

# Spiking neural network with blockchain for tampered image detection using forensic steganography images

Gurumurthy Shikaripura Basavanyappa, Ajit Danti

Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bangalore, India

## Article Info

### Article history:

Received Feb 11, 2024

Revised May 20, 2024

Accepted Jun 5, 2024

### Keywords:

Forensic steganography

Legitimacy

Misleading images

SNN blockchain

Steganography

Tampered image detection

## ABSTRACT

Accurate tools are required to acknowledge misleading images in order to maintain image legitimacy, and these tools must allow for legal operations on images. Additionally, after posting their images to the Internet, image owners lose rights over the images because there are no measures in place to safeguard them from misuse. One of the most well-liked techniques for addressing copyright disputes is the use of steganography technologies. The embedded steganography images can, sadly, be easily altered or deleted. To address this problem, this work presents the spiking neural network (SNN) with blockchain for tampered image detection utilizing forensic steganography images. Forensic steganography images that have been altered can be found with this SNN. Using steganography images from the database, SNN is trained in this model. The blockchain stores the owners' access policies. The Python platform is used to implement the proposed strategy. F-measure, specificity, accuracy, precision, recall false positive rate (FPR), and false negative rate (FNR) are used to gauge how well the proposed approach performs. When compared to state-of-the-art approaches, the proposed approach obtained an impressive rise of 98.65%, in classification accuracy.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Gurumurthy Shikaripura Basavanyappa

Department of Computer science and Engineering, CHRIST (Deemed to be University)

Bangalore, Karnataka, 560074, India

Email: gurumurthy.sb@res.christuniversity.in

## 1. INTRODUCTION

In the current digital era, images have become essential. "What we see is what we believe" is the primary rationale for the widespread appeal of images. These days, people share a lot of digital images not just on social media websites but also in courtrooms, news articles, insurance claims, and other settings. The growing usage of digital photographs in our daily lives is a result of the creation of image-editing software that is sold commercially [1]. Digital images can be quickly altered without noticeable artifacts with the use of robust image editing software. In our day-to-day lives, maliciously altered photographs could have some very negative effects. For this reason, within the past ten years, image forensics [2] has garnered a lot of interest. Manipulating image contents has become simpler thanks to the ease of use of these technologies. Two categories of picture alteration techniques include image forgeries and image steganography [3].

Images are altered using steganography to hide confidential information, while image forgeries change the original semantic meaning [4]. Steganalysis methods have been developed to uncover hidden information in digital images [5]. By comparing with the original data, the embedded data is restored during authentication. Forensic investigation then uses this verified data to ensure the integrity of digital media, determining if it has been fabricated [6]. Forensic professionals employ various steganographic methods to examine multimedia content [7]. The availability of user-friendly image editing software makes it easy to

tamper with digital images, which can conceal real information. Reliable authentication methods are urgently needed to accurately identify forgeries due to the simplicity of digital image modification [8].

A DCT watermarking architecture was proposed by Ernawan and Kabir [9] for copyright protection. Ouyang *et al.* [10] developed a method using an adjusted net from a pre-trained ImageNet model for the copy-move operation, which performed well against automatically generated fake images but not actual forgeries [11]. Efforts to enhance deep learning's accuracy in detecting deep forgeries have been made [12], and some methods aim to improve localization performance [13]. However, these studies addressed different aspects of forgery localization with various databases and experimental setups, making their real-world applicability uncertain. The prevalence of fake images online and the lack of adequate devices to detect and protect property rights complicate image authentication and copyright protection, as current techniques like steganography are insufficient for identifying altered images. To overcome this issue, we present a spiking neural network (SNN) with blockchain for tampered image detection using forensic steganography images in this study. The following are the paper's primary contributions:

- SNN with blockchain is presented to solve copyright dispute problems. SNN is used to detect tampered forensic steganography images.
- Steganography images are used to train the SNN.
- Blockchain is used to store the access rules of an owner.
- The proposed scheme's performance is evaluated in terms of throughput, storage cost, and detection rate.

The following sections of the paper will be organized in this manner. Section 2 provides a review of the related work. In section 3, the proposed methodology is presented. The experimental results and evaluation are provided in section 4. In the last section the conclusions are given.

## 2. RELATED WORKS

A reliable method for copy-move forgery (CMF) localization and detection in digital images was put forth by Mahmood *et al.* [14]. To reveal image forgeries, the approach extracted SWT-based characteristics. More particular, the stationary wavelet transform's approximation sub band was used since it contains the majority of the data that is most useful for forgery detection. Discrete cosine transform (DCT) was used to minimize the feature vectors' dimension. Two common datasets, the CoMoFoD, and the UCID, were used for experiments to assess the suggested method. The experimental results showed that the suggested strategy performed better based on true and false detection rates than the methods already in use. The post-processing operations made it considerably more difficult to detect CMF.

El-Bendary *et al.* [15] described an effective and straightforward method for forensic picture integrity verification. A concealed mark was applied to a secret image, enabling image integrity verification and detection of tampering or forgery. Various discrete transform domains, including DFT, DCT, and DWT, were investigated, with the DCT proving to be the most effective. The trials showed that the mark algorithm was resilient to various attacks and was not visible, making it a reliable tool for detecting image forgery in highly sensitive information such as nuclear and military applications. The study did not cover image transmission methods or several steganography, watermarking, and encryption approaches for effective and reliable image communication.

Alkawaz *et al.* [16] developed a method using DCT coefficients for copy-move image forgery detection, extracting features for various block sizes. They first converted an RGB image into grayscale. The study focused on three objectives to improve accuracy: detecting forged regions of different sizes, the distance between forged areas, and the threshold value used. Accuracy was influenced by block size, the separation of forged areas, and the threshold value. The main limitations were high computational complexity and inaccuracy in identifying tampered areas after post-processing.

Carvalho *et al.* [17] explored transformed spaces using image illuminant maps to design efficient and automated methods for detecting image forgeries. They proposed a methodology that incorporated statistical cues from various image descriptors, focusing on texture, shape, and color aspects. Their approach effectively detected targeted image forgeries involving humans, based on experiments with three open-access datasets. The method achieved a quick and accurate classification for identifying real or fake images. However, these experiments did not investigate the impact of lighting variations on the framework.

Li *et al.* [18] developed a methodology to improve forgery localization by integrating tampering possibility maps. They enhanced a statistical feature-based detector and a copy-move forgery detector to generate these maps. These maps were then used in a simple yet effective technique for final localization results. The final classifier was both fast and accurate in distinguishing real from fake images. Extensive testing demonstrated that their enhanced methodologies outperformed state-of-the-art processes, achieving the highest F1-score in the IEEE IFS-TC image forensics challenge. However, the algorithm could not compress JPEG images.

Korus and Huang [19] proposed three multi-scale fusion techniques and tested their effectiveness against various reference plans. They used mode-based first-digit features to distinguish between single and doubly compressed regions, which is a common tampering scenario. The results showed that the proposed fusion methods effectively combined the benefits of small-scale and large-scale analysis, improving tampering localization performance. However, the lack of flexibility hindered their automatic learning. Unlike other fusion algorithms that can quickly discard unreliable candidate maps, the SVM requires independent training for each combination of valid input.

Vega *et al.* [20] proposed a methodology to generalize the detection of manipulations across various color filters without compromising the accuracy found in RGB cases. This technique could be applied in various scenarios if periodic artifacts were detected in the image. However, while the methodology could extend to more devices, it was not universally effective, as shown by existing studies on this issue.

Le and Reira [21] developed an algorithm to enhance the authentication and location of forgeries in images by utilizing demosaicing artifacts from the image generation pipeline. This approach focused on the smooth region of the green band to minimize vulnerability to edge issues. Numerical examples demonstrated the approach's superiority and robustness. However, the algorithm struggled to identify fake parts of an image. Although the method produced promising results, the study concluded that automatic digital image authentication still performed poorly, and forgery localization was only effective with uncompressed or minimally compressed images.

### 3. METHOD

The owner uploads a stego image to the database. The verification tool validates the image's legitimacy, and the user accesses the image through a smart contract on the blockchain. SNN acts as the verifier, initially trained using database-stored steganography images. When a user sends an image-containing transaction to SNN, the classifier verifies it and, if the image is authentic, generates proof for it. If the image is found altered or inauthentic, the verifier rejects it. The transaction data and proof of authenticity are then posted to the blockchain. The main process is described in Figure 1.

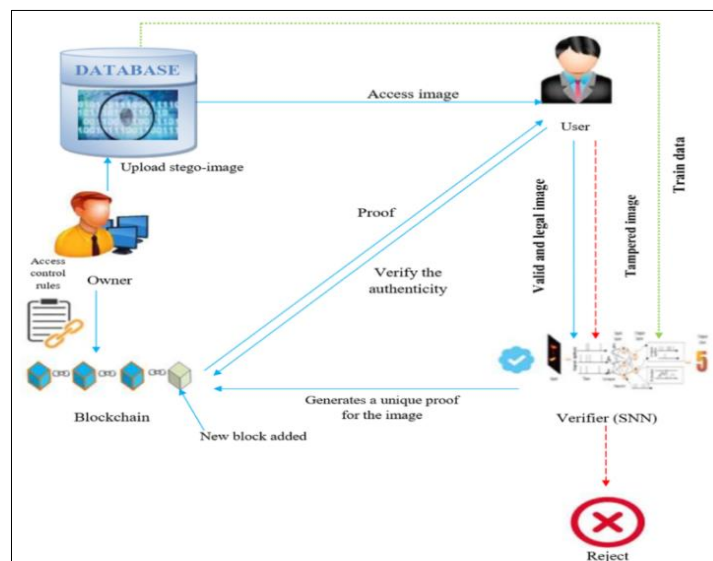


Figure 1. Structure of the proposed framework

#### 3.1. Proposed framework

A verifier, a database, an owner, and a user are the four components of the proposed framework as given below.

- **Owner:** the entity is responsible for uploading Stego images to the database. The owner can provide access control specifications for the blockchain image.
- **Database:** an off-chain entity used for storing Stego-images. To avoid directly storing Stego-images on the blockchain, the proposed method makes use of an off-chain database.
- **Verifier:** an entity that confirms the legitimacy as well as the authenticity of an image fed by a user. In the proposed solution, the blockchain system's classifier serves as the verifier.

- User: the entity is using a blockchain-based smart contract to access the stego-image. Through the use of smart contracts, the user can audit and trace images.

The system uses blockchain as an image retrieval ledger to store owners' image access control rules and image-related transaction data, while the rules themselves are kept in a database. The process involves the owner uploading a Stego image to the database, a verifier confirming the image's authentication and legality, and a user accessing the image through a blockchain-configured smart contract. Smart contracts manage the registration, verification, and access control of stored images. When a user uploads images, a smart contract registers the image on the blockchain, creating a unique hash value to represent it, and includes the access control rules specifying who can access the image and under what conditions. Upon receiving an access request, the smart contract verifies its validity and grants access if the request is legitimate. This system aims to ensure traceability, authentication, and copyright protection for image forensics while allowing legal transformations without increasing storage overhead.

### 3.2. The proposed blockchain-based image forensics system

The blockchain-based image forensics system aims to tackle image forgery, tracing, and copyright issues. Using SNN and blockchain, it provides authentication, copyright protection, and traceability. Once a new block is added to the blockchain, the information is permanent, preventing users or verifiers from denying their actions later. Blockchain, a distributed ledger system, allows multiple entities to manage a single database without a central authority. This technology, which supports Bitcoin, a peer-to-peer virtual currency without intermediaries like banks, was first introduced in 2008 [22].

Blockchain technology's decentralized nature is a key feature, enhancing resistance to censorship, hacking, and interference due to the absence of a central authority. This makes it ideal for applications requiring high security and transparency, such as financial transactions, supply chain management, and voting systems. Another important aspect is the use of encryption to secure transactions and protect user privacy [23]. Complex mathematical algorithms verify each transaction to ensure integrity and legitimacy, allowing users to remain anonymous while participating in transactions. Thus, the ability to store and transfer data in a secure, open, and decentralized manner offered by blockchain technology has the potential to change a wide range of businesses. Before it can be widely embraced, however, there are still a lot of obstacles that need to be solved, including scalability, interoperability, and regulatory concerns.

### 3.3. Detection of tampered forensic steganography images using SNN

When a user submits a transaction with an image to the verifier, the classifier checks the transaction. If the image is legitimate, it generates proof for the image, and both the proof and transaction details are uploaded to the blockchain. The user can then access the proof and the image via a blockchain-based smart contract. This proof confirms the image's validity, provides copyright information, and details its transformation history. If the image is altered or inauthentic, the verifier rejects it, records the user's misconduct, and denies access and validity guarantees.

#### 3.3.1. SNN

In this research, we employ a deep learning method to distinguish between altered and genuine images. Each uploaded image is assigned a distinct hash value and registered on the blockchain. When a user requests access to an image, the system alerts the blockchain's verifier, which generates a unique proof and validates the request. If a manipulated image is submitted by a malicious user, the verifier rejects it and records the user's dishonest actions. The SNN is used as the verifier, initially trained with Steganography Images from the database.

The spiking neurons and connecting synapses that make up the SNN architecture are represented by movable scalar weights [24]. Action potential generation dynamics and network dynamics are both present in biological brain networks. Artificial SNNs have greatly simplified network dynamics when compared to real biological networks. When the membrane potential of postsynaptic neurons crosses a threshold due to the activity of pre-synaptic neurons, an action potential or spike is produced. New input-output concepts need to be developed to provide relevance to the timing and presence of spikes in SNNs. Presume that while an input sample is being presented, and are the quantity of active synapses (that is, synapses that receive spike inputs) in a neuron and the quantity of active neurons (that is, neurons that send spike outputs) in a layer [25]. The structure of the SNN is depicted in Figure 2.

Additionally, throughout the paper, we will refer to the indices for active synapses and neurons in their simplified version as,

$$\begin{aligned} \text{Activesynapses} &= \{p_1, \dots, p_m\} \rightarrow \{1, \dots, m\} \\ \text{Activeneurons} &= \{q_1, \dots, q_n\} \rightarrow \{1, \dots, n\} \end{aligned} \quad (1)$$

In each time window, a pattern  $x$  is temporally coded relative to a fixed time  $T_{in}$  by one spike emission of a neuron  $q_i$  at the time  $t_i = T_{in} - p_i$  for all  $i$ . Spikes are used for transmission, communication, and computation in biological spiking neurons. The integrate-and-fire (IF), Hodgkin-Huxley (HH), and LIF neuron models are a few examples of spiking neuron models. To guarantee the validity and integrity of the images saved in the system, the verifier is essential. The proposed approach offers a secure and open solution to manage digital assets like images by using verifiers in the blockchain system as verifiers.

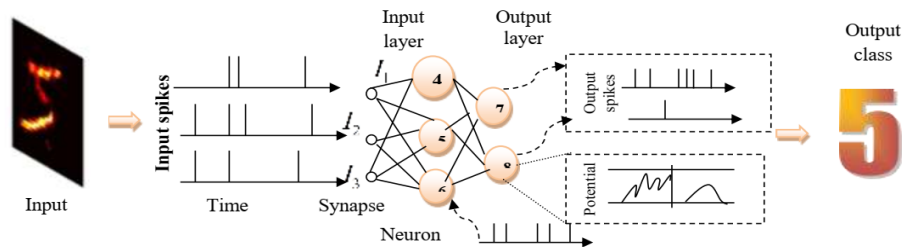


Figure 2. SNN

#### 4. RESULTS AND DISCUSSIONS

##### 4.1. Experimental results

The experiments were carried out on a Windows 10 system that has an Intel Core i7 processor, a 4 GB GPU, 64-bit architecture, and 8 GB of RAM. Deep learning tasks in Python 3.5 were used to implement the suggested approach. High processing power is offered by the Intel Core i7 processor, and machine learning computations run more smoothly thanks to the 4 GB GPU. Efficient management of larger datasets and memory-intensive activities is ensured by the use of an 8 GB RAM and 64-bit processor.

An in-depth comparison with existing neural network architectures, such as recurrent neural networks (RNN), convolutional neural networks (CNN), deep neural networks (DNN), and deep belief networks (DBN), was conducted in the analysis of tampered image detection using forensic steganography images. These were compared against a new method, the SNN integrated with Blockchain technology. The evaluation aimed to determine how well the proposed SNN enhanced detection abilities compared to existing models. Performance measurements included key metrics such as F-measure, specificity, accuracy, precision, recall, FPR, and FNR, offering detailed insights into the models' benefits and drawbacks in altered image identification. This study aims to provide insights into future developments in image forensics, focusing on integrating advanced technologies for improved security and accuracy in detecting tampered images in forensic steganography scenarios.

During the evaluation of different neural network designs, the accuracy of the performance measures for DNN, DBN, CNN, RNN, and SNN was assessed in Figure 3. The accuracy increased gradually from DNN at 88.25% to SNN at an impressive 98.66%, according to the results. With an accuracy of 90.42%, the DBN demonstrated a minor improvement over the DNN's 88.25% accuracy. CNN improved the performance even more to 93.45%, and RNN showed even greater accuracy at 96.49%. With an accuracy of 98.66%, the SNN was shown to be the best-performing architecture.

DBN attained 89.10%, CNN at 93.28%, RNN at 95.14%, and SNN at 98.46%, the highest precision among the neural network architectures evaluated for precision. The DNN achieved the highest precision of 87.27% over the neural network architectures evaluated. From DNN to SNN shown in Figure 4, there is an obvious increase in precision, and of the models kept in consideration, SNN performs the best accurately in terms of classification.

The SNN exhibited persistent superiority over other models in the evaluation of F-measure, recall, and specificity among different neural network configurations represented in Figures 5-7. With a recall of 99.14%, SNN outperformed RNN with 98.24%. SNN obtained the greatest F-measure score of 98.80%, demonstrating a balanced recall and precision. Specificity, which indicates how well the models can detect downsides, likewise demonstrated SNN's superiority with 98.04%.

The SNN outperformed other neural networks in terms of FPR and FNR, as shown in Figures 8 and 9. SNN had an FPR of 1.96%, the lowest percentage of true negatives incorrectly identified as positives. Additionally, it had the lowest FNR of 0.86%, indicating its effectiveness in minimizing true positives incorrectly predicted as negatives. Other models, including DNN, DBN, CNN, and RNN, showed different FPR and FNR values. These findings suggest that the SNN is superior at balancing the reduction of false positives and false negatives compared to the other architectures.

The proposed SNN achieved an AUC of 0.98, surpassing previous models in area under the curve (AUC) values for various neural network designs, thus demonstrating superior discriminatory performance in binary classification tasks. The RNN had the second-highest AUC of 0.95, followed by CNN at 0.92, DBN at 0.89, and DNN at 0.86. As shown in Figure 10, RNN, CNN, DBN, and DNN are the next best performers, with the SNN exhibiting the highest overall performance. The performance of the DNN, DBN, CNN, RNN, and the proposed SNN in binary classification is illustrated in the ROC graph comparison in Figure 11. The better overall performance is indicated by curves closer to the top-left corner, with the suggested SNN's curve likely being closest to this ideal corner, reflecting its superior discriminatory power.

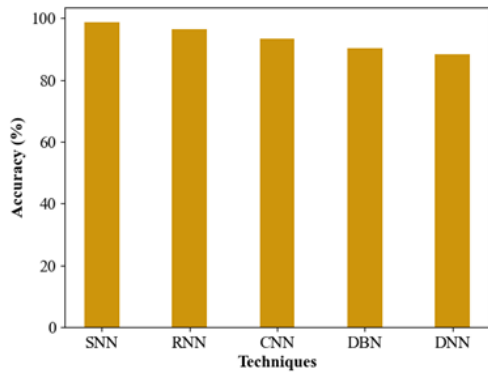


Figure 3. Comparative analysis of various techniques in terms of accuracy

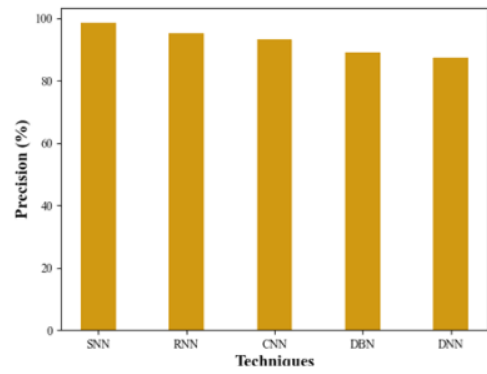


Figure 4. Comparative analysis of various techniques in terms of precision

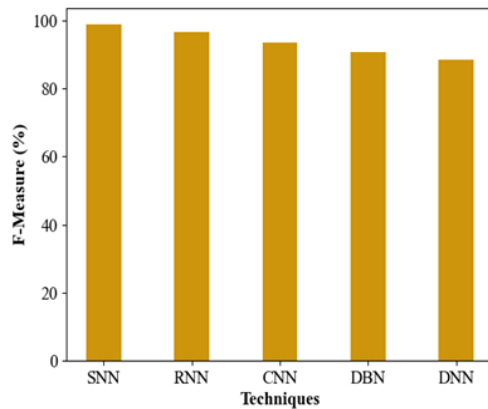


Figure 5. Comparative analysis of various techniques in terms of F-measure

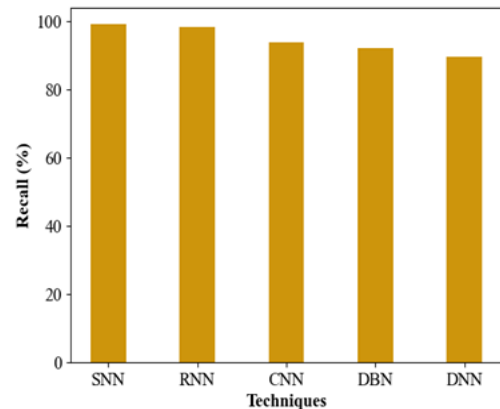


Figure 6. Comparative analysis of various techniques in terms of recall

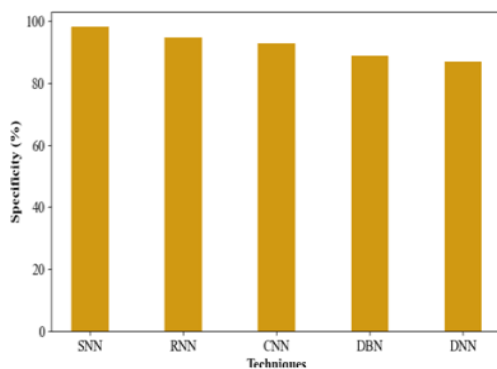


Figure 7. Comparative analysis of various techniques in terms of specificity

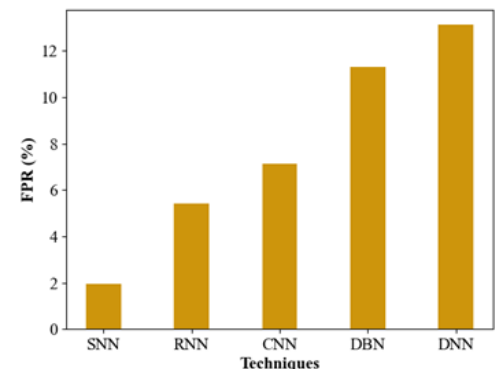


Figure 8. Comparative analysis of various techniques in terms of FPR

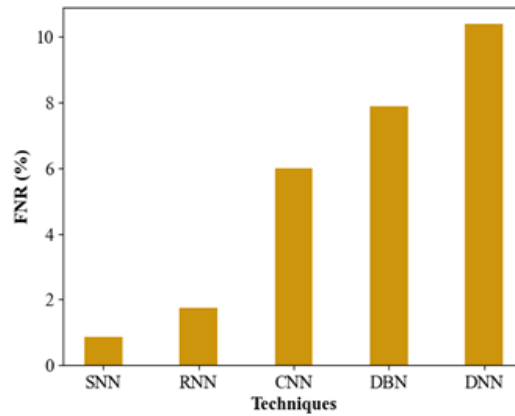


Figure 9. Comparative analysis of various techniques in terms of FNR

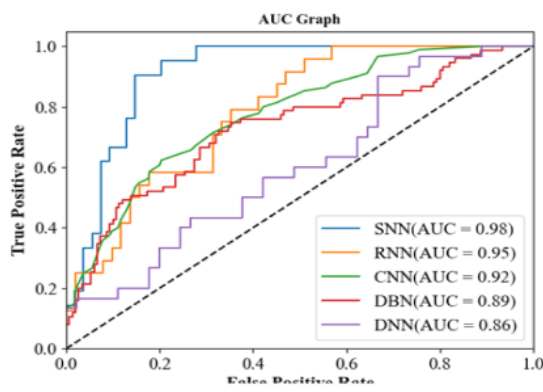


Figure 10. Comparison of AUC graph

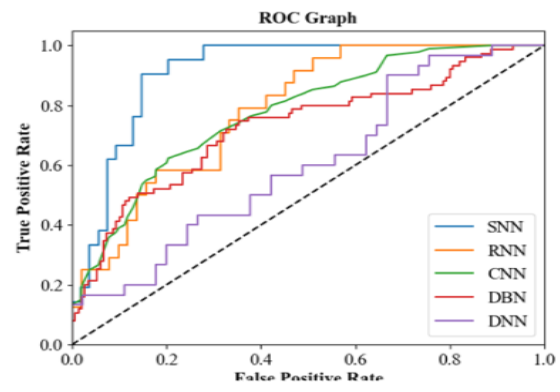


Figure 11. Comparison of ROC graph

Understanding the computational efficiency of different neural network designs during the training phase can be assessed by examining their “training time (ms)”, as shown in Figure 12. DNN’s training process is lengthy, taking 58,476 ms to complete. DBN’s training time is somewhat faster at 53,624 ms, showcasing its ability to accelerate hierarchical representation learning. CNN’s training time is 47,125 ms, while RNN’s training period of 42,698 ms demonstrates its effectiveness in learning consecutive patterns. Notably, SNN has the fastest training time of 37,485 ms, indicating superior computing efficiency and rapid adaptability to the dataset.

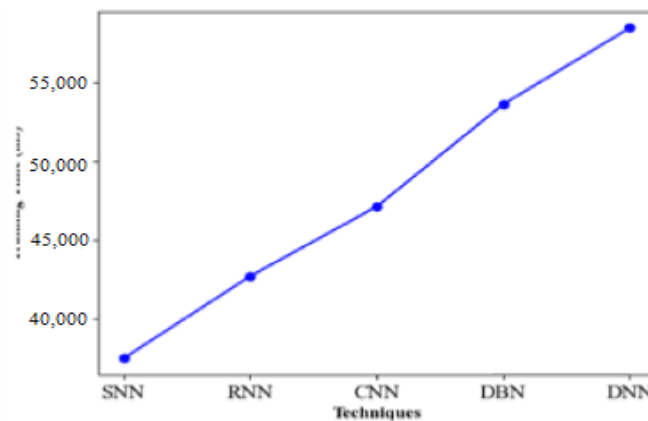


Figure 12. Comparative analysis in terms of training time (ms)

#### 4.2. Comparison of published works with proposed method

This section compares the suggested approach with previous research that is cited in [10], [12], [14], [15], [17] to conduct a thorough analysis. A thorough summary and an in-depth description of the methodology used in each of the studies are discussed in section 2. The goal of this comparative analysis is to provide a thorough overview of how the suggested method differs from existing methods.

A comparison of different approaches for a specific task was conducted in Table 1, considering multiple performance metrics. These included DCT, k-nearest neighbour (k-NN), multi-scale fusion, and CFA pattern detection, alongside the suggested support vector machine (SVM). DCT showed 63.52% precision, k-NN achieved 94% accuracy and 75.2% recall, multi-scale fusion had 91.96% accuracy and an F-score of 87, and CFA pattern recognition reached 59.73%. The suggested SVM approach excelled with 98.65% accuracy, 98.45% precision, 59.33% recall, and a 98.79% F-score. These results indicate that the SVM method performs exceptionally well in terms of accuracy and precision, making it an ideal option for tampered image detection.

Table 1. Comparison of proposed method

Ref	Methods	Accuracy (%)	Precision	Recall	F-score
Alkawaz <i>et al.</i> [16]	DCT	-	63.52	97.89	-
Carvalho <i>et al.</i> [17]	k-NN	94	-	75.2	-
Korus <i>et al.</i> [19]	Multi-scale fusion	91.96	-	-	87
Le <i>et al.</i> [21]	CFA pattern identification	-	59.73	-	59.53
Proposed	SVM	98.65	98.45	59.33	98.79

#### 5. CONCLUSION

By combining Blockchain technology with SNN integration, this work tackles the crucial issue of tampered image detection in copyright disputes. The proposed method offers a practical solution to maintain image reliability in a digital environment where authenticity is often compromised by sophisticated alteration tools, particularly in legal and commercial contexts. The system's robustness is enhanced by using SNN for forensic steganography image detection and securely storing ownership access rules on Blockchain. Implemented on the Python platform, the method is thoroughly evaluated using metrics like F-measure, specificity, accuracy, precision, Recall, FPR, and FNR, demonstrating its high-performance capabilities. Notably, it achieves a 98.65% improvement in classification accuracy compared to advanced techniques, underscoring its effectiveness in addressing altered images and copyright conflicts. Future research will explore advanced encryption techniques to enhance security and privacy of image data on the blockchain and develop automated tools for detecting and preventing malicious attacks on the SNN-based image authentication system.

#### REFERENCES




- [1] M. Islam, M. Shah, Z. Khan, T. Mahmood and M. J. Khan, "A new symmetric key encryption algorithm using images as secret keys," *2015 13th International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan, 2015, pp. 1-5, doi: 10.1109/FIT.2015.12.
- [2] M. C. Stamm, M. Wu and K. J. R. Liu, "Information forensics: an overview of the first decade," in *IEEE Access*, vol. 1, pp. 167-200, 2013, doi: 10.1109/ACCESS.2013.2260814.
- [3] D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, P. Shivakumara, and S. Sadeghi, "A novel forged blurred region detection system for image forensic applications," *Expert Systems with Applications*, vol. 64, pp. 1- 10, 2016, doi: 10.1016/j.eswa.2016.07.026.
- [4] G. Kessler, "An overview of steganography for the computer forensics examiner. an edited version, issue of forensic science communications," *Technical Report*, vol. 6, no. 3, 2004.
- [5] Z. Khan, M. Shah, M. Naeem, T. Mahmood, S. N. A. Khan, N. U. Amin, "Threshold based Steganography: a novel technique for improved payload and SNR," *International Arab Journal of Information Technology* vol. 13, pp. 380-386, 2016.
- [6] C. S. Rao and S. T. Babu, "Image authentication using local binary pattern on the low frequency components," in *Microelectronics, Electromagnetics and Telecommunications*, 2016, pp. 529-537, doi: 10.1007/978-81-322-2728-1\_49.
- [7] P. Hayati, V. Potdar, and E. Chang, "A survey of steganographic and steganalytic tools for the digital forensic investigator," in *Workshop of Information Hiding and Digital Watermarking*, 2007, pp. 1-12.
- [8] S. Sarreshtedari and M. A. Akhaee, "A source-channel coding approach to digital image protection and self-recovery," in *IEEE Transactions on Image Processing*, vol. 24, no. 7, pp. 2266-2277, July 2015, doi: 10.1109/TIP.2015.2414878.
- [9] F. Ernawan and M. N. Kabir, "A robust image watermarking technique with an optimal DCT-psychovisual threshold," in *IEEE Access*, vol. 6, pp. 20464-20480, 2018, doi: 10.1109/ACCESS.2018.2819424.
- [10] J. Ouyang, Y. Liu and M. Liao, "Copy-move forgery detection based on deep learning," *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Shanghai, China, 2017, pp. 1-5, doi: 10.1109/CISP-BMEI.2017.8301940.






- [11] F. Marra, D. Gragnaniello, D. Cozzolino and L. Verdoliva, "Detection of GAN-generated fake images over social networks," 2018 *IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, Miami, FL, USA, 2018, pp. 384-389, doi: 10.1109/MIPR.2018.00084.
- [12] J. Deng, W. Dong, R. Socher, L. -J. Li, Kai Li and Li Fei-Fei, "ImageNet: a large-scale hierarchical image database," 2009 *IEEE Conference on Computer Vision and Pattern Recognition*, Miami, FL, USA, 2009, pp. 248-255, doi: 10.1109/CVPR.2009.5206848.
- [13] P. Korus and J. Huang, "Improved tampering localization in digital image forensics based on maximal entropy random walk," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 169-173, Jan. 2016 <https://doi.org/10.3390/s20226668>.
- [14] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *Journal of Visual Communication and Image Representation*, vol. 53, pp. 202-214, 2018, doi: 10.1016/j.jvcir.2018.03.015.
- [15] M. El-Bendary, O. S. Faragallah, and S. S. Nassar, "An efficient hidden marking approach for forensic and contents verification of digital images," *Multimedia Tools and Applications*, vol. 82, no. 18, 2013, doi: 10.1007/s11042-022-14104-3.
- [16] M. H. Alkawaz, G. Sulong, T. Saba and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Computing and Applications*, vol. 30, pp. 183-192, 2018.
- [17] T. Carvalho, F. A. Faria, H. Pedrini, R. da S. Torres and A. Rocha, "Illuminant-based transformed spaces for image forensics," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 720-733, April 2016, doi: 10.1109/TIFS.2015.2506548.
- [18] H. Li, W. Luo, X. Qiu and J. Huang, "Image forgery localization via integrating tampering possibility maps," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1240-1252, May 2017, doi: 10.1109/TIFS.2017.2656823.
- [19] P. Korus and J. Huang, "Multi-scale fusion for improved localization of malicious tampering in digital images," in *IEEE Transactions on Image Processing*, vol. 25, no. 3, pp. 1312-1326, March 2016, doi: 10.1109/TIP.2016.2518870.
- [20] E. A. A. Vega, E. G. Fernández, A. L. S. Orozco, and L. J. G. Villalba, "Image tampering detection by estimating interpolation patterns," *Future Generation Computer Systems*, vol. 107, pp. 229-237, doi: 10.1016/j.future.2020.01.016.
- [21] N. Le and F. Retraint, "An improved algorithm for digital image authentication and forgery localization using demosaicing artifacts," in *IEEE Access*, vol. 7, pp. 125038-125053, 2019, doi: 10.1109/ACCESS.2019.2938467.
- [22] A. Hughes, A. Park, J. Kietzmann, C. A.-Brown, "Beyond Bitcoin: what blockchain and distributed ledger technologies mean for firms," *Business Horizons*, vol. 62, no. 3, pp. 273-281, 2019, doi: 10.1016/j.bushor.2019.01.002.
- [23] R. Ch., G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *Journal of Information Security and Applications*, vol. 55, 2020, doi: /10.1016/j.jisa.2020.102670.
- [24] A. Kugele, T. Pfeil, M. Pfeiffer, and E. Chicca, "Efficient processing of spatio-temporal data streams with spiking neural networks," *Frontiers in neuroscience*, vol. 14, 2020, doi: 10.3389/fnins.2020.00439.
- [25] J. Stuijt, M. Sifalakis, A. Yousefzadeh, and F. Corradi., "µBrain: an event-driven and fully synthesizable architecture for spiking neural networks," *Frontiers in neuroscience*, vol. 15, p.664208, doi: 10.3389/fnins.2021.664208.

## BIOGRAPHIES OF AUTHORS



**Gurumurthy Shikaripura Basavanyappa**    is having an experience of over 17 Years, in IT Industry. He has acquired a great deal of knowledge through his academic roots and research exposures. Currently, he is working as an Assistant Vice President in a tier 1 software giant company, Bangalore, India. He has a rich experience in various fields such as IT Industries/Research/Administration and Management. Currently he is doing my research at Christ University Bangalore, my research areas include image processing, block-chain, security, and network. He can be contacted at email: [gurumurthy.sb@res.christuniversity.in](mailto:gurumurthy.sb@res.christuniversity.in).



**Dr Ajit Danti**    received his bachelor of Engineering Degree from UVCE, Bangalore University in 1988 and Master's Degree in Computer Science from Shivaji University, Kolhapur in 1991. He has been awarded Ph.D. degree in Computer Science from Gulbarga University in 2006. He has authored more than 150 research papers in various peer reviewed International Journals and Conferences. His area of research includes computer vision, artificial intelligence, and machine learning. He is a senior member of IEEE. He can be contacted at email: [Ajit.Danti@christuniversity.in](mailto:Ajit.Danti@christuniversity.in).