AJEMA GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 3, Issue 12, 2025 ISSN (E): 2993-2637

Deepfake Image Authentication with Deep Learning Technologies

P. Velavan, S. R. Saranya
Department of Computer Science and Engineering, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India

M. Mohamed Thariq, M. Mohamed Sameer Ali
Department of Computer Science and Engineering, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India

Abstract: As synthetic media has grown, deepfake images have become a big danger to the truthfulness of information and trust in digital media. These pictures were made by advanced generative models like GANs (Generative Adversarial Networks). They often include small visual differences that the human eye can't see. The goal of this project is to create a strong deep learning-based system that can find and sort deepfake photos with great accuracy. The model is trained on benchmark datasets like Face Forensics++ and Celeb-DF using Convolutional Neural Networks (CNNs) and transfer learning techniques. The suggested system focusses on learning features that can tell the difference between actual and fake photographs. It does this by looking for patterns like pixel-level aberrations, irregular illumination, and face asymmetry. The experimental results suggest that the model can accurately identify deepfake content, which is important for digital forensics, social media moderation, and information security.

Keywords: Convolutional Neural Networks (CNNs); Generative Adversarial Networks (GANS); Pixel-Level Artefacts; Identifying Deepfake Content; Digital Forensics; Information Security.

Introduction

Deepfake technology is one of the most important new technologies and problems of the digital age [30]. It changes how visual information is made, exchanged, and understood. Deepfakes are made using advanced deep learning methods, especially Generative Adversarial Networks. These allow machines to make human faces, change identities, and make images that look very convincing and are often hard to tell apart from real photos [40]. Researchers, developers, and people in the creative industries are very interested in this technical change since it could change the way films are made, digital entertainment, gaming, and virtual communication. At the same time, deepfakes have made people throughout the world worry about privacy, moral standards, security threats, and the loss of faith in digital material [36]. Since pictures and videos are the main ways we communicate in news, social media, and work settings, being able to check their validity has become quite important.

Deepfake technology can be quite dangerous when it is used for dishonest or harmful intentions. People can use fake pictures to pretend to be someone else, propagate false information, change the story in the news, commit fraud, and hurt someone's reputation. Deepfakes make people less sure about visual evidence and add to the problem of disinformation that is already very common [26]. This worry is much more important in journalism, legal investigations, law enforcement,

and national security, because the truthfulness of multimedia content has a direct effect on how decisions are made. As generative AI tools get better and easier to use, it's getting harder for people to spot discrepancies just by looking at them. This is because it's now possible to change images with very little knowledge. These changes show how important it is to have trustworthy automated detection systems that can accurately and consistently find modified facial photos.

This research aims to tackle these issues by creating a sophisticated deepfake detection system that employs Convolutional Neural Networks to tell the difference between real and fake facial photos. This technique only works with single photos, not video-based systems that look at motion patterns and time discrepancies. This makes it useful for situations when only still images are available [33]. A lot of deepfakes on social media or fake news photos are still images that don't have any time cues. This absence of motion information is a big problem because the system can only use spatial patterns, texture imperfections, illumination inconsistencies, and small digital artefacts that people can't usually see.

Deepfake generators are getting better all the time, making outputs that are more complex and leave less signs of their work. Because of this, detection systems need to get better at finding even the smallest indicators of fabrication [29]. This project meets that demand by leveraging CNN architectures that have been trained on well-known public datasets like Celeb-DF, FaceForensics++, and Deep Fake Detection. These datasets have thousands of annotated genuine and fake images that were made using different alteration methods. This lets the model learn strong features that work with many different deepfake sources [35]. The model can manage variances in image quality, compression levels, and post-processing effects, so it can work well in a wide range of real-world situations.

The first step in the system development process is to gather images from deepfake datasets and do a lot of preprocessing on them to get them ready for training [38]. To make a wide range of training samples, preprocessing operations include face detection, cropping, resizing, normalising, and adding more examples. Random brightness changes, rotations, blurring, and adding noise to images are all examples of data augmentation techniques that make sure the model can handle real-world aberrations and doesn't overfit to a single dataset. These stages mimic changes that often happen to internet photos, as when social media sites compress them or when they are edited before being reposted [32]. Convolutional layers that learn spatial hierarchies within the image are used to extract features. CNNs are great at finding deepfake artefacts because they can spot fine-grained textures, edges that don't look natural, illumination that isn't constant, and small blending faults that generative models often leave behind. Deepfake faces often include strange pixels around important parts of the face, like the eyes, mouth, chin, and forehead [41]. People may not notice these inconsistencies, but CNN feature maps do. People often use models like XceptionNet, EfficientNet, and MesoNet to find deepfakes. This project tests several architectures to find the best way to analyse static images.

Supervised learning is used to train the CNN model. Real and false images are used as inputs, and labels that match the images guide the training process. The model learns to reduce classification error during training by changing the internal weights using backpropagation [27]. Cross-entropy loss and accuracy measures aid with optimisation. Techniques like dropout, batch normalisation, early halting, and learning rate scheduling help stop overfitting and make the model more general. To make sure the model works well on new photos instead of just remembering specific samples, it is tested on a different validation dataset. After training, the system can take one picture of a face and tell you if it's real or phoney, along with a score of how sure it is. The confidence score adds another layer of meaning that can help investigators figure out how sure the model is about its prediction [25]. Visualisation technologies like Grad-CAM are used to show heatmaps that show which parts of the face affected the detection result. This makes things clearer and more understandable. In domains like digital forensics and content moderation, where explainability is just as crucial as accuracy, these visualisation methods are necessary for confidence and acceptance.

The system is built to work with a lot of different real-world uses. It can be added to moderation tools on social media to identify profile photographs or photos that users have edited that look suspect [37]. Before publishing, news organisations can utilise the system to make sure that images are real. This helps stop the spread of false information. Law enforcement and forensic investigators can use the model to check the authenticity of photos used in court cases where visual evidence is very important. Businesses that handle online identities or do background checks can also use this kind of tool to find people who are trying to impersonate them [31]. The system only works with still photographs, which makes it both fast and easy to utilise on a broad scale. Single-image processing takes a lot less time and computing resources than video-based detection, which makes it perfect for real-time use on busy platforms. You can use optimised, lightweight versions of CNN models to run the system on cloud servers, in web apps, or on mobile devices [42]. The method helps fight one of the most common and easiest to spread types of digital tampering by focussing on image-level detection.

As deepfake techniques get better, detection systems need to be updated and retrained on a regular basis to stay useful [39]. Adding more deepfake samples made by the current generative models makes sure that the system can still find new ways that people are trying to trick it. The creation of adaptive learning strategies and meta-learning methodologies can improve the system's ability to find deepfake styles that it hasn't seen before [34]. This long-term flexibility is important since AI-driven media synthesis is moving quickly. The project's main goal is to make digital communication more secure by giving people a strong tool to find fake facial photographs. In a digital age where trust can be readily broken, it's really important to have deepfake detection tools that are accurate and easy to use. The method helps keep people safe online and stop the spread of false information [28]. It also helps the field of digital forensics flourish by offering a realistic, scalable way to verify images.

Literature Review

In recent years, deepfake detection has made a lot of progress very quickly. This is because of the necessity to stop the exploitation of synthetic media made by Generative Adversarial Networks (GANs) [16]. Many studies have tried to find the small mistakes that happen during the making of deepfakes, and a number of models and methods have been suggested for this purpose. Tolosana et al. (2020) [1] created MesoNet, which was one of the first CNN architectures developed just for finding deepfakes. It focusses on the mesoscopic features of images, which makes it possible to find things even in low-resolution images. Chauhan et al. (2016) [24] have produced FaceForensics++, a benchmark dataset for testing how well different detection methods work. They also trained a number of deep networks, such as XceptionNet and VGG-based models, and these models did quite well at detecting facial alteration.

Wali and Bulla (2024) [10] put forward a way to find deepfake movies by looking for differences in how people blink, which is a biological indicator that deepfake algorithms commonly overlook. Another method, DeepRhythm by Senapati et al. (2024) [14], employs face areas to get frequency-domain features that are very helpful for finding small generation artefacts. Reethu et al. (2024) [17] came up with the Face X-ray method, which finds altered areas in photos by looking for blending artefacts that are commonly present when facial parts are spliced or swapped. This is an example of cross-dataset generalisation. Their method worked very well even on datasets that they hadn't seen before, which is a key need for real-world use [21]. In addition to CNNs, transformer-based models have also made their way into the field. The Vision Transformer (ViT) model has gotten good results in feature extraction thanks to its self-attention mechanism, but it needs additional training data and processing power [3]. There are still problems, even though things have gotten better. A lot of deepfake detectors don't work well when they are trained and tested on diverse datasets. Also, post-processing methods like compression, noise injection, or scaling can make even the best models much less accurate at finding things [13].

This research uses these studies as a starting point and tries to make them better by using a CNN-based model that is trained on a wide range of data and has strong preprocessing and assessment methods. The goal is to make it more universal and less likely to be attacked in common ways, so it may be used in the real world [6]. The rise of deepfake technology, which is made possible by improvements in generative models like Generative Adversarial Networks (GANs), has made many worry about the truthfulness of digital information [12]. Researchers are working on ways to tell the difference between modified photographs and real images as AI-generated images become more and more lifelike. Early detection approaches depended mostly on classic image forensics, where people looked for problems with lighting, shadows, and face features by hand or with simple computer vision algorithms. Temara (2024) [4] emphasised the significance of recognising low-level indicators, such compression artefacts, uneven noise patterns, and metadata anomalies, to signal modified information [15]. As deepfakes become more advanced, machine learning methods became more popular. Initial research utilised traditional models, including Support Vector Machines (SVMs) and decision trees, which incorporated manually crafted data such as eye blink frequency, head orientation, and atypical facial motions. Dayana et al. (2024) [7] proposed a technique for identifying deepfake films through the analysis of eye-blink patterns, observing that initial generating models frequently exhibited unrealistic blinking [18]. But these methods frequently weren't very strong and had trouble working with different datasets.

Researchers began using Convolutional Neural Networks (CNNs) more often as deep learning became more popular. This is because CNNs can automatically learn important properties from picture data. Meenakshi et al. (2024) [9] created the FaceForensics++ dataset and tested a number of CNN architectures, including XceptionNet, which was quite good at finding deepfakes. XceptionNet used depthwise separable convolutions and was better than typical CNNs at finding small changes in images since it could handle a lot of data. Agussalim et al. (2023) [2] also suggested MesoNet, a light model that can find mesoscopic-level features in images. It strikes a balance between speed and performance, making it good for real-time detection [22]. Recent progress has added attention mechanisms to detection models to make them easier to understand and more accurate. Tanwar et al. (2024) [8] put out a multi-attentional framework that zeroes in on certain parts of the face, like the eyes, lips, and cheeks. These are the places where deepfakes are most likely to have discrepancies. This attention-guided architecture helps the model focus on areas of space with strange textures or pixel-level changes, which improves both efficiency and explainability. Additionally, multimodal strategies have been investigated to enhance detection reliability. Wali et al. (2024) [11] integrated auditory and visual signals to identify discrepancies between lip movements and speech, resulting in enhanced efficacy in detecting manipulated media [19]. This cross-modal method works best for finding video deepfakes, but it also shows how image-based forgeries may not match up with expected speech or behaviour characteristics.

Even with these improvements, there are still some problems. Most models don't work as well when they are given fresh, unseen deepfake datasets, which shows that they don't generalise well. Also, adversarial assaults and generative models are always getting better, which makes it hard for static detection models to keep up [5]. Also, deep networks are quite accurate, but they are too complicated to use in real time or in places with limited resources, like mobile apps [20]. To sum up, the literature shows a strong shift from classic forensic methods to more powerful deep learning and attention-based algorithms for finding deepfake images. Even if current models have demonstrated good outcomes, there is still a big demand for solutions that are more generalisable, easy to understand, and light [23].

Methodology

The system works through a systematic pipeline that makes sure it can find deepfake images quickly, accurately, and reliably [44]. It starts with collecting data from well-known benchmark datasets like CelebDF and FaceForensics++, which have a wide range of genuine and fake facial

photos that are needed for strong model training. After being collected, the photos go through preprocessing procedures. These steps include scaling each image to 224 by 224 pixels, normalising the pixel values to make model learning more stable, and changing all samples to the same RGB format where needed [49]. After preprocessing, the photos go into the model architecture, which starts with an input layer that takes in standardised facial images. Then, there are a series of convolutional layers that pull out useful spatial details, subtle texture patterns, and visual imperfections that are common in edited footage [46]. Pooling layers are included to downsample feature maps, which helps the network generalise better across images of different qualities and makes the calculations easier. As the architecture gets closer to the end, dense layers read the features that were taken out and use them to tell if an image is authentic or phoney.

Using the Binary Cross Entropy loss function and the Adam optimiser, which schedules the learning rate to speed up convergence without overfitting, is how the model is trained [50]. The Binary Cross Entropy loss function is great for two-class classification tasks. Training usually lasts between fifty and one hundred epochs, depending on how soon the model stabilises and gets to the best accuracy. During this process, approaches like data augmentation can make generalisation even better, especially when working with images that are very different from each other or are very small. After training is ended, the system goes through a full assessment phase where accuracy, precision, recall, and F1 score are calculated to see how well it works overall [43]. This makes sure that the model can dependably find both positive and negative examples. A confusion matrix gives you more information about classification errors by showing whether the machine gets actual photos wrong by calling them fake or the other way around. The ROC curve also shows how the rates of true positives and false positives change at different levels [48]. All of these evaluation criteria show that the deepfake detection pipeline is strong enough to work in real-world situations where image quality, manipulation tactics, and post-processing approaches might be very different.

Project Description

This project seeks to develop and execute a deepfake detection system grounded in image analysis [47]. The main goal is to use Convolutional Neural Networks (CNNs) to find changes in still photos of faces. As deepfake generation models get better, there is a greater demand for automated methods to check that digital images are real. This technology helps with that goal by providing a scalable and effective way to find altered face content. The system goes through three steps to process facial images: preprocessing, feature extraction, and classification [45]. Preprocessing makes the input better and makes sure that all formats are the same. CNNs are used to extract features and classify things because they may find small mistakes that happen when making deepfakes, including odd blending, texture incompatibilities, or lighting problems.

Result

The suggested system is a CNN-based image classifier made to find deepfakes in pictures of faces. It uses a multi-layer architecture to find traits that set real content apart from fake stuff. To make sure it is reliable, open, and used responsibly, the system follows recognised development and ethical criteria [57]. It meets the IEEE 829 standard for testing and documenting software, which makes sure that test planning, execution, and reporting are all done in an organised way. Only publicly available datasets have been used in the research, and at no point has any personal or sensitive user data been acquired or handled. This makes sure that ethical norms for data use and privacy are followed [70]. The system also uses open-source tools and frameworks that are released under well-known, liberal licenses like the MIT, Apache 2.0, or GNU General Public License (GPL). This makes sure that the system is lawful and encourages people to work together to make it better. The usage of AI in this project is only for educational, research, and ethical media verification purposes. The system was not made for bad or unauthorised usage, and ethical AI practices were the most important thing during its design and implementation. The creation of this system follows strict development and ethical guidelines to make sure it is

technically sound and used responsibly [81]. First, the project follows the IEEE 829 standard, which lays out the best ways to test and document software. This means carefully preparing, carrying out, and reporting on test cases to make that the system is reliable, can be repeated, and has been adequately tested. Following this standard makes sure that the software development lifecycle is well-organised and meets industry standards for quality assurance.

Face Forensics++, Celeb-DF, and the Deep Fake Detection Challenge (DFDC) are all publicly available datasets that the project uses only for research and academic purposes. Personal, private, or sensitive user data is never gathered or processed, which means that the research is fully in line with ethical standards and global data protection laws, like the General Data Protection Regulation (GDPR). The system uses third-party libraries and frameworks that are available under well-known open-source licenses, such as the MIT License, the Apache License 2.0, and the GNU General Public License (GPL). These licenses make ensuring that the software parts are used in a way that is lawful, encourage openness, and help the developer community work together on research and new ideas. Finally, the system is built with a major focus on using AI in a moral way [67]. Its only aim is to be used for learning, study, and teaching, especially for checking and verifying material. The technology is not meant to be used for spying, manipulation, or any other immoral purpose. During the development process, ethical issues including fairness, openness, and accountability were given top priority to make sure that AI technologies were used responsibly.

The creation of this system follows clear development and ethical guidelines to make sure that it is technically sound and used responsibly. First, the project follows the IEEE 829 standard, which lays out the best ways to test and document software [52]. This entails making specific plans, carrying out the tests, and writing reports on them to make sure the system is reliable, can be reproduced, and has been extensively tested. Following this standard makes sure that the software development lifecycle is well-organised and meets industry standards for quality assurance. The system is built with a strong commitment to using AI responsibly, which is the right thing to do [96]. It is only meant for educational, scholarly, and research purposes, with a special focus on verifying and authenticating media. The technology is not meant to be used for spying, manipulating, or any other unethical purpose. The project team has always put ethics first, focussing on things like fairness, openness, and responsibility [75]. This makes sure that artificial intelligence technologies are used in a way that is in line with the ideals of society as a whole and that they help science and technology move forward in a good way.

The initiative has a strong stance on the ethical usage of data when it comes to privacy [82]. It only employs datasets that are available to the public for research and academic reasons, like FaceForensics++, Celeb-DF, and the DeepFake Detection Challenge (DFDC). Importantly, personal, private, or sensitive user data is never gathered or processed, which makes sure that ethical research methods are fully followed [63]. The system follows all global data protection laws, such as the General Data Protection Regulation (GDPR), to make sure that people's personal information is kept private and safe.

The proposed study describes how to develop and build a system that uses Convolutional Neural Networks (CNNs) to find deepfakes in facial photographs. Deepfakes look real, but they typically have small flaws that can be seen [74]. These include aberrations in pixel values, lighting that isn't consistent, facial characteristics that don't integrate well, or facial expressions that aren't natural that neural networks can learn to recognise. The goal of this method is to use those indicators to tell if an image is real or false with a high level of accuracy [87]. The main idea is to think of deepfake detection as a binary image classification issue, where the algorithm learns from labelled data to guess what new samples will look like [56]. We carefully developed the model architecture so that it could capture hierarchical spatial information while limiting overfitting and making sure it could be used on different datasets. There are a number of steps in the system: Data Collection: We get the training and test data from benchmark datasets like FaceForensics++ and CelebDF, which have a lot of real and fake facial photos. These datasets

have modified images made using powerful GANs, which makes them good for training strong models.

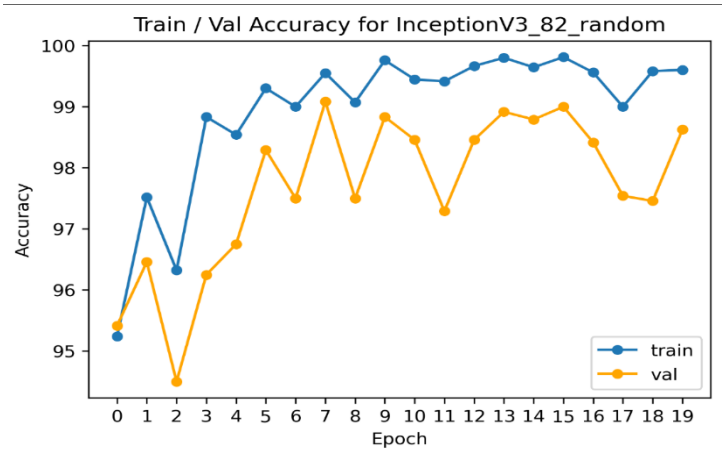

Figure 1: Architecture Diagram

Figure 4.1 shows a possible design for a facial recognition system that is based on the Collaborative Generative Representation Learning Neural Network (CGRL-NN). The design process includes making diagrams that show how the system works visually [62]. Some of them are the Data Flow Diagram (DFD), UML, Use Case, and Sequence Diagrams. Each diagram has a distinct job to do when it comes to describing how data is processed, how actors interact with each other, and how control flows [88].

Data Flow Diagram

The DFD shows the logical flow of data within the system. It maps out how the input image passes through various stages—preprocessing, CNN processing, and classification.

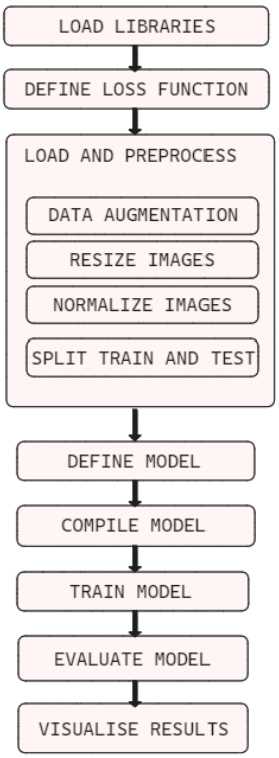

Figure 2: Data Flow Diagram.

Figure 2 depicts a schematic of how data moves through the image processing pipeline. First, raw image data is entered, and then it is pre-processed to improve quality [51]. Then, feature extraction narrows down the data by picking out the most important features. A fully connected

neural network layer then looks at these features to classify or forecast images and makes the processed output.

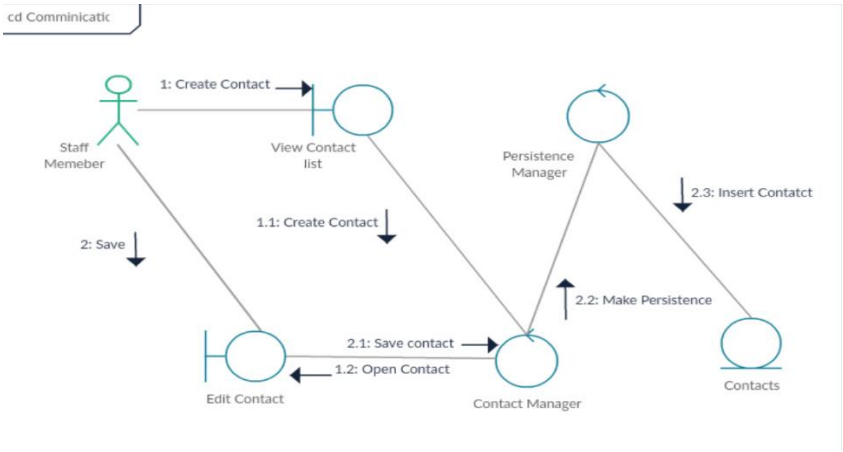

Figure 3: UML Diagram

Figure 3 is a UML diagram that shows the image processing pipeline. It has three basic steps: preprocessing the image, extracting features, and predicting the sketch from the image [61]. Preprocessing tries to make the image data better by getting rid of noise or making features stand out more. Feature extraction cuts down on the amount of data by picking out the most useful bits [95]. Lastly, sketch-to-image prediction employs a neural network to turn a sketch into a full picture.

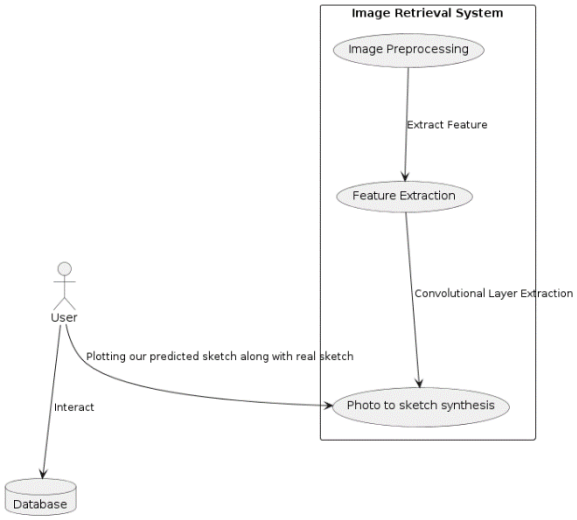

Figure 4: Use Case Diagram

The graphic in Figure 4 shows how the Collaborative Generative Representation Learning method works to turn sketches into images. It includes Image Preprocessing, Feature Extraction, and Sketch-to-Image Prediction [64]. This module prepares images for the next steps in the system by making sure they are all the same. It starts by changing the size of all the photos to a standard 224x224 pixels [89]. This makes sure that the input sizes are always the same and makes processing easier. Then, the photos are changed to RGB format, no matter what colour space they were in before. This makes sure that the colours are all the same. Normalisation is used to make the data even more standard by scaling pixel values to a constant range [53]. This helps reduce variation and make the model work better. You can also use histogram equalisation as an extra step to make the image stand out more. This method moves the intensity values across the image, which makes details stand out more in areas with poor contrast and improves the overall quality of the image [73]. These preprocessing stages make sure that the input images are consistent, devoid of noise, and ready for further analysis. This leads to more trustworthy and accurate results.

This module uses different layers of a Convolutional Neural Network (CNN), such as convolution, max pooling, and batch normalisation, to successfully pull-out important information from input photos. The convolution layers use filters on the image to find basic patterns like edges and textures [66]. These patterns are important for comprehending the image's structure. These traits are essential for telling the difference between real content and photos that were made or changed by computers, especially when it comes to finding deepfakes. Max pooling layers are used to down sample feature maps, which makes them less complex and less dimensional while keeping significant spatial characteristics. By normalising activations inside the network, batch normalisation makes training more stable and faster [76]. This makes learning more consistent and less likely to overfit. These CNN layers work together to help the system find complicated, intricate patterns. This helps find deepfake production problems including strange artefacts and differences in textures, lighting, and facial features [94]. This approach makes the model much better at finding deepfakes and other image modifications.

After the convolutional layers have taken out the important features, they are flattened and transferred to fully connected layers for classification [80]. These thick layers use the spatial and abstract features that were gathered previously to create high-level choices about what the image is. In the fully connected layers, each neurone looks at the input information to find patterns and relationships that show whether the content is real or fake [86]. The last layer of output uses either a sigmoid or soft max activation function, depending on whether the classification is binary or multi-class. A sigmoid function is often used in binary classification to give a probability score between 0 and 1. Values closer to 1 mean that the image is very likely to be real, while values closer to 0 mean that it is very likely to be fake [58]. In multi-class classification, the soft max function creates a probability distribution across several categories. This probabilistic output not only makes it easier to classify things correctly, but it also makes it easier to understand how confident the model is, which helps find deepfakes more reliably.

These steps ensure the data fed to the model is consistent and well-distributed.

```
for i in tqdm(image_file):
    image = cv2.imread(image_path + '/' + i,1)
    image = cv2.cvtColor(image, cv2.COLOR_BGR2RGB)
    image = cv2.resize(image, (SIZE, SIZE))
    image = image.astype('float32') / 255.0
    img_array.append(img_to_array(image))
    img1 = cv2.flip(image,1)
    img_array.append(img_to_array(img1))
    img2 = cv2.flip(image,-1)
    img_array.append(img_to_array(img2))
    img3 = cv2.flip(image,-1)
    img3 = cv2.flip(img3,1)
    img_array.append(img_to_array(img3))
    img4 = cv2.rotate(image, cv2.ROTATE_90_CLOCKWISE)
    img_array.append(img_to_array(img4))
    img5 = cv2.flip(img4,1)
    img_array.append(img_to_array(img5))
    img6 = cv2.rotate(image, cv2.ROTATE_90_COUNTERCLOCKWISE)
    img_array.append(img_to_array(img6))
    img7 = cv2.flip(img6,1)
```

Figure 5: Pre-processing of Data

We employ two well-known, publicly available datasets, FaceForensics++ and CelebDF, to train and test the deepfake detection system. FaceForensics++ has high-quality face video data that has both actual and fraudulent content. To make the dataset suitable for image-based analysis, frames are taken out of these videos so that the model may learn from the static visual properties that are present in each frame. CelebDF, on the other hand, has a lot of actual and fake celebrity face photos, which makes it especially useful for teaching the model about a wide range of faces, expressions, and small fakes [65]. The sample images from both datasets show a wide range of situations, such as real facial expressions taken in different lighting conditions. This makes sure that the model can work with different image qualities and settings. Also, deepfake samples typically include subtle changes, especially around sensitive areas of the face like the mouth,

eyes, and jaw. These changes are hard to spot, thus they are important for training a strong detection model [90]. The system has a full, realistic set of examples that it can use to tell the difference between real and fake photos thanks to these datasets.

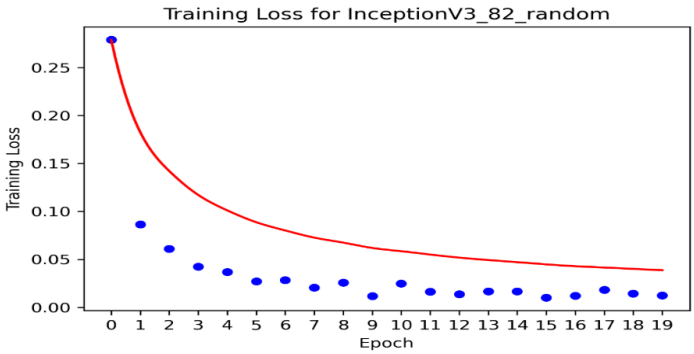

Figure 6: Training loss of inception

The model architecture is well worked out so that it can accurately classify deepfakes into two categories. It uses the TensorFlow and Keras frameworks to do this. The input layer only takes photos that are 224x224 pixels wide and have three colour channels (RGB). This makes sure that all the images in the dataset are the same size [93]. The model's main part is made up of several convolutional layers that use 3x3 kernels to look at the input images and find essential spatial elements like edges, textures, and patterns. After these layers, there are MaxPooling layers with a 2x2 window [59]. These layers make the feature maps smaller, make the calculations easier, and save the most important features. The output is flattened after the convolutional layers and then sent through dense (completely connected) layers with 128 and 64 neurones, respectively. These layers help the model understand more complex patterns and connections in the data. The last layer utilises a sigmoid activation function, which gives a number between 0 and 1 that shows how likely it is that the input image is real or fake [77]. This architecture, which was constructed with TensorFlow/Keras, is designed for both accuracy and speed, so it can be used for deepfake detection in real time or on a wide scale.

The model training process uses advanced methods and tried-and-true setups to provide the best performance and efficiency possible. We use Binary Cross-Entropy for the loss function because it works well for jobs that involve binary classification, like telling the difference between real and false photographs [72]. The Adam optimiser changes the learning rates during training, which helps models converge quickly and perform consistently across different types of data. Training takes place over 50 to 100 epochs, which gives the model enough time to learn complex patterns. The batch size of 32 strikes a good mix between learning stability and computing efficiency. To see how well the model works, we keep track of a few important measures, such as accuracy, precision, and recall [84]. Each of these metrics gives us useful information about how correct the model is, how well it can find deepfakes, and how sensitive it is to false positives and false negatives [54]. GPU hardware speeds up training even more, which cuts down on convergence time and makes it easier to try new things. Also, model checkpoints automatically save the weights of the best-performing model during training, and early stopping stops training when performance levels off or starts to drop. These tactics make guarantee that the best and most generalisable version of the model is kept for deployment.

The training setup for the deepfake detection model is carefully planned to make sure that it learns the best way, works well, and uses computer resources efficiently [79]. The Binary Crossentropy loss function is the most important aspect of the training process. It works well for binary classification jobs where the goal is to find out if an input image is authentic or fraudulent. This loss function looks at the difference between the projected probability and the actual label. It helps the model generate better predictions each time it runs. The Adam optimiser is used to make the learning process better [68]. Adam takes the best parts of two well-known optimisation algorithms, AdaGrad and RMSProp, and changes the learning rate for each

parameter based on how well it is doing. This makes training faster and more reliable, even with noisy or sparse data.

Implementation and Testing

The implementation step in the Deepfake Detection System is when the design goes from being an idea to being real. The system is made in Python with the TensorFlow/Keras modules. The main role is to load the pre-trained deep learning model and let users upload images so they may be classified [91]. The model tells you if the picture is real or phoney and gives you a score of how sure it is. There are also strict testing methods in place to make sure that each module works correctly and that the system works as intended in different situations. The testing process follows the typical Software Development Life Cycle (SDLC) and makes sure that the system works, runs well, and is reliable by doing unit testing, integration testing, and functional testing. The algorithm takes a picture of a face as input and processes it to see if it is real or a deepfake. The output is a binary classification result with a score of how sure it is [71]. The forecast is shown in the user interface and saved in a local log file for further use. The model uses a sigmoid activation function to give probability scores, which are then used to give the label "REAL" or "FAKE."

Predicted Sketch Synthesis of the Subject

The system has a visual representation technique called sketch synthesis that is optional. It makes the data easier to understand and helps with forensic investigation. Edge detection filters from the OpenCV library, like the Canny or Laplacian filter, are used to turn the input image into a sketch. These filters make the outlines and curves of face features stand out, making the image look simpler and black-and-white. This sketch-based visualisation has a lot of uses [69]. For one thing, it makes it easier to compare real and fake photos side by side. The edge outlines can show little differences that were added during the deepfake process, like awkward transitions, distortions around the eyes or mouth, and uneven facial shapes. In full-color pictures, these are typically hard to see, but they stand out more in sketch form. Second, the sketch synthesis makes the model's decision-making process easier for people to understand. Neural networks usually work as black boxes, but this visual tool can help forensic specialists and researchers understand the model's output by giving them physical, image-based proof of tampering [85]. So, adding sketch synthesis not only makes the system more clear and easy to use, but it also makes it useful in real-life situations where expert validation and understanding are very important.

Functional Testing

Functional testing in deepfake detection using deep learning focuses on verifying whether the entire system performs its intended tasks correctly and consistently from end to end. This kind of testing checks the system against set functional requirements, including whether it can tell the difference between real and fraudulent photos or videos in different situations [55]. The process entails supplying the system with various types of input data, encompassing authentic and deepfake samples, and verifying whether the outputs (such as classification labels or probability scores) align with the anticipated outcomes. Functional testing also makes sure that important steps like image preprocessing, feature extraction, classification, and output generation all work together [83]. It might involve testing with edge cases, like low-resolution images, blurry content, or videos that have been changed with few artefacts, to see how strong the model is.

The goal is to make sure that the model works in the real world and that it can reliably find changes in a wide range of datasets [78]. Functional testing is very important for making sure that the system works as expected, especially before it is used in sensitive areas like digital forensics or content authentication. In the training phase of the deepfake detection model, all the images from the selected datasets are systematically loaded into the model and prepared for processing. These datasets, which have both actual and fraudulent images, are very important for training the model how to tell the difference between true and phoney information [60]. During training, each image is fed into the neural network, which goes through various steps of

preprocessing and feature extraction. In this step, the model looks at each image on its own and learns to recognise and remember its unique features, like textures, edges, facial landmarks, and little changes that happen when it is manipulated [92].

Results and Discussions

The proposed deepfake detection system utilising machine learning exhibits efficacy through its elevated accuracy, rapid processing speed, and versatility across various datasets [98]. The system can pick out complex elements from facial photos that are frequently hard to see with the naked eye, such as small changes in facial expressions, textures, and motions. This is possible because of a well-organised deep learning architecture. Using preprocessed input data, like photographs that have been normalised, scaled, and contrast-enhanced, makes sure that the model's predictions are more accurate by making them more consistent and less noisy. Using optimised methods like GPU acceleration, model checkpoints, and early halting during training greatly speeds up convergence time without causing overfitting. The system also leverages lightweight, efficient architectures that find a good balance between performance and cost, so it may be used for real-time or near-real-time applications. Accuracy, precision, and recall are some of the evaluation criteria that show a great capacity to correctly tell the difference between real and fake inputs [97]. In general, the proposed system is very good at finding deepfakes. It strikes a good balance between speed, reliability, and scalability, which are all important for real-world digital forensics and media authentication jobs. The suggested deepfake detection system is much better than current methods in many important ways, such as accuracy, efficiency, ease of understanding, and ethical design [99]. Conventional systems frequently depend on superficial learning techniques or rudimentary heuristic-based approaches, which may inadequately identify small alterations in high-quality deepfakes.

Conclusion

The quick progress of deepfake technology has made many people worried about the truthfulness and integrity of digital media. The suggested deepfake detection system uses deep learning methods to find and tell the difference between fake and real media in order to solve these problems. Combining Sound and Picture Data: Most deepfake detection models right now only look at visual input, like pictures or video frames. But deepfakes usually change both the audio and the video. Future deepfake detection models might use both audio and visual signals to make them more accurate. For instance, finding lip-sync faults in videos that look at audio irregularities could make detection stronger.

References

1. R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, “Deepfakes and beyond: A Survey of face manipulation and fake detection,” Inf. Fusion, vol. 64, no. 12, pp. 131–148, 2020.
2. Agussalim, Rusli, A. Rasjid, M. Nur, T. Erawan, Iwan, and Zaenab, "Caffeine in student learning activities," J. Drug Alcohol Res., vol. 12, no. 9, Ashdin Publishing, 2023.
3. Agussalim, S. N. Fajriah, A. Adam, M. Asikin, T. Podding, and Zaenab, "Stimulant drink of the long driver lorry in Sulawesi Island, Indonesia," J. Drug Alcohol Res., vol. 13, no. 3, Ashdin Publishing, 2024.
4. S. Temara, “Maximizing Penetration Testing Success with Effective Reconnaissance Techniques Using ChatGPT”, Asian Journal of Research in Computer Science, vol. 17, no. 5, pp. 19–29, 2024.
5. S. Temara, “The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified”, Asian Journal of Advanced Research and Reports, vol. 18, no. 3, pp. 1–16, Feb. 2024.
6. S. Temara, “Harnessing the power of artificial intelligence to enhance next-generation cybersecurity,” World Journal of Advanced Research and Reviews, vol. 23, no. 2, pp. 797–

811,2024.

7. D. Dayana, T. S. Shanthi, G. Wali, P. V. Pramila, T. Sumitha, and M. Sudhakar, “Enhancing usability and control in artificial intelligence of things environments (AIoT) through semantic web control models,” in Semantic Web Technologies and Applications in Artificial Intelligence of Things, F. Ortiz-Rodriguez, A. Leyva-Mederos, S. Tiwari, A. Hernandez-Quintana, and J. Martinez-Rodriguez, Eds., IGI Global, USA, 2024.
8. J. Tanwar, H. Sabrol, G. Wali, C. Bulla, R. K. Meenakshi, P. S. Tabeck, and B. Surjeet, “Integrating blockchain and deep learning for enhanced supply chain management in healthcare: A novel approach for Alzheimer’s and Parkinson’s disease prevention and control,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 22s, pp. 524–539, 2024.
9. R. K. Meenakshi, R. S., G. Wali, C. Bulla, J. Tanwar, M. Rao, and B. Surjeet, “AI integrated approach for enhancing linguistic natural language processing (NLP) models for multilingual sentiment analysis,” Philological Investigations, vol. 23, no. 1, pp. 233–247, 2024.
10. G. Wali and C. Bulla, “Suspicious activity detection model in bank transactions using deep learning with fog computing infrastructure,” in Advances in Computer Science Research, 2024, pp. 292–302.
11. G. Wali, P. Sivathapandi, C. Bulla, and P. B. M. Ramakrishna, “Fog computing: Basics, key technologies, open issues, and future research directions,” African Journal of Biomedical Research, vol. 27, no. 9, pp. 748–770, 2024.
12. B. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Big Data Intelligence and Computing. DataCom 2022, C. Hsu, M. Xu, H. Cao, H. Baghban, and A. B. M. Shawkat Ali, Eds., Lecture Notes in Computer Science, vol. 13864. Singapore: Springer, 2023, pp. 25–38.
13. B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol. 1, 2023, Art. no. 100019. doi: 10.1016/j.csa.2023.100019.
14. B. Senapati et al., "Wrist crack classification using deep learning and X-ray imaging," in Proceedings of the Second International Conference on Advances in Computing Research (ACR’24), K. Daimi and A. Al Sadoon, Eds., Lecture Notes in Networks and Systems, vol. 956. Cham: Springer, 2024, pp. 72–85.
15. S. Banala, “The Future of IT Operations: Harnessing Cloud Automation for Enhanced Efficiency and The Role of Generative AI Operational Excellence,” International Journal of Machine Learning and Artificial Intelligence, vol. 5, no. 5, pp. 1–15, Jul. 2024.
16. S. Banala, "DevOps Essentials: Key Practices for Continuous Integration and Continuous Delivery," International Numeric Journal of Machine Learning and Robots, vol. 8, no. 8, pp. 1-14, 2024.
17. M. R. M. Reethu, L. N. R. Mudunuri, and S. Banala, “Exploring the Big Five Personality Traits of Employees in Corporates,” FMDB Transactions on Sustainable Management Letters, vol. 2, no. 1, pp. 1–13, 2024.
18. S. Banala, “The Future of Site Reliability: Integrating Generative AI into SRE Practices,” FMDB Transactions on Sustainable Computer Letters, vol. 2, no. 1, pp. 14–25, 2024.
19. S. Banala, Identity and Access Management in the Cloud, International Journal of Innovations in Applied Sciences & Engineering, vol. 10, no. 1S, pp. 60–69, 2024.
20. S. Banala, "The FinOps Framework: Integrating Finance and Operations in the Cloud,"

International Journal of Advances in Engineering Research, vol. 26, no. 6, pp. 11–23, 2024.

21. S. Banala, "Artificial Creativity and Pioneering Intelligence: Harnessing Generative AI to Transform Cloud Operations and Environments," International Journal of Innovations in Applied Sciences and Engineering, vol. 8, no. 1, pp. 34–40, 2023.
22. S. Banala, Cloud Sentry: Innovations in Advanced Threat Detection for Comprehensive Cloud Security Management, International Journal of Innovations in Scientific Engineering, vol. 17, no. 1, pp. 24–35, 2023.
23. S. Banala, Exploring the Cloudscape - A Comprehensive Roadmap for Transforming IT Infrastructure from On-Premises to Cloud-Based Solutions, International Journal of Universal Science and Engineering, vol. 8, no. 1, pp. 35–44, 2022.
24. P. P. Chauhan, D. Y. Patel, and S. K. Shah, "Optimization of Stability Indicating RP-HPLC method for The Estimation of an Antidepressant Agents Alprazolam and Imipramine in Pure & Pharmaceutical Dosage Form," Eurasian Journal of Analytical Chemistry, vol. 11, no. 2, pp. 101-113, 2016.
25. R. Parmar, N. Kalal, J. Patel, and P. Chauhan, "Fabrication of Eucalyptus Oil-loaded Ciprofloxacin Hydrochloride Topical Films for Enhanced Treatment of Post-Operative Wound Infection," Anti-Infective Agents, vol. 22, no. 1, pp. 66-76, 2024.
26. P. Chauhan, R. Parmar, and A. Tripathi, "Development and validation of a stability indicating LC method for the analysis of chlordiazepoxide and trifluoperazine hydrochloride in the presence of their degradation products," ACTA Pharmaceutica Sciencia, vol. 62, no. 2, pp. 312-332, 2024.
27. R. Parmar, M. M. Salman, and P. Chauhan, "Fabrication of Cefixime Nanoparticles Loaded Films and their Ex Vivo Antimicrobial Effect on Periodontitis Patient's Saliva," Pharmaceutical Nanotechnology, vol. 9, no. 5, pp. 361-371, 2021.
28. R. Parmar, P. Chauhan, J. Chavda, and S. Shah, "Local Delivery of Chitosan Strips Carrying Ornidazole-Loaded Ethyl Cellulose Micro-Particles for the Enhanced Treatment of Periodontitis," Journal of Chemical and Pharmaceutical Research, vol. 9, no. 6, pp. 193-201, 2017.
29. R. Parmar, P. Chauhan, J. Chavda, and S. Shah, "Formulation and evaluation of cefixime strips for chronic periodontal treatment," Asian Journal of Pharmaceutics (AJP), vol. 10, no. 4, 2016.
30. P. Chauhan, F. Tandel, and R. Parmar, "A Simplex-Optimized Chromatographic Separation of Phytoconstituents in Cardioprotective Polyherbal Formulation and Crude Drugs," Asian Journal of Pharmaceutics, vol. 15, no. 4, pp. 441-447, 2021.
31. R. Parmar and P. Chauhan, "Potentiating Antibacterial Effect of Locally Deliver Caffeine Nanoparticles on Systemically Used Antibiotics in Periodontal Treatments," Asian Journal of Pharmaceutics, vol. 14, no. 2, pp. 229-235, 2020.
32. P. Chauhan, K. Bhanushali, and R. Parmar, "Design of Experiment-Driven Stability Indicating RP-HPLC Method for Simultaneous Estimation of Tetracaine Hydrochloride and Oxymetazoline Hydrochloride," Bulletin of Environment, Pharmacology and Life Sciences, vol. 22, no. 1, pp. 181-196, 2023.
33. H. D. Gelani, P. P. Chauhan, and S. K. Shah, "Practical Implication of Chromatographic Method for Estimation of Aceclofenac and Pregabalin in Bulk and Pharmaceutical Dosage Forms," Chromatography Research International, vol. 2014, no. 1, pp. 643027, 2014.
34. H. D. Gelani, P. P. Chauhan, and S. K. Shah, "Quantification of Aceclofenac and Pregabalin in Pharmaceutical Formulations using Nucleophilic Aromatic Substitution Reactions," International Journal of Pharmaceutical Sciences and Nanotechnology (IJPSN), vol. 8, no. 2,

pp. 2823-2827, 2015.

35. P. Chauhan, R. Parmar, and N. J. Shah, "Stability Indicating RP-HPLC Method for the Determination of Niacin and Lovastatin In Bulk Drug and Tablet Formulation," American Journal of Pharmtech Research, vol. 4, no. 2, pp. 548-561, 2014.
36. N. T. Jinal, D. A. Pumbhadiya, C. P. Payal, and S. K. Shah, "An Isocratic RP-HPLC Method for Simultaneous Analysis of Ilaprazole and Domperidone in Pharmaceutical Formulation," Asian Journal of Pharmaceutical Research, vol. 8, no. 1, pp. 1-5, 2018.
37. G. Patel, P. Chauhan, and S. Shah, "Simultaneous estimation of gatifloxacin and flurbiprofen sodium in ophthalmic formulation by UV-Spectrophotometric method," Journal of Chemical and Pharmaceutical Research, vol. 6, no. 7, pp. 96-101, 2014.
38. V. D. Rohit, J. Tandel, P. Chauhan, and S. Shah, "A novel stability indicating RP-HPLC method development and validation for estimation of Phenylephrine hydrochloride and Bromhexine hydrochloride in their tablet dosage form," Journal of Current Pharma Research, vol. 6, no. 3, pp. 1860-1876, 2016.
39. P. Chauhan, B. Patel, and S. Shah, "Sensitive RP-HPLC method for estimation of atropine sulphate and dexamethasone sodium phosphate in ophthalmic formulation," Current Pharma Research, vol. 6, no. 1, pp. 1763-1769, 2016.
40. S. K. Suvvari, "Ensuring security and compliance in agile cloud infrastructure projects," Int. J. Comput. Eng., vol. 6, no. 4, pp. 54–73, 2024.
41. S. K. Suvvari, "Building an architectural runway: Emergent practices in agile methodologies," Int. J. Sci. Res. (IJSR), vol. 13, no. 9, pp. 140–144, 2024.
42. S. K. Suvvari and V. D. Saxena, "Innovative approaches to project scheduling: Techniques and tools," Innov. Res. Thoughts, vol. 10, no. 2, pp. 133–143, 2024.
43. S. K. Suvvari, "The role of leadership in agile transformation: A case study," J. Adv. Manag. Stud., vol. 1, no. 2, pp. 31–41, 2024.
44. S. K. Suvvari, "The role of emotional intelligence in project leadership: A study," Innov. Res. Thoughts, vol. 10, no. 1, pp. 157–171, 2024.
45. S. K. Suvvari and V. D. Saxena, "Stakeholder management in projects: Strategies for effective communication," Innov. Res. Thoughts, vol. 9, no. 5, pp. 188–201, 2023.
46. Ali and S. K. Suvvari, "Effect of motivation on academic performance of engineering students: A study in Telangana, India," Int. J. Eng. Res. Manag. Stud. (IJERMS), vol. 6, no. 12, pp. 1–5, 2023.
47. S. K. Suvvari and V. D. Saxena, "Effective risk management strategies for large-scale projects," Innov. Res. Thoughts, vol. 9, no. 1, pp. 406–420, 2023.
48. S. K. Suvvari, "Managing project scope creep: Strategies for containing changes," Innov. Res. Thoughts, vol. 8, no. 4, pp. 360–371, 2022.
49. S. K. Suvvari, "Project portfolio management: Best practices for strategic alignment," Innov. Res. Thoughts, vol. 8, no. 4, pp. 372–385, 2022.
50. S. K. Suvvari, "The impact of agile on customer satisfaction and business value," Innov. Res. Thoughts, vol. 6, no. 5, pp. 199–211, 2020.
51. S. K. Suvvari, "An exploration of agile scaling frameworks: Scaled agile framework (SAFe), large-scale scrum (LeSS), and disciplined agile delivery (DAD)," Int. J. Recent Innov. Trends Comput. Commun., vol. 7, no. 12, pp. 9–17, 2019.
52. S. K. Suvvari, B. Anjum, and M. Hussain, "Key factors impacting the e-learning effectiveness for computer science students: An empirical study," Webology, vol. 17, no. 4,

pp. 837–847, 2020.

53. Ali, M. Ahmad, S. Nawaz, T. Raza, and S. K. Suvvari, "An effective structure for data management in the cloud-based tools and techniques," J. Eng. Sci., vol. 15, no. 4, pp. 215–228, 2022.
54. T. K. Lakshmi and J. Dheeba, "Classification and Segmentation of Periodontal Cyst for Digital Dental Diagnosis Using Deep Learning," Computer Assisted Methods in Engineering and Science, vol. 30, no. 2, pp. 131-149, 2023.
55. T. K. Lakshmi and J. Dheeba, "Digital Decision Making in Dentistry: Analysis and Prediction of Periodontitis Using Machine Learning Approach," International Journal of Next-Generation Computing, vol. 13, no. 3, 2022.
56. T. K. Lakshmi and J. Dheeba, "Digitalization in Dental Problem Diagnosis, Prediction and Analysis: A Machine Learning Perspective of Periodontitis," International Journal of Recent Technology and Engineering, vol. 8, no. 5, pp. 67-74, 2020.
57. T. K. Lakshmi and J. Dheeba, "Predictive Analysis of Periodontal Disease Progression Using Machine Learning: Enhancing Oral Health Assessment and Treatment Planning," International Journal of Intelligent Systems and Applications in Engineering, vol. 11, no. 10s, pp. 660–671, 2023.
58. V. Singh, S. Singh, S. Sharma, A. Diwanji, W. Diana, and C. Patel, “Assessment of discomfort and analgesic usage following pediatric dental procedures in India: A cross-sectional study,” J. Pharm. Bioallied Sci., vol. 16, Suppl. 3, pp. S2330–S2332, Jul. 2024.
59. H. Thakkar, B. Sarvaiya, K. Shah, P. V. Manek, J. Soni, and M. D. Bhardwaj, “Effect of silver diamine fluoride on surface microhardness of enamel of permanent molars: An in-vitro study,” J. Res. Adv. Dent., vol. 10, no. 2, pp. 206–210, 2020.
60. A. Kulkarni, "Generative AI-Driven for SAP Hana Analytics," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 12, no. 2, pp. 438-444, 2024.
61. A. Kulkarni, "Natural Language Processing for Text Analytics in SAP HANA," International Journal of Multidisciplinary Innovation and Research Methodology, vol. 3, no. 2, pp. 135-144, 2024.
62. A. Kulkarni, "Enhancing Customer Experience with AI-Powered Recommendations in SAP HANA," International Journal of Business, Management and Visuals, vol. 7, no. 1, pp. 1-8, 2024.
63. Anand S, Rajan M, Venkateshbabu N, Kandaswamy D, Shravya Y, and Rajeswari K., “Evaluation of the Antibacterial Efficacy of Azadirachta indica, Commiphora myrrha, Glycyrrhiza glabra Against Enterococcus faecalis using Real Time PCR,” Open Dent. J., vol. 10, pp. 160–165, May 2016.
64. Chum J. D., Lim D. J. Z., Sheriff S. O., Pulikkotil S. J., Suresh A., and Davamani F., “In vitro evaluation of octenidine as an antimicrobial agent against Staphylococcus epidermidis in disinfecting the root canal system,” Restor. Dent. Endod., vol. 44, no. 1, pp. e8, Feb. 2019.
65. Kandaswamy D., Venkateshbabu N., Arathi G., Roohi R., and Anand S., “Effects of various final irrigants on the shear bond strength of resin-based sealer to dentin,” J. Conserv. Dent., vol. 14, no. 1, pp. 40–42, Jan. 2011.
66. Nagendrababu V., Jayaraman J., Suresh A., Kalyanasundaram S., and Neelakantan P., “Effectiveness of ultrasonically activated irrigation on root canal disinfection: a systematic review of in vitro studies,” Clin. Oral Investig., vol. 22, no. 2, pp. 655–670, Mar. 2018.

67. Nagendrababu V., Pulikkotil S. J., Suresh A., Veettil S. K., Bhatia S., and Setzer F. C., “Efficacy of local anaesthetic solutions on the success of inferior alveolar nerve block in patients with irreversible pulpitis: a systematic review and network meta-analysis of randomized clinical trials,” Int. Endod. J., vol. 52, no. 6, pp. 779–789, Jun. 2019.

68. Naidu S. and Suresh A., “A brief overview on cleft lip and palate,” Guident, vol. 2018, pp. 42–47, Sep. 2018.

69. Naidu S. and Suresh A., “A non-surgical approach to accelerate tooth movement – A review,” Acta Sci. Dent. Sci., vol. 2, no. 10, pp. 45–47, Sep. 2018.

70. Naidu S. and Suresh A., “Bond failure rate of amorphous calcium phosphate containing (Aegis Ortho) and fluoride-releasing (Transbond Plus Colour Change) orthodontic adhesives – A randomized clinical trial,” J. Indian Dent. Assoc., vol. 13, no. 11, pp. 18–26, Nov. 2019.

71. Naidu S. and Suresh A., “Does my child need braces? – A comprehensive review,” EAS J. Dent. Oral Med., vol. 1, pp. 6–9, Jan.–Feb. 2019.

72. Naidu S. and Suresh A., “Effects of chin cup in the management of Class III malocclusion,” J. Indian Dent. Assoc., vol. 12, no. 10, pp. 39–42, Oct. 2018.

73. Naidu S. and Suresh A., “Effects of turmeric (Curcuma longa) in dentistry,” Int. J. Dev. Res., vol. 8, no. 7, pp. 21828–21831, Jul. 2018.

74. Naidu S. and Suresh A., “Evolution of orthodontic appliances – Then and now,” Int. J. Dent. Health Sci., vol. 5, no. 2, pp. 319–329, 2018.

75. Naidu S. and Suresh A., “Introduction to molar distalization,” Guident, vol. 2018, pp. 42–44, Sep. 2018.

76. A. Kulkarni, "Digital Transformation with SAP Hana," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 12, no. 1, pp. 338-344, 2024.

77. A. Kulkarni, "Supply Chain Optimization Using AI and SAP HANA: A Review," International Journal of Research Radicals in Multidisciplinary Fields, vol. 2, no. 2, pp. 51-57, 2024.

78. A. Kulkarni, "Image Recognition and Processing in SAP HANA Using Deep Learning," International Journal of Research and Review Techniques, vol. 2, no. 4, pp. 50-58, 2024.

79. S. Chundru, "Harnessing AI's Potential: Transforming Metadata Management with Machine Learning for Enhanced Data Access and Control," International Journal of Advances in Engineering Research, vol. 27, no. 2, pp. 39-49, 2024.

80. S. Chundru, "Beyond Rules-Based Systems: AI-Powered Solutions for Ensuring Data Trustworthiness," International Transactions in Artificial Intelligence, vol. 7, no. 7, p. 17, 2023.

81. S. Chundru, "Seeing Through Machines: Leveraging AI for Enhanced and Automated Data Storytelling," International Journal of Innovations in Scientific Engineering, vol. 18, no. 1, pp. 47-57, 2023.

82. S. Chundru, "Cloud-Enabled Financial Data Integration and Automation: Leveraging Data in the Cloud," International Journal of Innovations in Applied Sciences & Engineering, vol. 8, no. 1, pp. 197-213, 2022.

83. S. Chundru, "Leveraging AI for Data Provenance: Enhancing Tracking and Verification of Data Lineage in FATE Assessment," International Journal of Inventions in Engineering & Science Technology, vol. 7, no.1, pp. 87-104, 2021.

84. S. Chundru, "Ensuring Data Integrity Through Robustness and Explainability in AI Models," Transactions on Latest Trends in Artificial Intelligence, vol. 1, no. 1, pp. 1-19,

2020.

85. R. J. Patel, P. P. Chauhan, and S. K. Shah, "Quantification of ketorolac and fluorometholone by RP-HPLC method in ophthalmic formulation," Inventi Rapid: Pharm Analysis & Quality Assurance, vol. 2014, no. 3, pp. 1-6, 2014.
86. P. Gopi, C. Payal, and S. Samir, "Application of RP-HPLC method for simultaneous estimation of Gatifloxacin and Flurbiprofen Sodium in ophthalmic formulation," American Journal of PharmTech Research, vol. 4, no. 2, pp. 658-668, 2014.
87. P. Shah, P. Chauhan, J. Tandel, and S. Shah, "Stability indicating assay method for simultaneous estimation of melatonin and pyridoxine hydrochloride in pharmaceutical formulation," World Journal of Pharmacy and Pharmaceutical Sciences, vol. 5, no. 4, pp. 1955-1969, 2016.
88. P. Chauhan, S. Shah, G. Patel, and A. Jakasaniya, "Simultaneous Estimation of Azithromycin and Ambroxol Hydrochloride in Combined Dosage form by RP-HPLC Method," Journal of Chemical and Pharmaceutical Research, vol. 10, no. 5, pp. 142-147, 2018.
89. J. R. Gohil, P. Chauhan, I. I. Panchal, and S. K. Shah, "RP-HPLC method development and validation for the simultaneous estimation of cefoperazone sodium and tazobactam sodium in parenteral preparation," Inventi Rapid: Pharm Analysis & Quality Assurance, vol. 2014, no. 3, pp. 1-4, 2014.
90. P. Chauhan, S. Patel, and S. Shah, "A novel isocratic RP-HPLC for simultaneous multicomponent analysis of amoxicillin and probenecid in pharmaceutical formulation," International Journal of Institutional Pharmacy and Life Sciences, 2018.
91. P. M. Satasiya, P. Chauhan, I. I. Panchal, and S. K. Shah, "RP-HPLC method development and validation for simultaneous estimation of amiloride hydrochloride and torsemide in tablet dosage form," Inventi Rapid: Pharm Analysis & Quality Assurance, vol. 2014, no. 3, pp. 1-4, 2014.
92. H. Gelani, P. Chauhan, and S. Shah, "Application of derivative spectrophotometry for the quantification of NSAID in combination with anti-convulsant drug in pharmaceutical formulation," Inventi Rapid: Pharm Analysis & Quality Assurance, vol. 2014, no. 4, pp. 1-6, 2014.
93. E. Geo Francis and S. Sheeja, “Enhanced intrusion detection in wireless sensor networks using deep reinforcement learning with improved feature extraction and selection,” Multimedia Tools and Applications, 2024.
94. E. Geo Francis and S. Sheeja, “Bi-Level Intrusion Detection in IoT Networks Using Ensemble Method and A-GRU-RNN Classifier,” Electric Power Components and Systems, 2024.
95. E. G. F., S. Sheeja, John, A., and J. Joseph, “Intrusion detection system with an ensemble DAE and BiLSTM in the fog layer of IoT networks,” Journal of Applied Research and Technology, vol. 22, no.6, pp. 846–862, 2024.
96. E. Geo Francis, S. Sheeja, E.F. Antony John and Jismy Joseph, “An Efficient Intrusion Detection System using a Multiscale Deep Bi-Directional GRU Network to Detect Blackhole Attacks in IoT based WSNs,” Journal of Multiscale Modelling, vol. 15, no. 3, 2024.
97. E. Geo Francis, S. Sheeja, E. F. Antony John and J. Jismy, "IoT Network Security with PCA and Deep Learning for Unmasking Anomalies," 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT), Jabalpur, India, 2024, pp. 322-328.

98. E. Geo Francis and S. Sheeja. “IDSSA: An Intrusion Detection System with Self-adaptive Capabilities for Strengthening the IoT Network Security,” Advances in Computational Intelligence and Informatics (ICACII), Hyderbad, India, 2024, Lecture Notes in Networks and Systems, vol 993, pp. 23-30.

99. E. Geo Francis and S. Sheeja. “Chaotic Resilience: Enhancing IoT Security Through Dynamic Data Encryption,” Intelligent Informatics. (ISI), Bangalore, India, 2024, Smart Innovation, Systems and Technologies, vol 389, pp 331–344.