影(錄)像鑑定技術趨勢之探討

楊文超／中央警察大學鑑識科學學系副教授

一、序論

隨著資訊技術與數位科技的快速發展，許多犯罪過程都被政府或民間所設置的監視系統所錄影，或者被目擊者以數位相機、手機或車輛行車記錄器等攝錄影裝置所紀錄，犯罪案件相關的數位影（錄）像，已成為刑事偵查與司法審判常利用的偵查分析與證據資料，例如轟動一時的一銀ATM盜領案及美國波士頓馬拉松爆炸案，即為典型的應用案例。

再則，數位攝（錄）影設備（如手機或數位相機）已成為人人必備的設備，其易取得及易用的特性，衍生許多不

當使用的案件，如洩漏秘密（違反國家安全法）、妨害秘密（偷拍談話或身體隱私部位）及網路毀謗或霸凌（散佈不實之影像）案件頻傳，且有上升趨勢，另外，近來人工智慧技術的快速發展，使數位影（錄）像資料的編修技術突飛猛進，造成數位影（錄）像資料的編修變的容易且編修處不亦察覺。法務部亦針對侵害性影像及深度偽造技術（Deepfake）等類犯罪行為，進行刑法第 28 章之 1「妨害性隱私及不實性影像罪章」增修。

因應上述科技進步與社會變遷所帶來的問題，影（錄）像鑑定的新興需求便相映而生，從過往的影像強化及車牌號碼辨識，逐漸發展出影像（含人臉）比對（Photographic comparison）、影像量測（Photogrammetry）、影（錄）像內容分析（Content analysis）及影（錄）像驗證（Image/Video authentication）等鑑定類別項目[1,2]。

本文非介紹基礎的影像處理技術，乃著重於探討影（錄）像鑑定技術、類別以及於犯罪案件上的相關應用，並介紹影（錄）像鑑定新興需求與未來挑戰。

二、影（錄）像鑑定技術探討

如前所述，由於科技進步及相關設備普及影響，影（錄）像鑑定需求日益增加，以下分別介紹國內外常見的影（錄）像鑑定類型與新的應用技術。

● 影像量測（Photogrammetry）

影像量測類型的影像鑑定，即利用透視投影法等技術，於二維的影像資料中進行視角內實體物或環境空間的三維維度資訊推估，此類方式常用來分析犯罪現場實體物長度或高度資訊，或是環境空間的距離等，例如：ATM盜領者或銀行搶犯的身高。近年來，有些車禍案件亦藉此類鑑定協助進行車輛速度分析，釐清肇事責任。根據美國國家標準暨技術研究院（The National Institute of Standards and Technology, NIST）下之法醫學科學領域委員會（The Organization of Scientific Area Committees for Forensic Science, OSAC）所提出鑑識影像分析指引[1]，定義影像量測為對電磁紀錄或其他方式產生的照片與特徵資訊，進行記錄、測量和闡釋等程序，獲取有關的實體物和環境所含可靠信息的一門藝術、科學和技術。

刑事攝影亦常應用此類技術，例如透視窗格量測（Perspective grid photogrammetry）、透視碟量測（Perspective disk photogrammetry）、自然窗格量測（Natural grid photogrammetry）以及反向投影量測（Reverse projection photogrammetry）等[3]，推估拍攝視角內的三維維度資訊之問題，國內偵查與鑑識實務工作中亦常使用反向投影量測技術推估犯罪嫌疑犯身高，圖1即為反向投影量測之示意圖，紅色方框左

圖1、反向投影量測比對示意圖

半為犯罪現場犯罪者於監視錄影所記錄之影像，紅色方框右半為犯罪嫌疑人配合至犯罪現場，於相同地點同一監視器鏡頭所紀錄之影像，透過反向投影技術，獲知犯罪嫌疑人自腳底到肩膀之高度及自腳底到頭頂之高度與犯罪者極為接近。

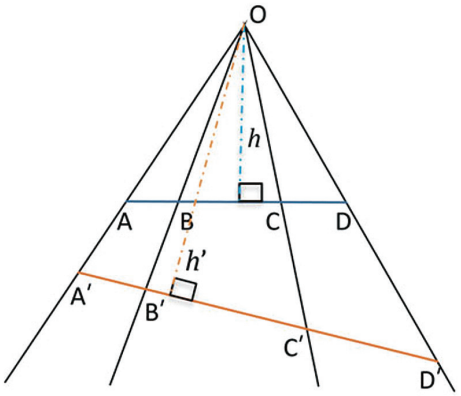

圖1、反向投影量測比對示意圖

近年來，由於車用攝影機設備（俗稱行車紀錄器）普及，應用所紀錄之影錄像資訊進行交通事故重建與肇責釐清，亦時有所聞，我們引入交叉比值（Cross ratio，以下簡稱交比）用於行車記錄影像量測估算，並進行實驗驗證[4]，交叉比值介紹如下： 圖2為交比示意圖，A, B, C, D四點共線，A’, B’, C’, D’四點共線，O, A, A’ 三點共線，O, B, B’ 三點共線，O, C, C’ 三點共線，O, D, D’ 三點共線，h及h’分別為O點到 $\overline{AD}$ 及 $\overline{A'D'}$ 的距離，則交比 $\frac{\overline{AC}/\overline{AD}}{\overline{BC}/\overline{BD}}$ （以 $A,B;C,D$ 表示）等於交比 $\frac{\overline{A'C'}/\overline{A'D'}}{\overline{B'C'}/\overline{B'D'}}$ （以 $A',B';C',D'$ 表示），其證明如（１）所示。

$$
\begin{aligned}
(A,B;C,D)&=\frac{\overline{AC}/\overline{AD}}{\overline{BC}/\overline{BD}}=\frac{\left(\overline{AC}\times h/2\right)/\left(\overline{AD}\times h/2\right)}{\left(\overline{BC}\times h/2\right)/\left(\overline{BD}\times h/2\right)}=\frac{\triangle OAC/\triangle OAD}{\triangle OBC/\triangle OBD}\\
&=\frac{\overline{OA}\,\overline{OC}\sin(\angle AOC)/\overline{OA}\,\overline{OD}\sin(\angle AOD)}{\overline{OB}\,\overline{OC}\sin(\angle BOC)/\overline{OB}\,\overline{OD}\sin(\angle BOD)}\\
&=\frac{\sin(\angle AOC)/\sin(\angle AOD)}{\sin(\angle BOC)/\sin(\angle BOD)}\\
&=\frac{\sin(\angle A'OC')/\sin(\angle A'OD')}{\sin(\angle B'OC')/\sin(\angle B'OD')}\\
&=\frac{\overline{OA'}\,\overline{OC'}\sin(\angle A'OC')/\overline{OA'}\,\overline{OD'}\sin(\angle A'OD')}{\overline{OB'}\,\overline{OC'}\sin(\angle B'OC')/\overline{OB'}\,\overline{OD'}\sin(\angle B'OD')}\\
&=\frac{\triangle OA'C'/\triangle OA'D'}{\triangle OB'C'/\triangle OB'D'}=\frac{\left(\overline{A'C'}\times h'/2\right)/\left(\overline{A'D'}\times h'/2\right)}{\left(\overline{B'C'}\times h'/2\right)/\left(\overline{B'D'}\times h'/2\right)}\\
&=\frac{\overline{A'C'}/\overline{A'D'}}{\overline{B'C'}/\overline{B'D'}}=\left(A',B';C',D'\right)
\end{aligned}
\qquad (1)
$$

其中$\triangle XYZ$表示由X,Y,Z三點所構成的三角形面積。

交叉比值分析應用估算車速之示意圖如圖3，行進車輛（前後輪距為l）於兩時間點（T1與T2）的位移量（d）， B, D與A, C四點分別代表T1時間與T2時間之前後輪胎中心點，如間格時間

極短，A, B, C, D四點必為共線，A’, B’, C’, D’ 四點則為錄影機所紀錄影像中的A, B, C, D對應四點，則交比 $A^{'},B^{'};C^{'},D^{'}$ 即可透過畫素計算得知。

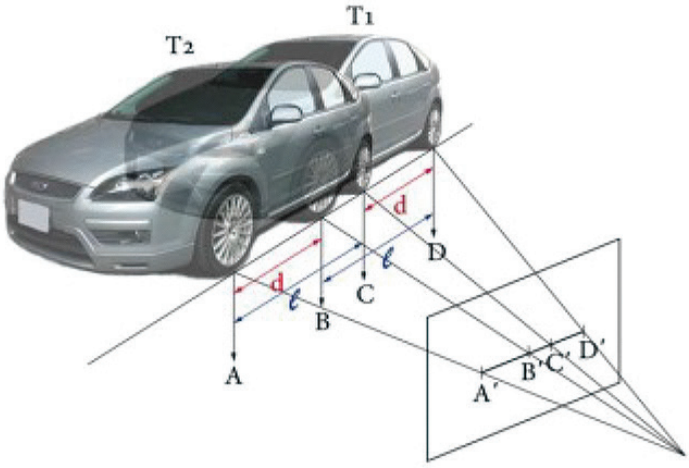

圖3、車速估算示意圖(4)

由於已知交比 $A^{'},B^{'};C^{'},D^{'}$ 數值及前後輪距（l）透過（2）即可獲得行進距離d。

$$\begin{aligned}\left(A^{'},B^{'};C^{'},D^{'}\right)&=\left(A,B;C,D\right)\\&=\frac{\overline{AC}/\overline{AD}}{\overline{BC}/\overline{BD}}\\&=\frac{l/(l+\mathrm{d})}{(l-\mathrm{d})/l}\\&=\frac{l^2}{l^2-\mathrm{d}^2}\end{aligned}\qquad(2)$$

以不同拍攝角度及不同速度條件下，進行方法驗證，計算示意圖如圖4，推估行進車速平均值與實際車速（GPS車速）差異如表1，觀察表1中GPS車速及估算車速的平均值，可發現即使在不同拍攝角度及不同速度條件下，兩者的差異均小於0.5km/h，故得知，此推估方法極接近真實車速，確實適用於交通事故重建與肇責釐清。

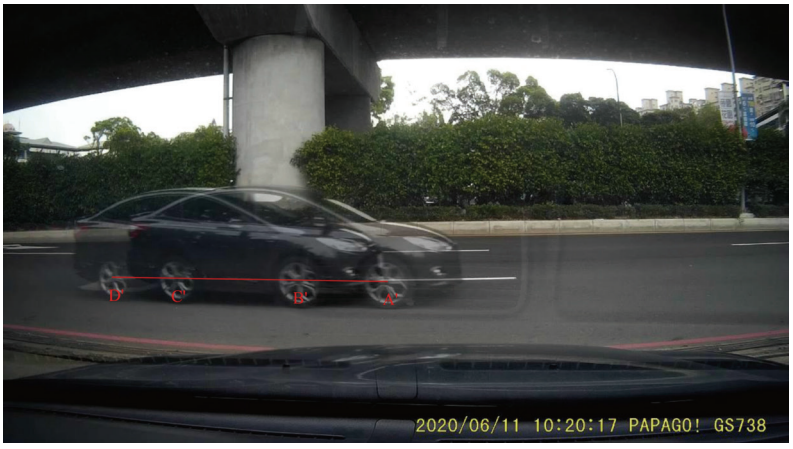

圖4、運用交叉比值分析估算車速之示意圖示意圖(4)

表1、實驗車輛於不同拍攝角度及不同速度下之估算車速[4]

GPS車速（計算次數）	44km/h（19次）			54 km/h（16次）			64 km/h（13次）		
拍攝角度	0度	45度	90度	0度	45度	90度	0度	45度	90度
平均值	43.78	43.89	44.05	54.15	53.98	53.91	64.00	64.00	63.56
標準差	0.790	0.789	0.897	0.892	0.618	0.777	0.805	0.561	0.659
變異係數	0.018	0.018	0.020	0.016	0.011	0.014	0.013	0.009	0.010

● 影像比對（Photographic comparison）

影像比對鑑定之目的為確認或排除影像資料中的實體物或人物，是否為特定實體物或人物，依據OSAC鑑識影像分析指引[1]，定義影像比對為利用圖像特徵對應關係，比較所記錄的實體物或人的過程，並提出識別或排除之意見，如圖5及圖6分別為衣物影像比對與人貌比對的範例。

圖5、衣物影像比對[1]

圖6、人貌影像比對[1]

過往對於人貌影像比對方法，存有錯誤迷思，認為只要特徵相符即可確認為同一人，或者反之，認為只要特徵不相符即可排除，非同一人，殊不知由於對於選用之特徵未進行穩定或可靠性評估，其比對過程與結果存有極大風險，易造成錯誤鑑定。OSAC歸納相關研究，進行人貌特徵分類，分為頭顱、臉、眉、眼、鼻及嘴等類型（示意圖如圖7），並探討前述各類特徵於表情變化、長時間、短時間、體重減輕、疾病及化妝等6個因子下之影響，訂出各類型人貌特徵於6個因子下之穩定與可靠度[5]，並經美國材料和試驗協會（American Society for Testing and Materials International, ASTM）訂定為人貌特徵比對標準E3149-18[6]。

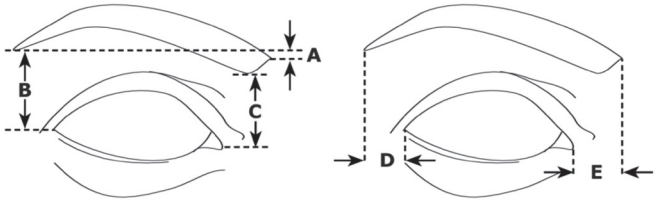

圖7、眉與眼之關係特徵示意圖[5]

此外，在人貌影像比對方法上尚存有另一個高風險的迷失，即未注意青少年人貌的不穩定性，僅以一般性的人貌比對規範及方法，進行成年與青少年的人貌比對。圖8為成年與青少年的人貌比對示意圖，根據Caplova等人的研究結果[8]，僅有利用臉部瑕疵，例如唇顎裂、下巴凹陷等，或者系爭影像臉上具較多的痣，才能將比對錯誤率降低到小於20%。

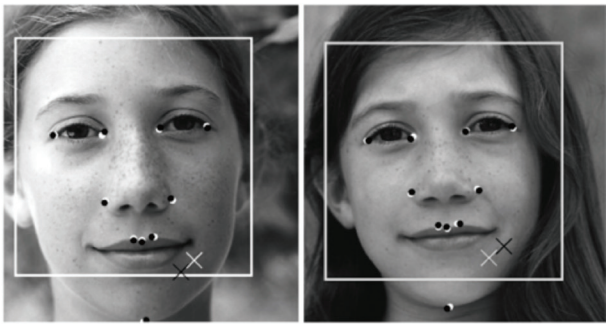

圖8、成年與青少年人貌比對示意圖[7]

● 影（錄）像內容分析（Content analysis）

影（錄）像內容分析鑑定，目的在於透過圖像分析，提取影（錄）像資料內所具有資訊，例如拍攝地點、拍攝時間、拍攝角度、車牌號碼分析、車型分析及圖像廠牌分析等，依據OSAC鑑識影像分析指引[1]，定義內容分析鑑定為應用鑑識影像分析技術，提取影像內容資訊。此類運用技術極為廣泛，分析資訊內容視案件需要而定，但基礎影（錄）像處理技術仍為其不可避免之前處理項目。

以往進行拍攝地點或被攝物之分析十分困難，除非事先建立各景點或物件資料庫影像或者是透過對於拍攝地點或被攝物熟悉者協助，方可進行影像資料庫搜尋，獲得拍攝地點或被攝物資訊。近年來，由於網路與多媒體科技發展迅速，建議可使用Google Lens[8]工具，利用圖像特徵快速搜尋其拍攝地點或被攝物資訊，再進行驗證鑑定。

● 影（錄）像驗證（Image/Video authentication）

影（錄）像驗證鑑定目的在於經由分析影（錄）像資料的描述資料（Metadata，或稱元資料）、檔案格式、紀錄內容及雜訊資料等，確認影（錄）像資料內容資訊及真實性，例如確認影（錄）像資料是否經偽造、變造、二次壓縮、其拍攝地點、拍攝條件及拍攝設備等，依據OSAC鑑識影像分析指引[1]，定義影（錄）像驗證為驗證影（錄）像資料內容及是否如其所紀錄。

影（錄）像驗證之分析資料，依屬性可分成兩大類：描述資料（元資料）以及內容資料。描述資料（元資料）即檔案容器資訊及檔案格式資訊，Cohen於2007年[9]討論影像描述資料格式標準有ITU-T T.81、JETF、EXIF、CIFF及DCF等，使用上最為廣泛的者為EXIF標準。目前市售數位相機或手機在產生JPEG或TIFF影像時，多依循此類標準，所產生的影像多可利用描述資料中的紀錄，進行影（錄）像驗證，例如：拍攝條件描述資料（圖9）或GPS描述資料（圖10）。近年來，我國史上最高詐貸案–潤寅實業詐貸案件，即藉著手機照片中的GPS描述資料，獲取事證確認詐貸事實以及獲取資金藏匿的地點，惟應用此類資料進行影像驗證亦有其風險之處，因數位資料的易修改性，影像的描述資料紀錄易遭去除或修改，使用時須小心確認描述資料正確性與完整性。另外，影像檔案格式中的量化表以及錄像檔案格式中的影像群組（Group of picture）亦為確認偽變造以及二次壓縮的重要資訊。

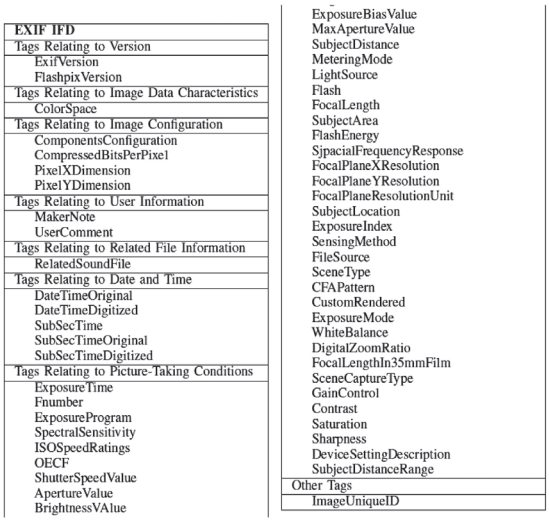

圖9、EXIF描述資料拍攝條件記錄[9]

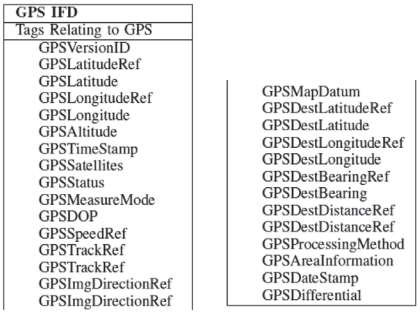

圖10、EXIF描述資料中GPS記錄[9]

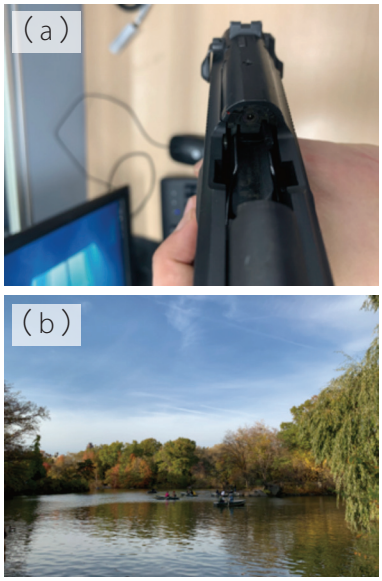

圖11、取像設備溯源技術應用示意圖

內容資料分析，即利用取像設備所紀錄的資訊，進行拍攝環境或條件的分析，或於產生紀錄過程中，因軟硬體處理所留存的雜訊資料，亦可用以進行拍攝設備溯源或驗證其影像完整性。2009年英國蘇格蘭（Scotland）的一件兒童性侵案[10]為拍攝設備溯源技術最早應用於鑑識科學上的案例，當時娃娃車司機將兒童猥褻的影（錄）像上傳色情網站而遭逮捕，再藉由拍攝設備溯源技術鑑定該兒童猥褻的影（錄）像為該司機所擁有之相機所拍攝，使其認罪。圖11為取像設備溯源技術另一個應用示意圖，假設圖11（a）為購物社群中歹徒散播的槍枝檢視影片，圖11（b）為採證嫌疑犯手機內之影片，可透過取像設備溯源技術進行鑑定確認同一手機所拍攝。

近年來由於數位與雲端科技的進步，每個人皆可方便的進行隨時錄影並透過電子郵件或社交網路分享所拍攝的錄影資料，但當這些科技遭到誤用，也使得洩漏秘密（違反國家安全法）及妨害秘密（偷拍談話或身體隱私部位）等案件容易進行，並造成了執法人員偵辦的困擾，拍攝設備溯源技術鑑定需求因此大增。並因拍攝設備品質的提升，案件相關的靜態照片量大且皆為千萬畫素以上，錄影檔案亦量大且檔案為10MB至幾GB不等，造成以往拍攝設備溯源技術的分析速度，遭受極大挑戰，我們提出基於光響不均勻性（Photo response non-uniformity，PRNU）❶偵測技術的取像設備溯源方法[11]，相較過往技術，我們多考量了拍攝光軸的角度，並利用視頻中I幀（Intra-frame）的重要性，提高處理速度和正確性。經實驗證明，所提出的方法與現有鑑識科學的拍攝設備溯源方法相比，平均速度至少快24倍（表2），並且具有更低的偽陽性錯誤（表3）。

表2、分析速度比較[11]

	Chen 等人[12]	Yang 等人[11]
處理每幀所需秒數	1.5406	1.7789
每個錄像檔案平均幀數	2048.77	72.54
每個錄像檔案處理秒數	**3156.33**	**129.04**

表3、錯誤率比較[11]

錯誤率	Chen 等人[12]	Yang 等人[11]
偽陽性（%）	0.0070	0
偽陰性（%）	0.0093	0.0140

❶光響不均勻性，指的是光感原件（CCD或CMOS）於製造時，因製程技術所限，造成每個光感單元，無法完全等距或均質，即使以均勻的光進行照射，仍會有不同的電壓產出。

三、未來趨勢探討

深度偽造（Deepfake）一字起源於深度學習（Deep learning）及偽造（Fake）。其技術乃是將目標者的臉影像或聲音特徵，疊合至影（錄）像原始者臉部影像或聲音特徵上，產生所謂的深度偽造影像（Deepfake images）、錄像（Deepfake videos）或音檔（Deepfake audio）。此技術為深度學習技術（Deep learning）的一項應用，可用於協助有聲帶損傷狀況的演員配音或在不重新拍攝的情況下，置換電影片段中的演出者[13]。近年來由於深度學習技術的快速發展，深度偽造技術應用自動編碼（Auto-encoder）或生成對抗網路（Generative adversarial network，GAN）模式，已能產生相當真實的影像或錄像[14-17]，並因其偵測方法的技術落差，深度偽造影像或錄像已可欺騙人類眼睛及複雜的電腦演算法[18]。亦同水可載舟亦可覆舟，深度偽造技術的惡意使用，將造成國家安全及社會秩序的嚴重危害，例如：有駭客利用深度偽造技術，偽造公司董事長的語音，成功詐騙該公司執行長轉帳22萬歐元[19]或台灣發生「小玉、笑笑集團換臉謎片」案件，造成與論譁然以及部分刑法修訂，深度偽造已成為現行影（錄）像鑑識無法忽視的重要部分。

由於深度偽造技術的誤用，可能影響選舉或觸犯刑事案件，目前世界各國十分重視，並進行深偽影（錄）像鑑定技術研究與規範研擬中，如有相關案件，建議可以上述影（錄）像驗證鑑定技術與規範進行，並結合人臉影像內容分析技術，例如：確認瞳孔角度一致性及臉部對稱性等方式，併同進行鑑定。

參考文章

1.SWGDE, Guidelines for Forensic Image Analysis, 2017.

2.SWGDE, Best Practices for Digital Forensic Video Analysis, 2018.

3.E. M. Robinson, Crime Scene Photography, 3rd Edition, Academic Press, 2016, pp. 411-453.

4.蘇愷安，以數位影像評估行車速度方法之探討，中央警察大學碩士論文，民國110年。

5.FIWSG, Facial Image Comparison Feature List for Morphological Analysis, Ver. 2.0, 2018.

6ASTM, Standard Guide for Facial Image Comparison Feature List for Morphological Analysis, ASTM E3149-18, 2018.

7.Z. Caplova, V. Compassi, S. Giancola, D. M Gibelli, Z. Obertová, P. Poppa, R. Sala, C. Sforza, C. Cattaneo, “Recognition of children on age-different images: Facial morphology and age-stable features,” Science Justice, vol. 57, no. 4, pp. 250-256, 2017 Jul.

8.T. Townsend, Google Lens is Google’ s future, Vox Media. https://www.vox.com/2017/5/19/15666704/google-lens-key-example-ai-first-computer-vision [Accessed May 11, 2022].

9.K. Cohen, "Digital still camera forensics," Small scale digital device forensics Journal, vol. 1, no. 1, 2007, pp. 1-8.

10.Spy Blog - Watching Them, Watching Us, Operation Algebra child rape convictions in Scotland: open WiFi tracking, digital camera image forensics. https://spyblog.org.uk/ssl/spyblog/2009/05/09/operation-algebra-child-rape-convictions-in-scotland-open-wifi-tracking-digi.html [Accessed May 11, 2022].

11.W. Yang, J. Jiang, C. Chen, "A Fast Source Camera Identification and Verification Method Based on PRNU Analysis for Use in Video Forensic Investigations," Multimedia Tools Application, vol. 80, no. 5, pp. 6617–6638, 2021.

12.M. Chen, J. Fridrich, M. Goljan, J. Lukás, "Determining image origin and integrity using sensor noise," IEEE Transaction on Information Forensics and Security, vol. 3, no. 1, pp. 74-90, 2007.

13.B. Marr, "The Best （And Scariest） Examples Of AI-Enabled Deepfakes," Retrieved from https://www.forbes.com/sites/bernardmarr/2019/07/22/the-best-and-scariest-examples-of-ai-enabled-deepfakes/#94b7c652eaf1, [Accessed May 11, 2022].

14.Y. Guo, L. Jiao, S. Wang, S. Wang, F. Liu, "Fuzzy Sparse Autoencoder Framework for Single Image Per Person Face Recognition," IEEE Transaction on Cybernetics, vol. 48, no. 8, pp. 2402-2415, 2017.

15.A. Tewari, M. Zollhoefer, F. Bernard, P. Garrido, H. Kim, P. Perez, C. Theobalt, "High-Fidelity Monocular Face Reconstruction based on an Unsupervised Model-based Face Autoencoder," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 2, pp. 357-370, 2020.

16.W. Yang, C. Hui, Z. Chen, J. Xue, Q. Liao, "FV-GAN: Finger Vein Representation Using Generative Adversarial Networks," IEEE Transaction on Information Forensics and Security, vol. 14, no. 9, pp. 2512-2524, 2019.

17.J. Cao, Y. Hu, B. Yu, R. He, Z. Sun, "3D Aided Duet GANs for Multi-view Face Image Synthesis," IEEE Transaction on Information Forensics and Security, vol. 14, no. 8, pp. 2028-2042, 2019.

18.T. T. Nguyen, C. M. Nguyen, D. T. Nguyen, D. T. Nguyen, S. Nahavandi, "Deep Learning for Deepfakes Creation and Detection," submitted, 2019, arXiv: 1909.11573.

19.J. Damiani, "A Voice Deepfake Was Used To Scam a CEO Out of $243,000." Retrieved from https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#47f7b0712241, [Accessed May 11, 2022].