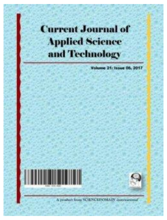

Current Journal of Applied Science and Technology

30(5): 1-13, 2018; Article no.CJAST.44481
ISSN: 2457-1024
(Past name: British Journal of Applied Science & Technology, Past ISSN: 2231-0843, NLM ID: 101664541)

Standardising the Capture and Processing of Custody Images

Shelina Khalid Jilani[1,2*], Hassan Ugail[1], Stephen Cole[2] and Andrew Logan[3]

[1]Faculty of Engineering and Informatics, Centre of Visual Computing, University of Bradford, United Kingdom.
[2]Acumé Forensic Ltd, West Yorkshire, United Kingdom.
[3]Faculty of Life Sciences, Optometry and Vision Science, University of Bradford, United Kingdom.

Authors' contributions

This work was carried out in collaboration between all authors. Authors SKJ and SC alongside colleagues at Acumé Forensic Ltd designed and developed the Hardware for the Halo. Author SKJ also wrote the first draft of the manuscript and managed literature searches. Authors HU and AL managed the second version of the manuscript. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/CJAST/2018/44481
Editor(s):
(1) Dr. Luigi Maxmilian Caligiuri, Professor, Faculty of Science, University of Calabria, Italy and Foundation of Physics Research Center (Director)- FoPRC, Italy.
(2) Dr. Meng Ma, Associate Professor, Anhui University, Hefei, Anhui, China and Icahn Institute for Genomics and Multiscale Biology, Icahn School of Medicine at Mount Sinai, New York, USA.
Reviewers:
(1) Lei Zhang, University of Pittsburgh, USA.
(2) Zlatin Zlatev, Trakia University, Bulgaria.
(3) Irshad Ullah, Pakistan.
(4) Hui Yang, Institute of Science and Technology Development, Beijing University of Posts and Telecommunications (BUPT), China.
Complete Peer review History: http://www.sciencedomain.org/review-history/27329

Original Research Article

Received 14 September 2018
Accepted 12 November 2018
Published 20 November 2018

ABSTRACT

Custody images are a standard feature of everyday Policing and are commonly used during investigative work to establish whether the perpetrator and the suspect are the same. The process of identification relies heavily on the quality of a custody image because a low-quality image may mask identifying features. With an increased demand for high quality facial images and the requirement to integrate biometrics and machine vision technology to the field of face identification, this research presents an innovative image capture and biometric recording system called the Halo.
Halo is a pioneering system which (1) uses machine vision cameras to capture high quality facial images from 8 planes of view (including CCTV simulated), (2) uses high quality video technology to

**Corresponding author: E-mail: S.Jilani@bradford.ac.uk, shelinajilani63@gmail.com;*

record identification parades and, (3) records biometric data from the face by using a Convolutional Neural Networks (CNN) based algorithm, which is a supervised machine learning technique. Results based on our preliminary experiments have concluded a 100% facial recognition rate for layer 34 within the VGG-Face model. These results are significant for the sector of forensic science, especially digital image capture and facial identification as they highlight the importance of image quality and demonstrates the complementing nature a robust machine learning algorithm has on an everyday Policing process.

Keywords: Custody imaging; face; machine learning; identification.

1. INTRODUCTION

Custody images are a critical component of the judicial system. Custody images are photographs of an individual who has been detained at a police station following an arrest on suspicion of committing a crime. In the UK, custody images are taken by the police, pursuant to Code D of the police and Criminal Evidence Act 1984 (PACE) [1,2,3]. PACE permits custody images to be retained for preventing further crime [4-6]. Accordingly, to share intelligence for the purposes of crime detection and prevention, most police forces now upload custody images to the Police National Database (PND). As of July 2016, there were over 19 million custody images on the PND [4,5].

Technological innovations, such as the development of drone units or image recognition software, provide police forces with powerful tools to advance investigations and improve the detection and prevention of crime [6-9]. Despite their importance in the judicial system, however, the technology utilised to capture custody images has received surprisingly little investment.

Currently, the processes employed to capture custody images differ markedly across UK police forces. For example, three of eight investigated police forces reported using either a camera or a webcam to capture custody images [5].

Another three police forces, on the other hand, used a dedicated photo booth. These differences in the equipment used for image capture introduce considerable variation to custody images, particularly in terms of the lighting used to illuminate the suspect, background, the plane of view and shadows. Further, while some police forces rely upon a single, frontal-view image, others capture up to three images, from different viewpoints [4,5]. There is also considerable variation in the camera-suspect distance and the resolution of the captured images (see Table 1).

Standardising the capture of custody images offers many advantages. Firstly, developing a standard protocol will ensure that no police force is hindered by sub-optimal custody images. Secondly, a standard approach will ensure that custody images captured by different police forces are directly comparable. This would improve the effectiveness of intelligence sharing nationwide and has the potential to improve the detection and prevention of crime. Thirdly, a standardised protocol for custody image capture would mitigate the risk of misrepresenting or augmenting specific face features. Reducing this source of error is important because distorted features may influence the identification decision rendered by experts.

One route to standardising custody images is to provide all police forces with the same equipment (camera, lighting and background) for custody image capture. This equipment should be specifically designed to optimise conditions for the capturing of high quality and consistent images.

Halo (patent pending) is a new generation, high-resolution (2763 × 3684) custody image capture system. Halo captures images from eight viewpoints, five on a horizontal plane and three elevated.

The latter is intended to simulate CCTV camera views, which are often recorded from above. An additional DSLR camera is utilised to record soft biometric features; such as scars, tattoos and freckles etc.

In addition to the Halo, two systems for custody image capture are already available.

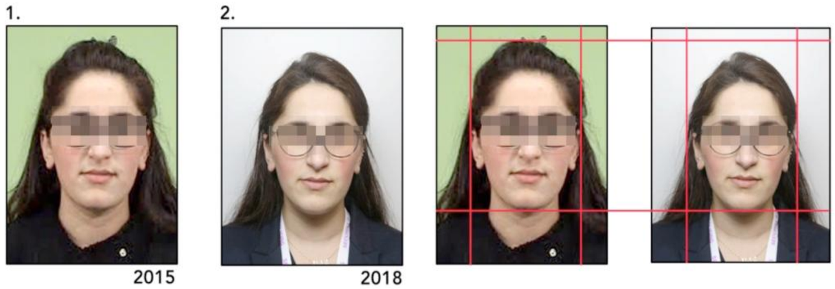

Figure 1: Comparison of two custody image capture methods:
(1) a standard camera/tripod set-up and (2) a purpose-specific, custody image photo booth. Both methods employed a non-standard light source. Image 1 is illuminated with general, indoor lighting. Image 2, on the other hand, is lit by a single LED panel, positioned directly above the head. Both approaches have resulted in shadowing within the lower part of the face, particularly around pronasale (tip of the nose). Further, while the face is centrally positioned within both images, the face occupies a greater area of the image 1's frame, relative to that for image 2 (highlighted with gridlines in the right images). The Halo offers significant advantages over both of these methods: (i) the number of images captured from a range of different view planes, (ii) homogenous and consistent illumination, which avoids shadowing and (iii) improved image resolution.

Viper [10] and Promat [11] are primarily video ID Parade systems, which are in operation across England and Wales. Both systems use video recording technology to create virtual identity parades. Image capture systems have been developed for use with both Viper (The National VIPER Bureau Identification Booth [12] and Promat (*standing for Profile Matching*). Table 1 provides a comparison of these image capture systems with the Halo.

In addition to capturing photographs, the Halo records high quality video footage, which is compliant with the requirements of the Viper™ and Promat™ virtual identity parade systems.

Another route to ensuring consistency in the custody images obtained by different police forces is to develop a national protocol for image capture. A standard protocol for the capture of custody images has been developed by the Home Office, in association with the National Policing Improvement Agency (NPIA).

This protocol requires that, as a minimum, custody images comprise a frontal, full-face photograph of a suspect with a neutral facial expression (both eyes open, mouth closed). The full head and hair should be clearly visible. Further, to optimise the images for use with facial recognition and biometric technology, the images should show the iris and pupil of the suspect's eye [5]. Lighting can transform the appearance of a face [13]. Accordingly, the proposed guidelines for custody image capture suggest that a uniform, balanced light source (e.g. three-point light source) should be used which minimises shadows, either on the face or background. The background should be smooth, flat with an 18% shade of grey. Finally, to accurately represent the proportions of the head and neck, the suspect should be centred within the frame.

Proposed future developments to custody image capture protocols include requiring additional photographs to be taken from non-frontal viewpoints: a 90° head turn (left and right), a partial (45°) head turn (left and right), a downward-facing (20° - 45°) image, to simulate CCTV, and an upward facing image (20° - 45°).

Images captured by the Halo are compliant will all requirements of the existing, and proposed, protocols for custody image capture.

The present study provides a description of the Halo system. In addition, we aimed to determine the suitability of the Halo to capture custody images which could then be submitted to an automated facial identification system, based on a machine learning algorithm.

Table 1. A comparison between the technical specification for custody image capture and video footage between (1) the Halo, (2) The National Viper Bureau Identification Booth and (3) Promat's Digital Image Capture Booth *(The data presented has been independently verified by personnel at Promat™. Information was also requested from Viper™ but was not supplied. Accordingly, fields have been classed as 'unknown' where applicable)*

	1. Halo	2. Viper Booth	3. Promat Booth
Custody Images	8	*Unknown*	Configurable 1 or 3.
Custody Image View • ***Single View (front)*** • ***Multi View***	Multi-view	*Unknown*	Single view
Custody Image Dimensions *(Post-Processing)*	2763 × 3684	1347 × 1684	1080 × 810
Custody Image File Size *(Pre-Processing)*	~ 70mb	*Unknown*	~ 2.5mb (configurable)
Custody Image File Size *(Post-Processing)*	~ 0.4 – 0.9mb		
Parameter Display • ***Face*** • ***Eyes*** • ***Other***	✓ ✓	Eyes	✓ Nose
Additional Images • ***Elevated Facial Images*** • ***Tattoo/Scar Images***	✓ ✓	Subject to the requirement of a police force.	Subject to the requirement of a police force.
Camera Type	Machine Vision	Cannon DSLR	Video camera
Total Cameras	4	1	11
Distance between camera and subject	~ 80 cm	Not fixed.	~ 80 cm
Sequential Custody Images	✓	*Unknown*	X
Custody Video Footage	✓	✓	✓
Video Quality • ***High Definition (HD)*** • ***4K***	High Definition	High Definition	High Definition
Video Dimensions *(Pre-Processing)*	1920 × 1374	*Unknown*	*Unknown*
Video Dimensions *(Post-Processing)*	720 × 516		720 × 540
Video File Size *(Pre-Processing)*	~ 58mb	*Unknown*	*Unknown*
Video File Size *(Post-Processing)*	~ 1mb		~ 1– 1.5mb

2. METHODS

2.1 Hardware

The Halo has been designed and manufactured by Acumé Forensic to enable consistent custody images to be captured by police forces. The Halo is a triple-panel steel unit, with rolled edges, and a non-slip floor plate, to minimise the risk of injury with non-compliant subjects. The Halo unit is designed to be sufficiently compact (191 cm height, 150 cm width) for custody suites.

The camera-subject distance is an important determinant of the consistency of custody images. Images which are taken too close to the subject may distort individual features. On the other hand, long distances significantly reduce image resolution. The Halo controls image distance by seating suspects in a high-backed chair which is fixed 80cm from the center panel. This fixed distance optimises the consistency and resolution of custody images.

Each of the three panels houses a single machine vision camera. This enables photographs to be captured simultaneously from three viewing angles. In addition, the centre panel includes a second camera, positioned above head-height, at an angle of 30°.

This fourth camera takes facial images from a simulated CCTV viewpoint from three positions; directly above the head, right 45° and left 45°. The latter two images are achieved by rotating the subject to different viewing angles.

Six LED light sources (two per panel) provide a consistent and bright light source. In line with the national protocol for custody image capture, this is a balanced 3-point light source. This enables the Halo to produce images which are free from shadows, across a wide range of viewpoints, see Fig. 3.

The Halo is controlled by an operator using a stand-alone terminal (see Fig. 2).

2.2 Camera

The Halo uses four iDS machine vision cameras which are encased within the three stand-alone panels. A single camera is positioned within the right and left panel, while the centre panel houses two cameras: one is positioned in the horizontal plane and another is 38cm above, fixed at an angle of 30°.

Each camera has a 1/2" rolling shutter and a CMOS colour sensor which captures images of 18 MP resolution, (4912 x 3684) with a frame rate of 12.2 (fps) [14]. Machine vision cameras were utilised in place of conventional digital cameras because the former afford significantly improved image resolution.

To ensure optical clarity, a Tamron lens with a focal length of 8mm and an aperture range of 1.8-22 is houses within each camera [15]. All four cameras share a common focal point.

(1) (2)

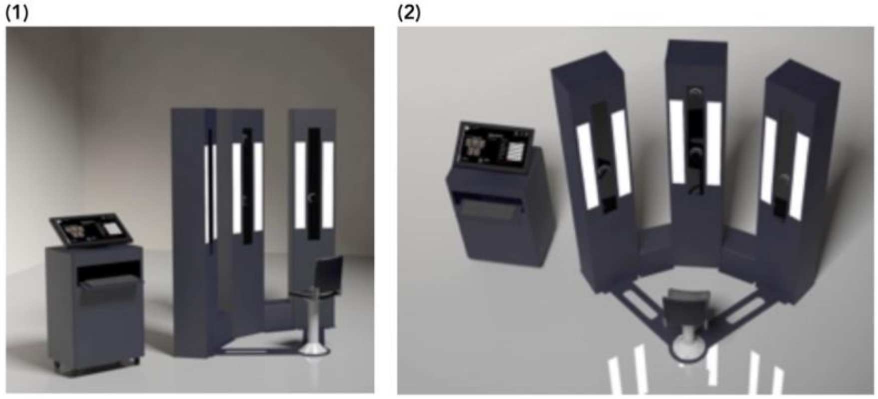

Fig. 2. 3D representations of the Halo capture system from (1) profile view and (2) aerial view. The Halo is a triple-panel unit which has a total of six LED light sources and uses high resolution, machine vision cameras to capture images. To ensure consistency during each photography session, a high-back chair is fixed into position, 80cm away from the camera panels. This fixed camera-subject distance ensures that all images are free from distortion and enables the capturing of repeatable images

Fig. 3. A sample of custody images taken using the Halo. Custody images are captured from eight viewpoints. The high-resolution cameras and fixed, uniform light source ensure that the images are of high quality and free from shadowing. Shadowing has been avoided on the images captured from an elevated viewpoint (top). This significant advantage of the Halo is attributable to the use of six independent and balanced light sources

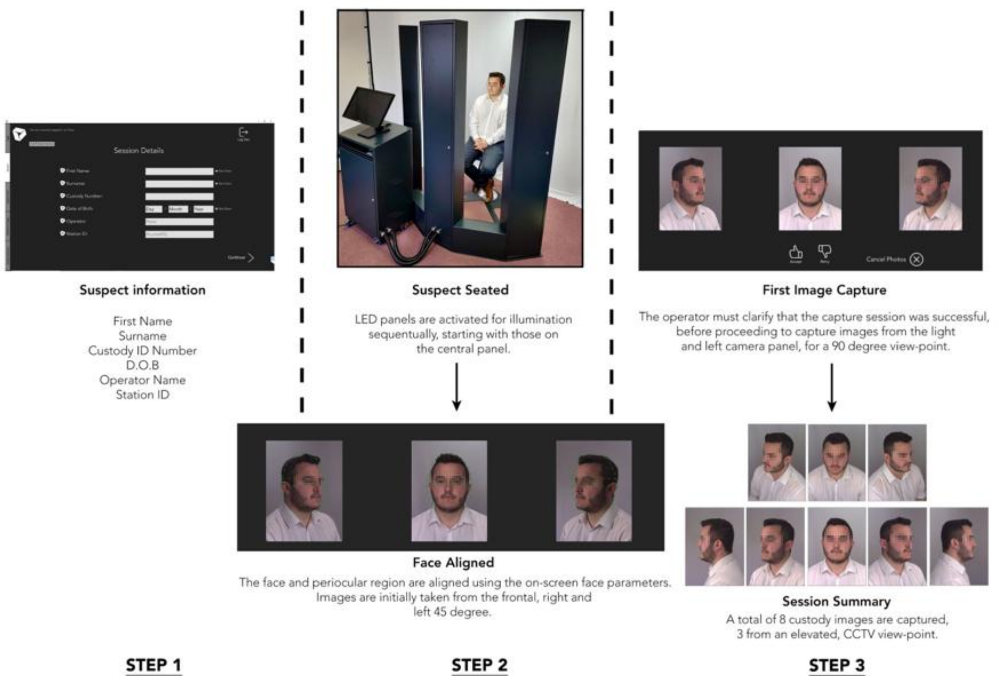

Fig. 4. The Halo custody image capture process. Firstly, the operator enters the suspect's identifying information. Next, the operator adjusts the vertical position of each camera to aligns the seated suspect's face within the pre-image capture guidelines. Three images (frontal, 45° left and 45° right viewpoints) are then captured. The subject is then rotated to face the right panel, and then left camera panels. This enables the capture of profile (90° right and left viewpoint) images. The three elevated (CCTV-simulated) face images are taken automatically during the capture session

To obtain a custody image, the subject initially faces the central panel. The Halo then utilizes three cameras (left, centre and right panel) to simultaneously capture an image of the suspect from each of the frontal, 45° left and 45° right viewpoints. To obtain profile (90°) images, the subject's chair is rotated to face the right and left panels respectively (Fig. 4).

Fig. 5. Pre-image capture guides (green outlines) are used to optimise face alignment within the centre of the frame

To enable the subject to be centred within the image frame, the vertical positioning of all cameras can be dynamically adjusted (range: 50cm). An additional, mobile DSLR camera is available to photograph soft biometric features (tattoos, scars, moles etc.). The camera has pre-set specifications for the focal length, light source and exposure ensuring consistency of image quality.

2.3 User Interface

Halo is controlled by a touch-screen user interface. In addition to recording identifying information (e.g. name, custody number), the interface assists the operator with the alignment of the suspect's face within the centre of the image frame (Fig. 5).

3. THE BIOMETRIC AUTHENTICATION MODULE AND RESULTS

As part of the Halo custody suite, we have also developed and tested a state of the art biometric face processing and authentication system. Our system is based on the most recent developments in face recognition and uses the deep learning based machine learning framework [16].

There many ways one can implement a computer based face recognition system. The techniques that can be utilised range from the use of simple Principal Component Analysis [17,18] to modern deep learning techniques. In this work, we have implemented a Convolutional Neural Network (CNN) based deep learning framework to develop a state of the face recognition and face matching system [19,20]. CNN models enable to extract high level knowledge from datasets and have the power to "learn" from training data which can then be applied in a diverse manner. In the context of face recognition, the idea here is to develop a CNN which can learn about human faces (such as complex facial features, facial colour, texture and so on).

There are various ways one can go about developing a CNN based face recognition architecture. One way is to develop a CNN model which requires a large dataset of faces to obtain the necessary baseline training of the network.

Alternatively, one can utilise a pre-trained model in which certain layers of the CNN can be adjusted according to the local dataset fed to the system.

Here, we have utilised a well-known pre-trained CNN model called the VGG-F. The VGG-F CNN architecture has been developed by Oxford Visual Geometry Group [20] and was trained

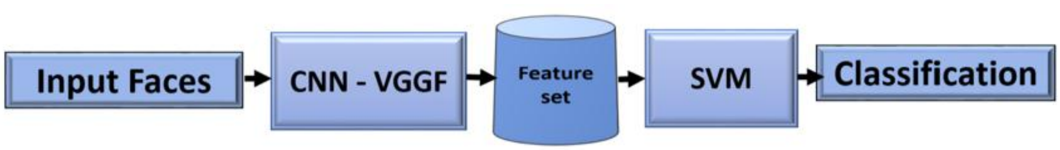

Fig. 6. A developed and tested deep learning based biometric face processing and authentication framework. The adopted deep learning method works in a supervised manner by training itself with the input faces (the halo images) and dissects aspects of the input face to learn the measureable characteristic of the data, to deduce a feature set. A support vector machine (SVM) classifier is then used to analyse and classify the data

using a dataset consisting of 2.6 million face images from 2,622 individuals. The architecture of VGGF comprises 38 layers which all can be adjusted according to the local dataset available. In Fig. 6, we show the basics of our CNN based face processing and authentication framework.

3.1 The VGG-Face Model and Feature Extraction

CNNs learn features through the training stage and use such features to classify images. Each convolutional layer learns different features, for example, one layer may learn about entities such as edges and colours of an image while others learn complex features as part of the deeper layers. A result from a given layer may involve numerous 2D arrays which are called channels. In VGGF, there are 37 layers, 13 of which are convolutions and the remaining layers are mixed between ReLU, pooling, fully connected and the last layer called the softmax.

To ascertain the best layer within the VGGF model for facial feature extractions, we carried out a number trial and error experiments. For our experiment, we tested layers 34 through to 37. To train the CNN we did not require extensive image pre-processing, hence we made use of the raw images captured by the Halo. Such criteria are one of the distinct advantages of using CNN based deep learning for face processing.

An important point to highlight when utilising a CNN framework is that it requires sufficient input facial data from an individual. Fig. 7, shows a typical set of faces we have used for learning. As can be seen, these are the raw faces which were captured using the Halo. Five halo images from the frontal, 90° right and left profile and 45° right and left profile, were augmented by cropping various sections from the face to generate a larger dataset. Thus, for a given individual we created an augmented dataset of about 200 pictures which are utilised by the VGG-F to train the various layers in the CNN.

3.2 Support Vector Machine Classifier and Recognition Rates

Once the CNN is trained with a given number of subjects in the dataset, given a probe image, classification will need to be carried out to comparing the probe image with the trained CNN. To do this we have utilised Support Vector Machines (SVM) [21]. SVMs are a supervised machine learning technique which can be used for both binary and multi classification problems.

An SVM focuses on identifying the "margin" via a hyperplane to separate the data into separate classes. Maximising the margin reduces the upper bound on the expected generalisation error by creating the largest possible distance between the separating hyperplanes. There are two types of SVMs linear and non-linear however in this work we made use of a linear SVM, to separate the data by fitting the images into the classifier [21].

Below, Fig. 7 shows a sample of images we used for training the CNN to learn about a face.

Fig. 7. (1) An example set of training images captured with the Halo. A total of 5 images were utilised and represent the following views per participant; frontal, 90° (left and right), and 45° (left and right). (2) Images were augmented (cropped to generate further images) to assist with the process of training. Augmented images were rotated 90°, 180°, 270° and sections of the face such as eyes, nose, and mouth were also isolated

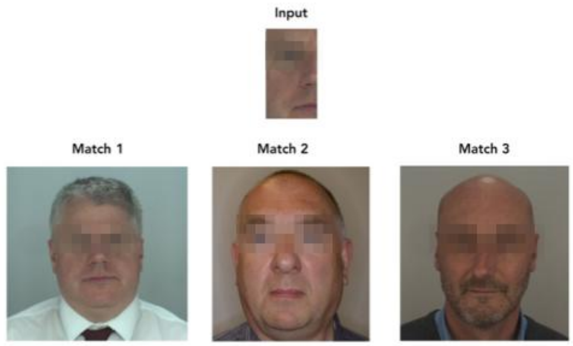

Fig. 8. Top: Input image (restricted view) result using the biometric authentication framework which shows a numbered match result that ranges from 1 (most likely) to 3 (least likely). The CNN has accurately also matched both sex and perceived race of the input image across all the 3 'matched' results. It should be noted that visual similarities in the shape of the eyebrow may have been one of the factors that the authentication framework took into consideration when concluding such matches. (Note: we did not make use of such demographic information during the training stage)

By using an authentication framework, we carried out several experiments on face recognition to test the suitability as well as the accuracy of our system. Because of the experiments, it was concluded that layer 34 provided the highest results and thus the best performance. With this layer, we have been able to obtain 100% face recognition rates, even when parts of the face such as the eyes, or a portion of a face image was used as an input.

Fig. 8 shows a typical face matching result from our framework. The input face is only a partial view, somewhat like a typical image of an individual retrieved from public CCTV cameras, especially if a CCTV camera is positioned obscurely or when only a fleeting glimpse is recorded of a suspect. Interestingly, even with an image of such limited visibility, we achieved 100% recognition.

The recognition results are presented in such a way that the output image corresponding to 'match 1' is most likely to be the face depicted in the image while 'match 3' is least likely. While our initial experiments always demonstrated 'match 1' as a correct recognition, the framework is produced to enable an operator to interpret the results and make the final decision.

Though we do attain a 100% matching results on the data of around 1000 individuals in our experimental dataset, our system does require rigorous tests and further verification tests before it can be fully deployed. To achieve this, we must work on real data on a large scale and therefore a suitable police trial is necessary to fully evaluate the power of our face processing and authentication framework.

4. DISCUSSION

This paper describes the development of a new custody image capture system and linked biometric identity authentication system for custody images. The design of the Halo system surpasses all relevant Home Office requirements. The novelty of the system lies in the application of machine vision cameras to the capturing of consistent and high quality images.

The Halo captures images from 8 planes of view, 3 of which are elevated to simulate CCTV viewing-angles. Currently, no other commercially-available custody image capture system provides high quality images from such a variety of viewpoints. Given that CCTV cameras predominately record from an angled and elevated viewpoint, it is perhaps surprising that no current system offers the opportunity to record custody images from these viewing angles. The CCTV-simulated images recorded by the Halo facilitate direct comparison between the representation of the defendant in custody and crime scene footage.

The use of machine vision cameras in combination with a custom lighting set-up enables the Halo to produce high quality images which are free from shadows on and around the face.

As part of the custody capture system, a biometric based deep learning technique has been implemented for facial recognition and is based on Convolutional Neural Networks (CNNS). The developed algorithm is very accurate and is capable of matching images of a limited view, without resorting to an exhaustive search. A partial facial image can present 3 matches ranging from the most likely ('1') to least likely ('3'). Based on the preliminary results the algorithm performs very well. The authentication system concludes an impressive recognition rate possibly due to its ability to learn from high quality input data (Halo custody images). While promising results are attained the current machine learning algorithm is still a prototype and is yet to undergo further experiments to fully evaluate both its capabilities and limitations.

The Halo's machine learning algorithm has the potential to assist Police with efficient intelligence sharing. For example, if a defendant is photographed with the Halo and then reoffends in another geographical location, the system will highlight the initial image stored within the database.

The use of facial images and biometric based technology is increasing. The advantages offered by operational deployment has been illustrated with the use of unconstrained images from the public domain in the case of Boston Marathon bombing suspect [22]. Non-invasive technology which can rapidly identify an individual from a single image offers considerable advantages over relying on human-based identification.

Face recognition systems, however, are not free from error. For example, Police forces such as South Wales, Leicestershire and the Metropolitan have reported a significant error rate with facial recognition software. During the 2017 Champions League final in Cardiff, South Wales Police reported that 2,297 people were wrongly identified as potential criminals. Similarly, an improved AFR 'locate' algorithm, used at the Anthony Joshua fight in October 2017, achieved 5 correct identity matches, but also made 46 false positive matches [23].

The force suggested that poor-quality images (the operator watch list database, and others that were supplied by UEFA) were one of the primary reasons for the sub-optimal performance of the face recognition system. In humans, it is well established that unfamiliar face matching is severely impaired by poor quality images [3, 24].

As a result, the quality of custody images impacts upon the effectiveness of crime detection and prevention. The quality of the images captured by the Halo system exceeds that of The National Viper Bureau Identification Booth and Promat's Digital Image Capture Booth (see Table 1). It should, however, be noted that both Viper and Promat are predominantly digital systems used to conduct identity parades. The failed match rates reported by South Wales Police demonstrate the detrimental impact poor quality images on the accuracy of face recognition systems. It is hoped that the improved image quality offered by the Halo will reduce the number of incorrect identifications made by both humans and machines.

There are limitations to the applied biometric framework within the Halo system. Firstly, while the match rates reported from the experiments are 100% for both full-view and partial-view single images, the images used for training the system were captured by the Halo. It may be that our algorithm utilized detail from the Halo images which would have been unavailable within images captured by other devices (e.g. a CCTV camera). Similarly, the images used to train the CNN were all full-colour images. It remains to be determined if similar results would be obtained with greyscale images (e.g. images recorded by CCTV systems at night using infra-red light). Future work will investigate the performance of the algorithm with 'real-world' images. Finally, the biometric framework was tested on only 1000 images, representing 200 different individuals. More extensive testing is required to determine the accuracy of the Halo's recognition system with a wider population.

A point for future consideration surrounding the confidentiality of the stored Halo images, is to have each image and video session be converted to a base64 string. The conversation would be carried out by breaking the file into an array of bytes and converting those to base64 and then saving the string into a specific field within the database. Then, when a specific file (suspects image file) is needed the string would be converted back to the original file (consisting of the full photography session and ID video) by retrieving the base64 string from the database and converting it back to an array of bytes and rebuilding the original file.

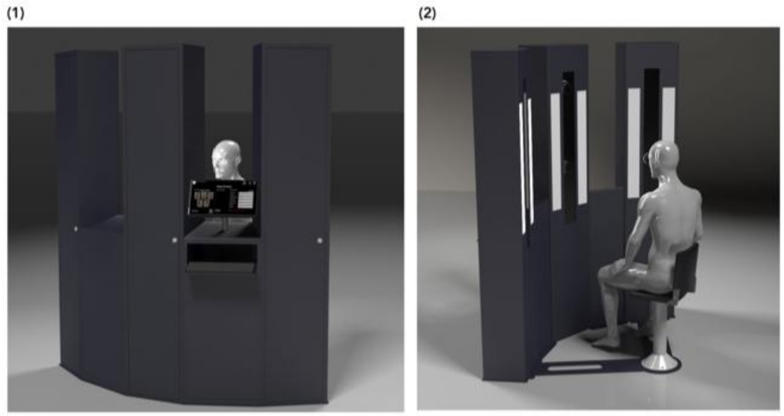

Fig. 9. The second-generation Halo custody system with (1) the integration of the terminal into the main body of the hardware. The screen is mounted onto an angled platform between two camera panels and a discrete keyboard and mouse compartment is located directly beneath. (2) A profile view of the Halo custody system with a test subject

The advantages of such a method is 2-fold; (1) local copies of files would not need to be stored on site subsequently reducing the amount of storage needed on-site, and (2) this method is far more secure that even if a file was moved or deleted locally it could still be retrievable.

A future development that has been addressed during this research has been the integration of the stand-alone terminal with the main body of the Halo system. The integration has drastically reduced the footprint of the hardware and has further simplified user interaction, see Fig. 9.

A custody capture system based solely on the photography of 2D images from a 1-3 viewpoints within a horizontal plane may not be able to meet the practical requirements of a 21st century custody suite. The Halo offers the facility to capture high quality images from a wide range of viewpoints, including elevated CCTV-simulated. Additionally, the images captured by the Halo benefit from the custom lighting arrangements, and an authentication framework based on a CNN machine learning algorithm.

The main contribution of this work is the development of the Halo, a new custody image capture system which aims to both standardise and optimize the process of custody image capture.

5. CONCLUSION

We have described an innovative biometric custody system which utilizes machine vision cameras to capture high resolution images. The Halo system is the only system to capture custody images from 8 view-points, including 3 elevated CCTV-simulated views. Preliminary experiments into the use of a machine learning algorithm found evidence of accurate biometric authentication. Further testing is, however, required before the system can be deployed operationally. Nevertheless, our results represent the first step towards the integration of a biometric authentication framework with a custody image capture system.

CONSENT

All authors declare that ‘written informed consent was obtained from the participants (for the publication of their face images.

ACKNOWLEDGEMENTS

This research was partially supported by a project which has received funding from the Innovate UK under the grant no. KTP010130.

Halo is a privately funded piece of equipment by Acumé Forensic, UK. The data testing and software development have been a collaborative effort with researchers at the University of Bradford, UK, namely Ali Maina Bukar and Ali ELmahmudi. Sincere thanks are extended to Rowan Knight, Peter Lowery and Michael Dixon at Acumé Forensic.

All opinions expressed are those of the authors and, unless explicitly stated otherwise, do not necessarily reflect the opinions or policies of any other individuals or organisations.

COMPETING INTERESTS

The authors have declared that no competing interests exist. The companies "ViperTM" and "PromatTM" used for this research are commonly selected in this area of research.

There is no conflict of interest between the authors and the companies mentioned because they do not intend to use any company as an avenue for any litigation, but the advancement of knowledge only. Also, the research was funded by the personal efforts of the authors.

REFERENCES

1. Police and Criminal Evidence Act 1984 (PACE) codes of practice [Internet]. GOV.UK; 2013. Available:https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice [cited 12 July 2018].
2. Office H. (Revised) Code of Practice for the identification of persons by Police Officers, [Internet]. Gov.uk. 2013 Available:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/592562/pace-code-d-2017.pdf [cited 12 July 2018].
3. Bruce V, Henderson Z, Newman C, Burton AM. Matching identities of familiar and unfamiliar faces caught on CCTV images. Journal of Experimental Psychology: Applied. 2001;7(3):207.
4. Office H. Review of the use and retention of custody images; 2017. Assets.publishing.service.gov.uk. 2018 Available:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf [cited 16 July 2018]
5. Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark & Tattoo Images; 2007. Whatdotheyknow.com. Available:https://www.whatdotheyknow.com/request/383407/response/939050/attach/6/017%2016%20NPCC%20Response%20attachment%2003%20of%2005.pdf [cited 16 July 2018]
6. Police drone unit is first in UK [Internet]. BBC News; 2017. Available:http://www.bbc.co.uk/news/uk-england-devon-40595540 [cited 17 July 2018]
7. Reeder M. Could this work in Yorkshire? Police launch drone unit to tackle crime in Devon, Cornwall and Dorset [Internet]; 2018. Yorkshirepost.co.uk. Available:https://www.yorkshirepost.co.uk/news/could-this-work-in-yorkshire-police-launch-drone-unit-to-tackle-crime-in-devon-cornwall-and-dorset-1-8447303 [cited 17 July 2018]
8. Police D. Use of drones [Internet]. Devon and Cornwall Police; 2015. Available:https://www.devon-cornwall.police.uk/news/behind-the-blue-line/technology-pilots/we-are-using-drones/ [cited 17 July 2018].
9. Police to use AI to identify child abuse images [Internet]. The Week UK; 2017. Available:http://www.theweek.co.uk/artificial-intelligence/90509/police-to-use-ai-to-identify-child-abuse-images [cited 17 July 2018].
10. VIPER - Video Identification Parade Electronic Recording [Internet]. Viper.police.uk. Available: http://www.viper.police.uk [cited 22 July 2018]
11. Software E. Promat Video Identification Parade Software [Internet]; 2017. Promatenvision.co.uk Available:http://www.promatenvision.co.uk [cited 22 July 2018].
12. The National VIPER Bureau [Internet]. The National VIPER® Bureau Identification Booth; 2017. Available:http://cjm-conference.co.uk/wp-content/uploads/2017/07/VIPER-Flyers.pdf [cited 22 July 2018].
13. Johnston A, Hill H, Carman N. Recognising faces: Effects of lighting direction, inversion, and brightness reversal. Perception. 2013;42(11):1227-37.
14. [Internet]. IDS. Available:http://en.ids-imaging.com/store/ui-35901e.html [cited 22 July 2018]
15. Lens, Tamron, M23FM08, 8 mm, 2/3" - Lenses - Accessories - Products [Internet]. En.ids-imaging.com Available:https://en.ids-imaging.com/store/products/accessory/lenses/lens-tamron-m23fm08-8-mm-2-3.html [cited 22 July 2018].
16. LeCun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015;521(7553):436.
17. Kim KI, Jung K, Kim HJ. Face recognition using kernel principal component analysis.

IEEE signal processing letters. 2002; 9(2):40-2.
18. Turk MA, Pentland AP. Face recognition using eigenfaces. In Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on 1991 Jun 3 (pp. 586-591). IEEE.
19. Bukar AM, Ugail H. Automatic age estimation from facial profile view. IET Computer Vision. 2017;11(8):650-5.
20. Parkhi OM, Vedaldi A, Zisserman A. Deep face recognition. In BMVC. 2015;1(3):6.
21. Cristianini N, Scholkopf B. Support vector machines and kernel methods: The new generation of learning machines. Ai Magazine. 2002;23(3):31.
22. Klontz JC, Jain AK. A case study on unconstrained facial recognition using the Boston marathon bombings suspects. Michigan State University, Tech. Rep. 2013;119(120):1.
23. Facial Recognition Technology - South Wales Police [Internet]. South Wales Police; 2018.
Available:https://www.south-wales.police.uk/en/advice/facial-recognition-technology/
[cited 10 August 2018].
24. Lee WJ, Wilkinson C, Memon A, Houston K. Matching unfamiliar faces from poor quality closed-circuit television (CCTV) footage. Axis: The Online Journal of CAHId. 2009;1(1):19-28.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sciencedomain.org/review-history/27329