C47 Face Recognition on CCTV Material Using a Biometric System

Arnout C. Ruifrok, PhD, NFI, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS*

The goal of this presentation is to inform the forensic community about the possibilities and limitations of biometric face recognition on CCTV surveillance material.

This presentation will impact the forensic science community by providing information about the possibilities and limitations of biometric face recognition on CCTV surveillance material.

Biometric face recognition is still advocated as a good option for person identification and detection of people on watch lists. However, the current state of the art in face recognition is mostly not sufficient for forensic appli- cations. Although some of the techniques reach reasonably high levels of recognition under controlled circumstances with frontal face images, of course surveillance images hardly ever capture a suspect frontal face, with good lighting conditions, and a neutral facial expression. Of interest for the forensic use of biometric systems is knowledge about the reliability of the matching results, even under imperfect conditions. The performance of the FaceVacs software from Cognitec using different public and private data- bases of different quality was studied.

Verification match results were used to construct receiver-operator curves (ROC), and the Equal Error Rate (EER, setting at which the fraction of false accepts is equal to the fraction of false rejects) was used as performance criteria. When using good quality controlled lighting and frontal pose images, an EER of 1.5% could be reached. However, the EER quickly increased to around 24% when non-frontal images were included. When less controlled, but still ISO/IEC nr952 compliant, frontal images were used, the EER was about 3%. However, when document scanner images of passports were used for the comparison, the EER increased to around 20%!

Verification using images with degraded quality (query as well as data- base) showed that at an eye distance below 30 pixels failure to enroll (FTE) quickly increased, but that the EER of the accepted images remained rela- tively constant. Compression of passport-type photo's had no clear influ- ence at files sizes of 5KB or more. Blurring of ISO/IEC nr952 compliant passport size images resulted in significant increase in the EER when Gauss filters with a radius of 5 or more pixels were used.

Hit list results (above a certain threshold level) were determined to study the influence of image quality on probability of detecting persons in a 'watch list' setting. When frontal, ISO/IEC nr952 compliant, frontal images were used, the correct identification level reached more than 80%, with 1-2% of the people incorrectly identified, and the remaining not recognized. It should be noted however, that these were images of cooperating people, not trying to conceal their identity and motivated to be correctly recognized. Reduc- tion of the resolution of the query images (but not the database images) below 30 pixels between the eyes resulted in a decrease in correctly identified peo- ple, due to the increased FTE. The number of incorrectly identified people did not increase when resolution was decreased. The results for increased compression were similar: reduction of the correct recognition of passport- type photo's 5KB or less due to an increased FTE, without an increase in incorrect identification. Blurring passport quality images resulted in a decrease in correct as well as incorrect identifications and an increase in FTE. A point to note is that some people gave a high number of false hits even with good quality images: up to 9 false hits for one person were found above default threshold level in a database of about 1200 people. This means that some (unfortunate) people will be highly prone to false 'identification' in a watch-list situation.

It is clear from the above that the performance of this biometric system is severely influenced by the quality of the images.

To study the performance of this biometric system using CCTV camera recordings, a surveillance system with multiple cameras, and made recordings under controlled conditions was acquired. Similarity scores of the biometric system using images made from the same person can then in turn be used to define an overall quality of the CCTV images at certain resolution and compression settings. Preliminary data indicate that the match values using the FaceVacs system are below the default threshold for all cameras and settings investigated, even when only zoomed-in frontal images under controlled lighting conditions at 2.5 m distance are used. These data suggest that the forensic value of biometric face recognition of faces on (704x576 pixel size) CCTV images is limited at best.

Face Recognition, Biometrics, Surveillance Images

 ** Presenting Author*