This project has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement n: 607480

LARGE SCALE INFORMATION EXPLOITATION OF FORENSIC DATA

2nd Workshop Minutes

LASIE Project

FP7 - SEC-2013.1.6-1 - Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes – Integration Project

Grant Agreement n°: 607480

Start date of project: 1 May 2014

Duration: 42 months

Document. ref.:

2nd Workshop training session minutes

LASIE workshop, 22 June 2016 (morning)

Questions during presentations

Q: It is very challenging to detect general items (cars, people, bags) in a scene, can the algorithm do that?

A: We tried to implement SOTA algorithms but it's very challenging. SOTA is not yet able to perform well with good quality for all problems. We define basic problems and focus on those. We were able to obtain promising results in detecting faces, logos, etc. with low resolution. We don't need to process all the content. We need to find features that are best descriptive of the video. With the current content, we introduced DROP in this project. We detect salient patches (distinctive features) in the image. And then search for the respective patches through the videos to find the best matches. What is interesting for us is the accuracy of our algorithms.

Q: Do you use Geolocations and temporal data for detection of people?

A: What we have so far is low-level processing of data. We have the extracted patches and features, and we are able to search within a temporal window in the videos. This is useful in the inference module, where the relationship between items are accounted for. We can define distances between objects as well. In reasoning features the focus would be on temporal data and in low-level analysis the Geolocations would be considered.

Q: How do you deal with the problem of languages not mapping onto one another?

A: At this moment we don't have cross-lingual search. But we have for English and Spanish. We shall investigate this in the future. Our text analysis can understand the structure of a sentence (Spanish, English). But we don't have a mixed language context. In UC2 all context is in Spanish. In UC3 we try to identify the language. This kind of analysis is based on the entities in the graph. The graph is a meta-language. You can change the language in the graph.

Q: How does this compare with commercially available projects? We have NLP analysis tools from 16 years ago and I imagine that the commercial parts have moved on and how does this interface work and how does this compare?

A: Commercial products and SOTA are looking at web platforms, not adaptive to forensic investigations. We are producing some very generic results, but they can be fine-tuned and adapted to

forensic investigations. Our NLP is adapted to forensic framework. The commercial products are impossible to adapt with our usage, as they are very generic. Many of them are not adapted to the document filters for example from court.

Q: Can we use a commercial product and adapt it? Aren't they more advanced? How much better are they in terms of maintenance?

A: You'd be surprised how difficult it is to adapt only for text, the commercial products, things like the reconstruction of temporal information. We use open source and it is much better for adaptation and development. We have involved SenseGraph in LASIE, which is a well-known linguistic feature. We have very advanced tools for English and Spanish that are comparable with equivalent commercial solutions. For a research project it is a must to start with openly available libraries and take things from there and develop. In the end of the project we shall do some benchmarking test to compare with commercial products. We do not yet have the complete solution and therefore cannot yet provide a benchmark.

Q: The statistics cannot solve the problem we are facing. The numbers cannot affirm a situation such as racism. What is the ratio of the socio element to the technical element in your project?

A: This dimension you are referring to is a bit higher. You are talking about strategic societal aspects. We are looking at local law enforcement by authorities. We have a complete system with ontologies, that can look in the loop who is responsible to make decisions in the system.

Q: The ethical aspect of privacy should not depend on technology. For instance, if on a phone you write a letter no one except a judge asking for this should know what I have written (on platforms such as WhatsApp). This is a real international problem, where sovereign states have different rules.

A: WhatsApp is the most used application, amongst other applications, there are other forms of encryption on those platforms and it is dependent on the encryption on the phone and what the application is providing, such as the end to end encryption now on WhatsApp.

Q: We are talking about constitution. Can we use the information on social media in groups where they are organizing some criminal events?

A: That's an ongoing discussion. What if a police officer makes a fake profile and gets added to a group to get information? That is connected to investigation. Probably it could not be legal without lawful rights, and that is an illegal fraud case for obtaining information.

Q: The law may be behind the technological developments. To what extent can they consider the impact of technological development in ethical principles in European countries? Is it set in stage in any European projects to look into this? In UK at least any information that can be used to identify you is personal data.

A: What is surprising in the UK is that when you arrive in the airport you can buy a SIM card without an ID. Then you can buy a cheap phone, and then you are absolutely not traceable. This is not the case in Italy. Why haven't they thought about that? It reflects the kind of legal approach taken in anglo-saxon countries. Where the court can only intervene when there is a real necessity.

Practical session, 22 July 2016 (afternoon)

Session: UC1

Q: If you select a part of a DROP, does the bounding box recognise this is only part of the DROP?

A: The descriptor recognises the colour first which is the most important part at the first step.

Q: Before you search do you have to normalise the video and transform the format?

A: Yes, for the process we have to convert them to specific format.

Q: When you convert the video did you merge the time? Do you consider the time for process? How long does it take to prepare the video?

A: It takes 10 minutes to process the video.

Q: Can you search over network and cloud?

A: Yes, it is possible.

Q: Have you considered the same tracking object from different angles of the camera?

A: We are not considering this in this project. We consider tracking form different angles and the geolocation is considered by the name of the street. Considering a group of people for the tracking if one of them has a distinctive pattern would make it easy to track the rest of the group.

Q: Are you using standard web components?

A: Yes.

Q: What is the database?

A: MongoDB for the multimedia data.

Recommendation: Would be interesting to use a system called Psim to connect multiple CCTV together and each of the CCTV could give specific SDK and you can use this SDK as a driver in the PSIM and connect all of them together.

Session: UC2 - 3D Scene Reconstruction:

Questions about the data acquisition:

Q: Can the resolution be increased?

A: Yes, at the expense of larger memory requirements. A trade-off between both parameters has to be achieved. The main limitation is the depth estimation. The model can be multi-resolution, providing a different resolution depending on the size or interest of particular objects.

Q: Are these functionalities included in the software kit provided with the cameras?

A: No, they have been developed on top of the provided software, which only includes depth and tracking information.

Q: Are these techniques patented (by Huawei)?

A: No, they are state-of-the-art algorithms proposed in the literature.

Q: What is the maximum size of the room for 3D reconstruction?

A: It depends on the memory of the machine, but it allows to model large rooms. It is possible to capture the information for the reconstruction and then generate the 3D model offline.

Q: Is the reconstruction importable to Sketch-up?

A: Yes, it is.

Q: Can other objects/people be integrated in the model?

A: Yes, this is possible and the scale of the objects is maintained.

Q: Does the system allow to reconstruct dynamic scenarios in which objects are moving?

A: Not yet, this is a very challenging problem and still under research.

Q: Can this be applied to the investigation of other types of accidents or crimes?

A: Yes, as long as the scene is static.

Q: Are measurements real?

A: Yes, the tool allows to measure any objects in the scene.

Other explanations:

- Outdoors a stereo camera is used and indoors a Kinect camera is used.
- The tool allows to integrate high definition multimedia content (video, photo, etc).
- The added value with respect to one camera 3D reconstruction is that it provides depth and distance information.
- The tool allows to save time in the development of the 3D models, which are currently performed by hand by ADM using Sketch-up. The presented functionality would not substitute the current process but it is a clear advance.
- The 3D model can be stored in html format and can be opened with any web browser, it does not require any specific format.
- Additionally, the system allows to generate a grid of points which can be reconstructed via Sketch-up, saving a lot of time to the officer.

Questions about the crime scene reconstruction:

Q: How does this system work and what kind of data is used to create a 3D scene.

A: The 2D reconstruction is done with data from a Kinect depth camera. You would walk around a scene and collect the depth data, then the algorithm creates the 3D scene. You can assign labels to

the scene components, and then create a storyline, by which it is possible to narrate the events in chronological order. We can have annotations for the scene as well, and moreover, we can add multimedia information for each part of the 3D scene.

Q: Can the reconstruction be done with a set of images of a scene?

A: Yes, but it will yield a very sparse representation for the 3D scene and is not visually accurate. Spatial accuracy will also be problematic using images.

Q: It would be nice to be able to put some animation inside the scene, such as people moving around, events happening, etc.

A: Noted.

Q: Can this be used in a court report?

A: Yes, this is implemented in HTML so it's very report-friendly and can be used across platforms. Currently the court does all of this on papers with sketches, but a 3D reconstruction can be much more useful in court reports.

Q: Can you do 3D reconstruction with 1 single camera?

A: Yes, but then we would have relative distances and sizes between objects, and we cannot directly infer the size and distance between objects. That is why we use 2 cameras of Kinect.

Session: UC3 - Text Analysis

The missing person's demo was presented to the End-Users from Lisbon/Portugal, UK Home Office. Fact sheet of Claudia Lawrence was presented together with face sheet of Calum Terras.

Q: Is the tool automatic?

A: The investigator manually identifies the end-points. Web, FB and Twitter. The tool is started by the investigator.

Q: How about the friends of the missing persons?

A: The unnecessary information or irrelevant information can be filtered by the investigator.

Q: Can the system be linked with the content management system of the organisation?

A: Yes, it is possible. It depends on the application.

Q: Can the platform secure already existing dataset?

A: Yes, it is possible.

Sense Graph was presented to show the relationships between the events and concepts.

Q: Does the platform support multimodality of the information associated to the specific case?

A: Yes, it is possible.

Q: What are the functionality of the final version?

A: Further refinements, all the models integrated.

Q: Additional end-user capabilities?

A: Automatic discovery of people, places, reconstruction of spatial-temporal events, causal relationships, build a repository of known cases to generate additional knowledge to guide the investigators. Pattern analysis from previous cases.

Q: Does the platform conform to industry standard technology?

A: Yes it does.

Q: What are the search capabilities of the platform?

A: The sources are added to the system and the automatic content processing modules provides indexing terms that enables the search capability of the system.

Session: Super-recognisers testing tool

Q: Is the video tracking algorithm automatically picking up every human individual passing through the scene?

A: Yes, it does. But practically, administrator of the system should choose tracks and select faces that will be used for the super-recogniser testing. No-one else can see the tracks but the administrator.

Q: Did you see with super-recognisers whether they are better to recognise their own race?

A: White super-recogniser tent to be better in super-recognising black face, than black people to recognise black.

Q: What about woman/man distribution in super-recognisers?

A: We have a pretty close man-female split. 60% more woman are participating to the tests.

Q: Does a tested person see only number of tracks preselected or unlimited number?

A: Its preselected set only.

Q: Why for some cases the system returns faces and in other cases it returns arm or partial face?

A: It's because in some cases people get obscured by other people or objects in front of the person. Face detection is done automatically.

Q: Can the system mistake dog and person?

A: No, the algorithm has been trained only for people.

Q: What kind of method you are using for person detection?

A: Deep learning.

Q: Does each clip work in isolation to the search you do?

A: Yes, this is the case.

Q: What sort of distance can the algorithm use? What about people far away in the background?

A: If we have enough videos for training the algorithm, it will work even with high distance cases. We need a big training set.

Q: Is the person tracking algorithm the same as integrated in the LASIE system?

A: Yes, it is the same module taking care of this process.

Q: How did you sort out permission when filming people in public?

A: We had signs around the area, so people were aware of being filmed and could avoid area if not wanting to be on the footage.

Q: Do I have to create an account for myself if I want to access the tool and try it?

A: Yes, you can create a fake account and you can try it.

Q: I upload a brand new video and I select tracks. What I would like to see is correct hits, and any people that are identified as not a target. Also it would be interesting to see the amount of time super-recognisers are looking at one video when keeping the cursor over the video.

A: Yes, we can track that per video. So far we track the overall time.

Recommendations:

The system looks good and it would be good to continue with the development and bring more features. We would like to test it with real super-recognisers, and on videos that we are using in real tests, to see how people interact with the UI and features.

2nd Workshop technical table session minutes

Session lead by Mattia Epifani, forensic analyst and representative of the EVIDENCE project

The following minute report in brief the most key discussions had during the session.

Q: What is Law enforcement and private sector position with respect to sharing and revealing of traced data?

A:

- We live in an international world and trace data sharing and revealing is key sometimes for ensuring security. Only some years ago we had just problems with passwords workover. Very appealing indeed. The way they are going to be handled have to take into account cultural differences (cultural approach).

It's good to work against each own vulnerability and it's best that private company can do it is to take care of data security by themselves.

- Technology is not making things easy: nevertheless there is the exigency of making society secure and investigations are focusing day by day more on technologies and data generated by technologies used, there are solutions which make this more complex. For example WhatsApp only recently started crypting chats (information exchange) and this is strongly complicating investigations when data of smartphone have to be analysed. As results, some countries (Brazil) banned the usage of WhatsApp. As a consumer I know WhatsApp is secure from coaptation point of view, but WhatsApp shouldn't prevent judges to access to its data.

Similar cases have occurred with Apple, for the access prohibited to iPhones in several occasion. In a nutshell, sometimes technology providers themselves if on the one side promote privacy of their users, are increasing investigations difficulties in case of crimes.

- Investigations sometimes can carried out not only by digital device is also by installing malware in the device to have access to the data to have access to content.

- The privacy should not depend on the technology used by citizens but ensured by law.

- On the other side, there are technology providers (like Google) largely used which not ensure privacy at all. I mean, you don't have privacy, they have access to all your information and history of your behaviours.

- It is not acceptable that private company have access to all such a data while investigators and judges cannot access in some occasions

Q - Is acceptable or not if I seek evidence among specific information available in social media?

A:

- Through open source and social media you can have access to a huge amount of information also if you are not authorised. What if a police officer makes a fake profile and use it in social media with the intend of taking information?

- It could be done, but it is not legal. It cannot be admitted in legal courts.

- Technology has to help to reduce the time of investigation, by the way.

- Technology also simplify criminal acts, so ti should contribute also in better fighting crimes. For example, by knowing the password of apple you can track the location of a smartphone or of anything has a GPS installed. Police forces can do it (also accessing to telephone providers data), but also criminal can do the same and it is the bad point of the technology. All people can use (also mis-using this): just as an example, a guy can find the location of his girlfriend by knowing the password of its profile and can track her location.

Q - Law is sometime behind the technology- how we sort out that where law can work? What is the European ethical commitment? Who do we consider in European project?

More, the focal point is personal data: in EU definitely there is not the same situation and the same approach. Sometimes there are contradictions. For example, in UK you can find everywhere CCTV and privacy almost don't exist in public locations. On the other side, I'm extremely surprised that in UK you can get sim card or phone without personal ID. How is this possible?

In UK you don't need to present a personal ID for buying a sim card. In Italy since 20 years you have to go and register the document for doing it. Why in UK is not the same? Where is the need of these two situations?

A:

- In Portugal you have to provide the document to register for sim card but it is also possible to escape it in some ways.

I suppose also in other countries you need to provide and store the copy of your ID?

- Yes they save them and store all the data

- There is no traceability of sim card and person in some countries and it's just because traditional difference

- If you want to do anything you can buy other country and pay for the roaming, there is no sense. Eu strongly need to adopt a unique approach. There is the need of standardisation in ethics and privacy, not only for the usage of data as evidence, but also for the possibility to use similar kind of data.

- The problem comes from a cultural difference; why some country use and other not? Some countries want to control and know all they can, others just the most key issues. We shold find a compromise at EU level. Also, in investigations we should be able to use all relevant data and relevant is the key word. Too many information can lead to nothing, you just need to see the key one.

- On the other side people will not to be traced also for common things. There is a strong reluctance to be subjected to control, and this brings to the UK approach. It is useless to control people on everything, especially if the is the possibility to escape. People is moving from traditional technology like calling by cell phone to WhatsApp and voice over IP as WhatsApp since it is more secure and no one can intercept the conversation, also if they speak about the weather. Technology has to ensure privacy, but enable law enforcement authorities (and judges) to have access to people data if relevant. And relevance is something that judges have to decide, not private companies (especially foreigner private companies).

- There is the possibility to retrieve massive information from data and there would be the question of who is managing the available data. When you got all the digital data how you are going to manage them to help the investigation. This is the key point.