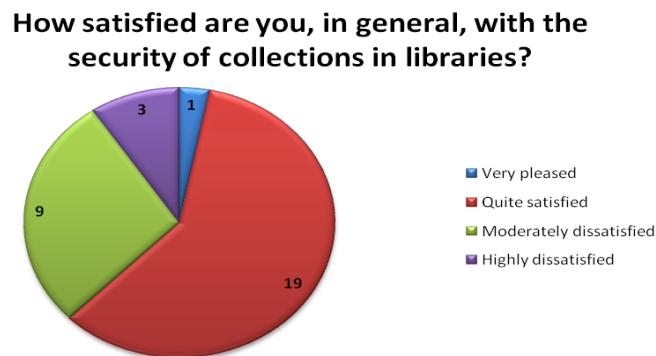


Fig. 26 Satisfaction of the librarians in Lot 2, on the security of libraries' collections

From the chart based on the analysis of the collected data, one can notice that the biggest problem regarding the security of the library collections, which the respondents in Romania and Moldova face, is the loss of the copies. 19.3% consider that the biggest problem is the lack of storage space, 15.9% claim that theft is the main problem in the security of collections, 6.9% believe that vandalism is a particularly important problem and 4.8% the inattention of employees .

What is currently the biggest problem of your security library collections?

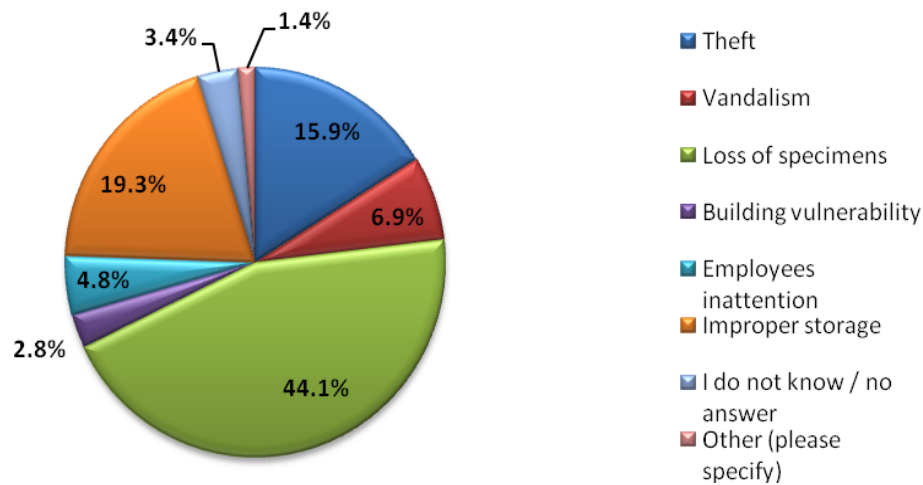


Fig. 27 The biggest problem of respondents in Romania and Moldova about the security of library collections

Most respondents in Lot 2, believes that employee inattention is the biggest security issue for collections in the library in which it operates, 7 said vandalism is the biggest problem, a number of 6 librarians have estimated that the vulnerability of the building is in the first position and 2 claimed that the spaces storage is the main issue on security of collections.

What is currently the biggest problem of your security library collections?

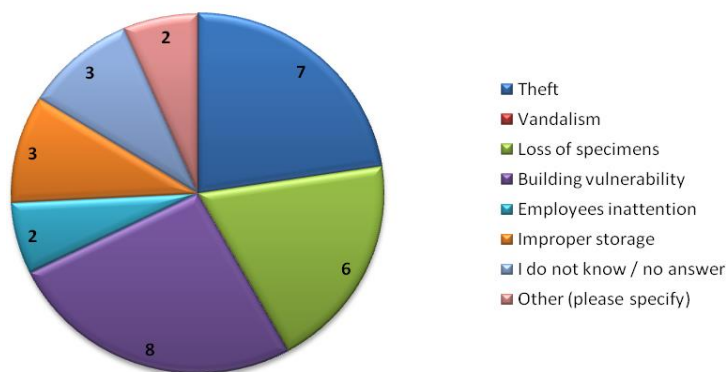


Fig. 28 The biggest problem of Lot 2 respondents about the security of library collections

Out of a total of 145 respondents in Romania and Moldova, the highest percentage, 56.6% said that someone had entered the library without a permit, and 35.2% said that it did not happen never in the library where it works.

You ever had anyone enter without a pass?

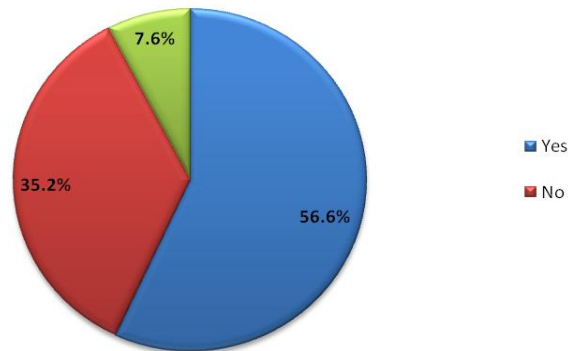


Fig. 29 *The answers of librarians from Romania and Moldova to the question "Has anyone ever gotten a permit without permission?"*

As a result of the data analysis, 16 librarians from the group of respondents from several countries have admitted that some people entered the library without a permit, and 11 respondents said this did not happen the case of their library.

You ever had anyone enter without a pass?

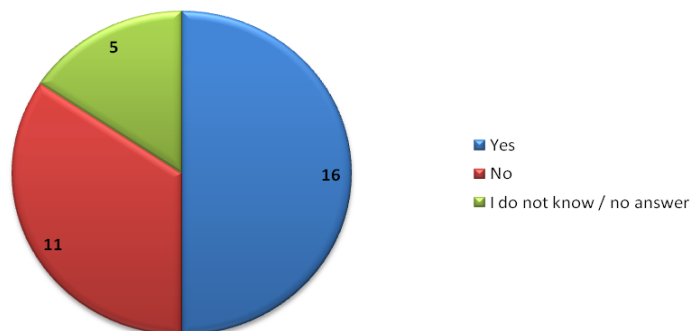


Fig. 30 *The librarians' answers, in Lot 2, to the question, "Has anyone ever been allowed to enter without a permit?"*

Regarding the issue of terrorism, 51,7%, ie 75 out of 145 respondents in Romania and Moldova, consider that additional measures should be taken regarding the security of the persons in the library, 33,1% did not think about this and 8.3% believed that the current security is sufficient.

On the issue of terrorism, do you think we should have additional measure concerning the safety of persons in the library ?

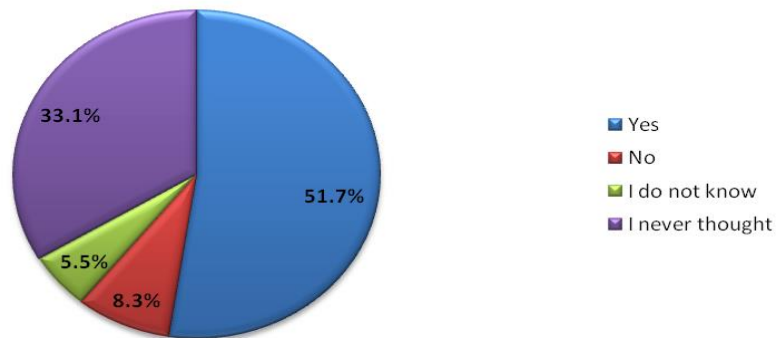


Fig. 31 The opinion of the respondents in Romania and Moldova regarding the additional measures regarding the security of the persons in the library

13 librarians from Lot 2 have said that it is necessary to take additional measures regarding the security of people in the library in the context of terrorism. 12 have not taken this issue into account and 6 consider that no further action should be taken.

On the issue of terrorism, do you think we should have additional measures concerning the safety of persons in the library?

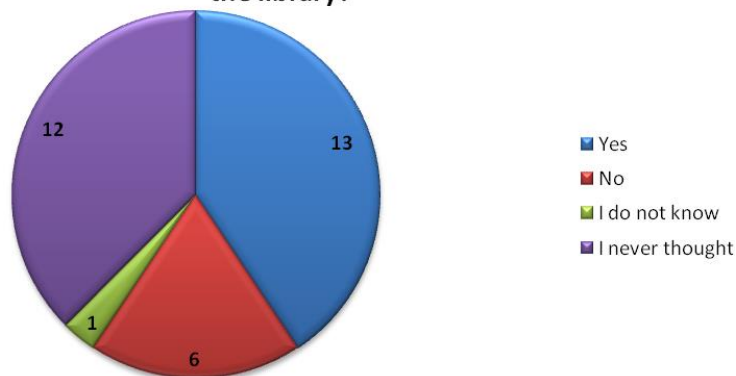


Fig. 32 The opinion of Lot 2 respondents on additional security measures for people in the library

Out of a total of 145 respondents in Romania and Moldova, 54.5%, ie 79 librarians believe that biometric recognition systems are the safest security systems that can be used in libraries and 33, 1%, ie 48 of the total respondents believe the RFID system is the safest.

What is, according to your opinion, the safest security system that can be used in libraries?

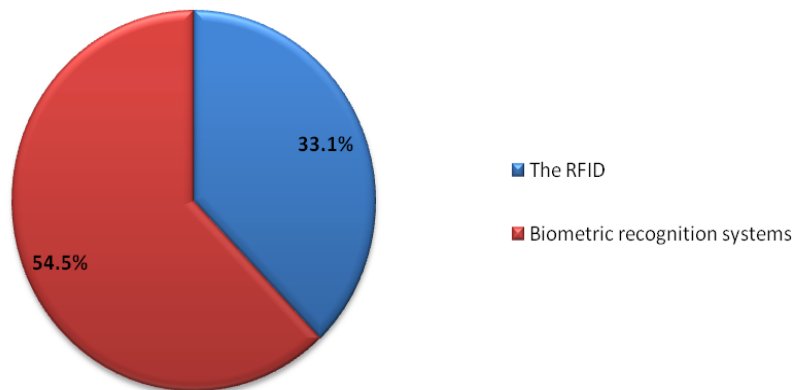


Fig. 33 Respondents from Romania and Moldova, regarding the safest security system, that can be used in libraries

Analyzing the answers of the Librarians in Lot 2 we can see that 19 of them believe that biometric systems are the safest security methods that can be used in libraries and 12 believe that RFID is the safest security system.

What is, according to your opinion, the safest security system that can be used in libraries?

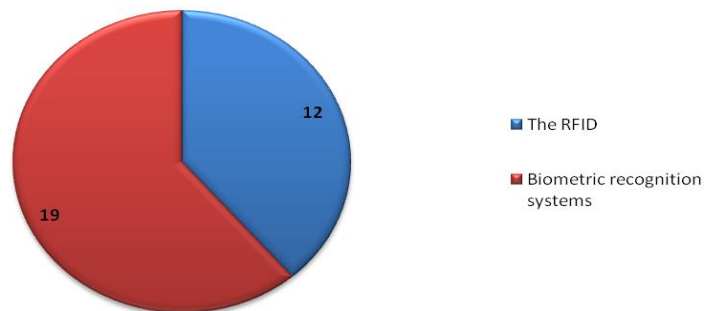


Fig. 34 The opinion of Lot 2 respondents about the safest security system that can be used in libraries

39.3% of respondents in Romania and Moldova believe that the most appropriate biometric security system for libraries is the one based on facial recognition, 13.8% believe that the dactyloscopic is the most appropriate and a fair percentage of 33.8% were unable to give an answer on this issue.

What is, according to your opinion, the best biometric recognition system for the security of collections and people in a library?

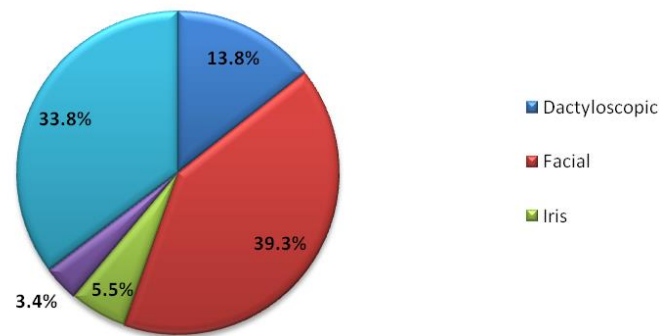


Fig. 35 The most appropriate security system for collections and people in a library, according to respondents from Romania and Moldova

The majority of respondents in Group 2 could not judge which is best biometric security libraries, five felt the facial recognition system is the best security collections and those from a library, 4 are of the opinion that the one based on iris analysis and 2 considered the dactyloscopic system to be the most appropriate.

What is, according to your opinion, the best biometric recognition system for the security of collections and people in a library?

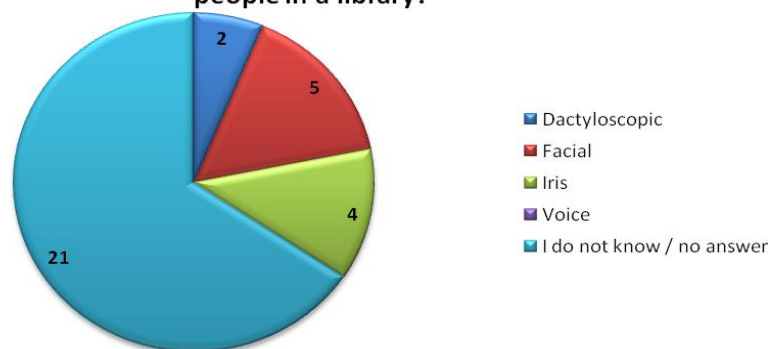


Fig. 36 The most appropriate security system for collections and people in a library, according to respondents in Lot 2

After analyzing the data, we can observe that 38.6% of Romanian and Moldovan librarians have quite a lot of confidence in facial recognition systems, 9% have a lot of confidence, 18.6% have not much, or little, on when 7.6% do not have much confidence and 0.7% do not trust at all.

How much do you trust the facial recognition systems?

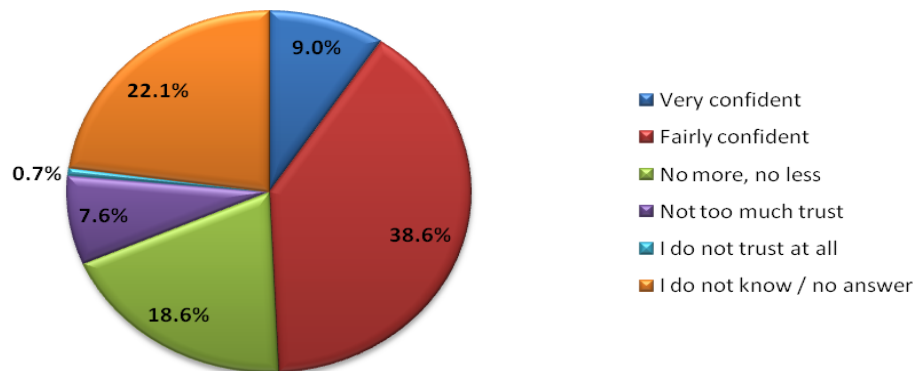


Fig. 37 The level of confidence of respondents in Romania and Moldova, with regard to facial recognition systems

Of the total of 32 respondents in Lot 2, 9 have quite a lot of confidence in facial recognition systems, 13 not much or a little, one respondent has little confidence, one does not trust at all, and one respondent has a lot of confidence .

How much do you trust facial recognition systems?

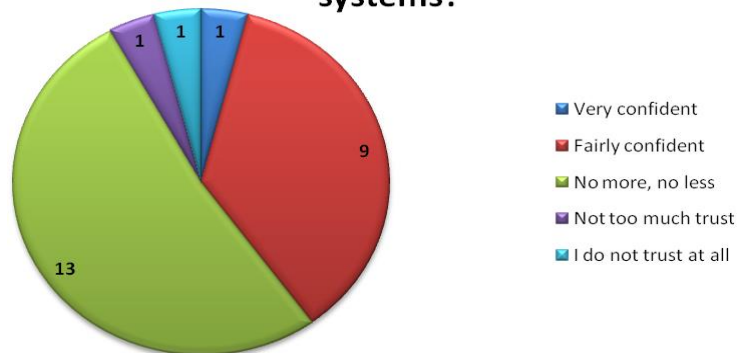


Fig. 38 The confidence level of respondents in Lot 2, with regard to facial recognition systems

Out of a total of 145 librarians in Romania and Moldova, 61.4% would agree to the implementation of a facial recognition system in their library, 12.4% disagree, and 23 , 4% did not comment on this.

Would you agree with the implementation of a facial recognition system in the library you work?

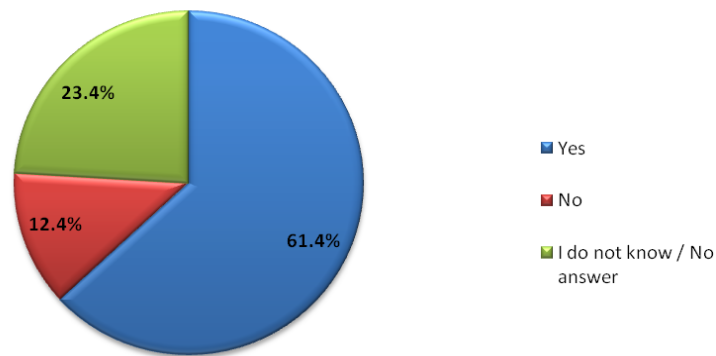


Fig. 39 The agreement of librarians in Romania and Moldova on the implementation of a facial recognition system

As for respondents from abroad, out of a total of 32, 13 agreed to implement a facial recognition system, 11 disagreed and 8 did not express their opinion.

Would you agree with the implementation of a facial recognition system in the library you work?

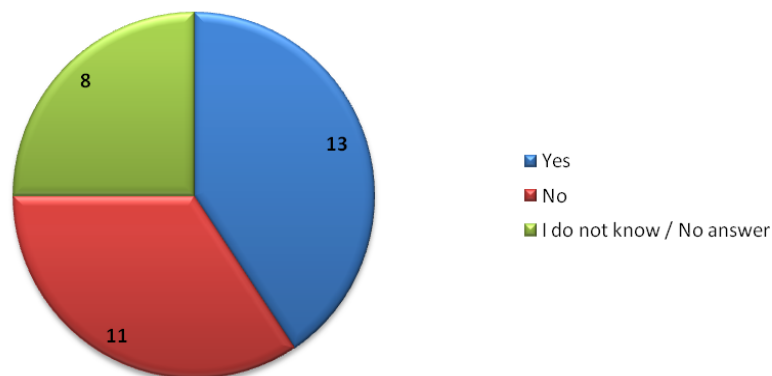


Fig. 40 The agreement of foreign librarians to implement a facial recognition system

3.2.2 Hypothesis testing

Ipoteza 1. Librarians concerned with the security of individuals, in the context of terrorism, are eager to implement a facial recognition system in the library in which they operate.

Next, we will formulate two hypotheses, the null hypothesis (H0) referring to the worst case and the alternative hypothesis (H1), the opposite of the null.

H0 - there is no correlation between the librarians' desire to take action on the security of individuals and the agreement of librarians to implement a facial recognition system;

H1 - there is a correlation between librarians' desire to take action on people's security and the agreement of librarians to implement a facial recognition system;

The probability of guaranteeing the results is 95%, the 5% error margin is the probability of error and under these conditions, the probability of testing the null hypothesis (p) will be 0.05.

The general rule of test for a 95% probability of guaranteeing results: $x_{\text{calculated}} < x_{\text{critic}} \Rightarrow$ rejects the hypothesis of null H_0 . Where: $x_{\text{calculated}} = p_{\text{calculated}}(\text{Sig.})$ and $x_{\text{critic}} = p$, iar $p = 0.05$.

According to the Pearson index, the variable measuring librarians' willingness to take action on the security of individuals in the context of terrorism is correlated to the level of 0.203, with the variable expressing the agreement of librarians to implement a facial recognition system. Sig= 0.008 is less than $p = 0.05$, [hence it results that](#) the null hypothesis is rejected and there is correlation between the librarians' desire to take action on the security of individuals and the agreement of librarians to implement a facial recognition system. Sig=0.008, $p < 0.01$ indicating a strong link between the two variables. Thus, the more librarians are concerned with the security of individuals in the context of terrorism, the more they are willing to implement a facial recognition system, and vice versa.

The hypothesis that librarians concerned with the security of individuals in the context of terrorism are eager to implement a facial recognition system in the library in which they work is confirmed.

According to the same explanation from hypothesis 1, 3 hypotheses are confirmed and 4 are rejected.

3.3 Conclusions

The research has led to the following conclusion: most librarians agree to implement a facial recognition system in their library to enhance security. It could be noticed that the respondents from abroad were more detained in comparison with those from Romania and Moldova.

Librarians concerned with the security of individuals in the context of terrorism are eager to implement a facial recognition system in their library. Also, librarians who believe that the most appropriate biometric recognition system for collections and people security is facial recognition, would agree to the implementation of such a system. The degree of trust in facial recognition systems plays an important role in the decision of librarians to increase the security of the library by installing the new system.

From the data analyzed, the library size, librarians' function, or the 31-year experience at work does not interfere with librarians' decision to implement the new facial recognition system. Also, the level of librarians' preparation does not interfere with this decision, probably because most have more than average education.

CHAPTER 4

OPTIMIZING THE LIBRARY SECURITY SYSTEM BY IMPLEMENTING A FACIAL RECOGNITION SYSTEM

4.1 Introductory Notions

The computer terms required to understand the operation mode of the VisageCloud facial recognition system, which is the subject of this chapter, are presented.

4.2 VisageCloud face recognition for authentication, quick verification, and smart security (protection)

The developed computer application monitors access to libraries and is designed to respond to the growing demand for an effective system to control access and presence in a location in the context of terrorism. The goal of the system is to ensure fast, secure and reliable monitoring of users' access to various public locations.

VisageCloud is a "end to end" solution for face recognition and classification. Can work on photos, stickers, identity cards and video streams. VisageCloud allows users to register at the library entrance, guests at a hotel, and more. The application provides information about suspected individuals (various offenses, terrorism, etc.). In addition, VisageCloud allows you to obtain additional information from existing surveillance cameras, obtaining real time notifications and reports. VisageCloud can function as a cloud or on-premise service. It is based on an Application Programming Interface (API), so it can be easily integrated into other applications or systems.

4.2.1 Domain Model of VisageCloud

In software engineering, a domain model is a conceptual model of the domain that incorporates both behavior and data.

In ontology engineering, a domain model represents a formal representation of a knowledge domain with concepts, roles, data types, individuals, and rules, typically based on descriptive logic and implemented in OWL (Web Ontology Language). A domain model is a system of abstractions that describes aspects of a sphere of knowledge, influence or activity (domain). The model can then be used to resolve issues related to that domain. The domain model represents a representation of significant real world concepts that belong to the field (activity) that must be modeled in the software. The concepts include the data involved in the chosen field and the rules used in the activity on these data. A domain model generally uses the domain vocabulary so that a representation of the model allows communication with non-technical stakeholders. A domain model is generally

implemented as an object model in a layer that has a lower level of persistence and emits an API at a higher level to gain access to model data and behavior. The domain model in the Unified Modeling Language (UML) is represented by a class diagram.

The domain model of VisageCloud contains four key elements:

1. **Account** - gives access to the management of multiple collections;
2. **Collection** - includes several profiles of different (different) individuals. E.g. users, employees, etc .;
3. **Profile** - identifies a distinct individual (eg Elena, Emilia, Radu, Alexandru, etc.) belonging to a collection, **and**
4. **Face** - an illustration of an individual's face as captured from a photo. The presence of multiple faces associated with a profile (preferably with different illumination, perspective, makeup, facial expression or other contextual features) helps to improve the accuracy of facial recognition.

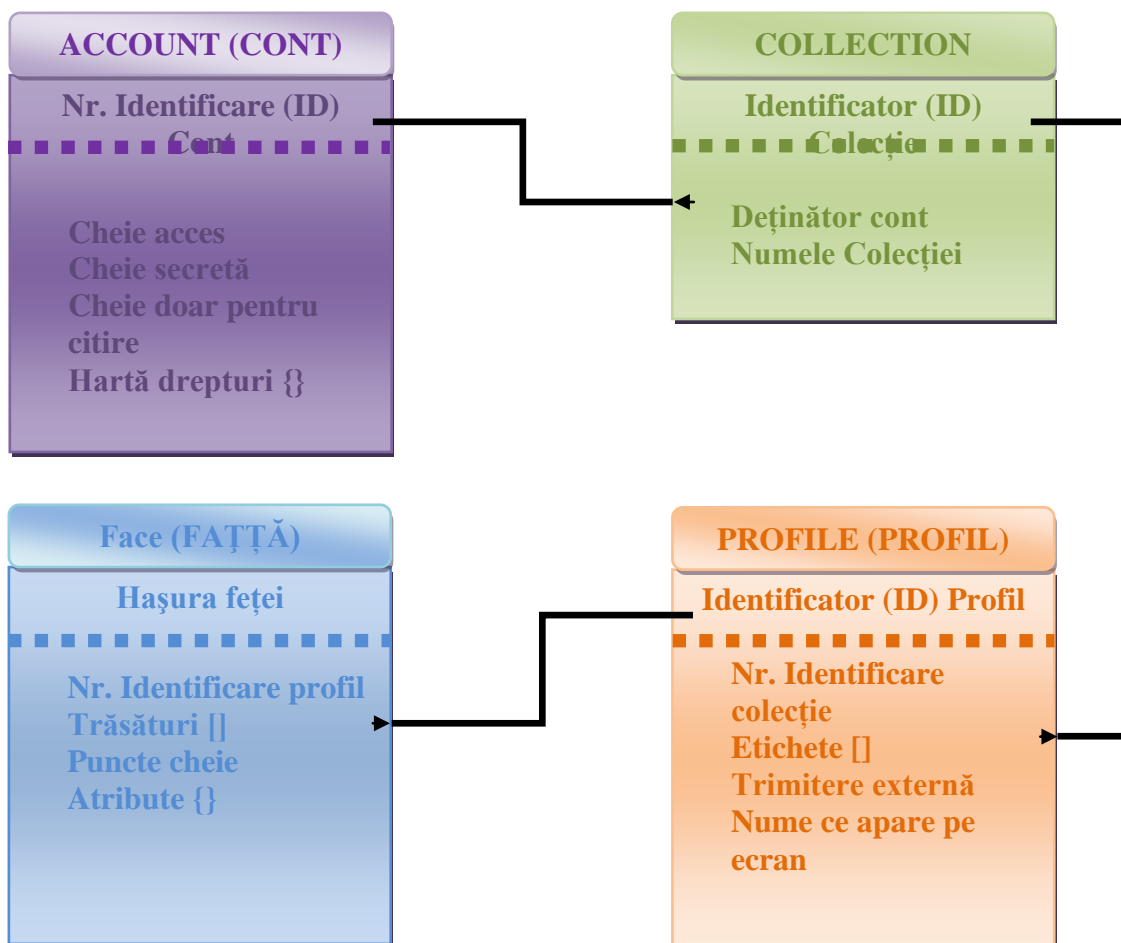


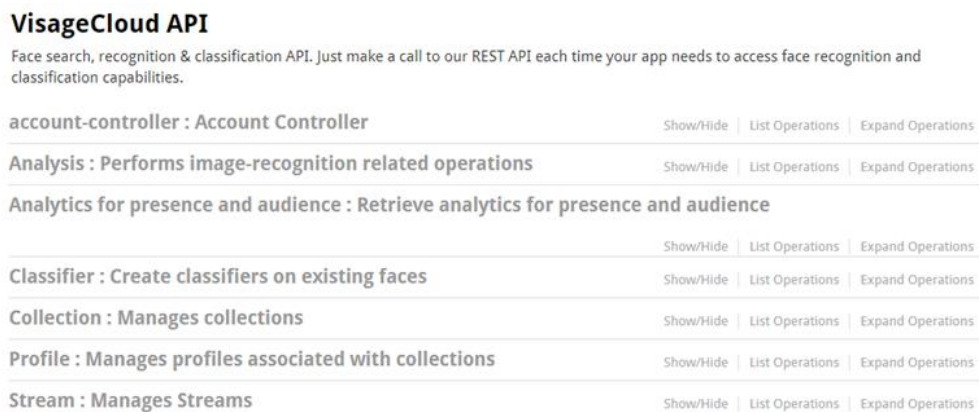
Fig.41 VisageCloud UML diagram

4.2.2 Visage Cloud: The programming interface (API)

The VisageCloud API is a Cloud REST API that can be used in applications to allow access to facial recognition and classification capabilities. Visage Cloud combines state-of-the-art algorithms for facial recognition and classification through query, tagging, and querying techniques to maximize data usage.

The Cloud API is a type of API that allows the development of applications and services used to provide hardware, software and cloud platforms. An API cloud serves as a gateway or interface that provides users with a direct and indirect cloud infrastructure as well as software services.

The Visage Cloud application programming interface appears in the following screen:



VisageCloud API			
Face search, recognition & classification API. Just make a call to our REST API each time your app needs to access face recognition and classification capabilities.			
account-controller : Account Controller	Show/Hide	List Operations	Expand Operations
Analysis : Performs image-recognition related operations	Show/Hide	List Operations	Expand Operations
Analytics for presence and audience : Retrieve analytics for presence and audience			
	Show/Hide	List Operations	Expand Operations
Classifier : Create classifiers on existing faces	Show/Hide	List Operations	Expand Operations
Collection : Manages collections	Show/Hide	List Operations	Expand Operations
Profile : Manages profiles associated with collections	Show/Hide	List Operations	Expand Operations
Stream : Manages Streams	Show/Hide	List Operations	Expand Operations

Fig.42. Visage Cloud Application Programming Interface.

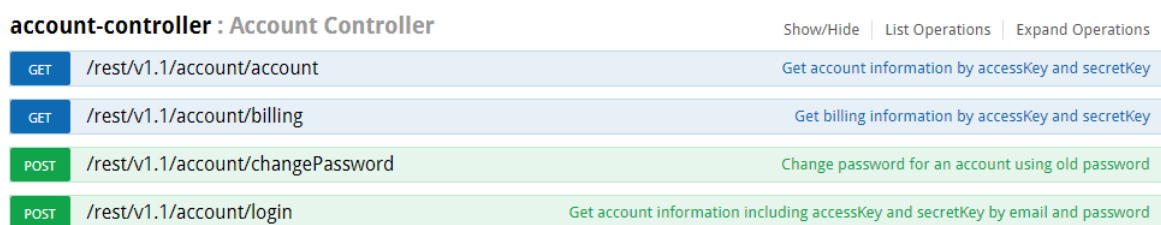
As you can see in the left-hand side of the screen, Visage Cloud submenus are displayed, namely:

- I. **Account-controller:** Account Controller;
- II. **Analysis:** Performs image-recognition related operations;
- III. **Analytics for presence and audience:** Retrieve analytics for presence and audience;
- IV. **Classifier:** Create classifiers on existing faces;
- V. **Collection:** Manages collections;
- VI. **Profile:** Manages profiles associated with collections;
- VII. **Stream:** Manages Streams,

and on the right appear on three columns the options that can be executed for each of the above mentioned submenus. The three options are: Show / Hide, List Operations, and Expand Operations.

I. Account Controller

When choosing Account controller, the following screen will appear:



account-controller : Account Controller			
GET	/rest/v1.1/account/account	Show/Hide	List Operations Expand Operations
		Get account information by accessKey and secretKey	
GET	/rest/v1.1/account/billing	Get billing information by accessKey and secretKey	
POST	/rest/v1.1/account/changePassword	Change password for an account using old password	
POST	/rest/v1.1/account/login	Get account information including accessKey and secretKey by email and password	

It can be seen that the Account option contains 4 submenus:

- a) Account
- b) Billing
- c) Change Password
- d) Login.

The four submenus of the Account option are described in the thesis.

II. Analysis

This option performs image recognition operations. By activating the option, the screen shown below appears.

Analysis : Performs image-recognition related operations			Show/Hide	List Operations	Expand Operations
GET	/rest/v1.1/analysis/compare	Compare several faces identified by faceHash, without depending on mapping faces to profiles			
POST	/rest/v1.1/analysis/detection	Perform detection on a given picture or picture URL			
GET	/rest/v1.1/analysis/listLatest	Retrieve the last *count* operations per current account			
POST	/rest/v1.1/analysis/recognition	Perform labeled recognition on a given picture or picture URL			
GET	/rest/v1.1/analysis/retrieve	Retrieve a complete analysis object including both detection and recognition information			

The operations performed for facial recognition are as follows:

- a) **Compare (Compararea)**. Compares multiple faces identified by "faceHash", without depending on face mapping to profiles. The VisageCloud API can compare two or more faces to evaluate whether they belong to the same person - even if that person is unknown.
- b) **Detection (Detectarea)**. Performs detection for a given image, or located in a Uniform Resource Locator (URL).
- c) **ListLatest** - By enabling this operation, the last count * operations for the current account can be retrieved.
- d) **Recognition (Recunoaşterea)**. Makes recognition labeled on a given image or at a URL.
Recognition or identification involves confirming a person's identity once his face has been detected in the image by searching for hundreds of thousands of faces known in less than a second. Each match is given a score so that the answer can easily be passed and an informed decision made.
- e) **Retrieve (Regăsirea)**. A completely analyzed image is obtained that contains both detection and recognition information.

III. Analytics for presence and audience

This operation allows for analytical techniques for presence and for audience, with the following options:

- a) Counting
- b) Presence/timeseries
- c) Presence/total.

IV. Classifier

Detected faces are **classified** by age, gender, ethnicity, or emotion, so this feature is especially useful for retail analytics and for designing digital real time targeting signals. Classification is not intended to highlight individual identities, but rather to use integrated analysis to generate the demographic composition of people in a particular area.

Clicking on this operation can create classifications for existing faces.

V. Collection

Collection Collection allows collection collections.

By enabling the Collection option, the following operations can be performed:

- a) retrieving all collections
- b) creating a new collection with a name
- c) Retrieve the contents of a collection for data analysis
- d) Delete the existing collection with associated profiles and faces
- e) Retrieve the contents of an existing collection
- f) Updating an existing collection with a specific identifier (specified name)
- g) Getting all profiles associated with a collection

VI. Profiles

Managing collections profiles can be done by selecting the Profile option in the VisageCloud application, which allows you to perform the following tasks:

- a) Obtaining profile registration status: information about the possibility of authentication
- b) Remove (deactivate) a face list, identified by faceHashes, from a profile identified by the profile ID
- c) Obtain all profile (faceHashes) associated with a profile
- d) Adding a list of faces, identified by faceHashes, to a profile identified by the profile ID
- e) Create a new profile without associated faces (empty profile)
- f) Deletes a profile and disables all faces belonging to that profile

- g) Retrieving a profile
- h) Update an existing profile with a given ID

VII. Stream

This operation allows you to manage streams. Related submenus include all flow-related operations: Display status (status) of all account flows; Obtain the last Ns recognized from the stream; Remove frames older than the specified range; Obtaining an individual frame image; Obtaining the last N frames processed from the stream; Start and end existing stream; Deleting existing stream Creating a new stream with a name; Updating an existing stream with a known ID; Get an existing stream with a certain ID (ID).

4.3 VisageCloud: Face detection and recognition

In the following, you will get from getting the API key to access the app when you create a known profile collection (a profile is a person) to detect people in photos and map them to your profile, and then using that collection to recognize people in new photos.

Step 1: Requesting an API key

In order to benefit from VisageCloud's facial recognition features, users can access the program at <https://visagecloud.com/>.

The interface shown in Figure 40 will appear:

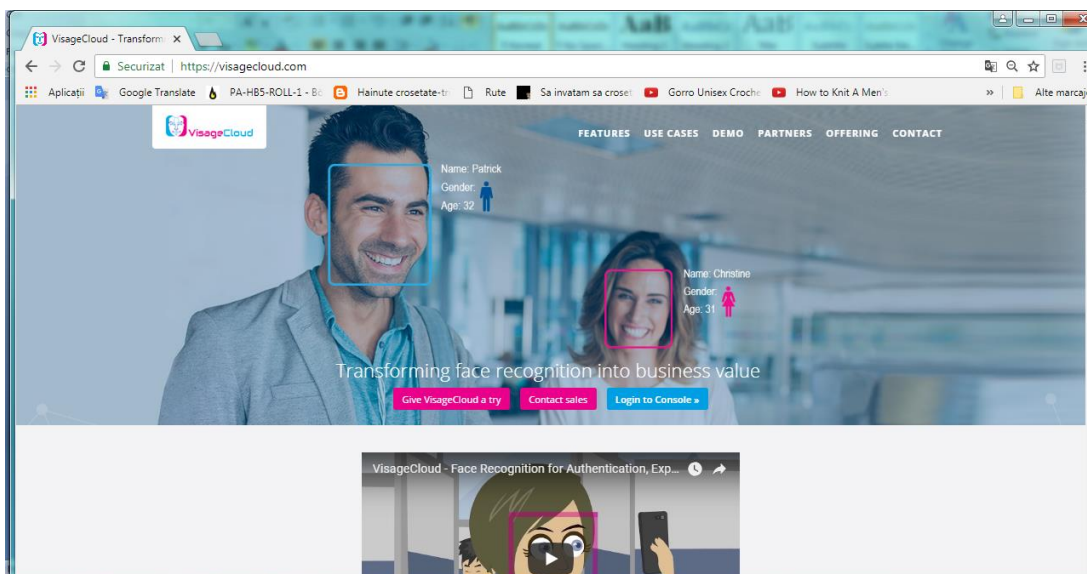


Fig. 93. VisageCloud interface: **Login to Console** option

where the Login to Console option will be selected. This will require logging data, namely: a username and a password, as can be seen in the following screen:

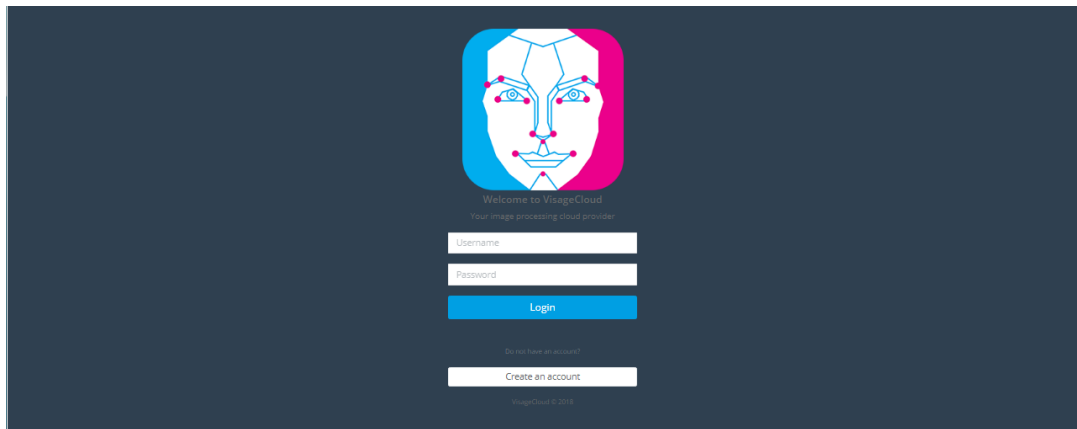


Fig. 94. VisageCloud interface: Login option.

It can be seen on the screen that the user has the possibility to request the creation of an account. The system response to this request is provided in the following interface:

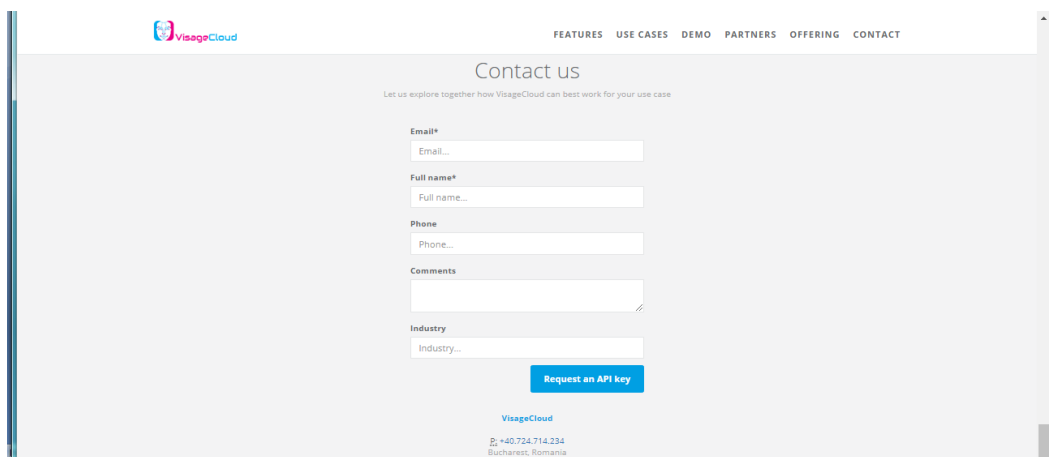


Fig. 95. VisageCloud Interface: Creating an Account.

After completing the Email and Full name fields that are required, the application will send the completed response to that request.

Three keys will be provided:

1. *accessKey* that uniquely identifies the user requested account
2. *secretKey* – this is the primary account key that allows the Holder either to perform detections / recognitions, create, modify, delete collections and profiles, and access sensitive (confidential) account information (such as the list of recent operations)
3. *readOnlyKey* – This key should also be secret, but it only allows for the detection / recognition operation without having the options to modify account data or to view sensitive (confidential) information.

All requests to the API must be authenticated by setting the GET "accessKey" parameter to the accessKey value and the "secretKey" parameter to the secretKey for write requests or readOnlyKey for detection / recognition requests.

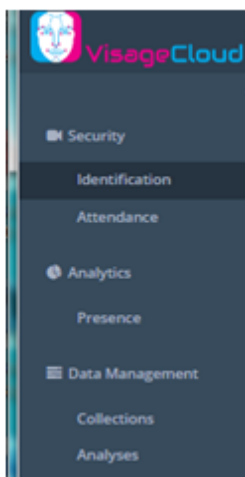
The final analysis and recognition points can be accessed by setting the GET "accessKey" parameter to the accessKey value and the "secretKey" parameter to the readOnlyKey value.

After obtaining this data, the user can log in to the VisageCloud facial recognition application. As a result of this action, the interface will appear:



Fig. 96. VisageCloud interface: the user login to the system

The name of the user who logged into the system appears in the upper right corner. On the left side of the screen are displayed the operations allowed by the user.



In the order in which they appear on the screen, they are:

- **Security** with options:
 - *Identification* and
 - *Attendance*
- **Analytics** with submenu:
 - *Presence*
- **Data Management** that provides data management through:
 - *Collections* and
 - *Analyses*.

Fig. 97. Visage Cloud operations available to the user.

Step 2: Creating a collection

For easier management of users registered in the system, it is necessary to create a collection (a set or a group of registered people). To do this, select the Collections option and it will appear:

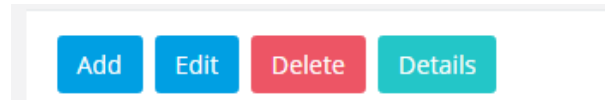


Fig. 99. Collection management options.

As can be seen from the analysis of this interface, it is possible to make the following options for managing collections:

- a) **Add:** which allows the addition of new collections.

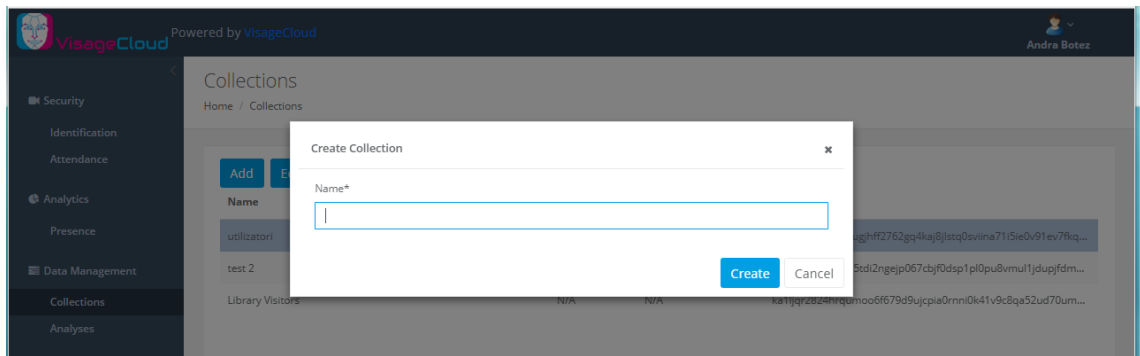


Fig. 100. **Add:** which allows adding new collections.

It is necessary to fill in the Name field. For example, "test". Then click **Create**.

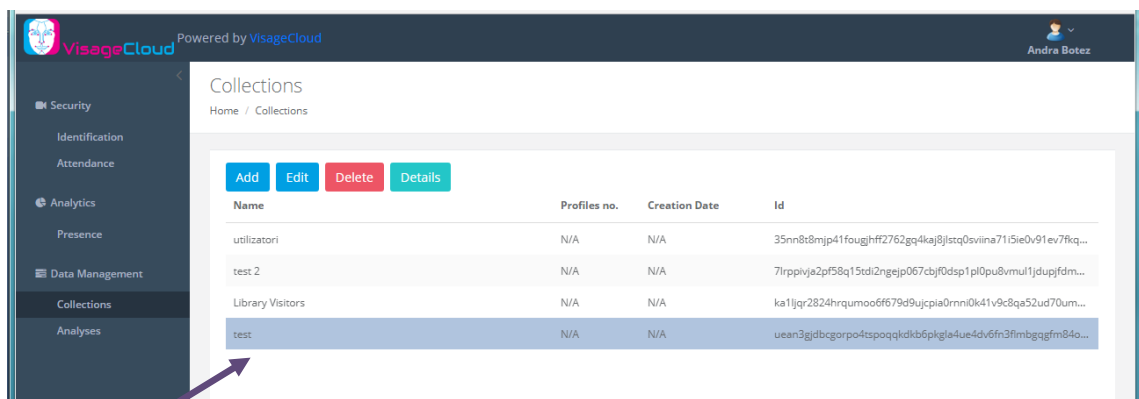


Fig. 101. Creating a new collection.

The test collection was created as you can see.

- b) **Edit** that allows the collection name to be updated.

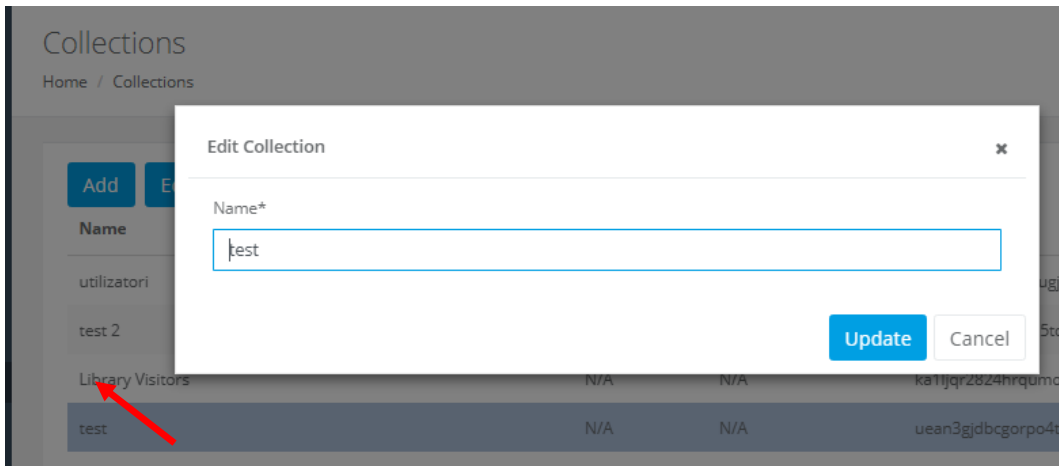


Fig. 102. **Edit:** Allows you to update the collection name.

Select a collection, click it, and the screen in the previous image will appear. An Update can be selected if an update to the name of that collection is desired or Cancel if the change is not intended.

c) **Delete** – when deleting a collection. For safety, the system asks for option confirmation.

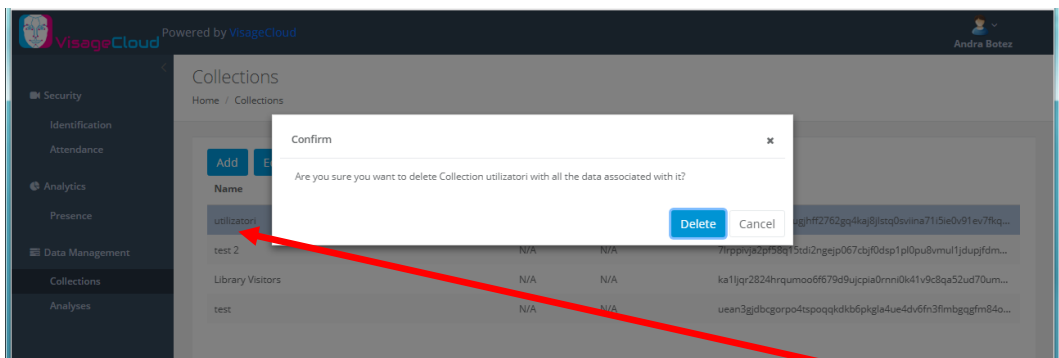


Fig. 103. **Delete:** allows deletion of a collection.

You can choose the Delete option which will delete the collection called users with all of its data, or Cancel, in which case the deletion will be dropped.

d) **Details** – an option that allows you to associate profiles for the created collection as shown in this screen.

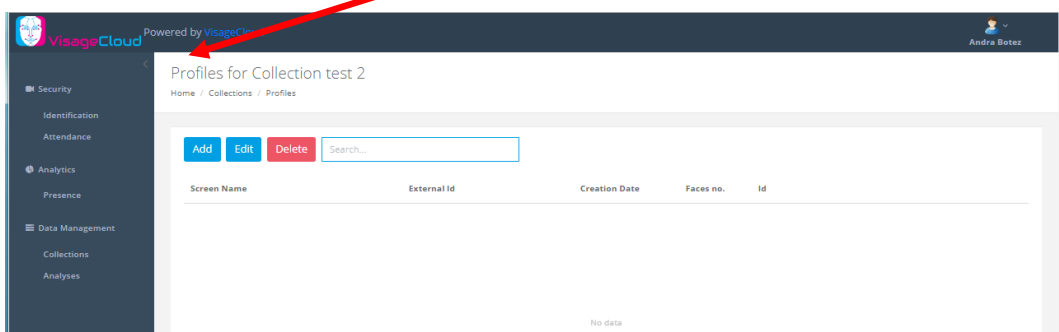


Fig. 104. **Details:** Allows you to associate profiles for the created collection.

This goes to step 3.

Step 3: Creating profiles for each person in the collection

A profile is a person. The parameters required to create a profile are:

- **accessKey, secretKey**
- **collectionId** - defines the collection in which you want to create the profile
- **externalId** - this allows you to link a profile to an external VisageCloud database
- **screenName** - is a label for each profile that can be read by man;
- **labels** - labels that will later allow us to perform a smoother filtering in face recognition.

To create a new profile, start from the interface in Figure 105.

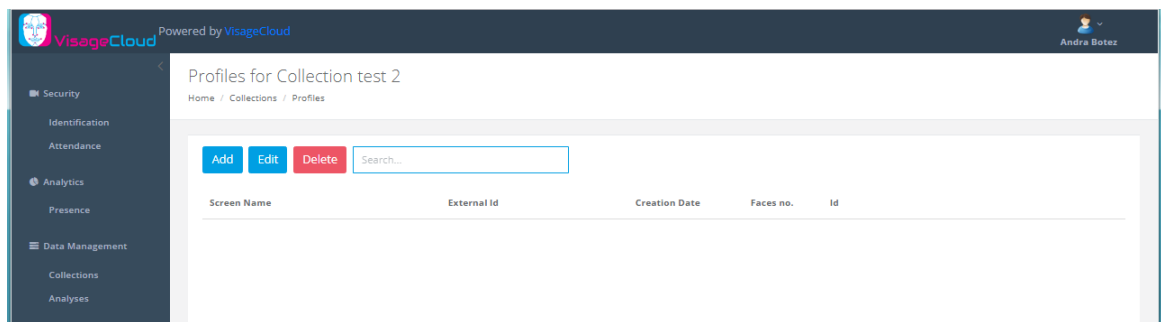


Fig. 105. Profile interface.

in which the Add option is selected and the following screen appears:

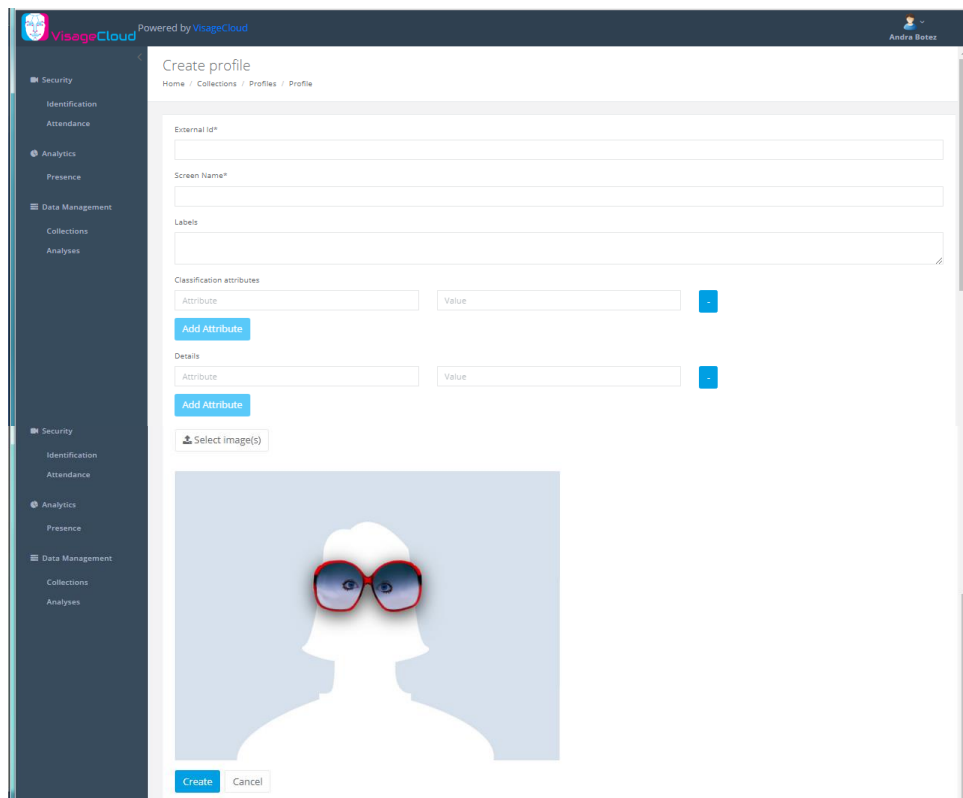


Fig. 106. **Add**: creates a user profile.

After completing the fields

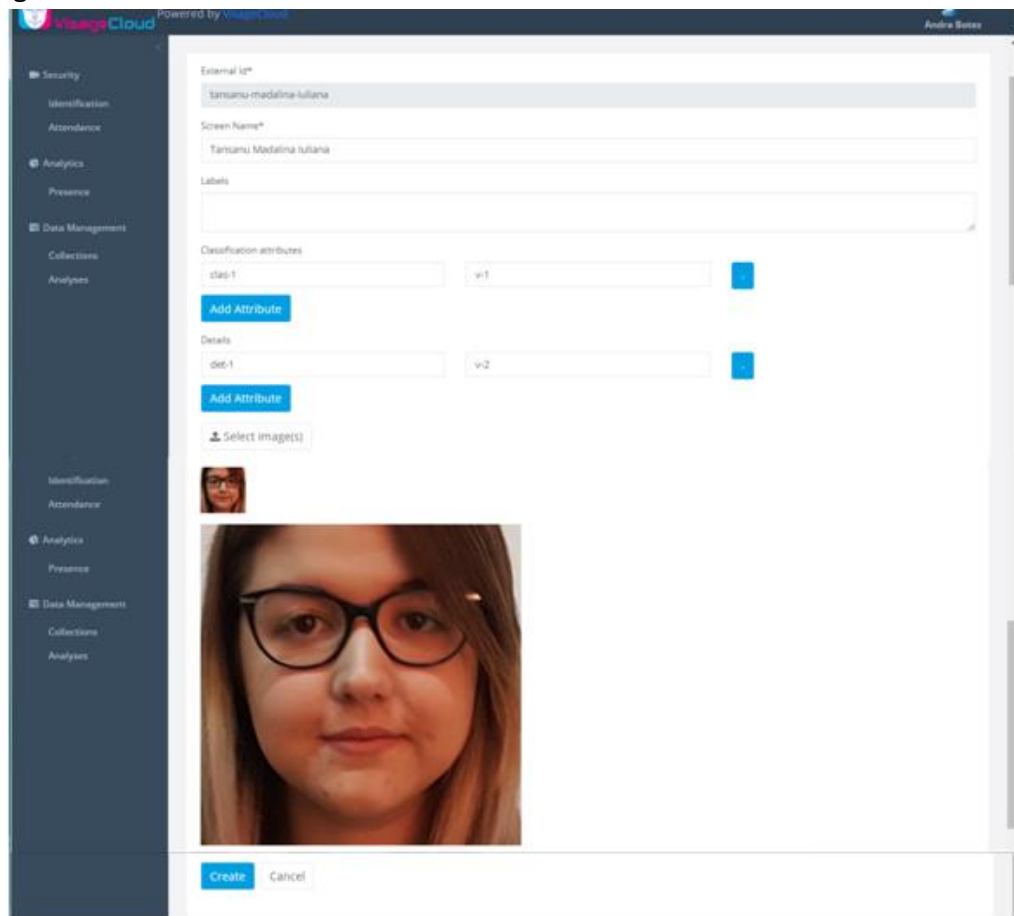


Fig. 107. Example of creating a user profile.

the Create option will be created and the profile for Tansanu Madalina Iuliana will be created. If you want to update an existing profile, select Edit and if it is necessary to delete a profile associated with the collection, the option will be Delete. Also in this case, as for the collection, the system asks for confirmation to avoid inadvertent deletion of the information.

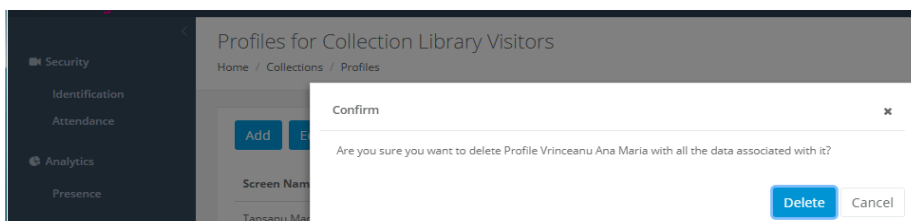


Fig. 108. Confirm: to avoid deleting a profile by mistake.

VisageCloud offers the facility to search for a profile or collections in the database. By filling in the search field of the searched name, the screen will appear:

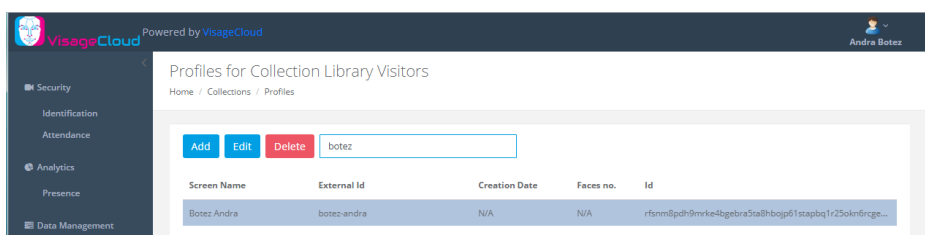


Fig. 109. Option to search for a profile or collections in the database.

Step 4: Face detection in photos

It consists in loading an image that may contain one or more faces.

POST /rest/v1.1/analysis/detection Perform detection on a given picture or picture URL

Response Class (Status 200)
OK

Model | Model Schema

```

RestResponse {
  message (string, optional),
  payload (object, optional),
  status (string, optional)
}
  
```

Response Content Type

Parameters

Parameter	Value	Description	Parameter Type	Data Type
accessKey	<input type="text" value="(required)"/>	The accessKey provided by VisageCloud	query	string
secretKey	<input type="text" value="(required)"/>	The secretKey or readOnlyKey provided by VisageCloud	query	string
storeAnalysisPicture	<input type="text" value="false"/>	Boolean value indicating whether you want the picture of the analysis to be stored for later retrieval	query	boolean
storeFacePictures	<input type="text" value="false"/>	Boolean value indicating whether you want the faces inside the picture to be stored for later retrieval	query	boolean
storeResult	<input type="text" value="true (default)"/>	Boolean value indicating whether you want the result of the analysis to be stored	query	boolean
retentionTime	<input type="text"/>	How many seconds the results should be retained in storage?	query	integer
pictureURL	<input type="text"/>	The URL of the picture, assuming it is served by a third party server. Server should be accessible from the Internet or through another network by VisageCloud infrastructure	query	string
picture	<input type="text"/>	The multipart/form-data version of the image, in case a direct upload is used. At least one of picture or pictureURL must be present	formData	string
algorithmVersion	<input type="text" value="V2 (default)"/>	Algorithm version (V2 is more performant but not backward compatible)	query	string
skipEXIF	<input type="text" value="false (default)"/>	Skip EXIF rotation processing	query	boolean
waitForPictureUpload	<input type="text" value="false (default)"/>	Waits until the picture is successfully uploaded, before returning the response back the the client	query	boolean
filters	<input type="text" value="Provide multiple values in new lines."/>	[For advanced users only] Change feature filters for robustness of feature extraction. Tweaking this parameter may affect per	query	Array[string]
options	<input type="text"/>	[For advanced users only] Options for preprocessing of image.	query	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		
401	Unauthorized		
403	Forbidden		
404	Not Found		

Fig. 110. The programming interface for the Detection option.

Depending on the value of the parameters set in the VisageCloud application programming interface for the detection operation, various situations may occur:

1. If the "storeFacePictures" parameter has the "false" value then VisageCloud will remove the original image after the analysis; in this case, "storeAnalysisPicture" will not contain any response.
2. If detection from a URL image is performed, VisageCloud will retrieve the image from the URL that was indicated by filling the pictureURL parameter and return the response when the detection is complete.

The image that has been loaded can contain multiple faces and each of them will be contained in the "faces" matrix. If no faces are detected in the image, this array will be empty. Each distinct face will have a unique "hash" attribute, which can therefore be added to the distinct faces of a profile (person). This association between faceHash and profile allows the system to determine whether "this face belongs to X" or "Y".

Step 5: Attaching each face detected to a profile

You can associate a particular face from a photo with an existing profile.

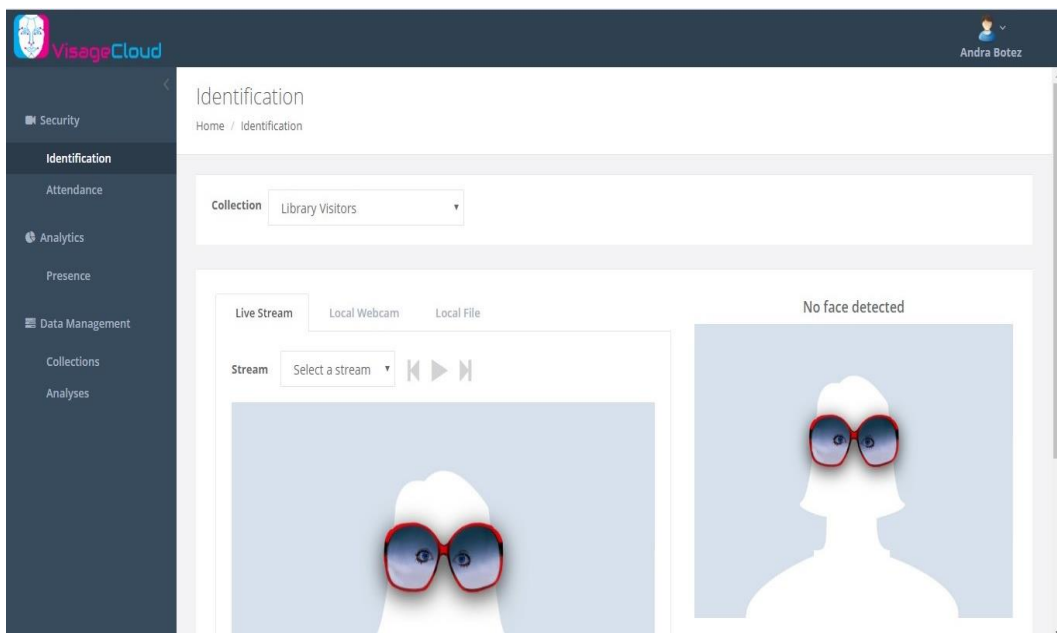


Fig. 111 Identifying users

Step 6: Performing facial recognition

Once more profiles have been created and one or more facets have been mapped for each of them, the last step is to test the recognition operation.

This means that a new image can be uploaded and the application will determine the person with the most similarities to the one in the image. This feature answers the question "Who does the X look like?"

As you can see, images can come from streams, Local Web Cam, or from an existing image on your personal computer.

The Local File option will be selected and the following screen will appear:

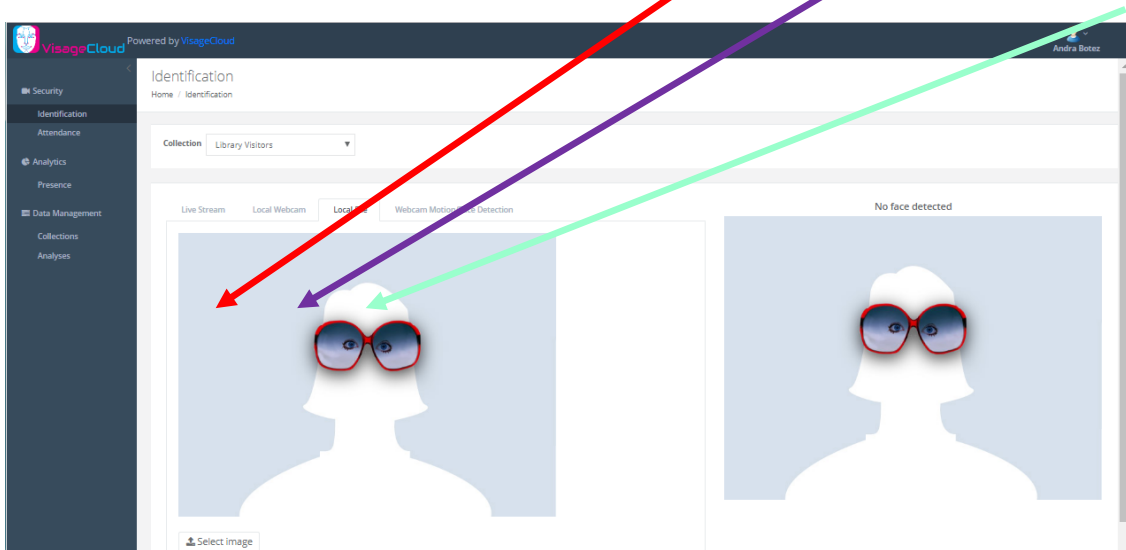


Fig. 112. Ways to obtain images for facial recognition.

where clicking Select image will load the image from your computer and associate it with your existing profiles. In order to do this, the name of the collection that VisageCloud has to consult should be specified. In this case, Library Visitor.

Will appear:

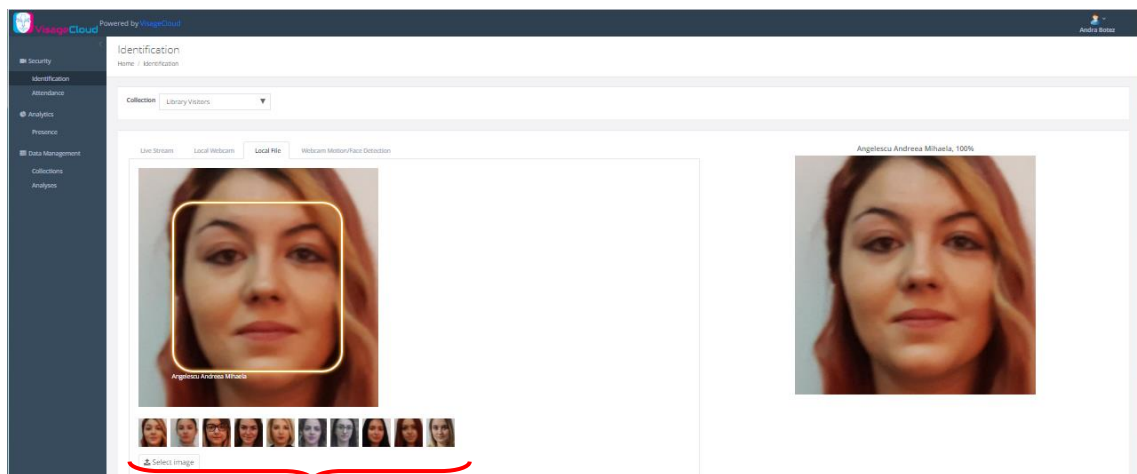


Fig. 113. Example of identification based on an existing image in the PC.

In the "Comparison" submenu, you can see that for each FaceHash detected, a series of matches ranged from the highest match (the smallest distance) to the smallest match (the longest distance) appear. By default, the API returns the first 10 similarities, so there is no overload with unnecessary data.

4.4. Facial Recognition experimental study

Using the system described above, an experimental facial recognition study was performed.

The study was conducted in collaboration with the Brasov County Library in February 2018, with a total of 40 participants, students at the Faculty of Communication and Public Relations at Transilvania University.

The first step in the experiment was to create the collection. By clicking on the Add button in the Visage Cloud application, the Create Collection window appears. I've filled in the Library Visitors collection name and created it by clicking the Create option.

We then recorded the photos of all the participants in the experiment, creating the user database, creating profiles for each person in the collection. These profiles contain one or more pictures, names, and other attributes such as gender or age group.

The last step was to test the recognition operation. Each experiment participant passed the webcam and by accessing the Analyze command it was possible to see the identity of those registered in the database.

Examples of facial recognition performed:

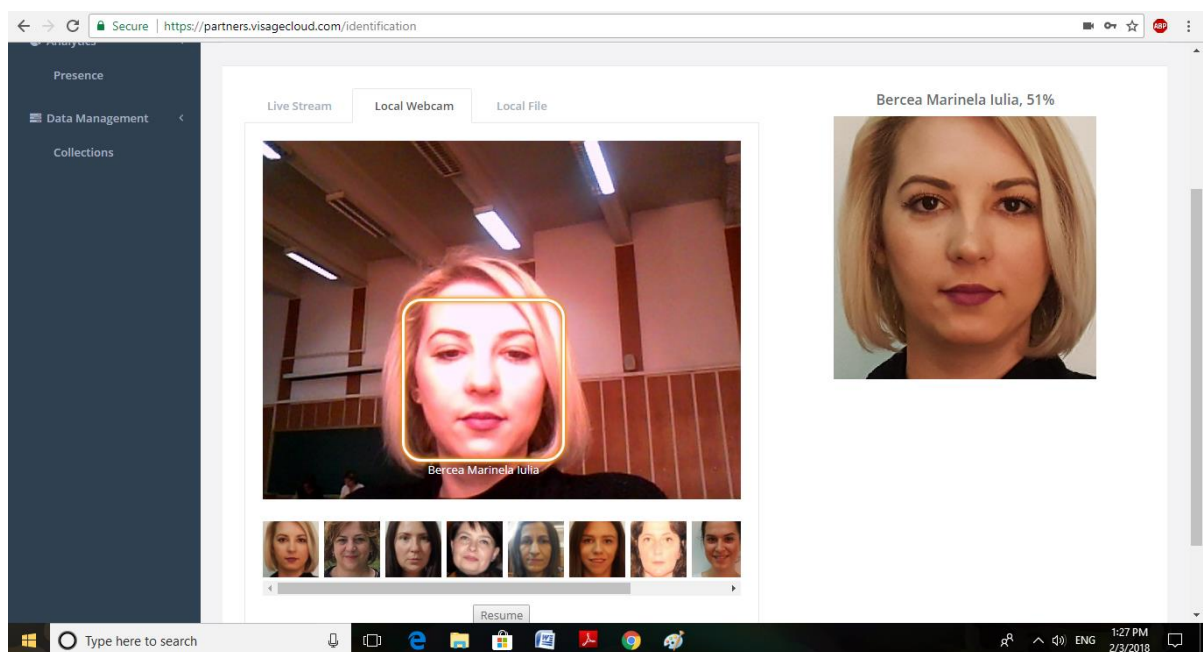


Fig. 115. Example 1 of facial recognition from the experiment.

A communication between the library management system, the user module, and the database created was attempted. Communication has demonstrated Visage Cloud's compatibility with user management software. The Visage Cloud software can be used as a standalone system, as well as a complementary system for the users. Study participants went through the system and, if they were not registered, the system sent an alert.

4.4 Conclusions

VisageCloud is a facial recognition program that uses state-of-the-art technology, based on research conducted in 2015-2016. In tests on large-scale public data sets, such as LFW (Labeled Faces in the Wild), VisageCloud managed to achieve the correct 94-96% recognition rate.

Detection, classification, and facial recognition are applicable in many areas: digital advertising; vending machines, outlets and interactive shops; photo labeling; Authentication for mobile and web applications intelligent surveillance systems.

- **Face Detection** refers to the process of identifying the general areas of an image containing a face. There may be several such areas and each of them must be individually detected and marked with a frame. Also, face key detection is part of face detection and fixes key facets, such as those that describe the contour of the jaw, mouth, nose, eyes and eyebrows.
- **Face classification**, as the name suggests, is a method of marking a face with multiple attributes: gender, age group, face expression, eye color, skin color, hair color. All of these attributes are supported by VisageCloud, and additional attributes may be added.
- **Face recognition** provides answers to two types of questions:
 1. "Who is most like the person in this image?" (face searched or 1: N face searched) and
 2. "Is the person in this picture really X / Y?" (face identification or 1: 1 face search). In the current version (V2) VisageCloud allows both face search and face identification.

As a growing number of institutions (organizations) implement the facial recognition system in their operations, it is also necessary to take into account aspects related to ensuring the confidentiality of the data subjects (clients, users, etc.) by application. Only responsible use, as well as a proactive concern with the safety of personal data, clearly provide the best results.

Individuals processing data on facial recognition should ensure not only effective data management but also their use only for the stated purpose.

Because face recognition needs a reference set to work, most confidentiality concerns begin with the nature of this reference set. It is essential that the set is created and stored in an ethical manner, and that responses are appropriate for both authentic and false situations.

The application can be particularly useful for intelligent surveillance, it can be applied in libraries as well as in the hospitality industry (tourism), especially when one of the objectives is to identify and reward loyal users.

CHAPTER 5

CONCLUSIONS

Biometrics refers to values related to human characteristics. Biometric authentication (or realistic authentication) is used in the field of information technology as a form of access identification and control. It is also used to identify people in groups that are supervised.

Biometric identifiers are the distinctive, measurable features used to label and describe people. Biometric identifiers are often classified as physiological and behavioral characteristics. The physical characteristics are related to the shape of the body. Examples include, but are not limited to, fingerprints, face recognition, DNA, hand geometry, iris recognition, etc. Behavioral characteristics are related to a person's behavioral pattern, including the pace of typing, walking, and voice.

Traditional means of access control include token-based identification systems such as driving licenses or passports and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more confident in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises confidentiality issues with regard to the subsequent use of this information.

Nowadays, recognition or authentication applications appeal to a multitude of parameters and biometric data including: voice, fingerprints, face, iris, hand geometry, style of writing, walking patterns, and combinations of these. In practical applications, the first four categories are encountered, as they allow for the use of sensors with adequate performance and low cost, and due to the theoretical foundation needed to process the available data.

None of the listed biometric systems can offer ideal information. For this reason, the application of recognition and verification techniques or procedures derived from that information is conditional on the acceptance of a minimum level of values. Their correct assessment is based on either standardization procedures or periodic competitions with wide participation, such as those under the aegis of the US National Organization of Standards and Technology. It is also necessary that within each application there is an acceptable ratio between the proportions of the two main categories of errors (acceptance and false rejection rates) to considerably reduce the probability of unauthorized access to resources or spaces protected without interfering with users with access rights.

It can be appreciated that facial recognition is an affordable and simple technology to implement due to the widespread use of built-in cameras (or relatively cheap webcams) in most applications. Equipping with such a security system can have many advantages, including: capturing the image remotely without using physical contact, making it easier for users to access the library (without an ID card). The system also captures images in public spaces, helping capture the villains. Legal databases can be used (in collaboration with the police or other state bodies that use such databases).

Currently identified facial identification patterns may encounter some difficulties in correctly identifying poorly illuminated areas as well as the person's state of life, which is necessary to achieve a competitive degree of security. [9] Variation in lighting conditions is one of the greatest challenges in remote facial recognition. In particular, when images are captured from large distances, you have no control over lighting conditions. As a result, captured images often suffer from extreme light (due to the sun) or poor light (due to shadow, bad weather, evening, etc.). [14] The performance of most existing RF algorithms is influenced by the smallest light variations. Various methods have been introduced to deal with this issue. They are based on light cones (Georghiades et al, 2001b; Belhumeur and Kriegman, 1996), spherical harmonics (Basri and Jacobs, 2003; Ramamoorthi and Hanrahan, 2001; Zhang and Samaras, 2003); Quotient images (Shashua and Riklin (Chen et al., 2006), albedou estimation (Biswas et al., 2009), photometric determination (Zhou et al., 2004), degraded faces (Zhang et al. et al., 2007), and dictionaries (Patel et al, 2011; Lee et al., 2005a). [14]

As a result of the research, we can specify that most librarians would agree to implement a facial recognition system in the library in which they operate to enhance security. It could be noticed that the respondents from abroad were more detained in comparison with those from Romania and Moldova.

Librarians concerned with the security of individuals in the context of terrorism are eager to implement a facial recognition system in their library. Also, librarians who believe that the most appropriate biometric recognition system for collections and people security is facial recognition, would agree to the implementation of such a system. The degree of trust in facial recognition systems plays an important role in the decision of librarians to increase the security of the library by installing the new system.

From the data analyzed, the library size, librarians' function, or the 31-year experience at work does not interfere with librarians' decision to implement the new facial recognition system. Also, the level of librarians' preparation does not interfere with this decision, probably because most have more than average education.

For development of the application, improvements can be made in terms of scalability, by building a larger database. If you run on a server database, security is much stronger, with the option of more efficient image and image encryption solutions. Another direction of development is to improve prediction in different contexts.

The 15 initial pictures are made consecutively and are almost identical, but we could define more hypostases and lighting conditions, so the software can correctly detect a person in multiple conditions.

Biometric authentication will never be safe, but it is one of the most reliable current security methods. The accuracy of biometric systems is affected by factors such as non-universality, noise, lack of invariant representation, and non-distinctive character. Integrating multiple markers can help overcome some of these disadvantages. Better methods of combining information from multiple sources have been the subject of extensive research. Startup levels of processing (sensor and feature levels) make it difficult to fuse the information, while the decision level does not have sufficient

information content. Consequently, the level of matching score is preferred by researchers, this being the compromise between ease of fusion and informational content. Biometric systems are not yet widely used because of unsatisfactory performance compared to requirements. As a result, improving system performance (ie the theme of this thesis) is the most important challenge for research.

PERSONAL AND ORIGINAL CONTRIBUTIONS

Personal and Original Contributions

The evaluation of the author's contributions to the development of scientific knowledge is based on the results of scientific research from different perspectives:

A. Contributions with synthesis character

- Study on the general framework of security of collections and persons in libraries.
- Study on the theoretical aspects of the security of collections and persons in libraries.

B. Contributions of theoretical and experimental character

- Developing the IT application for the security of people and collections in libraries.
- Realizing the database with users.
- Experimental determination on the security of individuals and collections in libraries.

C. Contributions of curricular nature

- Elaboration of the scientific research reports from the doctoral research program;
- Completion of doctoral thesis;
- Current state of research.

D. The novelty of the doctoral thesis

The doctoral dissertation presents novelty regarding:

- Topic and subject of theoretical investigations;
- Comparative analysis of security systems used in libraries.
- Statistical analysis of the requirement to implement a security system based on facial recognition in libraries.
- The architecture of the IT application architecture for the security of people and collections in libraries.

E. Usefulness of the research results

The usefulness and the scientific, didactic and applicative importance of the theoretical and practical results obtained by the author during the work are confirmed by the original contributions as well as the following aspects:

- From a scientific perspective, these achievements represent a significant contribution to the fundamental research field, by continuing and diversifying the studies on computer applications related to the implementation of security systems in libraries;
- As regards the didactic aspects, the results are important and useful as such, with particular emphasis on the applied research methodology and techniques;
- As regards the applicative aspects, the theoretical foundation of the knowledge gained through the practical experience associated with the realization of a security system for people and collections in libraries provides an adequate framework for future research in this field.

F. Valorisation and dissemination of the research results in the scientific academic environment

The valorisation and dissemination of the research results in the scientific academic environment was achieved by:

- Publishing 11 scientific works and articles in the proceedings of international and national scientific events as the first author and co-author. Among them, an article was published in an international conference accepted in the ISI journals, 2 articles in ISI indexed proceedings, 5 articles in BDI indexed proceedings, and 3 in the BDI journals.
 - a) Conference articles accepted in the ISI indexed proceedings:
 1. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A.,(2016), *Collection security management, based on facial recognition, at university libraries*. Globalization, Intercultural Dialogue And National Identity, Arhipelag XXI Press, Tîrgu Mureş, ISBN: 978-606-8624-03-7, Volume no. 3, pp 268-273. <http://www.upm.ro/gidni3/?pag=GIDNI-03/vol03-Soc>
 2. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A., (2016), *Environmental impact on general health. Attitudes, opinions and types of behavior*. Globalization, Intercultural Dialogue And National Identity Arhipelag XXI Press, Tîrgu Mureş, ISBN: 978-606-8624-03-7, Volume no. 3, pp 274-285. <http://www.upm.ro/gidni3/?pag=GIDNI-03/vol03-Soc>
 - b) International conference article accepted in the ISI journals:
 3. **Botez A.M.**, Volovici R., Volovici D., Repanovici A.,(2018), *Facial recognition system used in verification systems for library users*, **10thQualitative and Quantitative Methods in Libraries International Conference Chania, Crete, Greece.**

c) Articles in BDI indexed proceedings:

4. Repanovici A., Bîrsan I., **Botez A.**, Druguş D. (2015), *Scientific information management using information systems within the open access to knowledge context*. Journal Plus Education, ISSN: 1842-077X, E-ISSN (online): 2068-1151, Volumul 12, Numărul 2.
5. Repanovici A., **Botez A.M.**, Stoianovici M., Roman N. (2016), *Measuring the Quality and Impact of Scientific Information. Scientometry Research Using Web of Science in the field of: Ethics in medical recovery*. Trivent Publishing, Series: Philosophy, Communication, Media Sciences, Volume: Communication Today: An Overview from Online Journalism to Applied Philosophy , pp 52-60.
<http://triventpublishing.eu/communicationtoday.html>
6. Bejinaru-Mihoc A. **Botez A.M.**, Mitu G.L., (2015), *Regulations in the field of using medical devices. Overview. În: 6th International Conference „Computational Mechanics and Virtual Engineering”*. COMEC 2015, Braşov, pp.457-462.
7. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A., *Modele biometrice dactiloscopice cu aplicații în sistemele de identificare*. ISSN-L 1224-7928, Online: ISSN 2247-3548, Buletinul AGIR nr. 1/2016, pp 43-46.
http://www.buletinulagir.agir.ro/numar_revista.php?id=123
8. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A.,(2016), *Library security management based on biometric methods*. The International scientific Conference of Librarians Western Balkan Information Literacy Conference, Bihac, pp 97-101.

d) Articles in BDI journals:

9. **Botez A.M.**, Bejinaru-Mihoc A., Repanovici A.,(2017) *Sisteme de recunoaştere facială: Probleme şi perspective*, Buletinul AGIR 2, Creativitate, Inventică, Robotică.
10. Bejinaru-Mihoc A., **Botez A.M.**, (2017), *Cerinţe juridice în utilizarea dispozitivelor medicale*, Buletinul AGIR 2, Creativitate, Inventică, Robotică.
11. **Botez A.M.**, Repanovici A.,(2017) *Importanţa securităţii persoanelor şi a colecţiilor în biblioteci*, Revista Română de Biblioteconomie şi Ştiinţa Informării/ Romanian Journal of Library and Information Science ISSN 1841-1940, Volume 13, Issue 1, pp. 11-20.

Realization of the scientific research reports within the scientific training program, completion of the PhD thesis.

SELECTIVE BIBLIOGRAPHY

1. Akrouf S. (2011) *Une Approche Multimodale pour l'Identification du Locuteur*, These, Universite Ferhat Abbas-Setif, Republique Algerienne Democratique et Populaire.
2. Albrecht, S. (2012). Your local library can be a dangerous place. *Psychology Today*.
3. Albrecht, S. (2015). Library Security : Better Communication, Safer Facilities, American Library Association.
4. Biometrie-online.net. (2016). *Technologies*. [online] Disponibil la: <https://www.biometrie-online.net/technologies/voix?view=category&id=14&layout=> [accesat 2016].
5. Blansit, B.D., 2010. RFID Terminology and Technology: Preparing to Evaluate RFID for Your Library. *Journal of Electronic Resources in Medical Libraries*, 7(4), pp.344–354.
6. Botez A.M., Bejinaru-Mihoc A., Repanovici A. (2015) Modele biometrice dactiloscopice cu aplicații în sistemele de identificare. *Creativitate, Inventică, Robotică*, ediția a-XX-a, Braşov. Disponibil pe <http://www.agir.ro/buletine/2497.pdf>, [accesat la data de 25.10.2017]
7. Botez A.M., Bejinaru-Mihoc A., Repanovici A. (2016) *Collection security management, based on facial recognition, at university libraries*. Globalization, Intercultural Dialogue And National Identity 3rd Edition. Tîrgu Mureş. Disponibil pe: <http://www.upm.ro/gidni3/GIDNI-03/Soc/Soc%2003%2026.pdf>, [accesat la 25.08.2017]
8. Botez A.M., Bejinaru-Mihoc A., Repanovici A. (2016) *Library security management based on biometric methods*. The International scientific Conference of Librarians Western Balkan Information Literacy Conference, Bihac. Disponibil pe: http://wbilc2018.com/files/proceedings/PROCEEDINGS_WBILC2016.pdf, [accesat la 28.03.2017]
9. Botez A.M., Bejinaru-Mihoc A., Repanovici A.(2016) *Environmental impact on general health. attitudes, opinions and types of behavior*. Globalization, Intercultural Dialogue And National Identity 3rd Edition. Tîrgu Mureş. Disponibil pe: <http://www.upm.ro/gidni3/GIDNI-03/Soc/Soc%2003%2027.pdf>, [accesat la 28.10.2017]
10. Botez A.M., Repanovici A. (2017) *The importance of security for people and collections in libraries* (Importanța securității persoanelor și a colecțiilor în biblioteci). *Revista Română de Biblioteconomie și Știința Informării*, ISSN 1841-1940. Vol. 13, Issue 1, pp. 11-20. Disponibil pe: <http://www.rrbsi.ro/index.php/rrbsi/article/download/20/rrbsi-vol13-iss1-2017-p11-20.pdf/>, [accesat la:30.05.2017]
11. Brooks I. (2009) *Organisational Behaviour: Individuals, Groups and Organisation*. Pearson Education, 355 p.
12. Chellappa. R, Jie N., Vishal M.P. (2012) *Remote identification of faces: Problems, prospects, and progress*. *Pattern Recognition Letters*, 33(14), 1849–1859.

13. Guerrier Cl., Cornelia L-A., *Les aspects juridiques de la biometrie*. [Online] Disponibil pe: biometrics.it-sudparis.eu/.../rep4072e2adb7d5a.doc [accesat: 2015].
14. Harris J.L., Dimarco S.R. (2010). Locking Down a University Library: How to Keep People Safe in a Crisis: A Mansfield University of Pennsylvania Perspective. *Library & Archival Security*, 23(1), pp.27–36.
15. Heiko, K., Pohl H. (2004) RFID security. *Information Security Technical Report*, 9(4), pp.39–50.
16. Henrici D. (2008) *RFID Security and Privacy: Concepts, Protocols, and Architectures*, Berlin: Springer-Verlag Berlin Heidelberg.
17. Kahn MB (2007) *Library Security and Safety Guide to Prevention, Planning, and Response*, ALA Editions, Chicago. Disponibil pe: ProQuest Ebook Central.
18. Kitsos P., Y. Zhang (eds.) (2008) *RFID Security: Techniques, Protocols 3 and System-on-Chip Design*, New York (N.Y.): Springer Science+Business Media, 446p.
19. Kusuma G.P., Chua C.S. (2011) PCA-based image recombination for multimodal 2D+3D face recognition. *Image and Vision Computing*, 29, 306–316.
20. Latuszek Jr., T. (2002). Library Security: A Growing Awareness. *Library & Archival Security*, 15(2), pp.3–7.
21. Lupu Cătălin (2015) *Stadiul actual privind recunoaşterea persoanelor după iris şi amprentă*. Raport de cercetare nr. 1. Coordonator ştiinţific: prof. univ. dr. ing. Vasile-Gheorghişă GĂITAN. Suceava Disponibil pe http://perform.usv.ro/rapoarte/13/raport_cercetare_1.pdf, [accesat la 04.07.2016]
22. Maidabino A.A. & Zainab A.N. (2012). A holistic approach to collection security implementation in university libraries. *Library Collections, Acquisition and Technical Services*, 36(3–4), pp.107–120.
23. Mihăilescu M. I. (2014) Contribuţii asupra Securităţii Protocoalelor Biometrice de Autentificare. Rezumat teză doctorat. Universitatea din Bucureşti. Cond. şt.: prof.univ.dr. A. Atanasiu. Disponibil pe: <http://fmi.unibuc.ro/ro/pdf/2014/doctorat/rezumatMihaiulescu.pdf>, [accesat la 10.02.2017]
24. Molnar D., Wagner D. (2004) Privacy and security in library RFID: issues, practices, and architectures. *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pp.210–219.
25. Park K.Y, Hwang S.Y., (2014) *An improved Haar-like feature for efficient object detection*, Department of Electronic Engineering, Sogang University, C.P.O. Box 1142, Seoul 100-611, Republic of Korea, *Pattern Recognition Letters*, 42, 148–153.
26. Phillips P.J., Moon H., Rizvi S.A., Rauss P.J. (2000) The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactionson Pattern Analysisand Machine Intelligence*, 22(10), 1090–1104.
27. Piccolotto P., Maller P. (2014) Biometrics from the User Point of View: Deriving Design Principles from User Perceptions and Concerns about Biometric Systems, 2014, *Technology Journal*, 18(4).
28. Popa Gh. (2011) *Metode şi tehnici de identificare criminalistică*. Bucureşti: Ed. AIT Laboratories s. r. l., ISBN: 978-606-8363-01-1.

29. Pulli B.K., Baksheev A. (2012) Real-Time Computer Vision with OpenCV. *Communications of the ACM*. 55(6) pp.61-69.
30. Rajgarhia A. (2007) *Face Detection using Independent Component Analysis*, CS 229 Final Project Report. Disponibil pe: <http://cs229.stanford.edu/proj2007/Rajgarhia-FaceDetectionUsingICA.pdf> [accesat 5.10.2017]
31. Rath Subrat K., Siddharth S.R. (2014) A Survey on Face Detection and Recognition Techniques in Different Application Domain. *I.J. Modern Education and Computer Science*, 6(8), 34-44.
32. Sacu (Druguş) D. (2014) *Cercetări privind managementul serviciilor medicale în sistemul de sănătate din România*. Rezumat teză de doctorat. Cond. Şt.: prof. univ. dr. Doina Azoicăi. Iaşi. Disponibil pe [http://www.umfiasi.ro/Concursuri/sesapiu/mg_conf_p05_stiinte/7.%20rezumat%20teza%20doctorat%20\(romana,%20engleza\).pdf](http://www.umfiasi.ro/Concursuri/sesapiu/mg_conf_p05_stiinte/7.%20rezumat%20teza%20doctorat%20(romana,%20engleza).pdf) [accesat 15.09.2016]
33. Sahoo S.K., Tarun Choubisa and S. R. Mahadeva Prasanna (2012) Multimodal Biometric Person Authentication: a Review, *IETE Technical Review*, 29(1), 54-75.
34. Scribd. (2016). *Biometrie*. Disponibil la: <https://www.scribd.com/document/94778231/biometrie>, [accesat la 10.12.2016]
35. Scribd. (2017). *Capitolul1.pdf*. [online] Disponibil la: <https://es.scribd.com/document/335661736/Capitolul1-pdf> [accesat la data de 15.03.2017].
<http://scs.etc.tuiasi.ro/iciocoiu/courses/ESL/homeworks/hw2/Capitolul1.pdf>
36. Scribd. (2018). *Recunoaşterea_ feţelor*. [online] Disponibil la: <https://www.scribd.com/document/339937718/Recunoa%C5%9Fterea-fe%C5%A3elor> [accesat la data de 15.03.2018]
37. Suarez O.D. (2014) *OpenCV Essentials*, Olton: Packt Publishing - ebooks Account, 214 p. Disponibil pe: ProQuest Ebook Central.
38. Thompson, Samuel T.C. (2006) Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*. 25(4), pg. 222+.
39. Unar J.A., Woo Chaw Seng, Almas Abbasi (2014) A review of biometric technology along with trends and prospects. *Pattern Recognition*, 47(8), 2673-2688.
40. Ustundag, Alp (2013). *The Value of RFID*, London: Springer London, pp. 3-12.
41. vdocuments.site. (2017). *Sistem biometric - [PDF Document]*. [online] Disponibil la: <https://vdocuments.site/sistem-biometric.html> [accesat 11.08. 2017].
42. VisageCloud. (2017). *VisageCloud - Transforming face recognition into business value*. [online] Disponibil la: <https://visagecloud.com/faq>, [accesat la 17.12.2017]
43. VisageCloud. (2018). *VisageCloud - Transforming face recognition into business value*. [online] Disponibil la: <https://visagecloud.com/get-started> [accesat la data de 25.02.2018]
44. Visagecloud.com. (2018). *Features*. [online] Disponibil pe: <https://visagecloud.com/features> [accesat la data de 10.01.2018]
45. Visagecloud.com. (2018). *Swagger UI*. [Online] Disponibil pe: <https://visagecloud.com/swagger-ui.html> [accesat la data de 15.03.2018]

46. Visagecloud.com. (2018). *The VisageCloud Domain Model*. [online] Disponibil la: <https://visagecloud.com/domain-model> [accesat la data de 18.04.2018]
47. Vrejoiu M.H.; Hotăran M.A. (2013) Detectarea automată a fe elor umane. Metoda Viola-Jones, *Revista Română de Informatică și Automatică*, 23(2), 21-32. Disponibil pe: <https://vdocuments.site/aplicatii-rna-and-facial.html>. [Accesat la data de 15.05.2017]
48. Want R.(2006) An introduction to RFID Technology. *IEEE Pervasive Computing*, 5, pp. 25-33.
49. Webopedia.com. (2016). *What is Layer? Webopedia Definition*. [online] Disponibil la: <https://www.webopedia.com/TERM/L/layer.html> [accesat la data de 30.03.2016]
50. Webopedia.com. (2017). *What is Ontology Web Language (OWL)? Webopedia Definition*. [online] Disponibil la: https://www.webopedia.com/TERM/O/Ontology_Web_Language.html [accesat la data de 11.08.2017]
51. Westenkirchner S. (2008) Integrated Library Security Systems. *Library & Archival Security*, 21(2), p.159-167.
52. Woodward J.D., Horn C., Gatune J., Thomas A. (2003) *Biometrics. A Look at Facial Recognition*. Santa Monica, CA: RAND Corporation. [Online] Disponibil pe: https://www.rand.org/pubs/documented_briefings/DB396.html [accesat 17.07.2017]
53. [Xu Y.](#), [Zhang Z.](#), [Lu G.M.](#), [Yang J.](#) (2016) Approximately symmetrical face images for image preprocessing in face recognition and sparse representation based classification. *Pattern Recognition*, 54(C), 68-82.
54. Yang M.H., Kriegman D.J., Ahuja N. (2002) *Detecting faces in images: a survey*. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 24 (1), 34–58.
55. Zedner Lucia (2009). *Security: Key Ideas in Criminology*. Taylor and Francis, 206p. Disponibil pe: ProQuest Ebook Central.
56. Zhou C., Wang L., Zhang Q., Wei X. (2013) Face recognition based on PCA image reconstruction and LDA. *Optik - International Journal for Light and Electron Optics* 124(22) 5599– 5603.

THEORETICAL AND EXPERIMENTAL RESEARCH ON THE DEVELOPMENT OF BIOMETRIC SYSTEMS

The first chapter titled **General framework for the security of collections and individuals in libraries** addresses "security" issues, a term that can have a variety of connotations in the library world.

Subchapter 1 and 2 deal with **personal safety** (for users and staff): precautions against violence and in subchapter 3 are presented **precautions to protect library collections against theft** because these two aspects are the ones that directly influence customers.

Theoretical aspects of facial recognition systems is the title of the 2nd chapter, which aims to define and present biometric recognition systems. Biometrics is the automatic recognition of people based on their behavioral and biological characteristics.

A widespread theme in biometric research is face recognition in an image, which is covered in subchapter 2. The process of identifying or automatically checking people in frames or digital video images, based on the available database, is called face recognition. The objective of looking for faces in a source or video image is called face detection.

Classification of face detection techniques was performed, four of the facial recognition algorithms were analyzed in subchapter 3.

Difficulties and shortcomings in biometric verification systems have been mentioned in Chapter 2.

The statistical research on **determining the views of library managers and librarians for the need to implement a new security system and the existing systems in libraries** was carried out, study presented in Chapter 3. The design of the questionnaire, the analysis and the interpretation of the collected data are detailed in within the chapter.

The 4th chapter, **Optimizing the security system in libraries by implementing a facial recognition system** is entirely dedicated to VisageCloud. The developed computer application monitors access to libraries and is designed to respond to the growing demand for an effective system to control access and presence in a location in the context of terrorism. The chapter begins by presenting some introductory notions needed to understand the operation of the practical application. The next subchapter shows the **VisageCloud Application Domain Model** and the **Programming Interface (API)** needed to complete the application itself.

In subchapter 3, **VisageCloud: Face Detection and Recognition** the necessary steps to the actual operation of the application are taken.

The last chapter **Final conclusions, Own contributions (authentic)** present in a synthetic form the results of the research by highlighting their own contributions and the original solutions that made it possible to achieve the objectives set in the paper.

CURRICULUM VITAE

PERSONAL INFORMATION

Andra- Manuela Botez (name after marriage-Bejinaru Mihoc)

 Braşov (România)

EDUCATION AND TRAINING

- 2014- present **Phd. Student** in Engineering and Management
Transilvania University of Brasov, Faculty of product design and environment,
- 2009 – 2013 **University studies:** Spiru Haret University of Brasov, Faculty of Law and
Administration, Law specialization.
- 2010 – 2012 **Masteral studies:** Transilvania University of Brasov, Faculty of Medicine, Management
of preventive strategies and health policies.
- 2007 – 2010 **University studies:** Transilvania University of Brasov, Faculty of Law and
Sociology, Sociology specialization.
- 2003 – 2007 **Sports High School**

PROFESSIONAL EXPERIENCE

- 18.04. 2018 Human Resources Inspector /Referent
- present
- 2012-2013 Speciality Practice, Posdru Project.
- 2010-2011 Commercial Collaborator

ACTIVITATE ŞTIINIFICĂ

Published articles: 11 out of which: 2 ISI proceedings, 1 paper at an international conference accepted in the ISI journals, 5 articles in BDI indexed proceedings and 3 in the BDI journals.

FOREIGN LANGUAGE: English, French