Development of an Electronic Voting System using Blockchain Technology and Deep Hybrid Learning

MD. ABDUL BASED[1,*], ELIAS UR RAHMAN[1], MOHAMMAD SHORIF UDDIN[2]
[1]Department of Computer Science and Engineering,
Dhaka International University,
Dhaka,
BANGLADESH

[2]Department of Computer Science and Engineering,
Jahangirnagar University,
Dhaka,
BANGLADESH

[*]*Corresponding Author*

Abstract: - Democratic people cannot function properly in today's sophisticated societies (where voting is a prominent issue) without electronic voting technologies. This study explores the use of hybrid learning algorithms for biometric authentication of voters, and blockchain technology for secure electronic voting. The thorough analysis includes a collection of more than 50,000 fingerprint samples using custom Convolutional Neural Network (CNN), VGG16, VGG19, Xception, and Inception. The algorithms are evaluated using F1-score, recall, accuracy, and precision. By combining Random Forest with a specially designed CNN, a novel hybrid learning algorithm is developed for authentication purposes. This blended model provides the best outcome in terms of accuracy (99.32%) and precision (99.32%). In addition, a web application was developed. This application integrates blockchain technology for electronic voting using Flask, HTML, and Solidity. By using blockchain, tampering and unauthorized access are prevented. It also ensures impartial voting and secure storage. The tabular presentation of the results provides a clear summary of each candidate's total votes.

Key-Words: - Electronic Voting, Hybrid Learning Algorithms, Biometric Fingerprint Matching, Voting Security, CNN, Random Forest.

Received: November 16, 2023. Revised: June 19, 2024. Accepted: July 14, 2024. Published: August 14, 2024.

1 Introduction

Voting is one of the many aspects that are rapidly changing due to new technologies. Making sure that the votes are secure, reliable, and visible to all is essential as paper ballots are transited to electronic ones in Electronic Voting (e-voting). The goal of this paper is to integrate two significant technological advancements. One method is matching fingerprints using hybrid learning algorithms. The other is improving and securing electronic voting with blockchain technology. While e-voting offers great potential, there are drawbacks as well. The key concerns here are voters' eligibility and ensuring that the people casting votes are the actual voters. Using biometric identification techniques appears promising in this scenario. Significant studies [1], [2] have sparked interest in the safe and accurate use of fingerprints for voter identity confirmation. Like most other fields, voting electronically with fingerprints resolves the unique issues associated with selecting public officials.

As biometric identification becomes popular in e-voting, picking the right techniques is very important. Many researchers have seen the use of hybrid learning methods. These mixed ways can provide better results. The biometric system analyzed in this paper includes VGG16, VGG19, Xception, Inception, and a modified Convolutional Neural Network (CNN). Each of these algorithms is applied to spot special shapes in fingerprint information. This makes the task of matching fingerprints better and quicker. The reason for using mixed learning methods is because the blended method can pick out important details from hard data, helping to see unique features in each fingerprint. This research wants to use the good points of hybrid learning in different ways, [3].

Blockchain technology has become a big talk for its chance to change e-voting systems and make them safer and more open. Blockchain allows people to keep records without a big boss or any person changing the information, and offers a new way to deal with old problems that come up in traditional voting methods. An explanation of how blockchain can change things are discussed in [4] and [5]. It doesn't just keep voting data safe but also creates a permanent record of the whole election process. The blockchain to the voting system is implemented in this paper by creating a website using Flask, HTML, and Solidity. This application connects the voting system on computers with blockchain. It makes sure votes are safe, can be checked easily, and counted clearly. This study wants to fix the worries about vote rigging, sneaky access, and dishonest actions in elections by using blockchain's security features.

There are two main goals of this research. First, it plans to carefully study the chosen mixed learning methods (VGG16, VGG19, Xception, Inception, and CNN) to see how well they work for matching fingerprints. This approach looks to measure quality including accuracy, precision, recall, and F1-score. Second, the study tries to show how blockchain technology can be added to the design of the voting system. This gives a safe and open way for storing and counting votes. Working on the website application aims to make online voting systems stronger and grow trust in democracy.

2 Literature Review

The path of Electronic Voting (e-voting) systems has changed over many years. It grew together with progress in technology and the change society made towards becoming more digital. In the middle of the 1900s, punch cards were first used in e-voting systems. These are like beginning steps for having e-voting everywhere instead of paper ballots in polling stations.

In the late 1900s, fingerprints became a main way to find criminals after it was found out that the fingerprints were unique, [1]. This important and useful finding soon took over old ways, like using body size to find out who did bad things. Using fingerprints for checking bad people got popular. The police in many cases used them and made a database with fingerprints from the criminals. Then they started using lifted fingerprints found at crime scenes to know who did the crime and catch them. Biometric recognition has changed a lot in the past century. It's now used for safe logins and checks, making sure people have certain jobs. It's also used by legal authorities to figure out who was involved in a situation or check positive ID of individuals in many areas.

A combination of Convolutional Neural Network (CNN) and Back Propagation Neural Network (BPNN) is proposed in [6] for an improved Fingerprint Identification System. Although BPNN is a wonderful choice for hybrid learning, some of its drawbacks take it to the edge. As a result, CNN is combined with Random Forest (RF) in this paper to create a more suitable and robust hybrid learning algorithm. This gives freedom and is more suitable for hierarchical structures.

In [7], a method is proposed where the authors combined a Support Vector Machine (SVM) with CNN. Using their proposed method, they acquired an accuracy of 95%. However, Random Forest is more suited for matching fingerprint algorithms. As a result, in this study, using the combination of RF and CNN gives an accuracy of more than 99%.

In [8], another method is presented where for image preprocessing Improved Whale Optimization Algorithm (IWO), and for person detection, Teacher Learning-based Deep Neural Network (TL-DNN) are used. This proposed method gives the study a new edge as it combines different algorithms for the purpose of clear biometric identification.

Hybrid learning, a fusion of different machine learning architectures, has gained prominence in various applications, including biometric identification. A seminal overview is provided in [3] of deep learning, highlighting the capabilities of Neural Networks (NN) in extracting intricate features from complex datasets. In the context of electronic voting, hybrid learning algorithms offer the promise of improved accuracy and robustness in biometric matching.

Decentralized and tamper-resistant ledger blockchain has emerged as a revolutionary technology with remote references for the security of e-voting systems. The work in [4] clarifies the basic principles of blockchain and its potential applications in various areas, including elections. Blockchain technology can handle vote tampering, fraud, and unauthorized access in the voting systems.

Blockchain mining along with the mechanisms to offer the security of blockchain networks are discussed in [5]. The integration of blockchain in e-voting ensures the security of the voter and the verifiability of the vote by the voter. The blockchain also mitigates the vulnerabilities associated with centralized voting databases and provides a decentralized trusted system for recording and counting votes.

The hybrid learning algorithms for fingerprint matching in this research provide better performance compared to the relevant existing works. The evaluation of the VGG16, VGG19, Xception, Inception, and CNN algorithms is done using the performance metrics accuracy, precision, recall, and F1-score. This provides viability in real-world e-voting scenarios.

The blockchain technology in e-voting adds an additional level of security and transparency through its decentralized and tamper-resistant nature. This ensures that the votes are stored securely, verifiable, and tallied transparently in order to address the integrity of the e-voting system. Thus this research enhances the security, reliability, and transparency of e-voting systems by combining both biometric identification and blockchain technology.

3 Proposed Methodology

This study creates a new path to the future using efficient algorithms to identify fingerprint matching. Voter identification and voting security are some of the greatest threats to democratic countries. This paper tries to solve them using various methods containing hybrid deep learning algorithms for voter identification using fingerprints, and blockchain technology for the security of the voting system.

Thus, the path to a secure and trustworthy voting system is clearer. The hybrid deep learning model for voter authentication is shown in Figure 1.

The algorithm for the hybrid learning model is shown in Algorithm 1.

Algorithm1: Algorithm for the hybrid deep learning algorithm

1. Loading the dataset into a single variable as a multi-dimensional array
2. The arrays are shuffled randomly to train the model efficiently
3. Separating the training image and training labels
4. Converting the arrays for training
5. Creating or importing the model
6. Training the model
7. Extracting the features from the images
8. Using the features to train the Random Forest Classifier
9. Evaluating the hybrid model

3.1 Data Collection

Data Collection is a crucial part of the study as it vastly depends on the collected image data for evaluation of the algorithms. For this purpose, a team dataset of around 700 students was used. The open dataset of SOCOFing [9] was also used for the study. In the SOCOFing's dataset, it had Altered Fingerprint images. These Altered Fingerprint images contained Arch, Left Loop, Right Loop, Tented, and Whorl fingerprints. Combining this dataset with the team dataset, the study worked with upmost 50,000 fingerprint image datasets. All of these fingerprint images were combined for a more complex and versatile study. Figure 2 shows some samples of the fingerprint images.

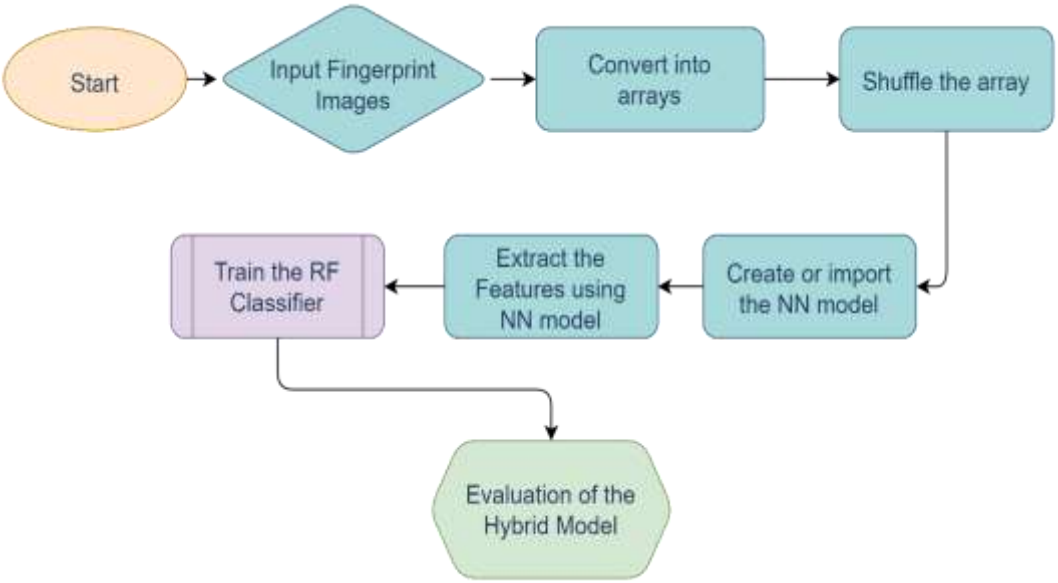

Fig. 1: The Hybrid Deep Learning Model for Voters' Authentication

Fig. 2: Fingerprint Image Samples for Dataset

3.2 Data Preprocessing

The dataset is loaded as a multi-dimensional array. Representing images as multi-dimensional arrays allows thepreservation of the structure of the images and makes it easier to interpret and process. Deep learning frameworks like TensorFlow and Keras work with multi-dimensional arrays as their primary data structure. Loading image data as multi-dimensional arrays makes it compatible with these frameworks. Neural Network (NN) model, including CNN, VGG16, VGG19, Xception, and Inception, expect input data in the form of multi-dimensional arrays. Each of these dimensions corresponds to a specific aspect of the data, such as the height, width, and channels for images. Converting images to multi-dimensional arrays allows them to normalize according to the needs of the deep learning algorithms.

3.3 Neural Network Models for Feature Extraction

Various NN models like CNN, VGG16, VGG19, Xception, and Inception were used to extract the features from the images so that the Random Forest Classifier could be trained upon the features. CNN is one kind of feed-forward neural network that is able to extract features from data. CNN does not extract features manually from the data as opposed to traditional feature extraction methods, [10], [11], [12]. This algorithm extracts the features using a convolutional structure which is very efficient. It can detect patterns in the images using these layers. Convolutional layers apply filters to the input to detect various features and pool layers down sample the spatial dimensions.

VGG16 and VGG19 are models that have a straightforward architecture with only 3x3 convolutional filters and 2x2 pooling layers, [13]. Although they might have a similar structure, VGG19 is deeper than VGG16. However, this increased depth comes at the cost of higher computational requirements.

Xception short for “Extreme Inception” replaces traditional convolutions with depth-wise separable convolutions. Although this reduces the number of parameters and computational cost it is quite inefficient in the context of finding matches in the fingerprint images.

Inception, also known as GoogLeNet, is a CNN architecture that consists of multiple stacked Inception modules, [13]. These modules allow the network to capture features at different scales and resolutions, enhancing its ability to recognize complex patterns.

3.4 Random Forest

Random Forest (RF) is used to train the model after extracting the features from the fingerprint image data. Combining the RF with other Neural Networks such as CNN, VGG16, VGG19, Xception, and Inception creates a unique blend of robustness, interpretability, and predictive accuracy, making it suitable for enhancing the performance of hybrid learning systems.

RF is a learning method based on decision tree classifiers, [14]. As a result, it brings several key points to the table which make it especially well-suited for integration with NN. Particularly RF is great in bringing the predictive power of multiple decision trees together, creating a stack that is often more resilient and accurate than individual models. RF can also capture complex non-linear relationships within the data, making them more effective in the context where the relationships are not easily modeled by linear algorithms. As a result, the combination of RF and other NNs is used in this paper to find out the best combination.

3.5 Evaluation Metrics

Several evaluation metrics such as accuracy, precision, recall, and F1-score were used to test all the applied algorithms in this paper. As a result, the combined models were evaluated thoroughly.

3.5.1 Accuracy

Accuracy is one of the fundamental metrics for evaluating the performance of machine learning models by measuring the overall performance of the predictions, [15]. Equation 1 represents accuracy as

the total percentage of correctly identified fingerprints out of the total dataset.

$$Accuracy = \frac{No.of\ Correct\ Predictions}{Total\ No.of\ Predictions} \times 100 \quad (1)$$

3.5.2 Precision

Precision is one of the main evaluation metrics in the biometric identification system deploying hybrid learning fingerprint matching algorithms. The accuracy of positively identified fingerprint matching among all instances is measured by precision, [15]. The precision that shows the model's ability to correctly identify and classify the genuine matches as True Positives (TP) while minimizing False Positives (FP) is shown in Equation 2.

$$Precision = \frac{TP}{TP + FP} \times 100 \quad (2)$$

3.5.3 Recall

The ability of a model in order to correctly identify and capture all relevant instances of positive cases within the dataset is measured by Recall or Sensitivity [15]. The Recall value is measured using Equation 3 where a high value indicates that the model performs better at identifying genuine matches. It also minimizes instances of False Negatives (FN) in which cases the original matches are overlooked.

$$Recall = \frac{TP}{TP+FN} \times 100 \quad (3)$$

3.5.4 F1-score

A model's performance can be assessed [15] using F1-score which is measured using Equation 4. The F1-score provides measurements of both false positives and false negatives. A high value indicates a desirable balance between the precision and recall values.

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \times 100 \quad (4)$$

Table 1. Performance metrics of the hybrid learning algorithms

Algorithm	Accuracy	Precision	Recall	F1 Score
VGG16	89.36	88.39	86.96	84.37
Vgg19	90.3	88.51	86.98	84.27
Xception	84.67	82.74	81.26	74.64
Inception	82.9	81.40	80.34	72.06
CNN	99.32	99.32	99.32	99.32

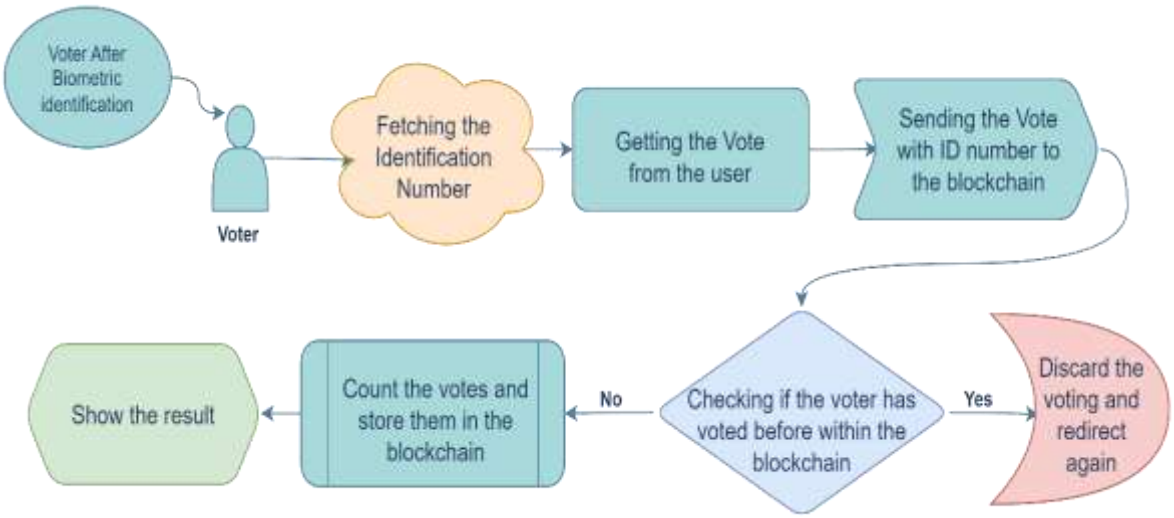

Fig. 3: Proposed E-voting System using Blockchain Technology

3.6 Blockchain-based E-voting System

Blockchain is a decentralized ledger that is most common in crypto-currency. Basically in a blockchain, the transactions are securely stored as a chain of blocks.

This chain continuously grows as new blocks are added after each transaction, [16]. Blockchain is a revolutionary technology that highlights the need for decentralized, persistent, anonymous, and authenticated data security.

The technology integrates the core elements such as cryptographic hash, digital signatures based on asymmetric cryptography, and distributed consensus mechanisms, [16]. It implies that transactions without the need for a central authority reduce costs and improve efficiency. As a result, blockchain technology can be used in various sensitive fields where data security is crucial. It can be used in Financial Services, Healthcare Services, Security Services, and most importantly Voting Services. In this paper, the blockchain technology was implemented using Flask, HTML, and Solidity. Figure 3 shows the voting system using blockchain technology. The voters are assumed to be authenticated by fingerprint using the proposed hybrid learning algorithm, and then voting is conducted with the blockchain technology as shown in Figure 3.

The use of blockchain technology ensures temper-resistant voting records, which can establish voters' trust as the records are transparent and immutable with the decentralized and cryptographic features of the technology. The use of hybrid deep learning algorithms enhances the security of the framework by being able to detect anomalies and fraudulent activities in real-life implementation. The paper's innovative approach not only addresses the core challenges of e-voting, but also opens up avenues for further exploration in optimizing system performance, scalability, and usability.

4 Results

This section shows the results of the experiments along with a comparative analysis of different algorithms that were applied.

4.1 Performance Evaluation of Hybrid Learning Algorithms

The hybrid learning algorithms such as VGG16, VGG19, Xception, Inception and CNN combined with Random Forest was subjected to rigorous evaluation using a dataset of over 50,000 fingerprint samples. The evaluation metrics shown in Table 1, including accuracy, precision, recall, and F1-score provide insight into the effectiveness of each algorithm in biometric fingerprint matching.

4.2 Comparative Analysis

Figure 4 shows the results of different hybrid learning algorithms. Compared to other algorithms, the combination of CNN and RF hybrid learning algorithms provides the highest accuracy of 99.32% for around 50,000 fingerprint images. This hybrid algorithm also provides higher precision, recall, and F1 scores. The combined CNN and RF had the ability to discern intricate patterns in fingerprint data, showing its superior performance and efficiency in biometric identification. Overall the other algorithms, the CNN and RF got the upper hand because of the hierarchical feature learning of the convolutional layers. CNN can find patterns regardless of their positions in the image since it can demonstrate translation invariance.

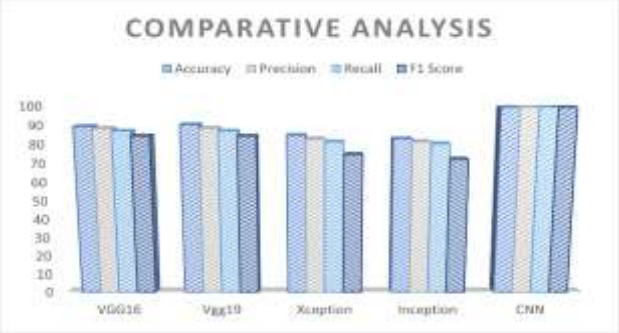

Fig. 4: Comparative Analysis of Hybrid Learning Algorithms

Compared to Xception and Inception, VGG16 and VGG19 show better performance, indicating the reliability of these architectures in fingerprint matching. Though the performance of Xception and Inception is slightly lower, these algorithms demonstrate competitive results and have potential areas for optimization and alternative applications.

Fig. 5: The Page after Casting the Vote by a Voter

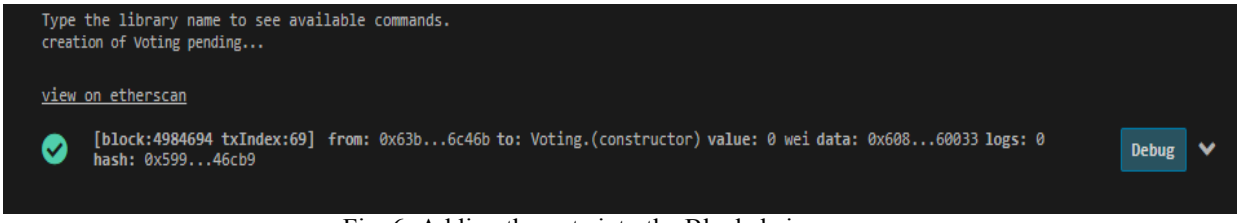

Fig. 6: Adding the vote into the Blockchain

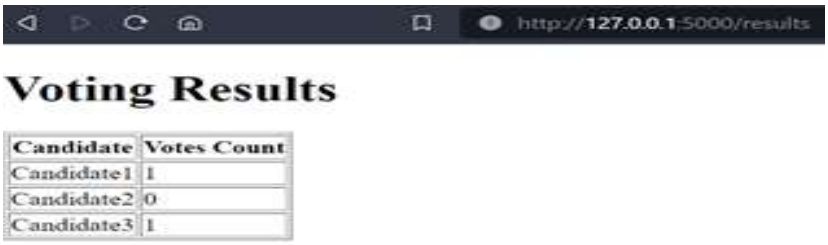

Fig. 7: Showing Voting Results

Table 2. Comparative Study of the Proposed Algorithm with other Published Works

References	Fingerprint classification technique	Accuracy (%)
[17]	Random Forest (RF) + CNN	96.75
[18]	ROIFE_CNN on Gabor filtering image of ROI	95.10
[19]	CNN	96.01
[20]	Decision trees	98.00
[21]	SVM algorithm + naive Bayes method	95.60
[22]	Random Forest algorithm	96.50
[23]	Support Vector Machine (SVM)	94.97
[24]	Fuzzy-neural network classifier	98.00
[25]	Fusion of CNN and Gabor features	99.87
Proposed Method	CNN (Feature Extraction) + RF	99.32

4.3 Blockchain Integration

The integration of blockchain technology into the electronic voting model demonstrates significant advancements in security and transparency. The decentralized and tamper-resistant nature of the blockchain ensures that each vote is securely stored, verifiable, and transparently tallied. The cryptographic features of blockchain mitigate several issues relevant to vote tampering, unauthorized access, and overall electoral misconduct. The results indicate that the blockchain-based electronic voting model provides an immutable and transparent ledger, addressing long-standing challenges associated with centralized voting databases.

Usability testing of the web application revealed a user-friendly interface, allowing voters to securely cast their votes with ease. The integration of blockchain does not compromise the usability of the electronic voting system, providing a seamless experience for voters while enhancing the security of the overall process. Figure 5, Figure 6 and Figure 7 demonstrate some snapshots of the blockchain integration into the proposed e-voting system.

5 Discussion

This section compares the findings of the proposed work with the existing related research works and assesses the contributions. It also delves into the practical use of the blockchain and explores efficient consensus mechanisms.

5.1 Comparative Study of the Proposed Algorithms with other Published Works

The results of the hybrid learning algorithms for biometric fingerprint matching were impressive. As shown in Table 2, the CNN+RF algorithm demonstrated exceptional accuracy, precision, recall, and F1 score. The comparison with other research papers validates the efficacy of the chosen algorithms.

The proposed method, combining CNN for feature extraction and RF, achieves a notable accuracy of 99.32%. This accuracy is competitive and comparable to other state-of-the-art techniques presented in Table 2. The fusion of deep learning-based feature extraction with the ensemble learning capabilities of RF contributes to the high accuracy of the proposed method. The utilization of CNN for capturing hierarchical representations in fingerprint images followed by RF for robust classification demonstrates the effectiveness of the hybrid approach in achieving superior accuracy compared to individual methods.

Referring to Table 2, it is notable that in all the published works the dataset size was much smaller than the dataset used in this paper. The exception is in [24] which uses more samples, however the accuracy is lower (98%) compared to the proposed method (99.32%). The work in [25] achieved more accuracy (99.87%) than the proposed method presented in this paper. However, they have used only 500 samples whereas the proposed method includes 50,000 samples.

In this research, the accuracy is found for the applied deep hybrid learning algorithms. The algorithm with the highest accuracy can be used in any e-voting system for biometric identification. Thus, it will enhance the security of the e-voting system instead of using the traditional algorithms. Furthermore, the integration of blockchain technology also improves the security of voting and counting and provides transparency.

5.2 Blockchain Systems

The integration of blockchain technology into the electronic voting model aligns with and builds upon the transformative potential highlighted in related research papers. Works in [4] and [5] underscore the foundational principles of blockchain—decentralization and immutability—and their applicability to secure diverse domains. The findings of the study echo the sentiments of [4], emphasizing the decentralized and tamper-resistant nature of blockchain as a robust solution for securing e-voting systems. The results demonstrate the successful implementation of blockchain in providing a secure and transparent ledger for storing and tallying votes, mitigating concerns raised in [5] regarding traditional centralized voting databases.

This paper not only contributes to the theoretical underpinnings of blockchain security but also addresses practical concerns related to usability. Usability testing of the web application revealed a user-friendly interface, affirming that the integration of blockchain does not compromise the accessibility or ease of use for voters.

6 Conclusion

This paper contributes to the advancement of online voting by identifying a robust biometrics technique and illustrating how blockchain technology can further enhance voting security. By incorporating these tools, the study paves the way for future advancements in electronic voting systems that seek to increase public acceptance of democracy, accuracy, and transparency.
This research is an innovative attempt to use cutting-edge technologies to advance electronic voting systems. The study aimed to strengthen the security and transparency of electronic voting by combining the transformative potential of blockchain technology with hybrid learning algorithms, such as CNN with Random Forest, Xception, Inception, VGG16, and VGG19, for biometric fingerprint matching. The best hybrid learning algorithm was CNN+RF, which demonstrated the highest levels of accuracy, precision, recall, and F1 score. These results established CNN+RF as a dependable method for validating voters. Contributing substantially to the field, the research addressed critical gaps by providing a comparative analysis of hybrid learning models for biometric identification and integrating blockchain to enhance security and transparency.

The study highlights the necessity of ongoing usability testing and recommends that future research concentrate on diverse datasets and iterative usability improvements while acknowledging limitations such as dataset specificity. This study represents a major advancement in electronic voting systems and provides a framework for more investigation and application. When combined with blockchain integration, the identified CNN+RF algorithm generates a model that anticipates the changing requirements of democratic processes. In the future, electronic voting will strike a balance between security, usability, and adaptability, fostering confidence and trust in the political process, according to the study.

References:

[1] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, vol. 14(1), pp. 4-20. DOI: 10.1109/TCSVT.2003.818349.

[2] Jain, A. K., & Kumar, A. (2012). Biometric recognition: an overview. Second generation biometrics: The ethical, legal and social context, *The International Library of Ethics, Law and Technology*, vol 11. Springer, Dordrecht. Pp. 49-79. DOI: 10.1007/978-94-007-3892-8_3.

[3] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, vol. 521(7553), pp. 436-444. DOI: 10.1038/nature14539

[4] Ishaan Swan, M. (2015). *Blockchain: Blueprint for a new economy*. 1st Edition, O'Reilly Media, Inc. ISBN-10: 9781491920497 ASIN: 1491920491.

[5] Kiayias, A., Koutsoupias, E., Kyropoulou, M., & Tselekounis, Y. (2016). Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation, Melbourne, Australia* (pp. 365-382). DOI: https://doi.org/10.1145/2940716.2940773.

[6] Kumar, R., & Patil, M. E. (2022). Improved Fingerprint Identification System Using Hybrid Deep Learning. *Industrial Engineering Journal*, vol. 15(11), pp. 24-30.

[7] SaiTeja, C., & Seventline, J. B. (2023). A hybrid learning framework for multi-modal facial prediction and recognition using improvised non-linear SVM classifier. *AIP Advances*, vol. 13 (025316), pp. 1-8. DOI: https://doi.org/10.1063/5.0136623.

[8] Jadhav, A.B, Deshmukh, N.K., & Humbe, V. T. (2023). HDL-PI: hybrid Deep Learning technique for person identification using multimodal finger print, iris and face biometric features. Multimedia Tools and Applications. Vol. 82(19), 30039-30064. DOI: 10.1007/s11042-022-14241-9.

[9] Sokoto Coventry Fingerprint Dataset. Kaggle. Date: 29/12/2023, [Online]. https://www.kaggle.com/datasets/ruizgara/socofing (Accessed Date: July 10, 2024).

[10] Lindeberg, T (2012). Scale Invariant Feature Transform. Chapter 7(5):104249, in book *Scholarpedia* (2012): 10491. DOI: 10.4249/scholarpedia.10491.

[11] Dalal, N., & Triggs, B. (2005). Histograms of oriented gradients for human detection. *IEEE computer society conference on computer vision and pattern recognition (CVPR'05), San Diego, CA, USA* (Vol. 1, pp. 886-893). IEEE. DOI: 10.13140/RG.2.2.23788.85122.

[12] Ahonen, T., Hadid, A., & Pietikainen, M. (2006). Face description with local binary patterns: Application to face recognition. *IEEE transactions on pattern analysis and machine intelligence*, vol. 28(12), 2037-2041. DOI: 10.1109/TPAMI.2006.244.

[13] Li, Z., Liu, F., Yang, W., Peng, S., & Zhou, J. (2021). A survey of convolutional neural networks: analysis, applications, and prospects. *IEEE Trans Neural Netw Learn Syst*. Vol. 33(12) pp. 6999-7019. DOI: 10.1109/TNNLS.2021.3084827.

[14] Rodriguez-Galiano, V. F., Ghimire, B., Rogan, J., Chica-Olmo, M., & Rigol-Sanchez, J. P. (2012). An assessment of the effectiveness of a random forest classifier for land-cover classification. *ISPRS journal of photogrammetry and remote sensing*, vol. *67*, pp. 93-104. DOI: https://doi.org/10.1016/j.isprsjprs.2011.11.002

[15] Yacouby, R., & Axman, D. (2020). Probabilistic Extension of Precision, Recall, and F1 Score for More Thorough Evaluation of Classification Models. *Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems,* pp. 79-91. DOI:10.18653/v1/2020.eval4nlp-1.9.

[16] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, vol. 14(4), 352-375. DOI: 10.1504/IJWGS.2018.095647.

[17] Nguyen, H. T., & Nguyen, L. T. (2019). Fingerprints classification through image analysis and machine learning method. *Algorithms*, vol. 12(11), 241, pp.1-11. DOI: https://doi.org/10.3390/a12110241.

[18] Yang, J., Wu, Z., & Zhang, J. (2018). A robust fingerprint identification method by deep learning with Gabor filter multidimensional feature expansion. In: *Sun, X., Pan, Z., Bertino, E. (eds) Cloud Computing and Security. ICCCS 2018,* Nagoya, Japan. *Lecture Notes in Computer Science*, vol. 11065. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-00012-7_41.

[19] Michelsanti, D., Ene, A. D., Guichi, Y., Stef, R., Nasrollahi, K., & Moeslund, T. B. (2017). Fast fingerprint classification with deep neural networks. In *International Conference on Computer Vision Theory and Applications,*

Porto, Portugal (pp. 202-209). SCITEPRESS Digital Library. DOI: 10.5220/0006116502020209.

[20] Everingham, M., Van Gool, L., Williams, C. K., Winn, J., & Zisserman, A. (2010). The pascal visual object classes (voc) challenge. *International journal of computer vision*, vol. 88, pp. 303-338. DOI: https://doi.org/10.1007/s11263-009-0275-4.

[21] Hong, J. H., Min, J. K., Cho, U. K., & Cho, S. B. (2008). Fingerprint classification using one-vs-all support vector machines dynamically ordered with naı¨ve Bayes classifiers. *Pattern Recognition*, vol. 41(2), pp. 662-671. DOI: 10.1016/j.patcog.2007.07.004.

[22] Strobl, C., Malley, J., & Tutz, G. (2009). An introduction to recursive partitioning: rationale, application, and characteristics of classification and regression trees, bagging, and random forests. *Psychological methods*, vol. 14(4), 323-348. DOI: 10.1037/a0016973.

[23] Cristianini, N., & Shawe-Taylor, J. (2000). *An introduction to support vector machines and other kernel-based learning methods*. Cambridge university press. DOI: 10.1017/CBO9780511801389.

[24] Mohamed, S. M., & Nyongesa, H. (2002). Automatic fingerprint classification system using fuzzy neural techniques. *IEEE World Congress on Computational Intelligence. 2002 IEEE International Conference on Fuzzy Systems, Honolulu, HI, USA. FUZZ-IEEE'02. Proceedings (Cat. No. 02CH37291)* (Vol. 1, pp. 358-362). DOI: 10.1109/FUZZ.2002.1005016.

[25] Nur-A-Alam, Ahsan, M., Based, M. A., Haider, J., & Kowalski, M. (2021). An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning. *Computers and Electrical Engineering*, vol. *95*, 107387. DOI: https://doi.org/10.1016/j.compeleceng.2021.107387.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.