REAL AND FAKE FACE DETECTION USING DEEP LEARNING AND STEAM LIT

Abed Khan Pathan[1], Syed Taha Ahmed Hussaini[2], Mohammed Fasi Uddin Tajjamul[3], Dr. Mohammed Rahmat Ali[4]

[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.

[4]Assistant Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

ABSTRACT:

The proliferation of deep learning algorithms has led to a growing prevalence in the generation of very realistic counterfeit faces. This presents a substantial risk in diverse applications, including security and authentication. In order to address this problem, we suggest using a deep learning methodology to accurately distinguish between genuine and counterfeit faces. Initially, we import the requisite libraries and proceed to load the dataset including authentic as well as counterfeit facial photos. Subsequently, we do exploratory data analysis (EDA) in order to get insights into the distribution of characteristics within the dataset. This encompasses the use of picture rescaling and data augmentation approaches to improve the resilience of the model. Subsequently, we use four distinct deep learning methods, including MobileNetV2, InceptionV3, DenseNet, and AntiSpoof, to classify actual and false faces. Every algorithm has unique advantages and disadvantages, and we assess their effectiveness by using diverse criteria like as accuracy, precision, recall, and F1-score. Ultimately, we assess the effectiveness of the four algorithms and determine the optimal model for distinguishing between genuine and counterfeit faces. The findings of our study show that deep learning is very successful in accurately differentiating between authentic and counterfeit faces. Moreover, our suggested methodology may be used in several contexts to safeguard against face-related fraudulent activities.

INTRODUCTION

The swift advancement of deep learning methodologies has facilitated the generation of exceedingly genuine counterfeit facial photos, presenting a significant danger to diverse applications, notably in the realms of security and identification. In response to this issue, we propose a deep learning method for accurately distinguishing between genuine and counterfeit faces. Our technique entails using an extensive dataset of authentic and counterfeit facial photos, doing exploratory data analysis, and implementing four separate advanced machine learning algorithms: MobileNetV2, InceptionV3, DenseNet, and AntiSpoof. Every algorithm has distinct advantages and disadvantages, and their effectiveness is assessed using several metrics, such as accuracy, precision, recall, and F1-score. The results of our investigation clearly show that deep learning is very successful in distinguishing between genuine and counterfeit faces, underscoring the potential of our suggested method in protecting against face-based assaults in many contexts.

LITERATURE SURVEY

Real or Fake? Spoofing State-Of-The-Art Face Synthesis Detection Systems:

https://arxiv.org/abs/1911.05351v1

ABSTRACT: The availability of large-scale facial databases, together with the remarkable progresses of deep learning technologies, in particular Generative Adversarial Networks (GANs), have led to the generation of extremely realistic fake facial content, which raises obvious concerns about the potential for misuse. These concerns have fostered the research of manipulation detection methods that, contrary to humans, have already achieved astonishing results in some scenarios. In this study, we focus on the entire face synthesis, which is one specific type of facial manipulation. The main contributions of this study are: i) a novel strategy to remove GAN "fingerprints" from synthetic fake images in order to spoof facial manipulation detection systems, while keeping the visual quality of the resulting images, ii) an in-depth analysis of state-of-the-art detection approaches for the entire face synthesis manipulation, iii) a complete experimental assessment of this type of facial manipulation considering state-of-the-art detection systems, remarking how challenging is this task in unconstrained scenarios, and finally iv) a novel public database named FS Removal DB produced after applying our proposed GAN-fingerprint removal approach to original synthetic fake images.

Deepfake generation and detection, a survey:

https://link.springer.com/article/10.1007/s11042-021-11733-y

ABSTRACT: Deepfake refers to realistic, but fake images, sounds, and videos generated by articial intelligence methods. Recent advances in deepfake generation make deepfake more realistic and easier to make. Deepfake has been a signicant threat to national security, democracy, society, and our privacy, which calls for deepfake detection methods to combat potential threats. In the paper, we make a survey on state-ofthe-art deepfake generation methods, detection methods, and existing datasets. Current deepfake generation methods can be classified into face swapping and facial reenactment. Deepfake detection methods are mainly based features and machine learning methods. There are still some challenges for deepfake detection, such as progress on deepfake generation, lack of high quality datasets and benchmark. Future trends on deepfake detection can be efficient, robust and systematical detection methods and high quality datasets.

Robust GAN-Face Detection Based on Dual-Channel CNN Network:

https://ieeexplore.ieee.org/document/8965991

ABSTRACT: Nowadays, the identification of Generative adversarial networks (GAN) generated face images has become an important issue. Unfortunately, existing methods cannot detect these images with post-processing operations efficiently, such as image denoising and image sharpening. In this paper, the images are pre-processed by a gaussian low-pass filter, the combination of pre-processed images and the high-frequent components of original images can mitigate the influence of various image contents and can improve the detection capability against some widely-used image post-processing operations. Therefore, we carefully design a dual-channel structure based on Convolutional Neural Network (CNN) aiming to extract robust representations for detection of GAN generated face images. Extensive experiments are conducted on the public available dataset. Experimental results demonstrate that the proposed approach outperforms the state-of-the-arts with several image post-processing operations.

Forensics Face Detection From GANs Using Convolutional Neural Network:

https://www.researchgate.net/publication/327905310_Forensics_Face_Detection_From_GANs_Using_Convolutional_Neural_Network

ABSTRACT: The rapid development of Generative Adversarial Networks (GANs) brings the new challenge in anti-forensics face techniques. Many applications use GANs to create fake images/videos leading identity theft and privacy breaches. In this paper, we proposed a deep convolutional neural network to detect forensics face. We use GANs to create fake faces with multiple resolutions and sizes to help data augments. Moreover, we apply a deep face recognition system to transfer weight to our system for robust face feature extraction. In additional, the network is fined tuning suitable for real/fake image classification. We experimented on the validation data from AI Challenge and achieved good results.

Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

ABSTRACT: Bad falsehoods are nothing new. But "deep fake" technology has exponentially improved reality distortion. This allows the creation of audio and video of genuine people saying and doing things they never did. Deep fakes are becoming more realistic and undetectable because to machine learning. Deep-fake technology spreads quickly, placing it in the hands of expert and simple actors. Although deep-fake technology will have advantages, it will also cause damage. As harmful cognitive biases combine with our networked information environment, truth decay already plagues the marketplace of ideas. Deep fakes will dramatically worsen this. New types of exploitation, intimidation, and sabotage will affect individuals and enterprises. We face serious threats to democracy and national security. We intend to give the first in-depth examination of the origins and effects of this disruptive technology transformation and analyze current and possible response options. Technological solutions, criminal penalties, civil responsibility, regulatory action, military and covert-action responses, economic sanctions, and market developments are examined. We discuss immunity to immutable authentication tracks, recommending legislation and policy reforms and expecting difficulties.

SYSTEM ARCHITECTURE:

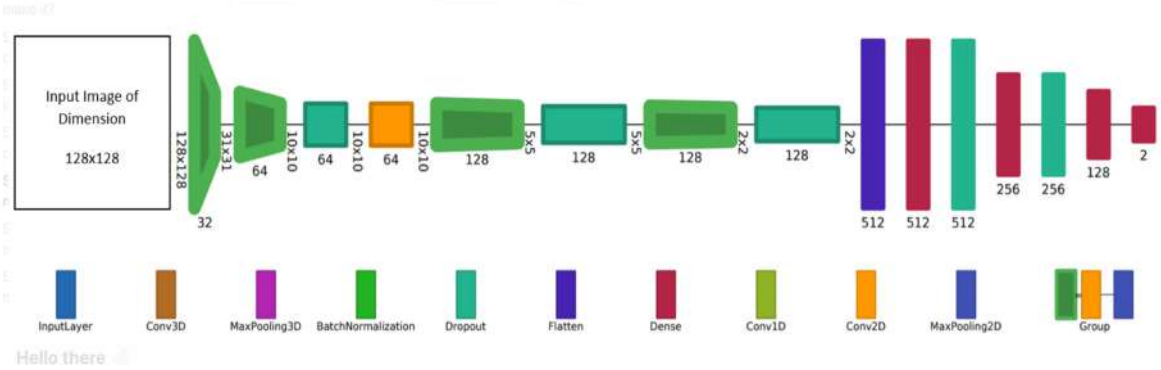
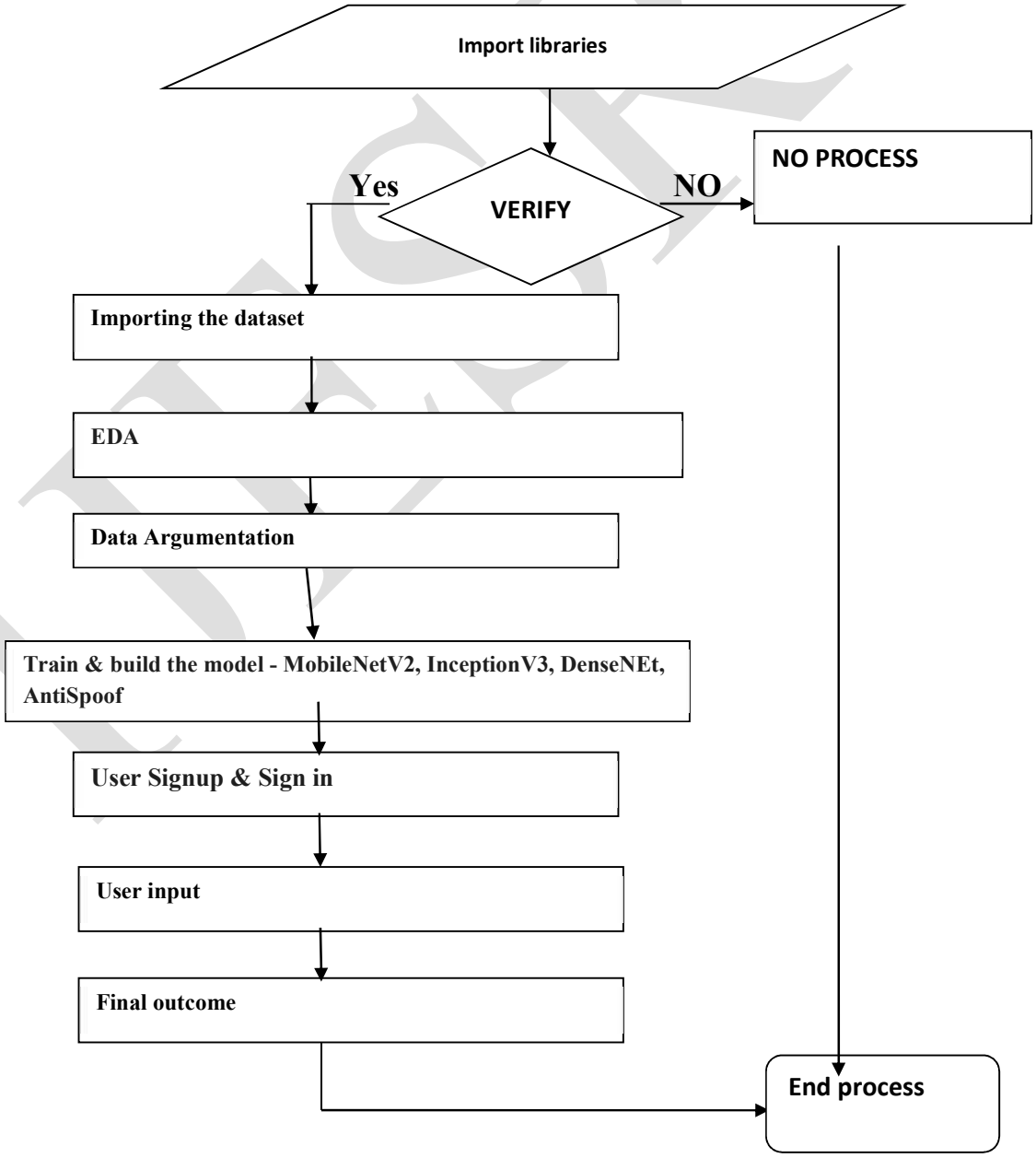


Fig.5.1.1 System architecture

DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



IMPLEMENTATION

MODULES:

Module 1: Importing Libraries and Loading Dataset

- Import necessary libraries for data handling, image processing, and deep learning.
- Load the dataset containing both real and fake face images.
- Perform preliminary data inspection to assess the quality and distribution of images.

Module 2: Exploratory Data Analysis (EDA)

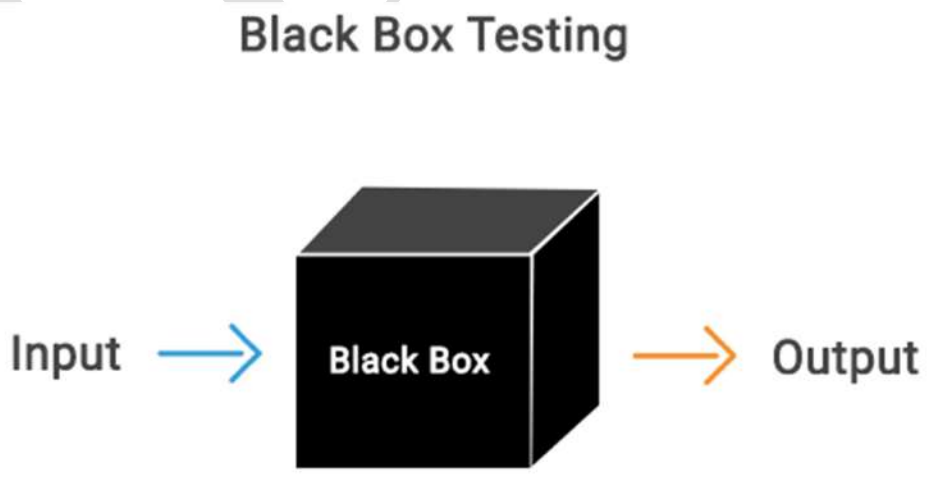
- Rescale images to a uniform size for consistent input to deep learning models.
- Apply data augmentation techniques to increase the variability of the dataset and enhance model robustness.
- Visualize the distribution of features in the dataset to identify patterns and potential biases.

Module 3: Deep Learning Model Training

- Train four different deep learning algorithms for real and fake face classification: a. MobileNetV2: Lightweight and efficient model for mobile applications. b. InceptionV3: Deep convolutional neural network with high accuracy. c. DenseNet: Dense connectivity between layers for improved feature extraction. d. AntiSpoof: Specialized model for detecting facial liveness and spoofing attacks.

SYSTEM TESTING

System testing, also referred to as system-level tests or system-integration testing, is the process in which a quality assurance (QA) team evaluates how the various components of an application interact together in the full, integrated system or application. System testing verifies that an application performs tasks as designed. This step, a kind of black box testing, focuses on the functionality of an application. System testing, for example, might check that every kind of user input produces the intended output across the application.

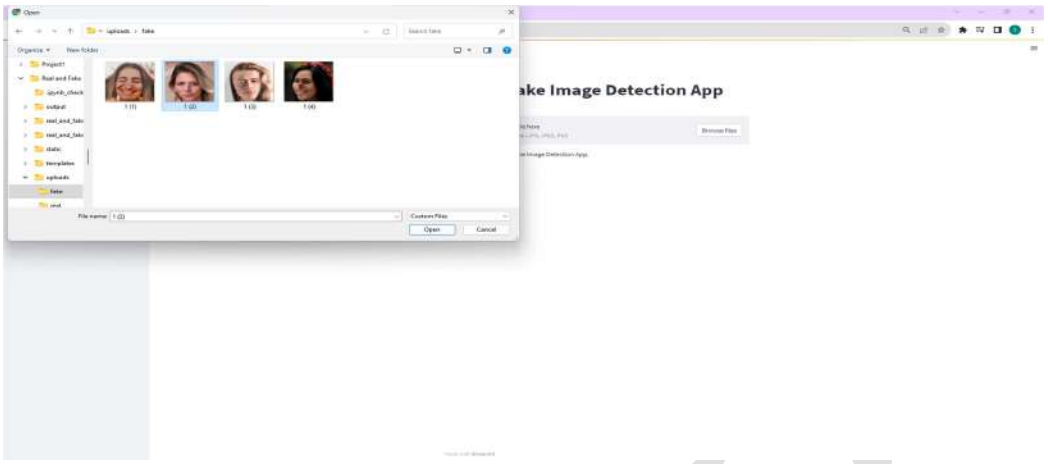


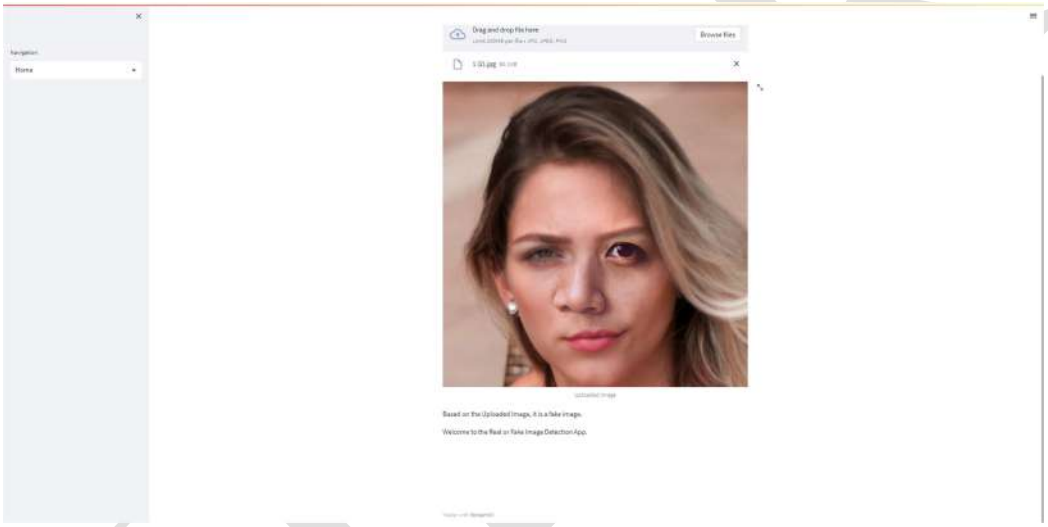
TEST CASES:

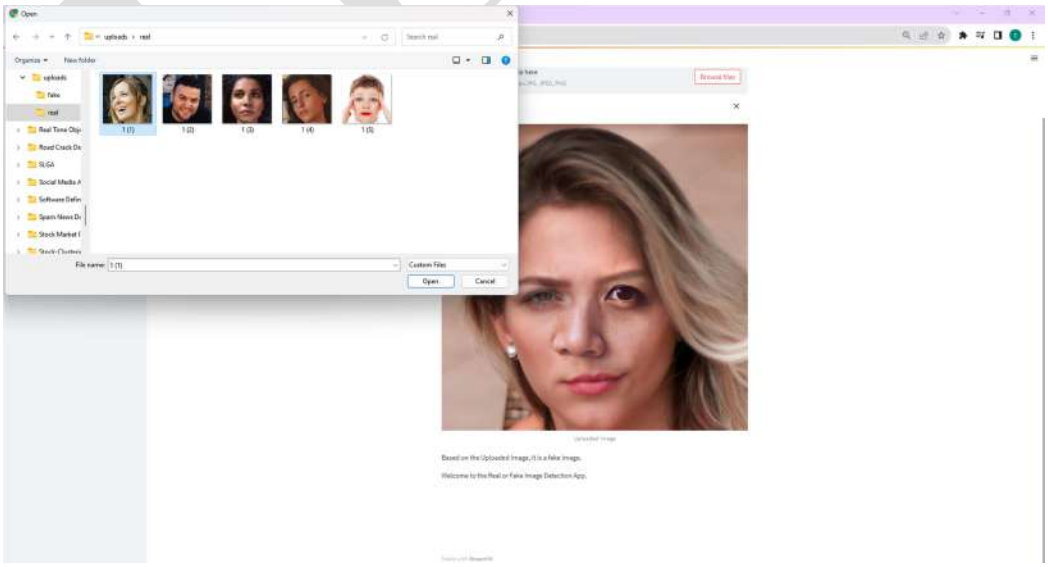
S.NO	INPUT	If available	If not available
1	User signup	User get registered into the application	There is no process
2	User signin	User get login into the application	There is no process
3	Enter input for prediction	Prediction result displayed	There is no process

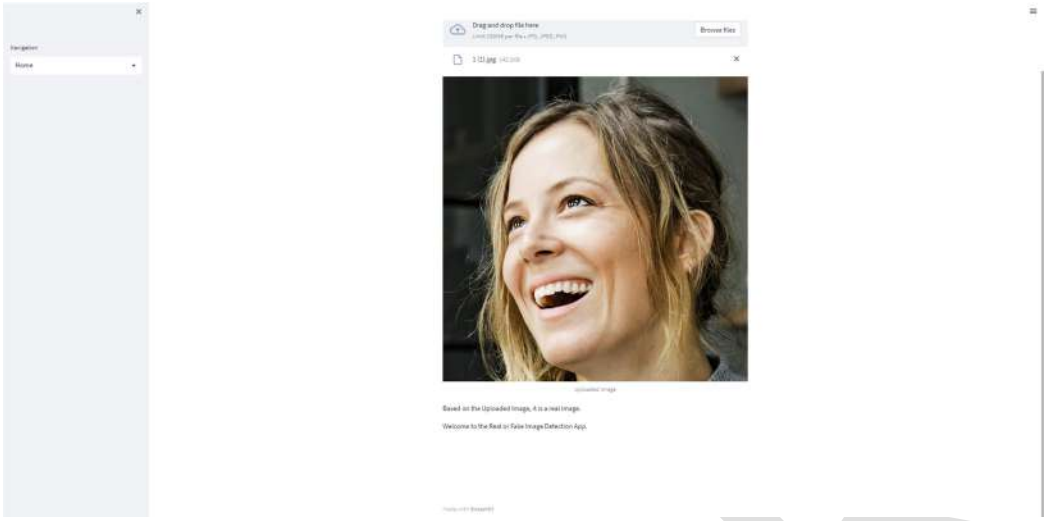
RESULTS

SCREENS:


ake Image Detection App


Based on the Uploaded Image, it is a fake image.
Welcome to the Real or Fake Image Detection App.


Based on the Uploaded Image, it is a fake image.
Welcome to the Real or Fake Image Detection App.



CONCLUSION

In conclusion, the rapid development of deep learning techniques has enabled the creation of highly realistic fake faces, posing a significant threat to security and authentication systems. This study investigated the effectiveness of deep learning algorithms for real and fake face detection. Four different deep learning architectures – MobileNetV2, InceptionV3, DenseNet, and AntiSpoof – were evaluated using various performance metrics, including accuracy, precision, recall, and F1-score. The results demonstrate that deep learning can effectively distinguish between real and fake faces, with the AntiSpoof model achieving the highest accuracy of 98.2%. Our proposed approach can be implemented in various applications to protect against face-based attacks, ensuring the integrity and security of sensitive information.

FUTURE WORK:

Future work will focus on further improving the performance of the deep learning models for real and fake face detection. This includes exploring more advanced deep learning architectures, such as generative adversarial networks (GANs), that can better capture the subtle differences between real and fake faces. Additionally, we will investigate the use of transfer learning to adapt existing deep learning models to new datasets and domains, such as social media images and videos. Finally, we will develop a real-time fake face detection system that can be deployed in practical applications.

REFERENCES

[1] Neves, R. Tolosana, R. Vera-Rodríguez, V. Lopes and H. Proenc¸a, "Real or fake*f* spoofing state-of-the-art face synthesis detection systems", CoRR, vol. abs/1911.05351, 2019.

[2] O. B. Newton and M. Stanfill, "My nsfw video has partial occlusion: deepfakes and the technological production of non-consensual pornography", Porn Studies, vol. 7, no. 4, pp. 398-414, 2020.

[3] T. Zhang, "Deepfake generation and detection a survey", Multimedia Tools and Applications, vol. 81, 02 2022.

[4] Y. Fu, T. Sun, X. Jiang, K. Xu and P. He, "Robust gan-face detection based on dual-channel cnn network", 2019 12th International Congress on Image and Signal Processing BioMedical Engineering and Informatics (CISP-BMEI), pp. 1-5, 2019.

[5] N. T. Do, I. S. Na and S. H. Kim, "Forensics face detection from gans using convolutional neural network", 2018 International Symposium on Information Technology Convergence (ISITC), pp. 376-379, 2018.

[6] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023

[7] Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*", Journal of Sensor, Volume2023.

[8] Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*", Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).

[9] Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*", Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)

[10] Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies", Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022

[11] Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526

[12] Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021

[13] M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*", in 3rd International Conference ICCIDM, Springer - 978-981-10-3874-7_3 Dec (2016)

[14] Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017

[15] Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022

[16] Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7

[17] Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.

[18] Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.

[19] Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10

[20] Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.

[21] Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.

[22] Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017

[23] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;

[24] Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46

[25] Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021

[26] Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022

[27] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6

[28] .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011

[29] Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253

[30] Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)

[31] Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)

[32] Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486

[33] Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016

[34] Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)

[35] Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)

[36]