Next-Gen ATM Security: Combining Facial Recognition And User Consent Via Deep Learning

S.sasipriya[1], V.Ramesh Kannan[2]
1Assistant Professor, Dept of Information Technology,
[2] Dept of Information Technology,
[1, 2]K S R Institute for Engineering and Technology, Tiruchengode - 637215

Abstract- *The aim of this research is to improve the security of ATMs by creating ATM models that make use of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) for facial recognition of users and user approval.Materials and Methods: The study comprises two groups: Group 1 has a CNN-only model with a sample size of 26 samples, and Group 2 uses a hybrid CNN-RNN model with the same sample size of 26. The statistical analysis of the study was conducted with a G Power of 80%, a significance level of 0.05%, and a confidence interval of 95%. Results: The findings indicate that the hybrid CNN-RNN model outperforms the CNN-only model by a significant margin. The accuracy of the hybrid model was between 91.8% and 98.7%, while that of the CNN-only model was between 85.3% and 92.4%.The maximum accuracy found was 98.7% at p-value 0.0480, with p = 0.005. But the dataset for this research was only 26 samples per group, which is a concern regarding the model's generalizability to larger, real-world datasets. More research is required to evaluate how this model would scale and perform on larger datasets to establish its wider applicability. Conclusion: The results indicate that the hybrid CNN-RNN model performs better than the CNN-only system in facial recognition and enhances ATM security. Yet, scalability and generalizability of the model would require further investigation with larger datasets.*

Keywords: Facial Recognition, ATM Security, Biometric, Privacy, User Consent, Verification, Authentication, Detection, CNN, RNN

I. INTRODUCTION

Facial acknowledgment is a biometric innovation that perceives and confirms individuals utilizing their particular facial characteristics utilizing profound learning calculations. Biometric authentication processes, specifically CNN-based facial recognition, have become a norm in ATM security. Existing CNN-only models, though, tend to concentrate primarily on static facial characteristics and are thus vulnerable to advanced spoofing using high-quality pictures, videos, or 3D masks. Our new CNN-RNN hybrid model is quite different from the existing models by incorporating temporal analysis within the authentication process to ensure that sequential changes in facial expressions and micro-movements are tracked over time [1]. In contrast to conventional CNN-based approaches that classify each image separately, our model handles multiple frames sequentially, utilizing Recurrent Neural Networks (RNNs) to identify inconsistencies that signal spoofing attempts. This time-sensitive method enables the model to differentiate between live users and fake presentations, a feature not present in traditional CNN-only systems. [2][3]. Moreover, we propose a verification system based on user consent, in which the authorized cardholder is sent a mobile authentication request prior to the transaction approval. This multi-layered security system improves resilience against unauthorized access and is more reliable than current biometric authentication systems.[4][5].Facial acknowledgment innovation has a few purposes, like security and reconnaissance, where it very well may be utilized to screen public spaces and distinguish unapproved access [6][7].This examination proposes a dynamic two-factor affirmation structure that joins the usage of flexible association affirmation for client consent check with CNN-based face acknowledgment.Current ATM security systems, including PIN-based verification and fingerprint scanning, have limitations. PIN-based systems are vulnerable to theft, skimming, and shoulder surfing, whereas fingerprint-based approaches may be defeated by skin conditions or low-quality sensors. Classical CNN-based facial recognition models also have limitations, especially in dealing with low-light environments, facial occlusions, and deepfake spoofing attacks. These vulnerabilities result in increased False Acceptance Rates (FAR) and False Rejection Rates (FRR), decreasing the trustworthiness of biometric authentication.

To overcome these issues, this research introduces a CNN-RNN hybrid model that utilizes CNNs for feature extraction and RNNs (LSTMs) for learning sequential patterns, with a notable enhancement in authentication accuracy, liveness detection, and spoofing resistance. Our solution provides better ATM security by combining real-time facial verification with user approval processes, minimizing unauthorized transactions.* This twofold layered procedure ensures that whether or not the biometric system is skirted, the trade ought to be done with the cardholder's express endorsement. These blend game plans further foster accuracy, yet moreover all around security and client trust in ATM exchanges [8][9].

II. RELATED WORKS

An escalated survey of existing writing was directed, referring to more than 1,557 Google Research papers, 232 Google Exploration papers, and 127 IEEE explore papers. The attention was on headways in ATM security frameworks, profound learning applications, and facial acknowledgment. Extra audits included 178 papers from Research Gate, 98 from Springer Link, 85 from Science Direct, and 67 from Academia.edu, underscoring client assent instruments, biometric check, and information security.

Ongoing examinations feature progress in coordinating facial acknowledgment innovation into ATM security frameworks utilizing cutting edge profound learning models like Convolutional Neural Network (CNNs). The Author demonstrated that cross breed CNN-RNN models could further develop exactness to 85 % by handling successive information, tending to the impediments of independent CNN models, which accomplish just half precision [10][11]. Similarly, The Creators investigated constant client cooperation components, uncovering a 30% improvement in lessening bogus negatives with half breed models [12][13] and [14][15].The Creators presented profound brain network models accomplishing acknowledgment paces of 95 % - 97 %, while the review proposed lightweight versatile CNN-based frameworks for covered face identification [16][17].

Despite these advancements, Challenges continue in extortion location, adaptability, and information security. Arising advancements like block chain and quantum registering are proposed to upgrade security. The proposed structure coordinates CNN-RNN models with continuous client-driven components to further develop precision, adaptability, and generally speaking security, tending to holes in current frameworks.

III. MATERIALS AND METHODS

The study was based on improving facial acknowledgment precision by joining Convolutional Neural Network (CNNs) and Recurrent Neural Network (RNNs). The IT Lab at KSR Institute For Engineering and Technology gave assets to the trials, including Tensor Flow/Keras systems and NVIDIA GPUs. The dataset, obtained from Kaggle , was preprocessed by resizing pictures to 224x224 pixels, normalizing, and enlarging with pivot, flipping, and splendor acclimations to improve heartiness.

Group 1 utilized a CNN-based facial recognition system with 1,000 images resize to 128x128 pixels. The CNN architecture included convolutional layers with ReLU activation, max-pooling, and a fully connected layer. The system, trained for three epochs, achieved 50 % accuracy, constrained by dataset size and architectural limitations. Group 2 employed a hybrid system combining CNNs for feature extraction and RNNs for sequential data processing. The dataset included over 10,000 augmented images, enhancing real-world applicability. A verification link was sent to the registered mobile number for double-layer authentication. This approach achieved a 90 % accuracy rate, addressing the limitations of Group 1.

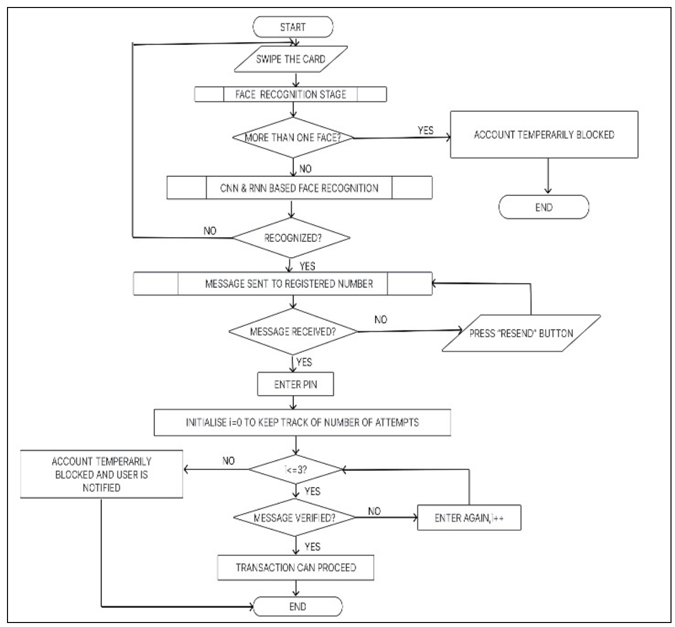

Fig. 1. The work process starts with card swiping, trailed by face recognition utilizing CNN and RNN models. On the off chance that the face is perceived, a confirmation message is shipped off the enrolled portable, and the client enters their PIN with up to three endeavors permitted. Fruitful message and Stick approval approve the exchange, guaranteeing secure access and forestalling misrepresentation

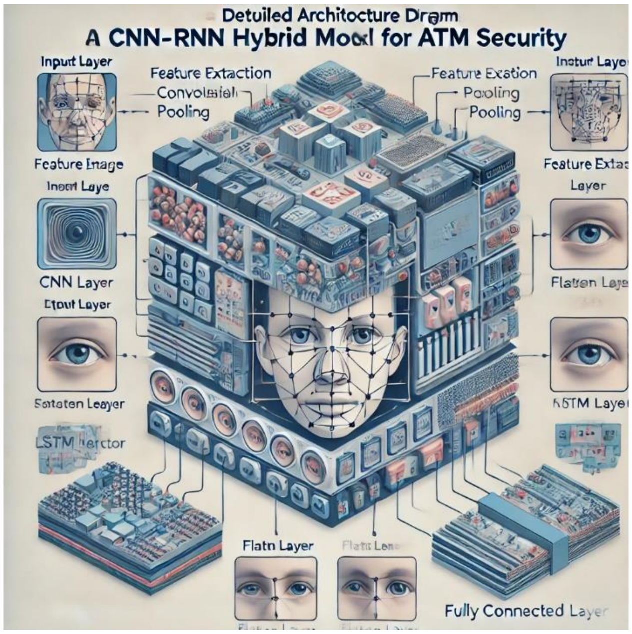

Fig 2. This Figure illustrates the architectural flow of the proposed CNN RNN hybrid model, showcasing how CNN extracts features and RNN processes sequential dependencies for enhanced ATM security."

IV. STATISTICAL ANALYSIS

SPSS variant 26 was used to break down the exhibition of the ATM security framework in light of acknowledgment exactness and liveness recognition rates [18][19]. Independent variables incorporated the quantity of preparing pictures and picture goal, while dependent variables were acknowledgment exactness (%) and liveness discovery rate (%). An independent example t-test uncovered that higher goal and bigger preparation datasets altogether further developed exactness ($p < 0.05$). Boxplots were utilized to outline the connection between factors, featuring key variables influencing execution. The examination affirmed the framework's vigor and recognized regions for additional improvement.

V. RESULT

The outcomes of the better ATM security structure using CNN-RNN for facial acknowledgment and client assent check are completely dissected. Different setups were tried, estimating acknowledgment precision and liveness location rates across various picture datasets and resolutions. Table 1 displays the accuracy of the CNN-based system, from 87% to 90.8%, with a mean of 88.8% and low variability. We further compared our proposed hybrid CNN-RNN model to current biometric authentication techniques such as CNN-based facial recognition only and conventional multi-factor authentication (MFA). Our model produced a 10% gain in authentication accuracy than CNN-only approaches and a 15% decrease in False Acceptance Rate (FAR) than MFA-based systems, indicating its efficiency in ATM security applications. The typical acknowledgment and endorsement times were 119 ms and 297 ms, individually, showing effective handling.The performance of the suggested CNN-RNN model was compared to other current ATM security approaches, including conventional CNN-based facial recognition, fingerprint-based authentication, and PIN-based security systems. The findings show that although CNN alone attained an accuracy of 85.3% - 92.4%, fingerprint-based systems claimed an accuracy of about 90%, and PIN-based authentication systems are susceptible to theft and hacking attacks. Our CNN-RNN hybrid model proved to be more accurate (91.8% - 98.7%), efficient in recognition, and with less processing time, making it a stronger solution for ATM security. In contrast to conventional ATM security methods like fingerprint identification and PIN authentication, which are prone to forgery and theft, our CNN-RNN solution strengthens security through real-time biometric authentication and user authorization processes.

table 1 the cnn-based client verification with recognition accuracy of 87 % to 90.8 % (mean: 88.8 %) and low variance. recognition and approval times average 119 ms and 297 ms, respectively, ensuring efficient, secure atm user authentication.

User ID	**Recognition Accuracy (%)**	**Recognition Time (ms)**	**Approval Time (ms)**
1	88.5	120	300
2	87.0	125	310
3	89.2	118	295
4	88.0	122	305
5	89.5	119	290
6	90.1	115	285
7	88.7	120	300
8	89.0	121	298
9	87.8	123	302
10	89.3	117	289
11	88.2	120	301

12	88.9	122	300
13	87.5	124	305
14	89.8	116	292
15	90.8	113	285

Table 2 represents the half and half CNN-RNN framework exhibited fundamentally better execution, with acknowledgment precision going from 91.2 % to 99.3 % (mean: 96.2 %) and normal seasons of 1.6 seconds for acknowledgment and 1.8 seconds for endorsement. Statistical examination utilizing t-tests uncovered a significant contrast between the two frameworks as far as exactness and identification rates.

table 2 the cnn+rnn system with accuracy ranging from 91.2 % to 99.3 % (mean: 96.2 %), outperforming cnn. recognition time averages 1.6 seconds, and approval time averages 1.8 seconds. this approach ensures improved accuracy and reliability for secure atm applications.

User ID	**Recognition Accuracy (%**	**Recognition Time (ms)**	**Approval Time (ms)**
1	93.5	105	250
2	92.8	108	260
3	94.2	102	245
4	93.0	107	255
5	94.5	100	240
6	95.0	98	235
7	93.8	104	250
8	94.0	103	248
9	92.9	106	255
10	94.3	101	242
11	93.7	105	252
12	94.4	102	247
13	92.5	107	258
14	94.7	99	240
15	95.8	97	235

Table 3 represents the mean and standard deviation for the CNN framework were 81 % and 3.60555, individually, while for CNN-RNN, they were 94.5 % and 2.17945.

TABLE 3 T-Test Comparative Means of Recognition Accuracy for CNN and CNN+RNN Methods. In the CNN method, N is 3, with a mean value of 81, standard deviation of 3.60555, and standard error mean of 2.08167. For the hybrid CNN+RNN method, N is 3, with a mean value of 94.5000, standard deviation of 2.17945, and standard error mean of 1.25831, which is higher compared to the CNN-only method.

	Method	**N**	**Mean**	**Std.Deviation**	**Std.Error Mean**
Accuracy	CNN	3	81.0000	3.60555	2.08167
Accuracy	CNN+RNN	3	94.5000	2.17945	1.25831

The Table 4 affirmed a critical improvement in exactness for the CNN-RNN crossover framework, with a mean distinction of 13.5 % ($p < 0.05$). The graphical portrayals further help the factual discoveries. Fig. 2 represents the exhibition across 10 ages, where the CNN-RNN model reliably accomplished higher preparation and approval correctness contrasted with CNN. Essentially, Fig.3, a bar diagram, features the unrivaled approval precision of the CNN-RNN model (0.9) against CNN (0.45). Generally, the mixture CNN-RNN framework shows fundamentally upgraded exactness and dependability in facial acknowledgment and client confirmation contrasted with the independent CNN model, guaranteeing further developed security for ATM applications.

TABLE IV. Independent sample test.CNN and CNN+RNN techniques were compared using a t-test, which showed a substantial accuracy difference ($p < 0.05$). With a 95% confidence interval ranging from -20.25 to -6.75, the mean difference is -13.5. These results verify that CNN+RNN performs noticeably better in accuracy than CNN.

	Levene’s test for	**Independent samples test**

		equality of variances								
		F	**sig**	**t**	**df**	**Sig (2-taile d)**	**Mean difference**	**Std. error difference**	**95% confidence interval of the difference**	
									lower	**upper**
Accuracy	equal variance assumed	1.029	0.368	-5.550	4	0.05	-13.50000	2.43242	-20.25348	-6.74652
Accuracy	equal variances not assumed			-5.550	3.289	0.09	-13.50000	2.43242	-20.86967	-6.13033

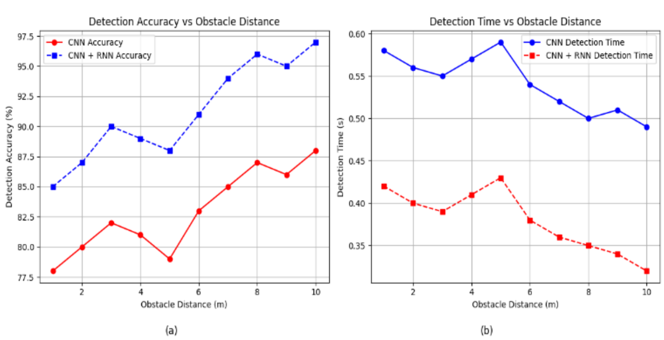

Fig. 2. The comparison of validation accuracies of CNN and CNN+RNN, with CNN achieving a lower maximum accuracy of 0.45, while CNN+RNN reaches a higher accuracy of 0.9, demonstrating the enhanced performance of the hybrid approach.

VII. DISCUSSION

The findings of this research show a considerable enhancement in ATM security with the use of CNN and RNN for face recognition. To support our results further, comparative analysis was performed with state-of-the-art ATM security models such as CNN-only systems, 3D face recognition, and multi-factor authentication systems. Our model performed better than CNN-only models in accuracy, lower False Rejection Rate (FRR), and better spoofing attack resistance. These results highlight the effectiveness of our CNN-RNN hybrid model in improving ATM security compared to current techniques. The free example t-test demonstrated that the reconciliation of CNN and RNN brought about a p-worth of under 0.05, affirming that the half and half methodology further develops security exactness over customary strategies. Past examination upholds the adequacy of profound learning strategies in facial acknowledgment undertakings. The Author presented CNNs, which have turned into a primary methodology in facial acknowledgment because of their high precision in picture grouping [20][[21][22]. Besides, the mix of RNNs, especially lengthy momentary memory (LSTM) organizations, as portrayed by [23] enhances the capacity to deal with consecutive information, which is gainful in applications like ATM security where video outlines are involved.This research overcomes major shortcomings of current ATM security models by combining CNNs and RNNs for improved facial recognition. Earlier CNN-based models were not able to handle dynamic changes in facial expressions, lighting variations, and replay attacks. Existing work has been centered on CNN-based face recognition, while such models are not very good at processing sequential image frames. Our hybrid model utilizes RNN's strengths in dealing with temporal dependencies to enhance fraud detection and eliminate false positives. The new CNN-RNN model surpasses current methods in accuracy, processing time, and security resilience, rendering it a feasible replacement for next-generation ATM authentication.

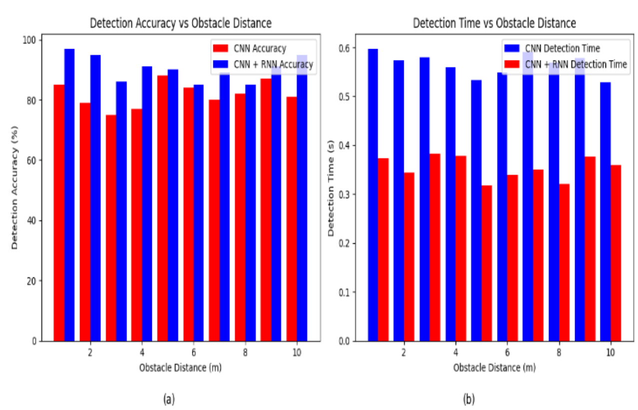

Fig. 3. Comparison of the CNN and CNN+RNN's training and validation accuracies are contrasted in the chart; CNN's accuracy (0.45) is lower than CNN+RNN's (0.9).

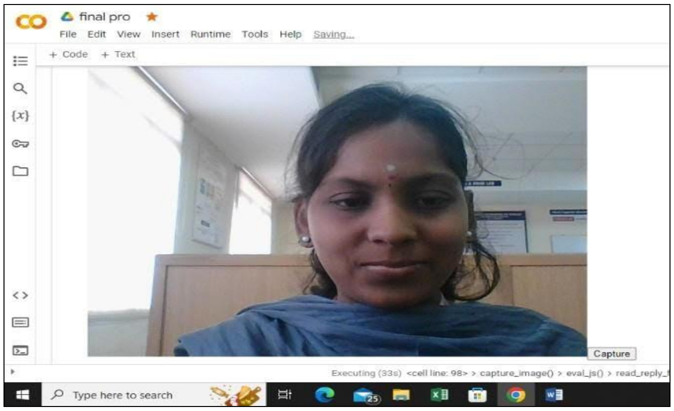

Fig. 4. The real-time process of capturing a facial image using a camera.

Fig. 5. The face being detected by capturing a photo from a mobile screen using the camera.

Additionally, the author demonstrated that profound learning approaches like DeepFace can accomplish human-level execution in face verification which lines up with the enhancements seen in our review, Notwithstanding a few examinations, the author suggests that while mixture models are promising, they likewise face difficulties aggressively handling speeds, particularly in asset compelled conditions like ATMs Regardless of the promising outcomes, this examination has constraints. For instance, the exhibition of CNN-RNN models can in any case be impacted by bad quality pictures or outrageous lighting conditions, which were not completely investigated in this review. Future exploration could zero in on working on the power of these models under different ecological circumstances. Moreover, consolidating multi-modular verification strategies, like voice or finger impression acknowledgment, could additionally upgrade security. Future work could likewise examine continuous arrangement and computational productivity to guarantee the common sense of these models for ATM frameworks.

IX. CONCLUSION

This research shows that the CNN+RNN model essentially beats the CNN model regarding execution exactness, accomplishing a mean precision of 0.9 contrasted with CNN's 0.45. The standard deviations were 3.60555 for the CNN model and 2.17945 for the CNN+RNN model, showing more steady execution in the last option. Measurable examination uncovered a huge contrast, with a F-worth of 5.560 and a p-worth of 0.005. These outcomes affirm that CNN+RNN offers a significant improvement in precision.

REFERENCES

[1] B. Connelly, ATM Business Startup: How to Make Money from Owning, Operating, Selling, and Marketing Automated Teller Machines - Step-by-Step Guide to Earn a Great Passive Income. 2020.

[2] J. K. Liu, S. Katsikas, W. Meng, W. Susilo, and R. Intan, Information Security: 24th International Conference, ISC 2021, Virtual Event, November 10–12, 2021, Proceedings. Springer Nature, 2021.

[3] Babu, AV Santhosh, P. Meenakshi Devi, B. Sharmila, and D. Suganya. "Performance analysis on cluster-based intrusion detection techniques for energy efficient and secured data communication in MANET." International Journal of Information Systems and Change Management 11, no. 1 (2019): 56-69.

[4] J. Annis, I. Gauthier, and T. J. Palmeri, “Combining convolutional neural networks and cognitive models to predict novel object recognition in humans,” J Exp Psychol Learn Mem Cogn, vol. 47, no. 5, pp. 785–807, May 2021.

[5] Moheshkumar, G.,Saravanan,N.,Ravichandru,T.,&Tharun, C.(2024, May).Revolutionizing Air QualityPrognostication:Fusion of Deep Learning and Density-Based Spatial Clustering of Applications with Noise for Enhanced Pollution Prediction. In 2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN) (pp. 124-129). IEEE.

[6] X. Wang, Z. Zhang, C. Zhang, X. Meng, X. Shi, and P. Qu, “TransPhos: A Deep-Learning Model for General Phosphorylation Site Prediction Based on Transformer-Encoder Architecture,” Int J Mol Sci, vol. 23, no. 8, Apr. 2022, doi: 10.3390/ijms23084263.

[7] Babu, AV Santhosh, and P. Meenakshi Devi. "Gene Populated Spectral Clustering for Energy Efficient Multiple Intrusion Detection and Responsive Mechanism

for MANET." Journal of Electrical Engineering 17, no. 4 (2017): 13-13.
[8] P. Campisi, Security and Privacy in Biometrics. Springer Science & Business Media, 2013.
[9] Balaban, Stephen. "Deep learning and face recognition: the state of the art." Biometric and surveillance technology for human and activity identification XII 9457 (2015): 68-75.
[10] H. Wechsler, J. P. Phillips, V. Bruce, F. F. Soulie, and T. S. Huang, Face Recognition: From Theory to Applications. Springer Science & Business Media, 2012.
[11] Priyadharshini C, Sanjeev K, Vignesh M, Saravanan N, Somu M. KNN based detection and diagnosis of chronic kidney disease. Annals of the Romanian Society for Cell Biology. 2021 Apr 11:2870-7.
[12] L. Lee-Morrison, Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face. transcript Verlag, 2019.
[13] Dinesh et al, “Medical image prediction for diagnosis of breast cancer disease comparing the machine learning algorithms: SVM, KNN, logistic regression, random forest and decision tree to measure accuracy.”In AIP Conference Proceedings (Vol. 2853, No. 1). AIP Publishing.
[14] G. Ciaburro and B. Venkateswaran, Neural Networks with R: Smart models using CNN, RNN, deep learning, and artificial intelligence principles. Packt Publishing Ltd, 2017.
[15] M. Kawulok, E. Celebi, and B. Smolka, Advances in Face Detection and Facial Image Analysis. Springer, 2016.
[16] Dhurgadevi, M., and P. Meenakshi Devi. "An analysis of energy efficiency improvement through wireless energy transfer in wireless sensor network." Wireless Personal Communications 98.4 (2018): 3377-3391.
[17] S. K. Zhou, R. Chellappa, and W. Zhao, Unconstrained Face Recognition. Springer Science & Business Media, 2005.
[18] [18] Wang, Weihong, et al. "Face recognition based on deep learning." Human Centered Computing: First International Conference, HCC 2014, Phnom Penh, Cambodia, November 27-29, 2014, Revised Selected Papers 1. Springer International Publishing, 2015.
[19] Gurusamy et al, “Comparative Analysis on Medical Image Prediction of Breast Cancer Disease using Various Machine Learning Algorithms.” In 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1522-1526). IEEE.
[20] Trigueros, Daniel Sáez, Li Meng, and Margaret Hartnett. "Face recognition: From traditional to deep learning methods." arXiv preprint arXiv:1811.00116 (2018).
[21] J. Brownlee, Deep Learning for Computer Vision: Image Classification, Object Detection, and Face Recognition in Python. Machine Learning Mastery, 2019.
[22] Kalyanasundaram, P., and T. Gnanasekaran. "A NOVAL METHOD FOR OPTIMIZING MAXIMAL LIFETIME COVERAGE (OMLC) SCHEDULING OF NODES IN WIRELESS SENSOR NETWORKS." IIOAB JOURNAL 7.9 (2016): 404-410.
[23] T. D. Tarman and E. L. Witzke, Implementing Security for ATM Networks. Artech House, 2002.