International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Image Vaccinator an Image Tamper Resilient and Lossesless Auto-Recovery using Invertible Neural Network

B.Hemalatha
Electronics and Communication Engineering
Bannari Amman Institute Of Technology Sathyamangalam

Hemalatha.ec20@bitsathy.ac.in

N.L.Deepsikha
Computer Science and
Engineering
Bannari Amman Institute Of Technology
Sathyamangalam

Deepsikha.cs20@bitsathy.ac.in

Abstract— **Rapid advancements in digital tools make image editing easy and free. The main problem is the compromised credibility of digital images due to the ease of manipulation through advanced digital image processing tools. This vulnerability leads to the creation and dissemination of maliciously fabricated images, fostering the potential for misinformation and influencing public opinion, especially on online social networks. Today, people frequently interact with their families, friends, and colleagues through online social networks (OSN). People enjoy posting and sharing their photos in online communities, blogs, and content sharing sites. The problem addressed in this project is the susceptibility of digital images to tampering, which compromises security and privacy. Traditional image forgery detection methods face challenges in reproducing original content after manipulation. This project introduces an advanced Image Immunization System leveraging Invertible Neural Networks. The system, comprising the Cyber Vaccinator, Vaccine Validator, Forward Pass for Tamper Detection, and Backward Pass for Image Self-Recovery, aims to proactively immunize images against various attacks. Run-Length Encoding in the backward pass to transform hidden perturbations into information, facilitating lossless recovery of the authentic image.**

Keywords—Image Tamper Resilient, Invertible Neural Networks (INN), Vaccine Validator, Pixel Classification Module, User Interface (UI), Run-Length Encoding

I. INTRODUCTION

In our increasingly digitalized world, the vulnerability of visual data to tampering and manipulation has become a critical concern. The pervasive use of images in various applications, from social media to medical imaging, demands innovative solutions to safeguard their authenticity and integrity. Our research endeavors to address this challenge head-on, introducing a cutting-edge approach that not only fortifies images against tampering but also ensures seamless recovery in the face of malicious interventions. Multitask learning is a machine learning paradigm that involves training a model to perform multiple tasks simultaneously. Instead of training separate models for each task, multitask learning aims to leverage shared information across tasks to improve overall performance. Invertible Neural Networks represent a specialized class of neural networks designed to be reversible, allowing for the reconstruction of input data from the network's output. Often used in generative models for realistic data generation. INNs offer a unique ability for reversible data transformations, making them valuable in various applications. By harnessing the power of Invertible Neural Networks (INNs), we have devised a sophisticated framework that not only detects tampering but also employs lossless auto-recovery mechanisms. This amalgamation of advanced technology not only ensures the authenticity of images but also guarantees their unaltered preservation, even in the aftermath of tampering attempts. The concept of an "Image Vaccinator" encapsulates our vision for a resilient, tamper-proofing system that goes beyond conventional security measures. By leveraging the capabilities of INNs, we have devised a sophisticated framework capable of detecting and mitigating tampering while ensuring the preservation of image fidelity. will unravel the intricate layers of the Image Vaccinator system, delving into the mechanics of INNs and showcasing their prowess in safeguarding digital images. Our empirical evidence and real-world applications will highlight the robustness of our approach, demonstrating its potential impact across various domains such as forensics, secure image communication, and archival preservation.

II. LITERATURE REVIEW

In recent years, the field of image manipulation detection has experienced significant strides, fueled by the development of sophisticated algorithms and methodologies aimed at discerning an array of image manipulations and forgeries. Among these advancements, Dong et al. introduced MVSS-Net, a pioneering multi-view multi-scale supervised network. This architecture

stands out for its utilization of diverse perspectives and scales, effectively enhancing the accuracy of manipulation detection [1]. Liang et al. contributed significantly to the domain with their robust hashing techniques tailored for image copy detection. Their methods, including local tangent space alignment and efficient hashing utilizing 2D–2D PCA, have notably fortified the foundations of image copy detection [2][3]. Lin et al. furthered the discourse by proposing a method predicated on multiple tampering traces and edge artifact enhancement, a strategy that amplifies sensitivity to subtle manipulation cues [4]. Zhang et al.'s dual-branch approach, leveraging noise and edge features, marked another pivotal development, bolstering detection robustness [5]. The landscape of manipulation detection also saw contributions from Liu et al.'s PSCC-Net, Wu et al.'s focus on robust forgery detection over online social networks, and Li et al.'s innovative fusion of multi-scale features for precise manipulation localization [6][7][8]. Meanwhile, Wang et al.'s ObjectFormer introduced a novel paradigm encompassing both detection and localization tasks, while Chen et al.'s emphasis on multi-view multi-scale supervision underscored the importance of holistic analysis approaches [9][10]. Complementing these scholarly contributions, resources like Matthes' Python Crash Course, Sweigart's Automate the Boring Stuff with Python, Ramalho's Fluent Python, Grinberg's Flask Web Development, and Tahaghoghi and Williams' Learning MySQL furnish practitioners with indispensable insights and guidance for implementing manipulation detection algorithms in practical contexts.In addition to these academic contributions, practical implementation resources such as Python Crash Course by Matthes [1], Automate the Boring Stuff with Python by Sweigart [2], Fluent Python by Ramalho [3], Flask Web Development by Grinberg [4], and Learning MySQL by Tahaghoghi and Williams [5] provide valuable insights and guidance for implementing manipulation detection algorithms in real-world applications.

III. TECHNICAL SPECIFICATIONS OF COMPONENTS USED:

A. Social Networking Web App:

Table Name: SN1_user1

S.No	Field	Data Type	Field size	Constraint	Description
9	id	int	11	Primary Key	User id
2	Name	varchar	20	Null	User Name
3	Gender	Varchar	10	Null	User Gender
4	Dob	Varchar	40	Null	User dob
5	mobile	Big int	20	Foreign Key	User Mobile
6	email	Varchar	20	Null	User Email
7	adhaar	Varchar	11	Null	User aadhar
8	Username	Varchar	20	Null	Post username
9	password	varchar	20	Null	Post password
10	Date_time	Time_stamp	Time_stamp	Null	Post Date time

B.

The social networking web app is meticulously crafted using Python, Flask, MySQL, Bootstrap, and Wampserver 2i to deliver a secure, responsive, and feature-rich user experience. The User Authentication module guarantees secure access, employing features such as user registration, login, password hashing, and two-factor authentication. The User Profile module fosters personalization, allowing users to create and customize profiles with responsive design elements.

C. End User Interface:

The End User Interface module provides a seamless and intuitive experience for social network users, encompassing essential functionalities such as registration, login, social connections, image sharing, download, and interaction with shared content. The module also includes features for applying digital attacks to images, sharing tampered content, and receiving notifications.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

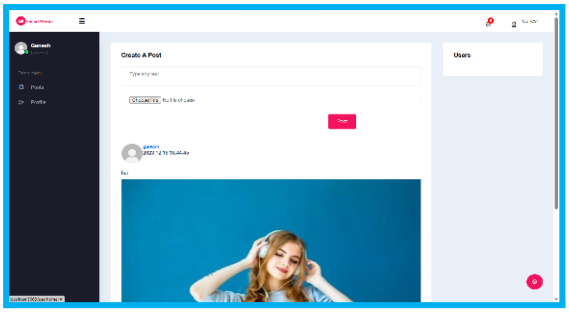

Fig.2 Interface

D. Adversarial Simulation: Training Against Threats

The system employs adversarial simulation, leveraging the capabilities of the Invertible Neural Network, to fortify its resilience against potential threats. Three malicious attacks - copy-move, splicing, and benign attacks like rescaling and blurring - are simulated during the training process. The Invertible Neural Network, is well-prepared to detect and counteract a diverse array of potential attacks, thereby enhancing its robustness in maintaining the integrity of the digital landscape.

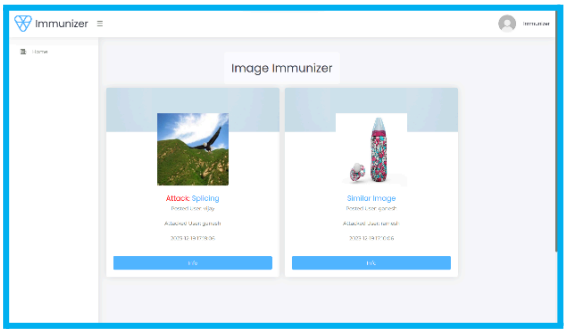

Fig.3 Identified Attack

E. Image Immunizer Middleware:

The Image Immunizer Middleware is a crucial component within a system designed to enhance the security and integrity of digital images. This middleware employs Cyber Vaccinator Framework to discern between vaccinated and unvaccinated, if unvaccinated means transform an original image to its edge map into an immunized version. Invertible Neural Network (INN) employs Forward pass to determine tampered areas by predicting the tamper mask and type of attack. Backward pass the recovery of the original image and its associated metadata. The module operates in real-time, seamlessly integrating into the image processing pipeline.

F. Objective Loss Function:

Lossless image recovery using Run-Length Encoding (RLE) is a technique that focuses on preserving the original image data while achieving efficient image recovery. Run-Length Encoding (RLE) can be a valuable tool in achieving this, ensuring that the original image is restored without loss of information after tampering has been detected and addressed. Subsequent to tamper removal, the image is subjected to RLE compression. Runs of consecutive identical pixel values are encoded to represent sequences more efficiently. The integration of tamper detection, removal, and lossless recovery using RLE enhances the overall resilience of the system against malicious manipulations.

G. Notification:

The Notification Module serves as a vital component in keeping users informed and empowered when it comes to shared vaccinated images on other social networks. Specifically, when a user downloads and shares a vaccinated image without any attack, the Image Immunizer detects the shared image and triggers an email notification to the user. The email prompts the user to make a decision regarding the shared image.

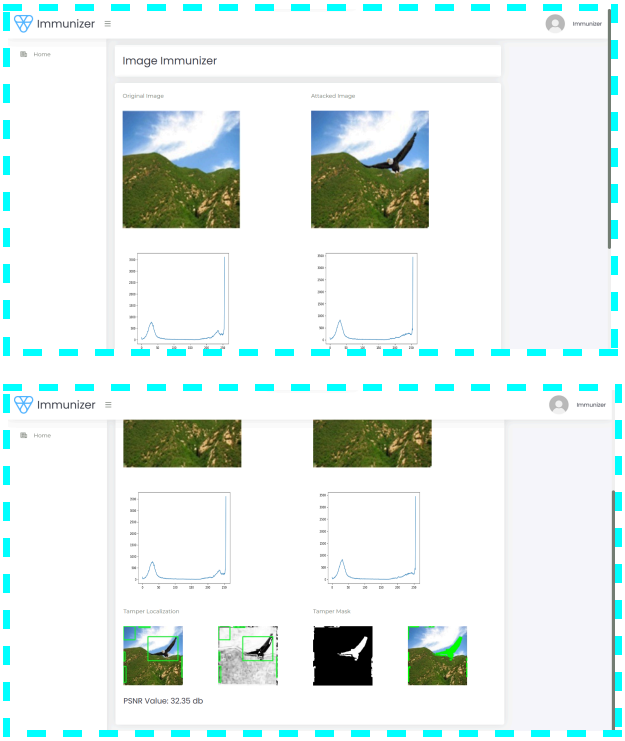

Fig.4 Image Immunizer

IV. PROPOSED METHODOLOGY

Digital forensics involves the examination of digital evidence to identify and analyse patterns of forgery. This may include analysing metadata, compression artefacts, and other forensic traces within the image. Signature-based methods use known patterns or signatures of forgery to identify manipulated images. These signatures may include noise patterns, repeated patterns, or specific features associated with common tampering techniques. Watermarking involves embedding invisible or visible marks within an image to identify its origin or ownership. Watermarks can help in tracking and verifying the authenticity of images. Image hashing involves generating a unique hash or fingerprint for an image. Any alterations to the image, even minor ones, result in a significant change in the hash value, allowing for the detection of forgery. Image processing techniques, including error level analysis (ELA) and noise analysis, are used to identify inconsistencies in pixel values or compression artefacts that may suggest tampering. Steganalysis techniques focus on detecting hidden information within images. This includes identifying alterations made through steganography, where additional information is concealed within the image. Some systems use block chain technology to timestamp and authenticate images. This ensures that the image's origin and content remain unchanged over time, providing a form of tamper-proofing. The Image Immunizer Middleware for Online Social Networks (OSN) using Invertible Neural Network (INN) is designed to enhance the security and integrity of images shared on social media platforms. Accurate tamper detection fortifies shared images against potential threats. Preserves original image quality during the recovery process. Prepares the system for OSN-specific threats, including deepfake attempts. Easily integrates with existing OSN architectures for widespread adoption.The proposed system comprises several key modules and functionalities to achieve this objective:

A. Deeps Learning:

Deep learning is a method in artificial intelligence (AI) that teaches computers to process data in a way that is inspired by the human brain. Deep learning models are computer files that data scientists have trained to perform tasks.

B. Multi Task Learning:

Multi-task learning (MTL), including learning services, is emerging as a pivotal concept in the rapidly evolving landscape of artificial intelligence. Multi-task learning (MTL) involves training a model to perform multiple tasks concurrently in machine learning. In deep learning, MTL pertains to instructing a neural network to undertake several tasks, achieved by distributing certain network layers and parameters across these tasks.

C. Hard Parameter Sharing:

This component involves sharing the hidden layers of a neural network while keeping task-specific output layers. It reduces overfitting by sharing layers across similar jobs.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

D. Soft Parameter Sharing:

Each model has its own set of weights and biases, and the spacing of these parameters in the model is regulated so that the parameters are homogeneous and representative of all applications.

E. Task Clustering:

MTL uses task clustering to group tasks. This guarantees that AI models learn from tasks with similar characteristics, resulting in improved knowledge transfer.

F. Shared Layers:

AI systems with shared layers enable models to learn shared representations across tasks. These shared layers promote learning synergy and eliminate redundancy.

G. Loss Functions:

MTL models can assign varied levels of importance to different activities thanks to tailored loss functions for each activity. This adaptability helps with performance enhancement in tasks of varying complexity.

H. Feature Extraction:

MTL uses feature extraction techniques to help AI models find task-specific and shared elements in data. This encourages efficient knowledge transfer.

I. Invertible Neural Network:

Invertible neural network (INN) is a promising tool for inverse design optimization. While generating forward predictions from given inputs to the system response, INN enables the inverse process without much extra cost. The inverse process of INN predicts the possible input parameters for the specified system response qualitatively. For the purpose of design space exploration and reasoning for critical engineering systems, accurate predictions from the inverse process are required. Moreover, INN predictions lack effective uncertainty quantification for regression tasks, which increases the challenges of decision making. A new loss function is formulated to guide the training process with enhancement in the inverse process accuracy. INN is a bidirectional mapping network based on affine coupling blocks, considered as an excellent approach for solving inverse problems. The forward process of an INN predicts the output from the input while the inverse process derives the distribution of the input parameters. The key information of its inverse process is captured by the latent variables. INN shines not only in the field of computer vision, but also has distinctive achievements in the field of inverse design. The forward process of the standard INN only gives the prediction result without presenting uncertainty.

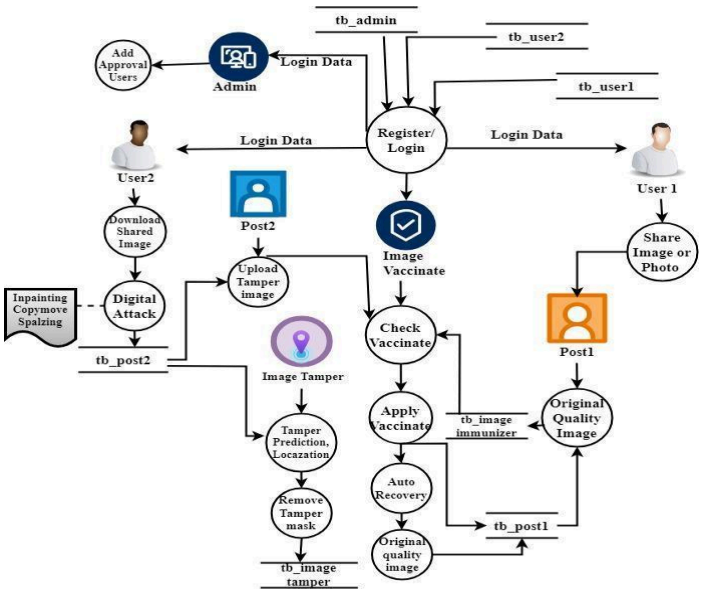

Fig 5. Block Diagram

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

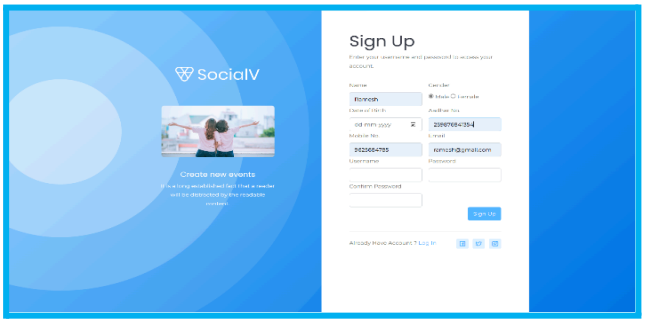

Fig 6. Website

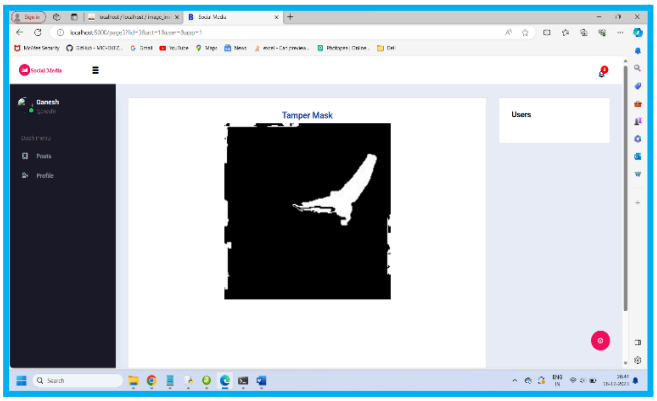

Fig 7. Tamper Mask

V. RESULT

The implementation of the image Immunizer Middleware for Online Social Networks (OSN) using the Invertible Neural Network (INN) has yielded promising results in enhancing the security and integrity of shared images on social media platforms. The system encompasses several key modules and functionalities designed to achieve this objective effectively. In the context of the broader Social Networking Web App, which serves as the foundation for the proposed system, the User Authentication module ensures secure access to user accounts through robust authentication mechanisms such as password hashing.

VI. APPLICATIONS

The Future enhancements for the Image Immunizer Middleware for Online Social Networks using Invertible Neural Network (INN) aim to strengthen its capabilities and adapt to evolving technology. Integrating blockchain technology can enhance transparency in image transactions, ensuring a tamper-evident record. The middleware's expansion to multimodal content analysis, including videos and audio, provides a more comprehensive defense against digital manipulation within OSN. These advancements reflect a commitment to robust security and holistic content integrity. The End User Interface module provides users with intuitive access to essential functionalities, including registration, login, social connections, image sharing, and notifications. Notably, the ability to apply digital attacks to images and share tampered content underscores the platform's commitment to raising awareness about potential threats and educating users about digital security. The Adversarial Simulation module plays a crucial role in training the system to detect and counteract malicious attacks such as copy-move, splicing, and in-painting. By leveraging the capabilities of the Invertible Neural Network, the system is equipped to identify and mitigate a diverse array of potential threats, thereby enhancing its resilience against digital manipulation. Central to the system's security architecture is the Image Immunizer Middleware, which employs the Cyber Vaccinator Framework and INN to distinguish between vaccinated and unvaccinated images, detect tampered areas, and facilitate image recovery. This real-time processing capability seamlessly integrates into the image processing pipeline, ensuring the authenticity and integrity of shared media. The Objective Loss Function,

incorporating techniques like Run Length Encoding (RLE) and Peak Signal-to-Noise Ratio (PSNR), further enhances the system's ability to detect and recover from tampering while preserving image quality and minimizing data loss.

VII. CONCLUSION

In conclusion, the project Image Immunizer Middleware for Online Social Networks offers a cutting-edge solution to combat the growing threat of digital image attacks. Invertible Neural Network technology and incorporating adversarial simulation, the system provides a formidable defense, securing the authenticity and integrity of images shared on social networking platforms. Through process involving the Cyber Vaccinator Module, the system adeptly pre-processes, vaccinates, and post-processes images, introducing imperceptible perturbations to fortify them against potential tampering. The Vaccine Validator ensures a vigilant distinction between vaccinated and unvaccinated media, enhancing the overall security posture. The Forward Pass, employing INN, and the subsequent Backward Pass for image self-recovery collectively contribute to the identification and restoration of tampered areas. This dynamic approach ensures that the recovered image closely aligns with the original, reinforcing the reliability of shared media. Adversarial simulation during training further strengthens the system, exposing it to a spectrum of potential threats, including both malicious and benign attacks. This proactive strategy equips the network to discern and counteract diverse forms of manipulation, enhancing its resilience. The middleware's seamless integration with existing OSN architectures not only ensures compatibility but also facilitates widespread adoption across popular social media platforms. Additionally, the system's ability to notify users about the status of shared images and its capability to restore tampered images contribute significantly to fostering a secure and trustworthy social media landscape. This project represents a state-of-the-art solution, combining advanced technologies and thoughtful design to safeguard the digital integrity of shared images in the dynamic realm of online social networks.

Table:IM_Tamper

S.No	Field	Data Type	Field size	Constraint	Description
1	id	int	11	Primary Key	User id
2	Posted user	varchar	20	Null	User Post
3	Attacked user	Varchat	20	Null	User Details
4	Original_id	Int	40	Null	User Photo
5	Post id	Int	20	Foreign Key	Date_Time Status
6	Original image	Varchar	20	Null	Post Status
7	Attacked Image	Varchar	11	Null	User Previious_Post Id
8	Attack Details	Varchar	20	Null	Post attack datails
9	Request status	Int	11	Null	User Request Status
10	Social app	Int	11	Null	User Social APP
11	Date_Time	timestamp	Null	Null	User Date_Time

Table.2 Tampered Data

REFERENCES

[1] Carducci, C. G. C., Monti, A., Schraven, M. H., Schumacher, M., & Mueller, D. (2019). Enabling ESP32-based IoT Applications in Building Automation Systems. 2019 II Workshop on Metrology for Industry 4.0.

[2] M.H. Schraven, C. Guarnieri Calo' Carducci, M.A. Baranski, D. Muller, ¨ A. Monti, "Designing a Development Board for Research on IoT Applications in Building Automation Systems," 36th International Symposium on Automation and Robotics in Construction (ISARC 2019), Banff, Canada, 2019, in press.

[3] ESP32 Overview by Espressif Systems (Shanghai) Co., Ltd. [Online].Available:https://www.espressif.com/en/products/hardware/e sp32/ overview

[4] Guide to Open Protocols in Building Automation, Schneider Electric, 2015. [Online]. Available: https://download.schneider-electric.com/files? p enDocType=Brochure&p File Name=SE+Protocols+Guide.pdf

[5] A. Maier, A. Sharp and Y. Vagapov, "Comparative analysis and practical implementation of the ESP32 microcontroller module for the internet of things," 2017 Internet Technologies and Applications (ITA), Wrexham, 2017, pp. 143-148

[6] D. Ghosh, A. Agrawal, N. Prakash and P. Goyal, "Smart Saline Level Monitoring System Using ESP32 And MQTT-S," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-5

[7] Rai, P., & Rehman, M. (2019). ESP32 Based Smart Surveillance System. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET).

[8] Pahuja, R. and Kumar, N., 2014. Android Mobile Phone Controlled Bluetooth Robot Using 8051 Microcontroller. International Journal of

Scientific Engineering and Research, 2(7), pp.14-17.

[9] Singh, P., Sharma, D. and Agrawal, S., 2011. A Modern Study of Bluetooth Wireless Technology. Dept. of Computer sci. & Eng. Raipur, (Chhattisgarh).

[10] Chinmayi, R., Jayam, Y. K., Tunuguntla, V., Dammuru, J. V., Nadella, H., Anudeep Dulla, S. S. K., … Nair, J. G. (2018). Obstacle Detection and Avoidance Robot. 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).

[11] Arvind Kumar Saini1, Garima Sharma2, Kamal Kishor Choure3, "BluBO: Bluetooth Controlled Robot," International Journal of Science and Research (IJSR) National Conference on Knowledge, Innovation in Technology and Engineering (NCKITE), 10-11 April 2015, pp. 325-328.

[12] Singh, A., Gupta, T., & Korde, M. (2017). Bluetooth controlled spy robot. 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC).

[13] Hossai, M. R. T., Shahjalal, M. A., & Nuri, N. F. (2017). Design of an IoT based autonomous vehicle with the aid of computer vision. 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE).

[14] Bairy A. (2022). Modeling Explanations in Autonomous Vehicles. In: ter Beek, M.H., Monahan, R. (eds) Integrated Formal Methods. IFM 2022. Lecture Notes in Computer Science, vol 13274. Springer, Cham.

[15] Aiman Ansari, Yakub Ansari, SaquibGadkari, AartiGoku: Android App Based Robot; Aiman Ansari et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6
(2) , 2015, 1598-1600

[16] Singh, P., Sharma, D. and Agrawal, S., 2011. A Modern Study of Bluetooth Wireless Technology. Dept. of Computer sci. & Eng. Raipur, (Chhattisgarh).

[17] Sairam, K.V.S.S.S.S., Gunasekaran, N. and Redd, S.R., 2002. Bluetooth in wireless communication. IEEE Communications

[18] Magazine, 40(6), pp.90-96

[19] Madhav, A.V.S., Tyagi, A.K. (2023). Explainable Artificial Intelligence (XAI): Connecting Artificial Decision-Making and Human Trust in Autonomous Vehicles. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P., Ganzha, M. (eds). Proceedings of Third International Conference on Computing, Communications, and Cyber-Security Lecture Notes in Networks and Systems. Springer, Singapore.

[20] Li Q, Wang Z, Wang W, Yuan Q. Understanding Driver Preferences for Secondary Tasks in Highly Autonomous Vehicles. In: Long S, Dhillon BS, editors. Man-Machine-Environment System Engineering. MMESE 2022. Lecture Notes in Electrical Engineering, vol. 941. Singapore: Springer; 2023.Kolb,

[21] A., Barth, E., & Koch, R. (2008). ToF-sensors: New dimensions for realism and interactivity. 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. doi:10.1109/cvprw.2008.4563159

[22] Monika Jain, Aditi, AshwaniLohiya, Mohammad Fahad Khan: Wireless gesture control robot; International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012 Viraj Mali, AnkitGorasia, MeghanaPatil, Prof. P.S.WawageDepartment of Information Technology, Vishwakarma Institute of Information Technology, Pune

[23] Prof. Horacio Espinosa: Robotic Control with Bluetooth Wireless Communication; Northwestern University