An Image Processing Based Framework Using Crowdsourcing for a Successful Suspect Investigation

Hasna El Alaoui El Abdallaoui(✉), Fatima Zohra Ennaji, and Abdelaziz El Fazziki

Computing Systems Engineering Laboratory, Cadi Ayyad University, Marrakesh, Morocco
h.elalaoui@edu.uca.ac.ma, f.ennaji@edu.uca.ma, elfazziki@uca.ma

Abstract. The invasion of new technologies in people's life has allowed a great interactive collaboration between citizens and law enforcement agencies. The appearance of crowdsourcing has become a new source of research and development especially in the suspect investigation domain that needs the combination of human intelligence and the technical tools to lead the investigation towards the greatest results. The objective of this paper is to exploit the pervasiveness of image processing techniques (face detection and recognition) to design a crowdsourcing framework that may be chiefly used by government authorities to identify a suspect. This framework is primarily based on the surveillance video analysis and the sketch generation tools supported by the intelligence of the crowd.

Keywords: Crowdsourcing · Image processing
Face detection and recognition · Suspect investigation

1 Introduction

Human intelligence has been the key to all the technological advances that humanity is experiencing. With the advent of the Internet and mobile devices, human intelligence has taken on a new form in our actual societies and has, however, enabled a better supply and processing of information. This has been conceptualized as 'crowdsourcing' and has been officially coined by Howe [1].

Crowdsourcing is defined as participatory production based on a collaborative logic, users use the creativity, intelligence and know-how of each one to answer a given problem or to perform a task. Since its emergence, crowdsourcing has contributed in several areas and more governmental organizations have integrated it into their decision-making policy [2]. Crowdsourcing initiatives typically focus on citizen online mobility as a new resource for innovation and problem solving for government agencies: citizens are no longer claimants of rights but contribute in several situations such as the identification of suspects.

Although crowdsourcing is increasingly being used by many organizations, some tasks are far from being feasible for human beings, either because they involve a lot of

A. Abraham et al. (Eds.): SoCPaR 2017, AISC 737, pp. 70–80, 2018.
https://doi.org/10.1007/978-3-319-76357-6_7

resources, require considerable computing time, or because they need more sophisticated tools for their achievement. Image processing is one of the disciplines that marks this exception and has, however, incorporated a set of very advanced algorithms and methods enabling humans to better study the image and its transformations. The conditions of brightness, lightening and color [3] are still major constraints in the image processing and more particularly in the facial detection and recognition [4] that are widely used in law enforcement.

This paper aims to exploit the crowdsourcing potential to obtain more accurate values by supporting or correcting the results of image processing techniques. For this purpose, a framework is proposed which allows the identification of a suspect from surveillance cameras or the suspect identikit generated from the personal description provided by the crowd.

The rest of the paper is organized as follows: the Sect. 2 presents a state of art related to the crowdsourcing concept and the suspect investigation. In Sect. 3 the approach of the proposed framework and its architecture will be described. A case study was handled in Sect. 4 while Sect. 5 discusses the results in a conclusion.

2 State of the Art

In this section, we present some useful information in the form of a synthesis in the two areas of interest of this paper, namely crowdsourcing in e-governmental applications and suspect investigations that have improved thanks to technological and scientific advances.

2.1 Crowdsourcing

The emergence of crowdsourcing. The term "crowdsourcing" was first coined by Jeff Howe and Mark Robinson in a Wired magazine article [1] as a fusion of two words: 'crowd' and 'outsourcing'. It was defined as the outsourcing of a task to a person or a group of people in a form of an open call [1]. It is important to highlight that the call should not be limited to experts or selected participants. Crowdsourcing is often based on the idea of collective intelligence, the aim is to make the knowledge the most accurate by giving contributions from a distributed population – "all of us together are smarter than any one of us individually…" [5]. Since its creation, crowdsourcing has become the subject of several research and studies.

Crowdsourcing and E-government. Crowdsourcing became a tool used for a wide group of governance activities to help government to engage with citizens: when a decision maker has a problem to accomplish some activities, he may involve a crowdsourced participation. Through a crowdsourcing platform, the decision maker (the crowdsourcer) submits the task and the crowdsourcing platform transmits it to the crowd. The appropriate participants are chosen depending on the crowdsourcing activity. Once crowdworkers finish the task, they send the results via the same platform to the crowdsourcer who evaluates the received data and selects the satisfying results. In some crowdsourcing activities, incentives and rewards may be offered to the participants. The crowdsourcers and crowdworkers may have any direct communications, through email, telephone, etc.

2.2 Suspect Investigation

The most comprehensive, practical and reliable manual on criminal investigation have been developed in [6]. A definition of criminal investigation has been proposed as a process of: *"...Discovering, collecting, preparing, identifying and presenting evidence [before a tribunal of fact] to determine what happened and who is responsible"*.

The suspect investigation requires that a series of steps must be taken in the proper sequence. A suspect investigation is usually initiated by an observation or a reporting of a crime. Then follows a process that may include all of some of these steps [7]:

- Initial investigation: it identifies important and informative elements through essential methods. It emphazes two procedures: Collecting and preserving of evidences and collection and interpretation of testimonies [7].
- Documentation: consists of carrying out a complete and detailed synthesis of all available information.
- Follow-up investigation: based on two steps. The first one is the reconstruction that is gathering the results of all collected data and secondly, the identification of the suspect. In this paper, we will mainly focus on the 'personal description' method to identify the suspect, the most important among eight other techniques [7].
- Prosecution and arrest: is the pursuit of any trace that may lead to the suspect arrest.

2.3 Forensic Investigation

The same authors in [6] differentiated between the suspect and forensic investigation; which means the introduction of technological methods and scientific processes in a criminal investigation [6]. The forensic methodology extracts evidences from digital platforms or exploit them to identify or analyze digital evidence. Hereafter, two of these digital techniques heavily used in law enforcement.

Video-based surveillance systems. Governments, public companies, private sector companies and individuals spend a good budget on surveillance cameras in order to secure their properties, prevent crimes and apprehend criminals. During the past decade, video surveillance systems have grown thanks to advances in computer vision research. The proof is the worldwide, continuing demand for video surveillance systems: The world market for video surveillance forecasts to increase by 7% in 2017. In the same year, 28 million high-definition cameras will be marketed against 66 million IP cameras [8]. Despite the fact that many problems (object detection and recognition, occlusion problems, etc.), are still far from being perfectly solved, video surveillance systems are becoming increasingly intelligent. From analogue CCTV systems, to fully digitized and automated network-based video surveillance, these systems experienced a great technological evolution [9, 10].

Performing digital identikits (or facial sketches). Sketches are widely used in criminal investigations to help in the identification and apprehension of criminals. They are carried out by means of a verbal description provided by the victims and witnesses and are then distributed in the media or posted in public places for possible identification by the crowd [11]. Thanks to technological evolution, they're making moves from free hand sketching (forensic sketch) drawn by forensic artists to computer kits (composite sketches) [12].

3 The Proposed Approach

It is in this section of the paper that the proposed approach will be described. As a first step, we define the problem that this solution tries to solve and then suggest a scenario that details the steps of the process. In a second part, we design the architecture of the framework in addition to all the components and their implementation.

3.1 Problem Definition

New technologies offer very advanced functionalities and possibility for human being to carry out tasks hitherto difficult to complete by himself. Intelligent surveillance cameras and sketch generation tools are among the technological achievements that have marked the crime-solving domain. Crowdsourcing, has become a model of aid and support that is widely used in various domains including law enforcement where crowdsourcing was the culmination in the resolution of several cases. The principle is to appeal the human intelligence for the search or the description of a suspect. Within this schema, we propose a framework that will link human intelligence and technological advances based primarily on the techniques of automatic face analysis in suspect investigation. This framework aims to facilitate the interaction between the crowd and the police in order to collect, analyze and share useful information to bring the investigation to successful results. All the functionalities and the process that the framework we are proposing follows will be detailed in the section below.

3.2 The Suspect Identification Process

To describe the process followed by the framework (Fig. 1), we first suppose that a suspect committed a criminal act (aggression, an armed robbery, etc.) and then fled. The authorities, then, check the surveillance cameras surrounding the crime's place. If a video is available, then starts the video analysis stage to retrieve the clearest picture of the perpetrator. If the police obtains a clear-cut image of the suspect, the automatic face analysis techniques will be the best way to search for a matching between the suspect that the police is searching for and a former criminal previously registered in the police database. If a matching exists, the crowd ensure the identity of the suspect. The identified suspect is then regarded as a criminal with judicial case so his profile is shared with the public to start the search process. In the case where no matching is found, the picture retrieved from the surveillance video is disseminated. Contrariwise, i.e. if no video has been recorded or the video is heavily unclear, the personal description is a prominent key in the identification of the suspect. Thanks to the police expertise in interviewing the victims and eyewitnesses, they can obtain valuable information concerning the suspect profile. This helps to perform the facial identikit of the suspect that will be spread once approved by the interviewees.

The next crowdsourced task is to alert the police about the suspect's whereabouts. Nowadays, the crowd is always accompanied by mobile devices equipped with rich sensors enabling them to share real-time location data.

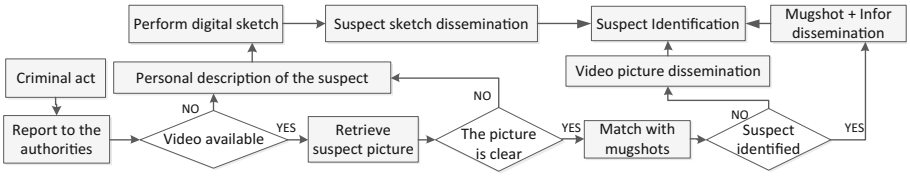

Fig. 1. The suspect identification process

3.3 The Proposed Approach Architecture

The framework we are proposing is a crowdsourcing application where several technical modules were incorporated and that are essentially based on facial detection and recognition methods. From the foregoing, the framework architecture is presented in Fig. 2 hereafter and each component is described separately.

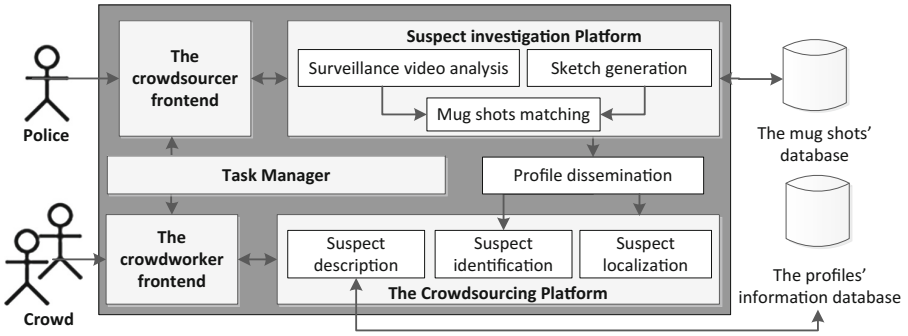

Fig. 2. The proposed approach architecture

The architecture's components can be described as follows:

- The crowdsourcer frontend: it is a Human-Machine Interface (HMI) that lets the police to control all the police investigation procedures. Thanks to this interface, all operations of the facial analysis will be carried out; this includes the analysis of surveillance videos and the generation of suspects' identikits. For any result obtained at the end of these operations, a matching with the profiles of former criminals will be performed for a possible identification of the suspect.
- The crowd frontend: it is the bridge that allows participants to access the crowdsourcing platform and permits them to perform all tasks assigned to them.
- Profile dissemination: is a common component between the police and the crowd. Its purpose is to widely disseminate the suspect profile (with the crowd and between the crowd's networks) in order to speed up the suspect identification.
- The task manager: As its name implies, this component is responsible for managing tasks between the crowdsourcer and the crowdworker. It defines the specifications of the crowdsourced tasks and their allocations (execution, participants, etc.).

Hereafter, a comprehensive description of the two platforms that constitute the contribution of this paper.

The Suspect Investigation Platform. It is the platform where all the image processing procedures occur. It integrates all the necessary modules:

Surveillance video analysis. Actually, surveillance cameras are real-time alerting systems. Thanks to image/video processing techniques, they are experiencing a continuous development. To do this, several methods of automatic face analysis will be exploited. In general, two main steps must be implemented:

- Face detection: It aims to distinguish a human face in an image. It is an indispensable phase in the process of facial recognition. The most known method is the Viola-Jones algorithm [13]. This method quickly became a standard in the field of computer vision since it incorporated new concepts and methods: The "Integral image" which is a notable gain in terms of calculating the HAAR characteristics. In the detection phase, the whole image is traversed by moving the detection window of a certain step in the horizontal and vertical directions. The second key element of the Viola and Jones method is the use of a boosting method to select the best features. The boosting algorithm used is in practice a modified version of AdaBoost [14]. One of the key ideas of the method to reduce the computational cost is to organize the detection algorithm into a cascade of classifiers. For more clarity, we have summarized the key steps of the Viola-Jones algorithm in Fig. 3.

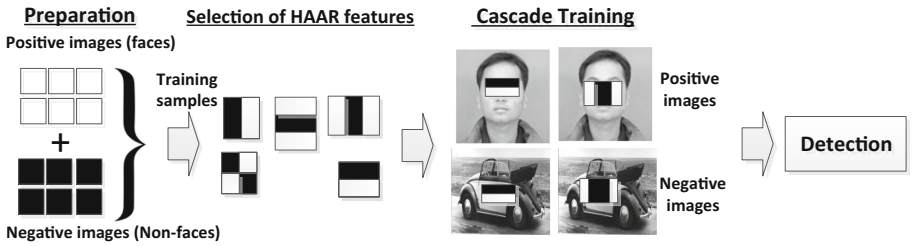

Fig. 3. The Viola-Jones algorithm

- Face recognition: is a field of computer vision consisting of automatically recognizing a person from an image of his/her face. Facial recognition algorithms extract the facial features and compare them to a database to find the best match. In this paper, we present the FisherFaces recognition method [15] based on two concepts: the EigenFace algorithm (PCA) and the Linear Discrimination Analysis (LDA). The first system of face recognition that yielded significant results was achieved using the so-called "Eigenfaces" method [16]. The "Fisherfaces" method has been proposed to solve the problem of robustness in the face of variations in pose, illumination and expressions that challenge the PCA. The Fig. 4 below presents the steps of the FisherFaces algorithm.

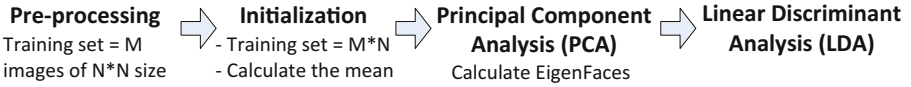

Fig. 4. The FisherFaces method steps

Identikit generation. Thanks to the description given by the crowd, the forensic artist will draw the suspect's sketch based on the suspect characteristics. The generation of identikits moves from free hand drawing to the use of recent technological tools. Police draughts men take special training to make sketches. To perform sketches, we used in this framework Faces IQ Biometrix software tool. It is used by worldwide police agencies because of its ease of use and its large facial features database.

The Crowdsourcing Platform. In the proposed framework, three major tasks will be the crowdsourcing activities delegated to the crowd. The first one is personal description, where the crowd is asked to provide the police with any information about the suspect (physical, vocal characteristic, etc.) using interview techniques [7]. The personal description is one of the main keys for a successful identification in the suspect investigation. In this framework, we did not use all the physical properties, but we were interested only on the facial attributes in addition to the gender and the skin color (see Table 1). These information are the most prominent for the sketch generation. The second task is the suspect identification that aims to confirm, directly or indirectly, the identity of the suspect by the crowd. The last task given to the crowd is the suspect localization. After the police disseminated the suspect's profile, the crowd has to report any trace of the suspect once located.

Table 1. Some examples of facial attributes for personal description

Facial attribute	Property
Gender	Male – Female
Human race	Black – White – Yellow – Red – Dark
Face shape	Oval – Round – Heart – Long – Triangle
Hair color	Black – Brown – Blond – RedHead – White
Hair length	Extra-long – Medium – Short – Extra short
Eyebrows	Soft – Thick – Unibrow – Straight – High/low arch
Eyes shape	Buried - Bent – Sharp – Small – Baggy – Round – Line
Nose shape	Pointed – Broken – Long – Droopy – Flat – Bulbous – Grecian
Mouth shape	Thin lips – Pulpy – Small – Big lips – Dissimilar lips

4 Case Study

A simulation of a police investigation has been done to test the effectiveness of our framework. The human intelligence cannot be compared with the machine one, more precisely in the facial analysis area. Whence comes the proposed solution that integrates the machine and human intelligence to contribute on the security of our country.

As a face recognition database, we used the MIT CBCL Face Data Set [17] provided by the Center for Biological and Computational Learning at MIT. All the people that exist in this database were considered as former criminals. Their images have been stored in addition to some supplementary information. Figure 5 shows a Java interface containing the suspects' information and their mug shots. In the following, we are going to give some examples of both cases.

Fig. 5. A part of the criminals' database

4.1 Surveillance Video Analysis

OpenCV image-processing library was used in our application. In most cases, the suspect is detected using the face detection and recognition algorithms explained in the previous section. However, the machine remains helpless and may give wrong answers like as it is illustrated in Fig. 6. The poor interpretation comes from several facts such as the quality of the video, the invisible parts of the face, etc. In such situation, crowd tasks are created to extract the maximum of personal information to construct a profile close to the suspect's one. The crowd interrogated had only a few seconds to visualize the face (the 4th face in Fig. 5) in all possible positions without knowing that they must provide details on each facial attribute. Table 2 shows the actual values and the percentage of people who responded correctly. The data provided from the crowd were closer to the actual values and allowed more precise personal description than that delivered by the algorithms of facial detection and recognition.

Fig. 6. A successful and a failed case in suspect identification from a real time video

Table 2. Some of the crowd results for personal description

Facial attribute	*Gender*	*Age*	*Human race*	*Face shape*	*Hair color*	*Hair length*
Real value	Male	20–30	White	Oval	Brown	Short
Answers	100%	51.2%	81.4%	30.2%	79.1%	74.4%
Facial attribute	*Hair density*	*Eyebrows*	*Eyes shape*	*Eyes color*	*Nose shape*	*Mouth shape*
Real value	Heavy	Thick	Round	Green	Pointed	Small
Answers	55.8%	55.8%	18.6%	23.3%	25.6%	30.2%

4.2 The Generated Sketch

The second experiment aims to simulate a digital sketch recognition. To do so, two faces were randomly chosen from the MIT face database to elaborate their sketch in addition of a real criminal image with its corresponding sketch (see Fig. 7).

Fig. 7. Two MIT faces and their corresponding sketches & a real criminal mug shot and sketch

As the previous experiment, the results show that the first and the last case were successful since it gives the corresponding image of each sketch (Fig. 8). Conversely, the second case when the quality of the sketch has been manipulated, our application couldn't figure out the owner of the sketch (see Fig. 8). This problem might happen either when the sketch is not well done or doesn't reflect the real face features of the suspect. Once again, a task is created making a use of the crowd intelligence to overcome this issue. The crowd participants were asked to recognize the owner of the sketch from four images under different positions. The results (in Fig. 9) show that the majority of the crowd (60.5%) have identified the right answer (suspect 3).

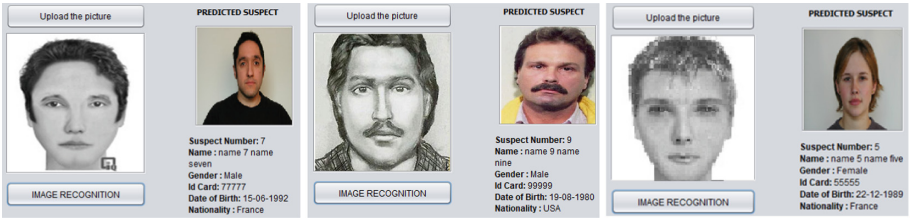

Fig. 8. Two successful sketch automatic recognitions and a fail case due to bad-quality sketch

Fig. 9. Crowd sketch recognition results

5 Discussion and Conclusions

Crowdsourcing gradually enters our society and tends to change some of our ways of thinking or acting. It creates a phenomenon of community and popular collaboration to perform various tasks. But crowdsourcing would never have gained so much extent without the enormous capabilities offered by new technologies.

In this paper, we concluded that crowdsourcing can be a great support for governmental organizations to access citizens as a source of information and particularly in suspect investigation where the accuracy of data is very important. The identification of suspects requires a good execution of the image processing methods, in particular the techniques of face detection and recognition applied to surveillance videos and identikits generation.

However, we have proved that the fusion of human intelligence and technological advances allows better analysis of data and more precise results and thus a success in the investigation and identification of suspects.

References

1. Howe, B.J.: The rise of crowdsourcing. Wired Mag. **14**(6), 1–4 (2006)
2. Doan, B.Y.A., Ramakrishnan, R., Halevy, A.Y.: Crowdsourcing systems on the world-wide web. Commun. ACM **54**(4), 86–96 (2011)
3. Yang, M.H., Kriegman, D.J., Ahuja, N.: Detecting faces in images: a survey. IEEE Trans. Pattern Anal. Mach. Intell. **24**(1), 34–58 (2002)
4. Ahonen, T., Hadid, A., Pietikäinen, M.: Face description with local binary patterns: application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 2037–2041 (2006)
5. Aitamurto, T., Leiponen, A., Tee, R.: The promise of idea crowdsourcing – benefits, contexts, limitations. Nokia IdeasProject White paper, vol. 1, pp. 1–30 (2011)
6. Hess, K.M., Orthmann, C.H.: Criminal Investigation, 9th edn. Cengage Learning, Boston (2016)
7. Sefanyetso, J.T.: Personal description: an investigation technique to identify suspects (2009)
8. Les Grands Tendances 2017 De La Vidéo Surveillance. http://www.video-surveillance-direct.com/content/88-2017-les-tendances-de-la-video-surveillance. Accessed 05 July 2017
9. Zhang, Z.: Intelligent distributed surveillance systems: a review. Chin. J. Electron. **14**(1), 115–118 (2005)
10. Swanson, C., Chamelin, N., Territo, L., Taylor, R.: Criminal Investigation (The Evolution of Criminal Investigation and Forensic Science). The Granger Collection, New York (2011)
11. Klum, S., Han, H., Jain, A.K., Klare, B., Church, F.: Sketch based face recognition : forensic vs composite sketches. In: International Conference on Biometrics, pp. 1–8. IEEE, Madrid (2013)
12. Streed, M.W.: Creating Digital Faces for Law Enforcement, 1st edn. Academic Press, Cambridge (2017)
13. Viola, P., Jones, M.J.: Robust real-time face detection. Int. J. Comput. Vis. **57**(2), 137–154 (2004)
14. Freund, Y., Schapire, R., Abe, N.: A short introduction to boosting. J. Japan. Soc. Artif. Intell. **14**(5), 771–780 (1999)

15. Hjelmas, E., Low, B.K.: Face detection: a survey. Comput. Vis. Image Underst. **83**(3), 236–274 (2001)
16. Turk, M.A., Pentland, A.P.: Face recognition using eigenfaces. In: Computer Society Conference on Computer Vision and Pattern Recognition, pp. 586–591. IEEE (1991)
17. Weyrauch, B., Heisele, B., Huang, J., Blanz, V.: Component-based face recognition with 3D morphable models. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. IEEE (2004)