Qualitative and Quantitative Methods in Libraries (QQML) 7: 539–544, 2018

Facial recognition system used in verification Systems for library users

Andra-Manuela Botez[1], Rodica Volovici [2], Daniel Volovici[3] and Angela Repanovici[4]

[1] Transilvania University of Braşov
[2] Lucian Blaga University of Sibiu
[3] Lucian Blaga University of Sibiu
[4] Transilvania University of Braşov

Abstract: Most of the literatures that deal with library security take into account the security of collections, buildings, or equipment. The security of the libraries is an important concern for library staff. There are security systems for collections, but in the context of terrorism, we are interested that people who have access inside the library to be in good faith. Checking the library card is the key to enter the library. It is non-transferable. We present a complementary system of the entrance permit through the facial recognition of users, developed and tested in a public library as collaboration between two Romanian universities: Transilvania University of Braşov, Lucian Blaga University of Sibiu and Brasov Public Library.

Keywords: libraries, users, security, public library, Romania

1. Introduction

Libraries, museums and archives are considered safe locations to be visited, used and to have a job within them. According to Kahn, (2007), the mental image of a "library" does not involve violent images, danger, fear or anxiety. On the contrary, people generally perceive libraries as quiet places for spending time, contemplation or study. (Shuman, 1996)

Most of the literature that deal with library security take into account, in the first place, the security of collections, of archives, art, buildings, equipment, electronic data and websites.

This article 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

Received: 2.5.2018 / Accepted: 28.5.2018 ISSN 2241-1925

is therefore essential to take action and to reinforce the view that libraries are safe places where everyone can spend their free time.

Albrecht (2015) argues that since libraries are public places, open for many hours, they offer a lot of ways for people to get in touch, creating various occasional conflicts, directed both towards staff and visitors.

Unfortunately, library staff and visitors are increasingly at risk, due to certain incidents that have led to the wounding or kidnapping of certain individuals, as well as to weapons or bomb threats (Kahn, 2007); (Shuman, 1996), Albrecht (2015) points out that there are no libraries that search the visitors at entrance. Also libraries are confronted with the problem of people bringing legal or illegal weapons into their institutions without the staff knowing about this.

Arndt, (2008) informs library staff, especially the information office, that they often have to deal with "problematic visitors" that are perceived as a primary source of discomfort or disruption of routine service.

The library is used by people with different types of personality and social status. Thus, there are all kinds of visitors who have offensive or illegal behavior towards public library employees. There are also visitors who ask strange questions just to talk to someone because they are alone; homeless people, visitors who quarrel with other visitors or staff; visitors who discuss with library staff about politics; unattended children, mentally ill, chronically complainers, those who use adult language, visitors who make sexual advances to employees or other visitors, internet weirdos / vulgar material enthusiast, criminals, the intoxicated, those who come to the library because they have no place to go (Albrecht, 2012) (Kahn, 2007) As long as these visitors do not bother anyone, nobody can forbid them access to the library.

Arndt, (2008), says that while improved building security is an important preventative measure, it will not eliminate every problem. The library must have well-conceived security policies and procedures in place for problem situations.

According to Kahn (2007), if someone in the staff gets a bomb threat, they have to ask the informant when will the bomb explode, what type of bomb it 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 should re-enter the building until the firefighters or the bomb team authorizes it.

Arndt, (2008), considers that the security is becoming more important as libraries face the challenges presented by problem patrons.

Kahn, (2007), mitigates the fact that the safety of users and staff is essential. In the first stage, the building should be examined, both outdoors and indoors, so that users and staff can enter, use the unit and get out without getting hurt, whether they are leaving 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.

2. Optimizing the security system in libraries

Violence is a fact of modern life and libraries are not immune. Risks can be lowered, however, by taking precautions to improve the security of collections and, above all, of individuals by implementing a security system based on facial recognition. We present a complementary system of the entrance permit through the facial recognition of users, developed and tested in a public library as a collaboration between two Romanian universities: Transilvania University of Brasov, Lucian Blaga University of Sibiu and Brasov Public Library.

The software application monitors access to libraries, being created in response to the growing demand to have an effective access control and presence in a location, in the context of terrorism. The purpose of the system is to ensure fast, secure, and reliable monitoring of users access to various public locations.

In a survey conducted by us, in 2017, 177 people working in libraries, both in Romania and abroad (Albania, Armenia, Belarus, Bosnia and Herzegovina, Bulgaria, Greece, Ireland, Montenegro, Norway etc) more than half of the respondents said that additional measures should be taken regarding the security of individuals, 19.3% do not think that further action should be taken and 35.48% did not think about it.

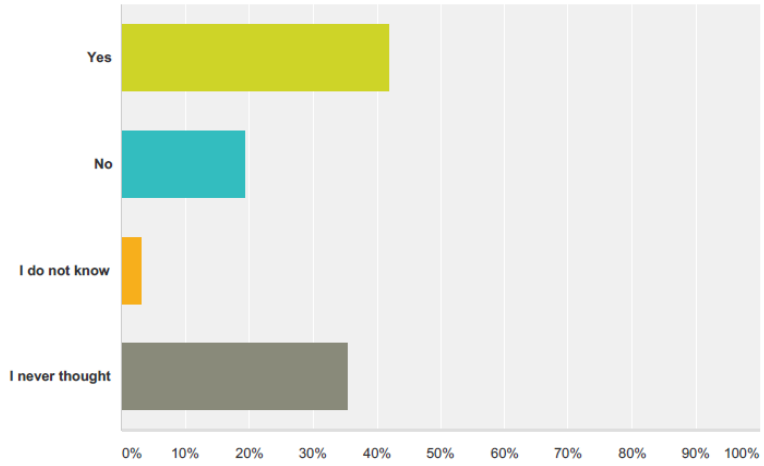

Fig.1 On the issue of terrorism, do you think we should have additional measures concerning the safety of persons in the library?

VisageCloud is a face-recognition service that uses state-of-the-art technology based on research conducted since 2015. In tests on large-scale public data sets such as LFW (Labeled Faces in the Wild), VisageCloud a managed to achieve a correct recognition rate of 94-96%. Face Detection, Classification and 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. VisageCloud helps us to focus our energy on the creativity and the specifics of the application we want to develop without wasting time with other issues such as deep learning, classifiers, perspective alignment, color space, etc..

3. Face Detection & Recognition set up

Step 1: Create a collection

In order to group all the people you want to register in your system in a more manageable way, you need to create a collection. Think of a collection a set or a group of registered people.

Step 2: Create profiles for each person in your collection

A profile represents a person.

- accessKey, secretKey
- collectionId - defines the collection you want to create the profile into
- externalId - this allows to link a profile to a database external to VisageCloud, where you can potentially store additional information you don't want to share with VisageCloud (a user's email address, passwords, user activity, description). In case you do not provide an externalId, it will be set to the same value as the profileId. If you set an

externalId which already exists in the collection, the existing profile with that externalId will be returned (externalId must be unique for each profile in the collection)

- screenName - this is a human-readable label for each profile. It is not mandatory, but setting it will allow you to more easily trace and debug responses from Visage Cloud (for instance, it can be "Bogdan Bocse")
- labels - labels are like tags which will later allow you to do finer filtering in face recognition. Let us say you have several types of user divided by citizenship (eg. "us", "uk", "poland", "romania"). If you label the profile accordingly, you can then only do the recognition by comparing only with those users with the label "uk". You can do this without having to go through the trouble of maintaining separate collections and you can also query the full collection without any label restriction

Step 3: Detect the faces in photos
You uploaded a picture that may contain one or several faces.

Step 4: Add each detected face to a profile
This associates a particular face instance detected from a photo to an existing profile.

Step 5: Perform the face recognition
After you have created profiles and mapped one or several faceHashes to each of them, it's time to test the recognition service. This means you can give a new image to VisageCloud and it will tell you who that person looks like most.
In order to do this, you must also specify the collection you want VisageCloud to look into by collectionId.

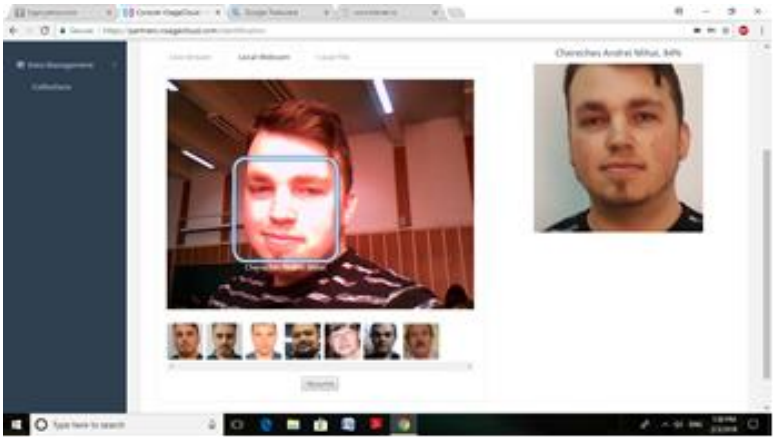

Fig. 2 Exemplu de recunoastere faciala realizata in Visage Cloud.

4. Conclusions

It is a sad fact but true that libraries and archives, historical societies and museums were the location for attacks with gunfire and bomb threats . (Kahn, 2007) Some unpleasant events can be avoided by implementing a facial recognition system. It's an easy-to-implement and affordable technology because it uses built-in cameras (or a relatively cheap webcam) to function. Equipping with such a security system has 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).

Reference

Albrecht, S. (2012). Your local library can be a dangerous place. Psychology Today.

Albrecht, S. (2015). Library Security : Better Communication, Safer Facilities, American Library Association.

Donald A. Arndt Jr. (2001). Problem Patrons and Library Security, Legal Reference Services Quarterly, 19:1-2, 19-40, DOI: 10.1300/J113v19n01_03.

Kahn, M.B. (2007). Library Security and Safety Guide to Prevention, Planning, and Response, ALA Editions, Chicago.

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.

Mika J.J.;Shuman B.A. (1988). American Libraries, Vol. 19, No. 4, Library Furniture, pp. 314-317, American Library Association.

Latuszek Jr., T., 2002. Library Security: A Growing Awareness. Library & Archival Security, 15(2), pp.3–7.

Thompson, Samuel T.C. (2006) Information Technology and Libraries; 25, 4; ProQuest, pg. 222. https://visagecloud.com/faq