https://doi.org/10.2352/issn.2169-2629.2020.28.27

Fake Video Detection Using Facial Color

Hadas Shahar and Hagit Hel-Or ; Dept of Computer Science, University of Haifa, Haifa, Israel

Abstract

The field of image forgery is widely studied, and with the recent introduction of deep networks based image synthesis, detection of fake image sequences has increased the challenge. Specifically, detecting spoofing attacks is of grave importance. In this study we exploit the minute changes in facial color of human faces in videos to determine real from fake videos. Even when idle, human skin color changes with sub-dermal blood flow, these changes are enhanced under stress and emotion. We show that extracting facial color along a video sequence can serve as a feature for training deep neural networks to successfully determine fake vs real face sequences.

Introduction

In recent years, with the increase of image and video data, along with the rising popularity of deep neural networks, image and video synthesization has become easier than ever before. Training deep neural networks on hundreds of thousands of videos has become possible, providing a basis for generating better and more realistic synthetic images and videos.

One of the most popular domains for image synthesis is human face generation. 2D face image generation using various deep networks have reached amazing quality ([8, 29, 26]) that fool even the human eyes [47].

More recently, several approaches to synthesis of videos with human subjects has been introduced colloquially termed *Deepfakes*, in which the original face in a video is replaced by a different individual. One approach involves swapping the original face in every frame with a new face. Earlier studies used computer graphics based approaches but recently deep learning techniques have been introduced with very impressive results [1, 2]. Another approach to face video generation involves re-enacting in which a given face is warped to conform with the pose and expression of the source video frames [17, 55, 7, 65].

On the other hand, the advance of biometric technology has promoted the use of biometrically controlled secure access. Along which developed a keen interest in spoofing attacks, using masks, fake images, fake videos and other fake data to forge entry into biometric systems.

Both synthetic generation of fake videos and the attempts at spoofing biometric systems has raised concerns about the reliability of face images and videos and the difficulty in distinguishing real from fake ([27]). Various methods have been proposed to determine real from fake videos as well as detect spoofing attacks, though typically in separate contexts. We consider that both problems deal with determining that the video at hand is a true rendering of a human subject with all the physical and physiological characteristics of a live person. Thus, we propose to utilize an aspect of the human face which is much harder to mimic: changes in facial skin color. In this paper, we attempt to test the viability of using changes in facial color as an indicator for both fake videos and for spoofing attacks.

This research was supported by grant no 1455/16 from the Israeli Science Foundation.

Previous work

The study of fake or forged images has long been a major player in the area of image forensics extending to various visual media (see surveys on 2D images [20, 42, 15], videos [5, 50], depth images [44] and more). Although classically, forgery detection focused on finding evidence of tampering following the image's acquisition by the camera, current technology eliminates the camera from the forensic loop and forgery detection now attempts to distinguish complete synthetic images from those acquired by a camera sensor. A more appropriate definition of forgery detection would now be to determine whether an image faithfully renders a true existing scene in the world.

Numerous approaches have been proposed to detect fake 2D images of faces ranging from image processing to computer vision techniques and machine learning as well as deep network based approaches [40, 35, 32, 54, 38]. See [37, 59, 25, 53] for reviews. Several approaches have also been suggested for detecting image based spoofing attacks [16].

Recent studies have attempted to tackle the rising success of deepfake generated videos. Most approaches rely on finding a discrepancy between known physical attributes, such as shading, angles or color, and those found in the video. Another approach to detection of fake videos, is to find traces of the generation operation, a type of fingerprint.

In [33], the authors attempted to identify the fake videos by detecting the face warping artifacts. As face-swapping generation has to map one face to another, there are some visible artifacts in the bounding box- those artifacts are a result of a resolution mismatch, blurring, or an angle misalignment between the source and the target. In [64], the authors proposed to use the head pose as a telling physical attribute. Since in deepfake face swapping is usually performed, sometimes the position of the target and the source are not the same. Using the facial landmarks the authors attempted to calculate the vector perpendicular to the plane of the face, describing the head position, and using it as a feature for an SVM classifier.

Recently, neural networks have been used to detect real from fake videos. CNN was used in [45] to determine synthetic from natural images and in [63] to detect manipulated images, specifically images which were generated using image warping. In [4], a shallow neural network was trained to detect tampered videos and in [47] a deep neural network was trained on a very large data set to determine real from fake videos. Both studies evaluate authenticity based on individual frames and showed excellent results. In [19] a CNN was used to extract features from each video frame which were then passed into a Recurrent Neural Network that determined whether the video was fake or real. The network trained and tested video streams rather than individual frames. They did not restrict their work to face videos.

Finally, in [36], much like our paper, the authors chose to focus on the color aspect of deepfakes. They focus on the spectral difference between GAN generated images and camera generated images, in RGB space. They used these differences as features in an SVM classifier, and achieved 70% accuracy on the MFC2018 dataset [3] Their focus on color however was more

technical regarding the way GAN generates images as opposed to how a camera generates an image, while we focus more on the biological aspect of color, and how machines will have a difficult time synthesizing changes in the skin tone.

Background

Facial Skin Color

In this study, we exploit the color changes in the skin to detect forged or tampered video sequences as well as videos used for spoofing. The human skin structure consists of two layers: an Epidermis layer and a Dermis layer [6] (see Figure 1). The Epidermis layer of the skin contains Melanin, a chemical pigment that causes facial color to change very slowly when exposed to UV light. The Dermis layer of the skin contains Hemoglobin, which is oxidized blood. Hemoglobin concentration can change very fast when blood flow under the skin is increased or decreased. This causes fast changes in facial color. The color of human skin is thus determined by the combined concentration of the melanin and hemoglobin in the two skin layers. Flushed skin tones are due to a greater concentration of hemoglobin, i.e. the skin takes on a more reddish hue. Darker skin tones are induced by an increase in melanin, as in suntanned skin. Characteristic skin tones of different human races is also determined by the concentration of melanin.

Blood flow in facial areas occur continuously though they tend to change density under emotional states especially, high intensity states such as stress and extreme emotions[58, 12, 13, 9]. Changes in blood flow implies changes in hemoglobin concentration under the facial skin [11], and consequently changes in facial color. In [22] it was shown that there is a direct correlation between the emotional state of an individual, and the level of oxygenated Hemoglobin.

Studies have attempted to model the concentration of melanin and hemoglobin in facial and hand skin from images of the skin using multispectral input [23, 24] or RGB input [43, 56, 46].

The human face contains a high concentration of blood vessels very close to the skin surface [39], thus, changes in blood flow have a significant effect on facial color. Specifically, the cheek areas of the face contain many blood vessels and is relatively unaffected by shading and unobstructed by facial hair and accessories such as eye glasses. Thus the cheek areas are a good candidate for observing the subtle changes in facial color.

In the context of synthesized and fake face images, we assume that the image generators do not directly implement the behavior of under-skin blood flow and thus do not necessarily capture the subtle color changes in the face induced by blood flow. Accordingly we attempt to exploit this assumption and use facial color changes to determine fake vs real videos as well as spoofing attacks.

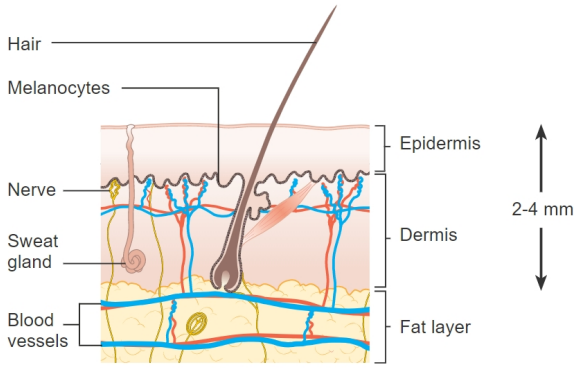

Figure 1. *2-layer skin model consisting of the Dermis and Epidermis layers.*

Color space for facial color analysis

Facial color analysis is based on detecting the changes in blood flow and concentration beneath the facial skin. Since, facial color is affected by the scene illuminant as well as by the local shading due to the face geometry, consideration should be given to the color representation to be used in the analysis. Specifically, it is advantageous to use a color space that provides good separation of the flushed red tones from the chromatic content. The color representation should also allow separation of the luminance channel in order to reduce the effect of scene illumination and object shading.

It has been shown that various color spaces outperform the standard RGB color space when dealing with faces, in terms of face detection [34, 52] as well as facial emotion analysis [61, 62, 31]. Testing over several color spaces, we found that the oRGB color space [10, 60] provides a good decomposition into the opposing chromatic channels and performs well in representing facial color change.

The oRGB color space is similar in nature to the HSV color space [60], but also provides an additional step of stretching and compressing regions of the color space in order to obtain a representation more similar to the traditional complementary colors scheme, of red-green and yellow-blue. To convert an RGB pixel to oRGB, a linear transformation is first performed:

$$\begin{bmatrix} L \\ C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 0.2990 & 0.5870 & 0.1140 \\ 0.5000 & 0.5000 & -1.000 \\ 0.8660 & -0.8660 & 0.000 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{1}$$

followed by a non-uniform rotation around the luma axis (L):

$$\theta_o(\theta) = \begin{cases} (3/2)\theta & \text{if } \theta < \pi/3 \\ \pi/2 + (3/4)(\theta - \pi/3) & \text{if } \pi \geq \theta \geq \pi/3 \end{cases} \tag{2}$$

where θ is the angle in the linear chroma plane, defined as: $\theta = atan2(C_2, C_1)$. θ_o is the new angle in the oRGB color space.

To calculate the two chroma channels (C_{rg}, C_{yb}) of the oRGB color space, the chroma vector (C_1, C_2) is rotated to align with the new angle using the non-uniform rotation matrix R:

$$\begin{bmatrix} C_{rg} \\ C_{by} \end{bmatrix} = R_{(\theta_o - \theta)} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \tag{3}$$

This provides the stretching and compressing effect of the oRGB color space, which is visualized in Figure 2.

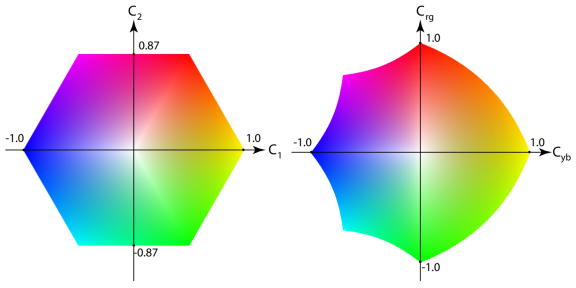

Figure 2. *The gamut of the oRGB color space before (left) and after (right) applying the non uniform rotation in chroma plane as given in Equation 3 (from [10]).*

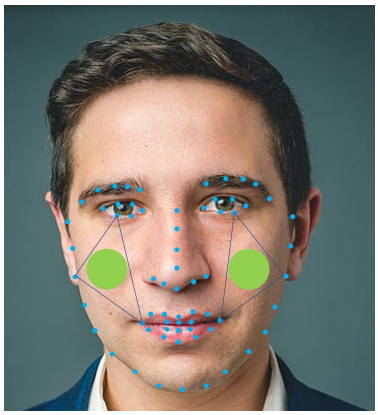

Figure 3. *Extracted facial landmarks and the calculated cheek patch.*

Facial Color Feature Vector

To determine fake vs real videos of human faces, We follow a similar approach to that proposed in [51] in which changes in facial color was exploited for micro emotion classification. We extract a feature vector per video segment representing statistics of the color information in regions of the face, over time. Since change in facial color is due to facial blood flow, we focus on the cheek areas as these areas contain a high concentration of blood vessels beneath the skin, and yet are not usually occluded by facial hair or accessories (glasses etc).

The input videos are partitioned into video segments of 50 frames each. This allows for variable length input videos, as well as allows the use of a voting scheme that provides additional robustness and accuracy. Thus, for each such video segment a feature vector is created and a segment based decision of real vs fake is determined.

For every frame of the segment, facial feature points are detected using a standard machine learning based landmark detector [28] and the patches associated with the cheek areas are determined (Figure 3). The circular cheek regions are robust under head and facial motion as well as variations and errors in the detected facial points. Color information from these cheek patches in each frame are collated into a feature vector.

We use the oRGB color space to represent the chromatic content (see Section 2). Thus, the RGB data of each video frame is transformed into the two chroma channels C_{rg}, C_{by} of the oRGB color space. These channels, being independent of luminance, allow our representation to be invariant under changes of light intensity of the scene and to shading due to the geometry of the face. For every video frame, the average and standard deviation of the oRGB values C_{rg}, C_{by} are computed within each cheek patch. Since the change in facial color is of interest rather than the absolute values, we normalize the mean oRGB values by subtracting the mean oRGB value of the cheek patches in the first frame of the video.

Thus, for each frame, the normalized mean and the std of the spectral content over the two selected patches (Figure 3) are collected, resulting in 8 features per frame. These are collected across all 50 frames of the video segment, and concatenated into a single feature vector of size 400. These feature vectors serve as input for training and testing the networks used for real/fake video detection.

Datasets

We show that facial color can be used to detect fake from real videos of human faces. We show this on several databases including deepfake generated faces as well as masked figures as used in spoofing attacks.

1. The DeepfakeTIMIT database [30], a recently developed database which contains short videos generated using a pre-trained Generative Adversarial network (GAN). The DeepfakeTIMIT database was generated from the vidTIMIT database [49], which contains short videos of individuals reading specific sentences. To generate the DeepfakeTIMIT database, the authors paired videos of individuals from the original vidTIMIT database, using one as the reference and one as the target of the face swap. Examples can be seen in Figure 4. DeepfakeTIMIT database contains 320 generated videos. Together with 860 real samples from the vidTIMIT database, the number of samples is 1180.
2. The FaceForensic++ database [48], a Deepfake database, with a larger collection of samples. For this study we used the 720 fake video samples produced using the Face2Face generator [55] and the 1000 real videos. Thus a total of 1720 samples were used. Samples can be seen in Figure 5 and Figure 6
3. The 3DMAD dataset [14], was designed for testing for spoofing attacks. It includes videos of unmasked individuals and videos of individuals wearing hyper-realistic face masks (to implement mask spoof attack). Examples from the dataset are shown in Figure 7. The database includes 85 samples of real videos and 85 videos of masked faces, where the masks were in the shape and color of the original unmasked individuals. Thus the database supplied a total of 170 video sample.
4. Animated database - Our generated database based on [7], which allows us to animate a still image based on an input video. We selected pairs of videos from the MMI dataset of emotion videos [41, 57]. We used one video of the pair as the source video, and the first frame of the second video as the source image. Thus creating fake videos. Examples can be seen in Figure 8. The dataset consists of 108 generated videos. The MMI dataset supplied the 48 real videos. Thus the dataset supplied 156 video samples.

From our generated database and the two Deepfake databases, we took the fake data as well as the respective original reference videos, in order to have both real and fake samples of similar nature.

Figure 4. *Samples from the DeepfakeTIMIT database [30].*

Figure 5. *Sample from the FaceForensic++ database [48].*

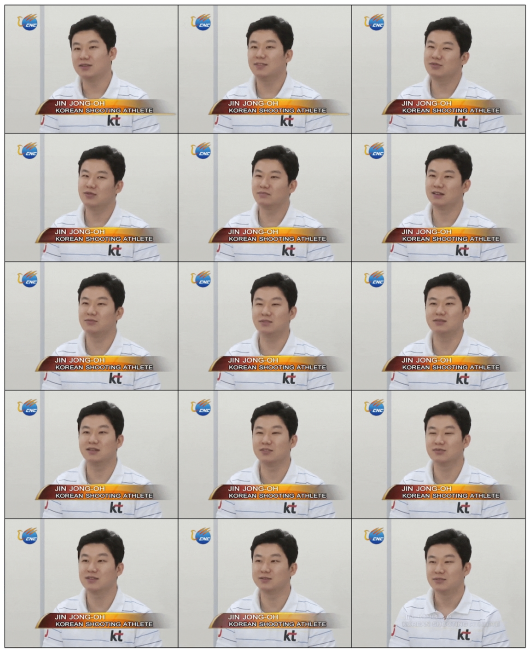

Figure 6. *Samples from the FaceForensic++ database [48].*

Figure 7. *Samples from the 3DMAD dataset. A real person (left) and an individual wearing a hyper-realistic mask of the real person (right).*

Fake vs Real Video Detection

To test for real vs fake over the 4 datasets, we extracted a facial color feature vector, as described above, (Section), for each video sample. These feature vectors were used to train a"Long Short-Term Memory" model (LSTM) [21, 18] (Figure 9-10). The network was structured as a binary classifier outputting either 'fake' or 'real'. The LSTM network consists of two layers - a single LSTM layer followed by a dense layer (Figure 11). Testing was performed using 10-fold cross validation. Training was performed for 750 epochs with batch size of 100. ADAM was used as the optimizer.

The results of classifying real vs fake on the 4 datasets are given in Table 1. Since our system relies on human facial color

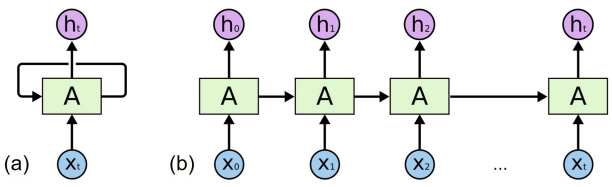

Figure 9. *(a) The LSTM is a type of recurrent neural network (RNN) which includes feedback loops that feed data back into the network together with new data. (b) The RNN can be "unrolled" to emphasize the repetition of the incoming and outgoing flow of data at each step.*

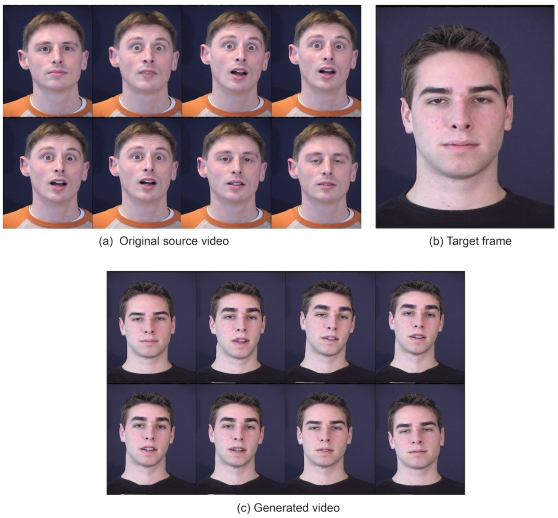

Figure 8. *Samples from our generated database, based on the work of Averbuch-Elor et al. [7].*

variations it was able to reach high accuracy results with 99% success rate on the 3DMAD data set, 97% success rate on our generated database, 80% on the much trickier deepfakeTIMIT database, and 82% on the deepfake FaceForensic++ database.

The high success rate is not surprising for the 3DMAD data set, as the material of the mask should not show blood flow effects, or facial color change. The Animated database showed high success rates, since the fake video was generated from a single still image and thus does not show facial color change. In terms of the deepfakeTIMIT and FaceForensic++ databases, these videos were created by models that work on a frame by frame basis and are aimed at perfecting the pose, and expression in each frame and are not focused on following the facial color changes of the source video.

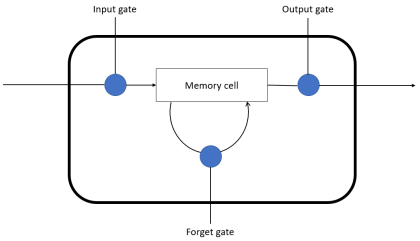

Figure 10. *A single LSTM unit.*

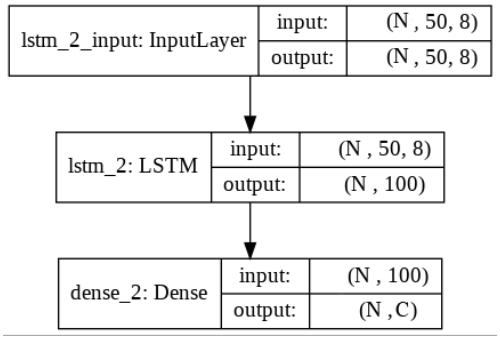

Figure 11. *The architecture of the network - consisting of an LSTM layer with 100 hidden layers, followed by a dense layer.*

Database	Accuracy
3DMAD [14]	99.0%
Portraits	97.0%
DeepfakeTIMIT [30]	80.0%
FaceForensic++ [48]	82.0%

Table 1: Success rates of using facial color for fake detection on the real vs fake datasets.

Conclusion

In this study we tested the ability of changes in facial color to determine fake from real videos as well as determine spoofing attacks by detecting masked vs real individuals in videos. We showed that by training a neural network with the color content of cheek regions of the face along a video sequence, we were able to successfully distinguish real from fake and real from masked faces in videos. We hypothesize that the facial color change is due to blood flow changes under the facial skin, but whether the significant factor is the heartbeat- amplitude or frequency, or the sheer blood flow volume, is unclear.

References

[1] Faceapp. https://www.faceapp.com/, Last accessed on 2020-03-31.

[2] Fakeapp. https://www.fakeapp.org/, Last accessed on 2020-03-31.

[3] The media forensics challenge 2018 (mfc2018). https://www.nist.gov/itl/iad/mig/media-forensics-challenge-2018, Last accessed on 2020-03-31.

[4] Darius Afchar, Vincent Nozick, Junichi Yamagishi, and Isao Echizen. Mesonet: a compact facial video forgery detection network. In *IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–7, 2018.

[5] Omar Ismael Al-Sanjary and Ghazali Sulong. Detection of video forgery: A review of literature. *Journal of Theoretical & Applied Information Technology*, 74(2), 2015.

[6] Mohammed Hazim Alkawaz, Dzulkifli Mohamad, Tanzila Saba, Ahmad Hoirul Basori, and Amjad Rehman. The correlation between blood oxygenation effects and human emotion towards facial skin colour of virtual human. *3D Research*, 6(2):13, 2015.

[7] Hadar Averbuch-Elor, Daniel Cohen-Or, Johannes Kopf, and Michael F Cohen. Bringing portraits to life. *ACM Transactions on Graphics (TOG)*, 36(6):196, 2017.

[8] David Berthelot, Tom Schumm, and Luke Metz. BEGAN: boundary equilibrium generative adversarial networks. *arXiv:1703.10717*, 2017.

[9] Isabelle Blanchette, Anne Richards, and Adele Cross. Anxiety and the interpretation of ambiguous facial expressions: The influence of contextual cues. *The Quarterly Journal of Experimental Psychology*, 60(8):1101–1115, 2007.

[10] Margarita Bratkova, Solomon Boulos, and Peter Shirley. oRGB: a practical opponent color space for computer graphics. *IEEE Computer Graphics and Applications*, 0(1):42–55, 2009.

[11] Craig Donner and Henrik Wann Jensen. A spectral BSSRDF for shading human skin. *Rendering Techniques*, 2006:409–418, 2006.

[12] Peter D Drummond and Saw Han Quah. The effect of expressing anger on cardiovascular reactivity and facial blood flow in chinese and caucasians. *Psychophysiology*, 38(2):190–196, 2001.

[13] Peter D Drummond and Daphne Su. The relationship between blushing propensity, social anxiety and facial blood flow during embarrassment. *Cognition & emotion*, 26(3):561–567, 2012.

[14] Nesli Erdogmus and Sébastien Marcel. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS*, pages 1–6, 09 2013.

[15] Hany Farid. A survey of image forgery detection. *IEEE Signal Processing Magazine*, 26(2):16–25, 2009.

[16] Javier Galbally, Sébastien Marcel, and Julian Fierrez. Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2:1530–1552, 2014.

[17] Pablo Garrido, Levi Valgaerts, Ole Rehmsen, Thorsten Thormahlen, Patrick Perez, and Christian Theobalt. Automatic face reenactment. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 4217–4224, 2014.

[18] Klaus Greff, Rupesh K Srivastava, Jan Koutník, Bas R Steunebrink, and Jürgen Schmidhuber. LSTM: A search space odyssey. *IEEE transactions on neural networks and learning systems*, 28(10):2222–2232, 2016.

[19] David Güera and Edward J Delp. Deepfake video detection using recurrent neural networks. In *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 1–6. IEEE, 2018.

[20] Anthony T. S. Ho and Shujun Li. *Handbook of Digital Forensics of Multimedia Data and Devices*. Wiley-IEEE Press, 2015.

[21] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8):1735–1780, 1997.

[22] Yoko Hoshi, Jinghua Huang, Shunji Kohri, Yoshinobu Iguchi, Masayuki Naya, Takahiro Okamoto, and Shuji Ono. Recognition of human emotions from cerebral blood flow changes in the frontal region: a study with event-related near-infrared spectroscopy. *Journal of Neuroimaging*, 21(2):e94–e101, 2011.

[23] Dainis Jakovels, Inga Saknite, and Janis Spigulis. Implementation of laser speckle contrast analysis as connection kit for mobile phone for assessment of skin blood flow. In *Biophotonics: Photonic Solutions for Better Health Care IV*, volume 9129, page 91293I. International Society for Optics and Photonics, 2014.

[24] Dainis Jakovels, Janis Spigulis, and Laura Rogule. Rgb mapping of hemoglobin distribution in skin. In *European Conference on Biomedical Optics*, page 80872B. Optical Society of America, 2011.

[25] Vaishali Joshi and Sanjay Jain. Tampering detection in digital video-a review of temporal fingerprints based techniques. In *International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 1121–1124, 2015.

[26] Tero Karras, Samuli Laine, and Timo Aila. A style-based generator architecture for generative adversarial networks. In *IEEE Conference on Computer Vision and Pattern Recognition*, pages 4401–4410, 2019.

[27] Jan Kietzmann, Linda W Lee, Ian P McCarthy, and Tim C Kietzmann. Deepfakes: Trick or treat? *Business Horizons*, 63(2):135–146, 2020.

[28] Davis King. Dlib-ml: A machine learning toolkit. *Journal of Machine Learning Research*, 10:1755–1758, 07 2009.

[29] Naveen Kodali, Jacob Abernethy, James Hays, and Zsolt Kira. On convergence and stability of gans. *arXiv:1705.07215*, 2017.

[30] Pavel Korshunov and Sébastien Marcel. Deepfakes: a new threat to face recognition? assessment and detection. *arXiv preprint arXiv:1812.08685*, 2018.

[31] Seyed Mehdi Lajevardi and Hong Ren Wu. Facial expression recognition in perceptual color space. *IEEE transactions on image processing*, 21(8):3721–3733, 2012.

[32] Haodong Li, Han Chen, Bin Li, and Shunquan Tan. Can forensic detectors identify GAN generated images? In *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pages 722–727, 2018.

[33] Yuezun Li and Siwei Lyu. Exposing deepfake videos by detecting face warping artifacts. *arXiv preprint arXiv:1811.00656*, 2, 2018.

[34] Ze Lu, Xudong Jiang, and Alex Kot. An effective color space for face recognition. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2019–2023, 2016.

[35] Scott McCloskey and Michael Albright. Detecting GAN-generated imagery using color cues. *arXiv:1812.08247*, 2018.

[36] Scott McCloskey and Michael Albright. Detecting gan-generated imagery using color cues. *arXiv preprint arXiv:1812.08247*, 2018.

[37] Simone Milani, Marco Fontani, Paolo Bestagini, Mauro Barni, Alessandro Piva, Marco Tagliasacchi, and Stefano Tubaro. An overview on video forensics. *APSIPA Transactions on Signal and Information Processing*, 1, 2012.

[38] Huaxiao Mo, Bolin Chen, and Weiqi Luo. Fake faces identification via convolutional neural network. In *ACM Workshop on Information Hiding and Multimedia Security*, pages 43–47, 2018.

[39] Giuseppe Moretti, Richard A. Ellis, and Herbert Mescon. Vascular patterns in the skin of the face. *Journal of Investigative Dermatology*, 33(3):103–112, 1959.

[40] Lakshmanan Nataraj, Tajuddin Manhar Mohammed, BS Manjunath, Shivkumar Chandrasekaran, Arjuna Flenner, Jawadul H Bappy, and Amit K Roy-Chowdhury. Detecting GAN generated fake images using co-occurrence matrices. *Electronic Imaging*, 2019(5):532–1, 2019.

[41] Maja Pantic, Michel Valstar, Ron Rademaker, and Ludo Maat. Web-based database for facial expression analysis. In *2005 IEEE international conference on multimedia and Expo*, pages 5–pp. IEEE, 2005.

[42] Alessandro Piva. An overview on image forensics. *ISRN Signal Processing*, 2013(496701), 2013.

[43] Ming-Zher Poh, Daniel J McDuff, and Rosalind W Picard. Advancements in noncontact, multiparameter physiological measurements using a webcam. *IEEE transactions on biomedical engineering*, 58(1):7–11, 2010.

[44] Noa Privman-Horesh, Azmi Haider, and Hagit Hel-Or. Forgery detection in 3d-sensor images. In *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 1561–1569, 2018.

[45] Nicolas Rahmouni, Vincent Nozick, Junichi Yamagishi, and Isao Echizen. Distinguishing computer graphics from natural images using convolution neural networks. In *IEEE Workshop on Information Forensics and Security (WIFS)*, pages 1–6, 2017.

[46] Geovany A Ramirez, Olac Fuentes, Stephen L Crites Jr, Maria Jimenez, and Juanita Ordonez. Color analysis of facial skin: Detection of emotional state. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 468–473, 2014.

[47] Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, and Matthias Nießner. Faceforensics++: Learning to detect manipulated facial images. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 1–11, 2019.

[48] Andreas Rössler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, and Matthias Nießner. FaceForensics++: Learning to detect manipulated facial images. In *International Conference on Computer Vision (ICCV)*, 2019.

[49] Conrad Sanderson and Brian C Lovell. Multi-region probabilistic histograms for robust and scalable identity inference. In *International conference on biometrics*, pages 199–208. Springer, 2009.

[50] Rohini Sawant and Manoj Sabnis. A review of video forgery and its detection. *Journal of Computer Engineering (IOSR-JCE)*, 20:1–4, 2018.

[51] Hadas Shahar and Hagit Hel-Or. Micro expression classification using facial color and deep learning methods. In *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pages 0–0, 2019.

[52] Chandni Sharma, Shreya Patel, Abhishek More, Kevin Maisuria, Saheli Patel, and Foram Shah. Review of face detection based on color image and binary image. *International Journal of Computer Applications*, 134(1):22–26, 2016.

[53] K Sitara and Babu M Mehtre. Digital video tampering detection: An overview of passive techniques. *Digital Investigation*, 18:8–22, 2016.

[54] Shahroz Tariq, Sangyup Lee, Hoyoung Kim, Youjin Shin, and Simon S Woo. Detecting both machine and human created fake face images in the wild. In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pages 81–87, 2018.

[55] Justus Thies, Michael Zollhofer, Marc Stamminger, Christian Theobalt, and Matthias Nießner. Face2face: Real-time face capture and reenactment of rgRGB videos. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2387–2395, 2016.

[56] Norimichi Tsumura, Hideaki Haneishi, and Yoichi Miyake. Independent-component analysis of skin color image. *Journal of the Optical Society of America (JOSA)*, 16(9):2169–2176, 1999.

[57] Michel Valstar and Maja Pantic. Induced disgust, happiness and surprise: an addition to the MMI facial expression database. In *Proc. 3rd Intern. Workshop on EMOTION (satellite of LREC): Corpora for Research on Emotion and Affect*, page 65. Paris, France, 2010.

[58] Olav Vassend and Stein Knardahl. Personality, affective response, and facial blood flow during brief cognitive tasks. *International journal of psychophysiology*, 55(3):265–278, 2005.

[59] Ainuddin Wahid Abdul Wahab, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan, Zaidi Razak, and Muhammad Rezal Kamel Ariffin. Passive video forgery detection techniques: a survey. In *nternational Conference on Information Assurance and Security*, pages 29–34, 2014.

[60] Brian A. Wandell. *Foundations of Vision*. Sinauer Associates, 1995.

[61] Su-Jing Wang, Wen-Jing Yan, Xiaobai Li, Guoying Zhao, and Xiaolan Fu. Micro-expression recognition using dynamic textures on tensor independent color space. In *IEEE International Conference on Pattern Recognition*, pages 4678–4683, 2014.

[62] Su-Jing Wang, Wen-Jing Yan, Xiaobai Li, Guoying Zhao, Chun-Guang Zhou, Xiaolan Fu, Minghao Yang, and Jianhua Tao. Micro-expression recognition using color spaces. *IEEE Transactions on Image Processing*, 24(12):6034–6047, 2015.

[63] Sheng-Yu Wang, Oliver Wang, Andrew Owens, Richard Zhang, and Alexei A Efros. Detecting photoshopped faces by scripting photoshop. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 10072–10081, 2019.

[64] Xin Yang, Yuezun Li, and Siwei Lyu. Exposing deep fakes using inconsistent head poses. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 8261–8265. IEEE, 2019.

[65] Egor Zakharov, Aliaksandra Shysheya, Egor Burkov, and Victor Lempitsky. Few-shot adversarial learning of realistic neural talking head models. In *Proceedings of the IEEE International Conference on Computer Vision*, pages 9459–9468, 2019.

Author Biography

Hadas Shahar holds an MSc from the Dept of Computer Science at the University of Haifa (2019). Her research focused on the utilization of facial color with deep learning methods for the classification of human emotions. She is currently a software engineer at Phillips Israel.

Prof Hagit Hel-Or is a faculty member in the department of Computer Science and head of the Computational Human Behavior Lab at the University of Haifa. Her background is in the area of Image Processing, Computer Vision and Machine Learning. Her current research interests are in interdisciplinary studies; integrating computer vision and learning algorithms for Human Behavior studies, in Medical and Cognitive Psychology studies.