Fake Face Detection Based on Colour Textual Analysis Using Deep Convolutional Neural Network

Wasin Alkishri[1*], Setyawan Widyarto[2] , Jabar H. Yousif[3] and Mahmood Al-Bahri[4]

[1*] Faculty of Computer Studies, Arab Open University, Muscat, Oman.
Wasan.k@aou.edu.om, Orcid: https://orcid.org/0000-0003-0833-5633

[2] Faculty of Communication, Visual Art, and Computing, Universiti Selangor (UNISEL), Selangor, Malaysia. swidyarto@unisel.edu.my, Orcid: https://orcid.org/0000-0002-6317-9875

[3] Faculty of Computing and IT, Sohar University, Sohar, Oman. Jyousif@su.edu.om, Orcid: https://orcid.org/0000-0003-2110-8347

[4] Faculty of Computing and IT, Sohar University, Sohar, Oman. mbahri@su.edu.om, Orcid: https://orcid.org/0000-0002-0176-0680

Received: June 21, 2023; Accepted: August 19, 2023; Published: August 30, 2023

Abstract

Detecting fake faces has become a crucial endeavour within the realm of computer vision. The widespread availability of digital media has facilitated the creation and dissemination of deceptive and misleading content. A prominent strategy for identifying counterfeit faces employs advanced deep-learning methodologies that scrutinise both colour and textural attributes. This investigation is geared towards devising a method for discerning fake faces by leveraging the capabilities of convolutional neural networks (CNNs). These networks are trained to discriminate between authentic and forged images by discerning nuances in their colour characteristics. To achieve this, the MSU MFSD dataset will be harnessed, allowing for exploring colour textures and extracting facial traits across diverse colour channels, including RGB, HSV, and YCbCr.The proposed framework marks a notable stride in the realm of computer vision research, particularly given the prevalent employment of digital media, which has eased the generation and distribution of misleading or deceitful content. Developing dependable systems for identifying counterfeit faces holds immense potential in curtailing the proliferation of false information and upholding the integrity of digital media platforms.

Keywords: Convolutional Neural Network (CNN), Colour Textual Analysis, Fake Face, Detection.

1 Introduction

With the escalating volume of data and a growing consciousness regarding information privacy and security, individuals have increasingly adopted a more vigilant stance towards safeguarding their sensitive information and ensuring the protection of their identities. In the realm of identity verification, time-honoured authentication methods like passwords, security questions, PINs, ID cards, driver's licenses, and token-based devices have enjoyed a longstanding history. Nevertheless, these conventional

---

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 3 (August), pp. 143-155.
DOI: *10.58346/JISIS.2023.I3.009*
*Corresponding author: Faculty of Computer Studies, Arab Open University, Muscat, Oman.

techniques are not impervious to threats like hacking and loss **(AlKishri, 2021)**. As a consequence, the attention of researchers has turned toward biometric identification technologies that offer a combination of high reliability, user-friendly interfaces, and steadfast stability.

Biometric identification methods encompass a range of techniques, such as iris scanning, speech recognition, fingerprint analysis, signature verification, and face recognition. These methods hinge on the automated examination of distinctive human traits to establish identity. Among these modalities, face recognition has garnered considerable prominence within the domains of computer vision and pattern recognition. Notwithstanding recent progress, the task of fortifying access control systems against hackers and malevolent assaults persists as a substantial hurdle **(Gupta & Tripathy, 2023)**.

The broader populace has experienced a heightened awareness regarding facial recognition technologies and the potential weaknesses they may entail. In the present times, it has become relatively effortless to discover websites and even YouTube videos that offer explicit guidance on exploiting and attaining unauthorised entry into facial recognition systems. This mounting apprehension has catalysed researchers to confront these issues by concentrating on the detection of counterfeit faces and devising robust strategies to shield users against endeavours aimed at spoofing.

Effectively addressing these challenges has emerged as a significant realm of investigation, with researchers dedicated to bolstering the security and dependability of automated access control systems. Through the progression of fake face detection methodologies, researchers are working towards mitigating the potential vulnerabilities linked with facial recognition technology, thereby establishing robust defences against unauthorised entry and malevolent misuse.

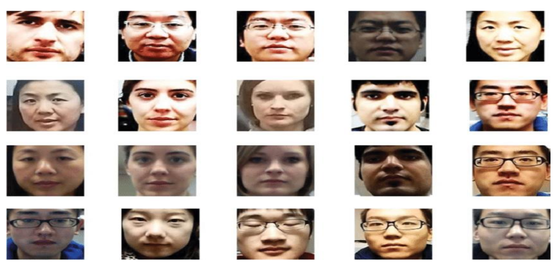

Figure 1: Some Original and Fake Face Pictures from MSU-MFSD Datasets

Figure 1, displays some original and fake face pictures from MSU-MFSD datasets were utilized in this study **(Wen, Han, & Jain, 2015).** As we notice that it is difficult to select the original face image from the fake face. Boulkenafet et al, 2017 examined the threat of posting a personal image on social media networks like Facebook against six commercial face authentication systems on social media such as Face Unlock, Facelock Pro, Visidon, Veriface, Luxand Blink and FastAccess. They found that 39% of images posted on social networks can be used for spoofing the face-based authentication system on social networks. Low-level skin colour analysis for face detection has been an important part of computer vision and picture processing for many uses, such as facial recognition, human-computer interaction, and surveillance. Several ways have already been made to deal with this problem: Threshold Methods, Backgrounds, Colour Space Transformation, and Machine Learning Approaches. However, there are some problems with low-level skin colour analysis for face recognition: When the lighting changes, the colour of the skin can look very different. Images can have noise, shadows, and artefacts that make it hard to find skin. Most images have a small number of skin pixels, which causes a class mismatch. Face anti-spoofing is one of the significant problems in biometric-based authentication. However, colour texture-based feature approaches have been more commonly used to evaluate grayscale images, thus discarding unnecessary colour information, which can be a critical visual indicator for discriminating original faces from fake ones. Texture analyses of grayscale face images can provide sufficient means to detect fake faces if only take into consideration the camera resolution. The high quality of the captured image means the details of the face can be successfully explored. To combat this problem, researchers and developers have turned to advanced technologies, particularly deep learning techniques, to develop robust and accurate methods for fake face detection. One such approach gaining traction is fake face detection based on colour textual analysis using deep convolutional neural networks (CNNs). This innovative method leverages the power of deep learning and exploits colour and texture cues within images to distinguish between genuine and manipulated faces.

The landscape of computer vision tasks, such as face recognition, object detection, and image classification, has been revolutionised by convolutional neural networks (CNNs). Their capacity to learn hierarchical representations of visual data positions them as ideal contenders for fake face detection. Through scrutinising visual features and patterns within images, CNNs can detect inconsistencies and irregularities that signal a counterfeit face. However, conventional CNN-based techniques often concentrate solely on pixel-level examination, disregarding essential contextual insights and intricate details that may emerge from colour and texture fluctuations. To overcome this limitation, **Crowley (2023)** has recently delved into the integration of color-texture analysis within the CNN architecture. By assimilating colour and texture data, the proposed models can encapsulate more refined attributes of fake faces, ultimately resulting in enhanced detection precision.

The progression of fake face detection grounded in colour-textual analysis using deep convolutional neural networks generally encompasses several distinct phases. To initiate, a comprehensive dataset encompassing genuine and fabricated facial images is curated and meticulously categorised. This dataset subsequently serves as the substrate for training the CNN model, equipping it to grasp discriminative attributes that set apart authentic from manipulated countenances. The training journey unfolds across multiple iterations, with the network incrementally adapting its parameters to minimise the margin of detection error. Throughout this training process, the CNN acquires the adeptness to extract characteristics from both the chromatic and textural facets inherent within the input images. This capacity empowers the model to encapsulate intricate particulars such as color gradients, skin textures, and various facial traits that are pivotal for achieving precise detection. The architectural composition of the network conventionally encompasses a series of convolutional layers, succeeded by pooling layers, fully connected layers, and culminating in an output layer that yields a probability score signifying the likelihood of an image being inauthentic.Post-training, the model undergoes assessment on an independent test set to gauge its performance. The error rate functions as the metric for gauging the model's efficacy in distinguishing between authentic and counterfeit visages. Often, researchers engage in the fine-tuning of the model, experimenting with diverse hyperparameters in a quest to attain the most optimal detection outcomes.

The potential uses of deep convolutional neural networks for detecting fake faces through color textual analysis are extensive. Social media platforms have the opportunity to employ this technology for the automated identification and removal of deceptive profile pictures, thus thwarting the establishment of fraudulent accounts. Online marketplaces can utilize these techniques to validate the legitimacy of seller profiles, thereby establishing a more secure and dependable trading environment. Moreover, law enforcement agencies can make use of this technology to uncover criminals concealing their true identities behind counterfeit personas during digital investigations.

This research paper outlines the following main objectives:

1) Creation of a fake face detection system using deep learning methods grounded in colour textual analysis.

2) Application of CNNs to scrutinise the colour attributes of images and differentiate between authentic and counterfeit faces.
3) Examination of the most effective colour bands for distinguishing real faces from fake ones, with potentially severe consequences for those found engaging in such activities.

2 Background and Related Work

The term "fake face detection techniques" encompasses a range of algorithms and approaches designed for the assessment of digital images or video streams to pinpoint faces that have been synthetically manipulated or generated. The ease of generating counterfeit faces, serving various purposes such as identity theft, online scams, and cyberbullying, has surged. This rise can be attributed to the accessibility of advanced image editing tools and deep learning algorithms **(Alkishri, 2023)**. Characteristics like facial expressions, skin texture, and landmarks fall within this scope. The scrutiny of these traits and the determination of an image's authenticity or fakeness often involve the application of machine learning algorithms. The pursuit of methods to detect fake faces remains an actively researched area, with consistent introductions of new methodologies and algorithms as potential solutions. However, the task of identifying fake faces is formidable, and no single approach guarantees 100% accuracy across all instances. A pivotal facet of face detection involves low-level analysis, encompassing the extraction of fundamental details like colour, texture, and edge information from an image. Skin colour-based detection stands out among the low-level analysis techniques frequently employed in face recognition. This approach leans on skin tone as a salient facial attribute that is comparatively simpler to process than other traits. The utilisation of skin colour in images aids in delineating the skin region, subsequently enabling its masking through a predetermined threshold, thereby facilitating the extraction of the facial region through a bounding box algorithm. Various colour models, such as RGB, HSV, and YCbCr, each carrying their own merits and demerits, can be harnessed for skin colour detection. This section offers a broad overview of face detection methodologies grounded in low-level skin colour analysis within this context.

Low-level Skin Colour Analysis

Color holds notable importance in human facial attributes. Employing skin colour as a factor in facial monitoring presents several advantages. Processing colour is notably simpler compared to other facial traits. Furthermore, colors are deemed invariant under varying lighting conditions.The optical flow function simplifies motion estimation by relying on a translation model. However, tracking human faces using colour presents difficulties due to object motion and ambient light, making identifying skin pixels challenging. Additionally, the perception of human colour can be influenced by the direction and position of light sources **(Holmqvist, 2022)**. To overcome these challenges, a calibrated colour histogram can be utilised to observe skin pixels and adjust for shifts in luminance strength. Transforming RGB vectors into [R, G, B] colour vectors can facilitate skin detection, making the process more efficient. However, this approach may not work when other body parts, such as arms and legs, are present in the image. An alternative skin colour classification system based on the YCbCr colour space has been developed. This system identifies skin regions with similar Cb and Cr values, utilising threshold values like [Cr1, Cr2] and [Cb1, Cb2]. A pixel is deemed to have skin tone if its [Cr, Cb] values fall below these thresholds. The skin colour distribution can identify the face region in the image, but this method requires that the image contains only the face region as the skin area. HSV colour space has established a colour predicate to distinguish tissue sections from the background **(Moreira, 2022).** The HSI skin colour classification is the same as the YCbCr skin colour classification except for the hue (H) and saturation (S) values. In this case, it set the threshold as [H1, S1] and [H2, S2], and it classified a pixel as having a skin tone if the value [H, S] fell within the threshold. Typically, three distinct algorithms for face detection are utilised: the RGB, YCbCr, and colour space technologies. To carry this out, there are three stages for implementing these algorithms. The following criteria are:

- Detector the pattern of skin region within the image.
- The skin region is masked using a predefined threshold.
- The face region is extracted using a bounding box algorithm.

- **RGB Colour Model**

The face is targeted and detected by RGB colours which are primary colours; Red (R), Green (G), and Blue (B). To detect skin colour pixels in an image, a normalised colour histogram can be used in the RGB colour space, which can be adjusted for changes in luminance to provide clarity **(Khanam, 2022).** However, the RGB colour model is considered photosensitive and has a significant downside compared to other colour models like YCbCr or HSI. The issue is that the colour (Chroma) and pixel intensity cannot be distinguished clearly, making it challenging to differentiate skin-coloured regions. This variable makes RGB less favourable for skin detection algorithms.

In contrast, **(Dhivakar, 2015)** proposed a two-component facial detection and identification process. The feature extraction step involves skin colour differentiation using threshold skin colour teams managed with the AdaBoost algorithm, which is faster and more effective in detecting faces. Various morphological operators are used to enhance facial detection efficiency. The recognition component consists of three steps: extraction of the Gabor function, reduction of measurements, and feature selection using PCA, followed by classification based on KNN. This program is versatile enough to identify faces in various lighting situations, scales, shapes, and skin colours.

- **HSV Colour Model**

The HSV colour space defines colours in terms of hue, saturation, and value (V), represented as H, S, and V, respectively. Hue corresponds to the 0–360-degree red, green, blue, and yellow colour spectrum. Saturation represents the degree of colour purity and ranges from 0 to 100 per cent, while the value corresponds to the brightness of the colour **(Venkatesh, 2019)**

The average pixel in a skin region should satisfy certain statistical conditions, such as:

$$0 \leq H \leq 0.25$$
$$0.15 \leq S \leq 0.9$$

The transformation between HSV and RGB colour models is nonlinear. The Hue (H) value may not be accurate for recognition when the intensity is low in the HSV colour model. However, the skin colour detection algorithm uses the HSV colour model rather than the RGB model.

- **YCbCr Colour Model**

The YCbCr colour model divides images into luminance (Y channel) and colour (Cb and Cr channels). See **Figure 2.** This colour space has uniform skin distribution among different races with only slight Cb and Cr value variations. The RGB colour model is photosensitive, making it useful for enhancing skin colour clustering. In medium-light and low-light regions, skin colour chrominance elements are almost independent of luminance **(Phuangsaijai, 2021)**. This means a nonlinear relationship exists between chrominance (Cb, Cr) and luminance (Y) of skin colour. Y ranges from 16 to 235, with 16 representing black and 235 representing white, while Cb and Cr are in the 16-240 range. The main advantage of the YCbCr colour model is that luminosity effects can be eliminated during image processing. A comparison was made between separate plots of Y, Cb, and Cr values for face pixels and non-face pixels to determine the Y, Cb, and Cr value ranges for face pixel resolution. **He and Luo (2019**) developed a spoof face detection approach based on local binary patterns (LBP) and the YCbCr colour model. Their method effectively captured texture and colour variations to distinguish between genuine and fake faces. The experiments were conducted on the Replay-Attack dataset, yielding commendable performance.

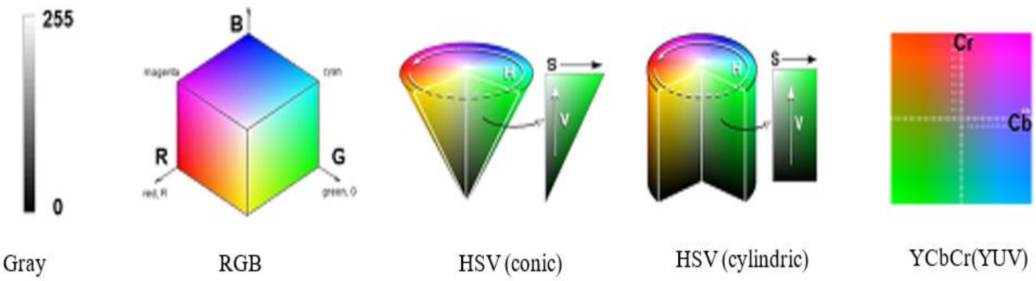

Figure 2: Colour Model

- **CIELAB Colour Model**

The International Commission on Illumination (CIE) proposed the CIELAB colour space in 1975 as a standard for colour use. The utilisation of the CIELAB colour model has gained prominence in recent studies on fake face detection. The CIELAB colour model was developed to mimic human perception of colour and is known for being device-independent and perceptually uniform. It comprises three constituents: L, a, and b, symbolizing lightness, green-red, and blue-yellow channels, respectively. This color model has been integrated into research concerning the detection of counterfeit faces, exemplified by the study conducted by **Hemajothi et al. (2019).** In this investigation, the scholars introduced a framework that amalgamated a pre-trained deep convolutional neural network with CIELAB color texture analysis. The objective was to harness color-based attributes extracted from genuine and fabricated facial images utilizing the CIELAB color model, with the aim of capturing subtle chromatic deviations that indicate manipulated faces. The experimental outcomes underscored the efficacy of integrating CIELAB color texture analysis into the realm of fake face detection, yielding heightened accuracy in comparison to conventional pixel-level scrutiny. This study underscores the potential of harnessing the CIELAB color model to amplify the dependability and resilience of algorithms designed for detecting fraudulent faces.

3 Proposal Approach

The outlined approach for detecting counterfeit faces can be dissected into four principal elements. Initially, facial images from the dataset undergo preprocessing to render them amenable to feature extraction. Subsequently, color texture attributes are employed to extract features. The conclusive phase employs a CNN classifier to ascertain the authenticity of a given face (Mansouri, S., 2025). A visual representation of the procedure is depicted in **Figure 3.**

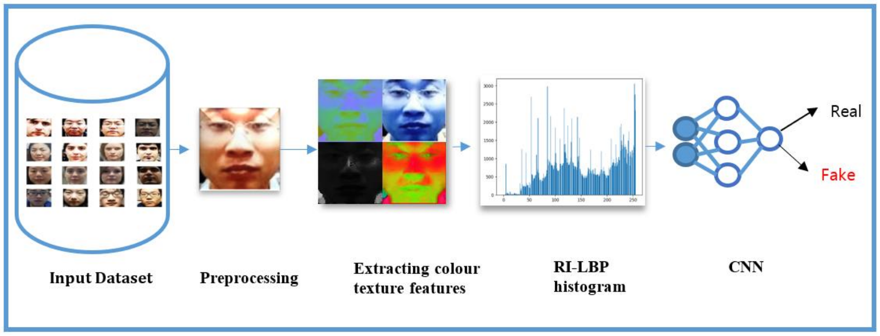

Figure 3: Visual Representation of the Approach

Dataset

This study employed the MSU MFSD database, as introduced by **Wen et al. (2015).** This publicly accessible dataset serves as a means to evaluate anti-spoofing techniques for facial recognition. Comprising 280 videos from 35 users subjected to photo and replay attacks, the database is bifurcated into training and testing sets, encompassing 15 and 20 instances, respectively. The database encompasses two categories of spoofing attacks: photo attacks and video replay attacks. Within each category, eight videos are present – two authentic and six fraudulent.

Preprocess the Face Images

In preparation for further analysis, a sequence of preprocessing procedures is implemented on the face images. The first stage of the process entails the utilisation of the Viola-Jones method, as employed by **AlKishri (2022),** for the purpose of detecting the face region within the datasets, including spoofing instances. This algorithm is renowned for its proficiency in face detection tasks and aids in pinpointing the exact facial area in each image. In order to enhance the alignment of face frames, we employed the Local Binary Features (FPS-LBF) technique, which is similar to the approach utilised by **Ren et al (2014).** This technique utilises a collection of 68 critical points to effectively find the facial area and extract correct facial pictures. Notably, FPS-LBF incorporates the retention of specific facial background frames to enhance the overall detection performance of the algorithm. This retention preserves certain facial background details, imbuing the method with robustness and the capacity to discern subtle variations in facial features. For consistency and streamlined analysis, the facial images are normalised to a standardised dimension of 64 x 64 pixels. This normalisation entails resizing the images to a uniform resolution, eliminating any inconsistencies in size across the dataset. This process facilitates efficient processing and seamless comparison of images during the subsequent stages of the fake face detection pipeline. The collective preprocessing stages, encompassing the Viola-Jones algorithm for face detection, the employment of the FPS-LBF method for meticulous facial alignment, and the normalisation of images to a consistent 64 x 64-pixel size, synergise to enhance the data's quality and suitability for subsequent analysis. By precisely identifying and aligning facial regions while standardising image dimensions, the ensuing phases of the fake face detection process can adeptly exploit the preprocessed images to extract pertinent features and classify them as authentic or manipulated.

Extract Colour Texture Features

The rotation-invariant local binary pattern, denoted as RI-LBP, is cited as the Chen et al. (2019) method in equation (1). It is a texture descriptor that will be applied to the dataset to extract features. Local

Binary Pattern (LBP) and RI-LBP are similar, but RI-LBP is more robust because it is rotation-invariant. Also, it works well for detecting fake faces. Instead of the uniform LBP, we use the RILBP operator to pull out features of a material. For a pixel (x, y) from a picture, the RI-LBP operator can be written like this:

$$LBP_{R,P}(x,y) = \begin{cases} \sum_{n=0}^{P-1} \partial(r_n - r_c) & if\ U \leq 2, \\ P+1 & otherwise, \end{cases} \quad (1)$$

$$U = |\partial(r_{P-1} - r_c) - \partial(r_0 - r_c)| + \sum_{n=1}^{P} |\partial(r_n - r_c) - \partial(r_{n-1} - r_c)|, \quad (2)$$

and

$$\partial(X) = \begin{cases} 1\ x \geq 0, \\ 0\ x < 0. \end{cases} \quad (3)$$

Equation (1) outlines the LBPR, P(x,y) equation, embodying the RI-LBP operator. This equation calculates the disparity between the intensity value of individual pixels encircling the central pixel and the intensity value of the central pixel itself. The outcomes of these calculations undergo thresholding using parameter U, as defined in equation (2), contingent upon the radius R and the pixel intensity values. The product of this operation is a binary code capturing the texture nuances of the central pixel and its neighboring ones. Subsequently, this binary code undergoes transformation into a histogram that tallies the incidence of each binary pattern, thereby encoding the image's texture attributes. Within this study, the RI-LBP operator is implemented on the M channel of the designated color space (HSV, YCbCr, RGB) to extract texture features. The resulting histogram from the RI-LBP operation is denoted as HS(i), where i ranges from 1 to M. These RI-LBP texture characteristics of the image are encapsulated by the resultant histogram. The sign function, represented by δ(x) as stated in equation (3), is defined as returning a value of one when its argument x is equal to or surpasses zero; otherwise, it yields zero. This function is instrumental in equations (1) and (2) for executing thresholding operations and determining whether a pixel's value should contribute to the ensuing binary code or not.

CNN Classifier

After the completion of the preprocessing stage, the subsequent phase entails the training of a Convolutional Neural Network (CNN) classifier with the objective of distinguishing between real and fake facial images. Convolutional Neural Networks (CNNs) are highly suitable for the task of image categorisation due to their ability to successfully learn intricate characteristics through the use of convolutional layers and pooling layers. The Convolutional Neural Network (CNN) architecture has been specifically devised to effectively transform input images into a feature space characterised by a large number of dimensions. The convolutional layers facilitate the process of local feature extraction by employing filters to collect patterns and visual signals present within the images. The use of these filters aids the neural network in discerning distinctive characteristics that differentiate real and fake facial images. Pooling layers are included into the network architecture to perform down-sampling of the feature maps, therefore decreasing their spatial dimensions while retaining the crucial information. This procedure facilitates the reduction of computational complexity and the extraction of dominating characteristics. During the training process, the Convolutional Neural Network (CNN) classifier undergoes optimisation to determine the decision boundary that effectively distinguishes between real and fake facial images. The optimising process involves reducing the binary cross-entropy loss function. The loss function measures the disparity between the expected probabilities and the actual labels, guiding the network to enhance its performance over successive rounds. Rectified Linear Unit (ReLU) activation functions are frequently employed in convolutional and pooling layers to incorporate nonlinearity and augment the model's ability to grasp intricate correlations. The Rectified Linear Unit (ReLU) activation function is designed to transform negative values to zero while preserving positive values. This characteristic of ReLU aids in enhancing the network's ability to capture complex patterns and nonlinear relationships that exist within the dataset. In the final classification stage, a dense layer is utilised, which is equipped with a sigmoid activation function. The sigmoid function is utilised to compress the output of the last layer, constraining it inside the interval of 0 and 1. This compressed output signifies the likelihood that the input picture is classified as belonging to the actual face category. The output of the model is interpreted as the probability of a picture being authentic, facilitating a binary classification task. **Table 1** displays an illustrative design of a Convolutional Neural Network (CNN) classifier.

Table 1: CNN Classifier Design

Conv2D	32 filters of size 3x3	ReLU
maxPooling2D	pool size of 2x2	ReLU
Conv2D	64 filters of size 3x3	ReLU
MaxPooling2D	pool size of 2x2	ReLU
Dense layers	single	sigmoid

Ethics

The experiment will adhere strictly to the principles and guidelines set forth by ethical standards. The dataset utilised in this research comprises authentic photographs and videos of real individuals, ensuring the preservation of privacy and consent. It is of utmost importance that the outcomes of this experiment are solely intended for academic study, with no intention of causing harm to individuals or any particular groups. To assess the efficacy of face anti-spoofing methods, the MSU MFSD database will be employed as a publicly available benchmark dataset. This dataset allows for comprehensive testing and evaluation while maintaining transparency and accessibility within the scientific community. By utilising such standardised resources, the experiment aims to ensure the reliability and reproducibility of its findings, thereby advancing the field of face anti-spoofing technology in an ethical and responsible manner.

4 Results

In the realm of fake face detection, extracting colour texture characteristics from images and videos plays a significant role. Different colour spaces, such as RGB, YCrCb, and HSV, are commonly used to capture these features. However, the effectiveness of colour texture features in detecting facial spoofing attacks can vary depending on the colour space utilised. To address this variability, a uniform local binary patterns (LBP) operator is employed with a radius of R=1 and 8 neighbours (P=8) to extract colour texture features from the primary colour spaces. The LBP operator computes the local texture patterns in the images, which can help capture the subtle variations indicative of facial spoofing. **Table 2** showcases the comparison of the Equal Error Rate (EER) obtained from the MSU MFSD dataset, which serves as an evaluation metric for performance. A lower EER indicates better performance in differentiating between genuine and fake faces. Analysing the results, it can be observed that the YCbCr colour space yields the most favourable outcomes. This is attributed to the fact that the human eye is primarily sensitive to the Y component of the video, while being less sensitive to changes in the chrominance components (Cb and Cr). Consequently, alterations resulting from subsampling the chrominance component may not be easily discernible to the naked eye. It is important to note that the success of colour texture features across various colour spaces can be influenced by the type of face spoofing attacks and the specific dataset used. Different types of attacks may have distinct characteristics that affect the performance of colour texture analysis. Similarly, the dataset employed for evaluation can impact the generalizability of the results to real-world scenarios. Opting for an appropriate colour space to extract colour texture attributes holds paramount importance in attaining precise and dependable fake face detection. The assessment performed on the MSU MFSD dataset underscores the supremacy of the YCbCr colour space over RGB, HSV, and a fusion of YCbCr and HSV. The heightened performance of the YCbCr colour space can be attributed to the human eye's heightened responsiveness to the Y component and its relatively subdued responsiveness to variations in chrominance components.

Table 2: EER% of Color LBP Descriptors on MSU MFSD Dataset

Colour space	**MSU MFSD dataset**
RGB	10
YCbCr	3.9
HSV	6.1
YCbCr + HSV	4

Table 3: EER% Results for RI-LBP Texture Descriptors on MSU MFSD Datasets

Texture descriptor	**MSU MFSD datasets**
RI-LBP	3.2

When considering the domain of fake face detection, the incorporation of texture descriptors holds significant sway over algorithm performance. As displayed in **Table 3**, the efficacy of the Rotation Invariant Local Binary Patterns (RI-LBP) texture descriptor is unveiled within the context of the MSU MFSD dataset. Evaluated through the Equal Error Rate (EER%) metric, RI-LBP yields an EER% of 3.2, underscoring its capability in extracting distinctive texture attributes for the identification of facial spoofing. Although RI-LBP stands as a potent texture descriptor, alternative strategies have been explored to enhance performance regarding rotation and grayscale invariance while retaining feature distinctiveness. One such avenue is the Improved Local Binary Patterns (I-LBP). Yet, within the scope of facial spoofing detection, RI-LBP demonstrates superior prowess in encapsulating pertinent texture details. In a bid to further gauge the potency of the proposed approach, **Table 4** furnishes a comparison of outcomes from various studies conducted on the MSU MFSD dataset, with EER% serving as the measuring yardstick once again. The employment of the Color LBP texture descriptor in one study yielded an EER% of 10.6, while another study integrating color texture attributes secured an EER% of 4.9.

In contrast, our method achieved the lowest EER% of 3.2, displaying superior performance in detecting facial spoofing compared to other approaches. These outcomes emphasize the significance of adeptly choosing texture descriptors for fake face detection duties. RI-LBP, the texture descriptor utilized, effectively captures nuanced texture changes associated with facial spoofing. By surpassing alternative methods in EER%, our proposed approach underscores its potential to attain remarkable precision and resilience in identifying manipulated faces.

Table 4: Contrast Findings with other MSU MFSD Studies (EER%)

Study	**Result**
Colour LBP (Boulkenafet, 2015)	10.6
colour texture (Boulkenafet, 2016)	4.9
proposed method	3.2

5 Conclusion

In conclusion, the escalating prevalence of digitally manipulated images underscores the pressing need for sophisticated and dependable fake face detection techniques. This paper introduces an innovative strategy for identifying counterfeit faces by synergising Convolutional Neural Networks (CNNs) with rotation-invariant local binary patterns (RI-LBP). The method involves extracting colour texture attributes via the RI-LBP operator, which is adept at capturing rotation-invariant local patterns. This operator effectively encodes image texture, facilitating the detection of subtle alterations indicative of a fake face. The incorporation of these RI-LBP features into a CNN classifier empowers the system to discern between authentic and fake faces. CNN's capacity to learn intricate hierarchies and recognise intricate patterns within the feature domain elevates the precision and robustness of the detection process. By fusing RI-LBP with CNNs, this approach holds promise for fake face detection, uniting colour texture analysis and deep learning techniques. Capitalising on distinct traits of manipulated faces while harnessing CNN's prowess in feature extraction and classification, this approach effectively tackles challenges posed by evolving image modification techniques. It is noteworthy that while this technique exhibits promising outcomes, the realm of fake face detection is evolving, necessitating further research to refine detection methods' accuracy and efficiency. Moreover, employing comprehensive and diverse datasets for training and testing is pivotal to ensuring the proposed approach's applicability and effectiveness in real-world contexts.

In summary, the fusion of CNNs and rotation-invariant local binary patterns (RI-LBP) establishes a sturdy framework for fake face detection. This method presents a promising solution to combat the escalating issue of image manipulation, upholding the authenticity of digital platforms and shielding individuals from the exploitation of manipulated visuals. Ongoing exploration in this domain will drive the advancement of sophisticated and dependable fake face detection techniques, countering the ceaselessly evolving complexities of digital image manipulation.

References

[1] AlKishri, W., & Al-Bahri, M. (2021). Object Recognition for Organizing the Movement of Self-Driving Car. *International Journal of Computation and Applied Sciences IJOCAAS*, *10*(1), 1-8.

[2] AlKishri, W., Abualkishik, A., & Al-Bahri, M. (2022). Enhanced image processing and fuzzy logic approach for optimizing driver drowsiness detection. *Applied Computational Intelligence and Soft Computing*, *2022*.

[3] Alkishri, W., Setyawan, W., Yousif, J.H., & Al-Bahri, M. (2023). Deepfake Image Detection Methods Using Discrete Fourier Transform Analysis And Convolutional Neural Network. *Journal of Jilin University (Engineering and Technology Edition)*, *42*(2).

[4] Boulkenafet, Z., Komulainen, J., & Hadid, A. (2015). Face anti-spoofing based on color texture analysis. *In IEEE international conference on image processing (ICIP)*, 2636-2640.

[5] Boulkenafet, Z., Komulainen, J., & Hadid, A. (2016). Face spoofing detection using colour texture analysis. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1818-1830.

[6] Boulkenafet, Z., Komulainen, J., Li, L., Feng, X., & Hadid, A. (2017). OULU-NPU: A mobile face presentation attack database with real-world variations. *In 12th IEEE international conference on automatic face & gesture recognition (FG 2017)*, 612-618.

[7] Chen, F.M., Wen, C., Xie, K., Wen, F.Q., Sheng, G.Q., & Tang, X.G. (2019). Face liveness detection: Fusing colour texture feature and deep feature. *IET Biometrics*, *8*(6), 369-377.

[8] Crowley, J.L. (2021). Convolutional neural networks. In *ECCAI Advanced Course on Artificial Intelligence*, 67-80. Cham: Springer International Publishing.

[9] Dhivakar, B., Sridevi, C., Selvakumar, S., & Guhan, P. (2015). Face detection and recognition using skin color. *In IEEE 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, 1-7.

[10] Gupta, M., & Tripathy, B.K. (2023). Artificial Intelligence-Based Behavioral Biometrics. *Encyclopedia of Data Science and Machine Learning*, 887-898.

[11] He, J., & Luo, J. (2019). Face Spoofing Detection Based on Combining Different Color Space Models. *In IEEE 4th International Conference on Image, Vision and Computing (ICIVC)*, 523-528.

[12] Hemajothi, S., Abirami, S., & Aishwarya, S. (2020). A Novel Colour Texture Based Face Spoofing Detection Using Machine Learning. *Acta Technica Corviniensis-Bulletin of Engineering*, *13*(2), 47-52.

[13] Holmqvist, K., Örbom, S.L., & Zemblys, R. (2022). Small head movements increase and colour noise in data from five video-based P–CR eye trackers. *Behavior Research Methods*, *54*(2), 845-863.

[14] Khanam, R., Johri, P., & Diván, M.J. (2022). Human Skin Color Detection Technique Using Different Color Models. *Trends and Advancements of Image Processing and Its Applications*, 261-279.

[15] Mansouri, S. (2025). Application of Neural Networks in the Medical Field. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 14(1), 69-81.

[16] Moreira, G., Magalhães, S.A., Pinho, T., dos Santos, F.N., & Cunha, M. (2022). Benchmark of deep learning and a proposed hsv colour space models for the detection and classification of greenhouse tomato. *Agronomy*, *12*(2), 1-23.

[17] Phuangsaijai, N., Jakmunee, J., & Kittiwachana, S. (2021). Investigation into the predictive performance of colorimetric sensor strips using RGB, CMYK, HSV, and CIELAB coupled with various data preprocessing methods: a case study on an analysis of water quality parameters. *Journal of Analytical Science and Technology*, *12*(1), 1-16.

[18] Ren, S., Cao, X., Wei, Y., & Sun, J. (2014). Face alignment at 3000 fps via regressing local binary features. *In Proceedings of the IEEE conference on computer vision and pattern recognition*, 1685-1692.

[19] Venkatesh, S., Ramachandra, R., Raja, K., Spreeuwers, L., Veldhuis, R., & Busch, C. (2019). Morphed face detection based on deep color residual noise. *In IEEE Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 1-6.

[20] Wen, D., Han, H., & Jain, A.K. (2015). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746-761.

Authors Biography

Mrs. WASIN ALKISHRI is a PhD candidate and researcher in computer vision and image processing. A lecture at an Arab Open University - OMAN. She holds a master's degree. And BA in Computer Science. She has experience in various courses in the field of computer science—extensive knowledge of computer vision and image processing. Actively participate as a speaker in international and local conferences and professional research.

Dr. Setyawan Widyarto is an Associate Professor of Industrial Computing. He has Sarjana's Certificate (IPB, Bogor), Masters (University of Bradford, England), PhD (UTM, Malaysia). He is the Dean of the Department of Computing, School of Communication, Visual Arts, and Computing. His areas of research expertise are (Modeling and Simulation, Digital, Image Processing, Computer Science, and Systems Engineering and Management).

Dr. Jabar H. Yousif is an Associate Professor at the Faculty of Computing and Information Technology at Sohar University. He completed his postdoctoral work on computer graphics and virtual/augmented reality at the National University of Malaysia (UKM) in 2007–2008. He earned a PhD in Artificial Intelligence and Natural Language Processing from the Faculty of Information Science and Technology, National University of Malaysia (UKM) in 2007.

Dr. Mahmood Al-Bahri is an assistant professor at Sohar University with five years of experience teaching undergraduate and graduate courses in Info- communication and computer science. Extensive knowledge of the Fourth Industrial Revolution technologies. Author of the Internet of Things books in Arabic Language. Actively participate as a speaker in international and local conferences and professional research. Believe in students' learning abilities and inherent thirst for knowledge in the right environment. Actively work to connect students to their material to transform lives.