INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Check for updates

OPEN ACCESS

Received: 22/06/2025

Accepted: 14/08/2025

Published: 08/09/2025

Citation: Trivedi R, Mishra VK, Dewangan RN, Dadsena PK, Thakur VS, Dewangan MK, Masiyare VK, Sharma MK (2025) Image Forgery Detection Forensic Tool Utilizing the Fusion of SIFT-PCA, SURF-PCA, ORB, ORB-PCA and Interval Type-2 Fuzzy Logic Methodologies. Indian Journal of Science and Technology 18(33): 2690-2700. https://doi.org/10.17485/IJST/v18i33.1150

* **Corresponding author**.

vm21084@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Image Forgery Detection Forensic Tool Utilizing the Fusion of SIFT-PCA, SURF-PCA, ORB, ORB-PCA and Interval Type-2 Fuzzy Logic Methodologies

Ruchi Trivedi[1], Vikas Kumar Mishra[2]*, R N Dewangan[3], Pradeep Kumar Dadsena[2], Vikrant Singh Thakur[4], Manoj Kumar Dewangan[5], Vinay Kumar Masiyare[6], Manoj Kumar Sharma[7]

1 Department of Mathematics, Bhilai Institute of Technology, Raipur Chhattisgarh, India
2 Department of Mathematics, Government Engineering College, Jagdalpur, Chhattisgarh, India
3 Department of Mathematics, Government Engineering College, Raipur, Chhattisgarh, India
4 Audio Vedio and Cyber Forensic Division, State Forensic Laboratory Raipur Chhattisgarh, India
5 Department of Mathematics, Shri Shankaracharya Institute of Professional Management and Technology, Raipur Chhattisgarh, India
6 Department of Mathematics, Government Naveen College, Thelkadih, Dist.-Khairagarh, Chhattisgarh, India
7 Department of Mathematics, Shaheed Nandkumar Patel Govt College, Birgaon, Chhattisgarh, India

Abstract

Objective: To detect forensic image forgery, fusion of SIFT-PCA, SURF-PCA, ORB, ORB-PCA and Interval Type-2 Fuzzy Logic (IT2FL) model is proposed. **Method:** The CASIA 2.0 standard dataset is applied for evaluating the proposed method. The proposed method is the combined version of several existing methods such as ORB, SURF-PCA, SIFT-PCA and ORB-PCA. The combined outcome was achieved by using the IT2FLS. Interval type-2 fuzzy logic has been implemented in MATLAB fuzzy logic toolbox. Mamdani type-2 fuzzy inference system has been used. **Findings:** The suggested model and the current approaches are compared. The average specificity for various techniques is 65.5205%, whereas the proposed model has 75.7%; the average precision for various techniques is 72.33075%, whereas the proposed model has 77.9%; and the average accuracy for various techniques is 70.293%, whereas the proposed model has 78.8%. **Novelty:** There are notable differences between the results obtained from different image forgery detection methods. A single image is subjected to several procedures since no one method can effectively manage all image modifications, including blurring, intensity variation, and noise addition. To address this issue, many researchers were proposed Type-1 fuzzy logic approach for image forgery detection. Type-2 fuzzy logic performs better than type-1 fuzzy logic to control higher level of uncertainty. Thus, an interval type-2 fuzzy logic-based cloning detection system is proposed in this study. Experimental results show that the detection system combines many forgery detection techniques to obtain a single accuracy rate. The suggested method produces a better outcome than the mean value of outcomes obtained from different methods. Also, the proposed method performs well than the several existing methods.

Keywords: Image Forgery Detection; Interval Type-2 Fuzzy Logic; Fuzzy Inference System; Triangular Membership Function; Fuzzy Logic Toolbox; Decision-Making; Image Forensic Research

1 Introduction

Digital cameras and high-resolution smart phones have changed photography and made it an important component of daily life. Because of the widespread use of cell phones as cameras, a variety of algorithms and techniques have been developed to improve image quality and user experience[1],[2]. But the reliability and validity of digital photos have also come under investigation as a result of this technological development. It's interesting to note that in spite of with the increased availability of mobile photography; many users remain unable to produce results of high quality. In order to fill the knowledge gap between theory and practice, innovative approaches to this problem have been created, such as augmented reality (AR)-based smart phone photography apps[2]. Also, methods using deep learning have been employed to improve images recorded by cameras with limited capabilities, that may improve the standards of mobile photography overall[1]. As digital images have come to be used as evidence in different industries, it is critical to verify their validity. Methods for photo forensics have been developed to confirm digital photos and detect manipulation[3]. These approaches identify signs of manipulation by using the benefit of geometric, statistical, and physical regularities in the imaging pipeline. Robust methods for authentication are likely to grow more essential as digital photography develops further as a way to ensure the validity of visual evidence in technical, legal, and media contexts[4].

Copy-move forgery[5], is a kind of image manipulation which is cloned these days, as one of the most common and challenging tampering technique. This is a technique of copying a section of part of the image and moving it to a different location in the image, usefully to cover or double features[6],[7],[8]. This approach is extremely challenging to detect since the pasted region has characteristics similar to that of the other parts of the image[6],[7]. It is interesting to note that despite its widespread popularity, there are different methods for detecting copy-move forgery. The block-based techniques, such as with DWT (6) or DCT[9] or Discrete Cosine Transform (DCT)[9], are well working for smooth areas but may be computationally demanding[8],[10]. Meanwhile, key-point-based methods such as SIFT are faster and more stable for geometrical deformation, but they cannot work well in a smooth region[11],[12]. To tackle such issues, the hybrid methods which integrated the block-based and the key-point-based algorithms are proposed by scholars. For example, a method of Fourier-Mellin Transform feature for smooth regions and SIFT feature for textured regions, has been proved to be efficient on different types of copy-move forgery scenarios[11]. Additionally, deep learning approaches, such as Convolutional Neural Networks[13] (CNN) combined with Convolutional Long Short-Term Memory (ConvLSTM) networks, have demonstrated high accuracy in forgery detection across multiple datasets[7].

Digital picture forgeries are easily identified using either an active or passive strategy[14]. Digital signatures and watermarking[14] are examples of active approaches that depend on previously encoded information. Passive techniques, on the other hand, have gained adoption since they do not need any setup and can be used on more types of images. These blind methods, referred to as passive detection techniques, are independent of any existing information in the image[6]. To detect tampering, these methods analyze a number of the image's inherent characteristics. Copy-move forgery, which is copying and pasting part of an image somewhere else in the same image, is one of the most prevalent forms of image modification because it is so simple to use[15],[6]. To detect copy-move[16] forgeries, a variety of passive methods have been developed. These include block-based[17] methods, key-point-based approaches, and more recently, deep learning-based methods. Block-based[17] methods split the image into overlapping blocks and compare features, while key-point-based approaches use local interest points for detection[18]. Smaller VGG Net and Mobile Net V2, two deep learning models that achieve a balance between accuracy and computational efficiency, have shown encouraging results in forgery detection[19],[20]. In conclusion, passive methods offer a more flexible approach to image authentication, while active forgery detection methods have limitations in usage. In the face of more difficult forgery techniques, researchers are investigating a number of methods to increase detection efficiency and accuracy as the field develops.

To meet the challenges posed by progressively complex image modification techniques, image forensics undergone significant changes. Modern forgeries often require multiple processing tools, requiring a more comprehensive approach than traditional methods that focused on detecting single manipulation techniques[21],[14]. Deep learning techniques[22] have gained prominence in image forgery identification[22] because of their capability to automatically extract features and achieve high accuracy[(15)],[(21)]. For instance, the MobileNetV2-based model proposed in[(15)] demonstrates an 84% True Positive Rate in detecting copy-move forgeries, even when subjected to multiple post-processing attacks[(23)],[(13)] such as brightness changes, blurring, and geometric transformations. However, as each technique responses differently to image tampering, applying multiple forgery detection tools develops a new challenge[(24)],[(25)]. To address this, researchers have developed deeper approaches. For example, the GPNet proposed in[(26)] combines Transformer and CNN architectures to build global context while preserving low-level details, outperforming existing advanced manipulation detection and localization approaches[(26)].

The complexity of the analyzed images does affect how effective image forgery detection techniques are, and merely combining individual outputs might not yield the best results. In the context provided, this challenge is addressed in a number of papers using various approaches. By combining accelerated KAZE (A-KAZE) and speeded up robust features (SURF)[(27)] to generate descriptive features, the approach described in[(27)]. Similarly to this,[(12)] offers a copy-move forgery detection system based on A-KAZE and SURF, establishing low response thresholds to obtain sufficient information in smooth regions[(12)]. Remarkably, while fuzzy theory is not openly mentioned in the provided papers, some approaches align with its principles of handling uncertainty and imprecision. As an example,[(26)] introduces GP-Net, which combines Transformer and CNN together to establish global connections and capture details with precision. Like the application of fuzzy theory, this method might be viewed as a way of handling the complex nature and uncertainty of image forgery detection. To sum up, even though the papers mentioned do not specifically address fuzzy theory, they offer a number of strategies to increase the precision and resilience of forgery detection against complicated image manipulations. The difficulties brought on by image complexity and post-processing methods are proposed to be addressed by these strategies, which include feature fusion, multi-scale feature learning, and combining various detection techniques. To further improve forgery detection capabilities, future studies may investigate the combination of fuzzy theory with these current methods. In existing literature type-1 fuzzy logic approaches were proposed to detect and analyze image forgery. Membership values use in type-1 fuzzy logic are crisp while in type-2 fuzzy logic fuzzy membership values are uses. So, type-2 fuzzy logic performs better than type-1 fuzzy logic to analyze complex problems. This higher level of uncertainty handling capability of type-2 fuzzy logic gives more precise outcome in image forensic research.

It has been observed that the outcome obtained from different techniques have significant variations and arises the complication in decision making process. To address this issue, the effectiveness of the forgery detection system by employing SIFT-PCA, SURF-PCA, ORB, and ORB-PCA methods are evaluated, and a fuzzy-based system to obtain more precise outcomes have been created. The organization of the paper is structured as follows: The fundamental principles of fuzzy logic and operational methodologies are given in Section 2. In section 3, details the proposed approach and algorithmic process, including an explanation of the type-2 fuzzy logic based working procedure. Finally, in section 4 findings are presented and validated with the previous results.

2 Methodology

The proposed approach combines several existing techniques: SIFT-PCA, SURF-PCA, ORB, and ORB-PCA. The initial stage involves pre-processing, which is responsible for extracting essential data for future steps. This data contains feature vectors from images obtained through each tool, which are then transformed into decision values using a fuzzy-based classifier. These decision values are used for fusion dependent on an interval type-2 fuzzy logic system. The final stage involves the analysis of results and the formulation of conclusive decisions. The structure for fusion of forgery detection tools is illustrated in Figure 1.

2.1 Rule Creation and Unification

Now, let's examine the method for transforming the decision values into inputs for the forgery detection tool fusion process. All decision values are expressed as detection rates and need to be normalized to meet IT2FLS requirements. This involves converting them to numbers within the range of [0 1]. The primary objective is to derive probability values from the IT2FLS-based classifier's decision outputs. Three linguistic variables L (Low), M (Medium) and H (High) have been used. To achieve this, we employ a Gaussian membership function, which is defined as follows:

$$\mu_A(t) = e^{\frac{-(t-k)^2}{2\sigma^2}} \tag{1}$$

Where k is the mean and σ is the standard deviation.

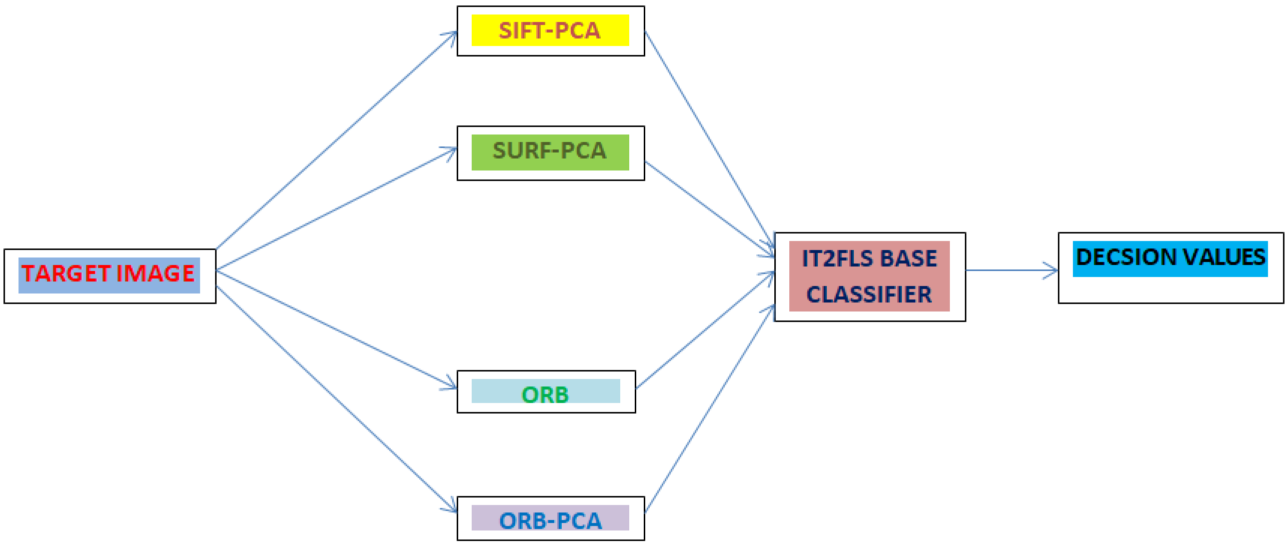


Fig 1. Proposed Model of Forgery Detection System

The architecture of the proposed fuzzy-based forgery classification system is illustrated in Figure 1. A weight value is computed based on the difference between the original duplicated region and the detected duplicate region. This weight serves as the input to the proposed fuzzy classifier. The set of fuzzy rules used for classification is summarized in Table 1.

2.2 Fuzzification and De-Fuzzification

Fuzzification refers to the method of transforming crisp values into degrees of membership within a fuzzy set. Triangular membership functions for both input and output variables have been used. If-then rules are defined for performing operation. For defuzzification Centre of area (COA) method have been used.

$$\mathrm{COA} = \frac{\int x\mu_A(x)dx}{\int \mu_A(x)dx} \tag{1}$$

Figure 2 illustrates the creation of Fuzzy Inference System (FIS) variables, fuzzy rule base are shown in figure 3, IT2FLS outputs are shown in figure 4, 5, 6 and the 3D output is shown in figure 7.

.

Specificity and Precision are essential in achieving the final outcome. To move forward, we will establish the following definitions.

True Positive (TP): The image is identified as forged, and it is indeed a forged image.

False Positive (FP): The image is identified as authentic, but it is actually a forged image.

True Negative (TN): The image is identified as authentic, and it is genuinely an authentic image.

False Negative (FN): The image is identified as forged, but it is actually an authentic image.

Mathematically,

$$\begin{aligned}
\text{Precision} &= \frac{\text{Total TP Images}}{\text{Total TP Images} + \text{Total FN Images}} \\
&= \frac{\text{Total TP Images}}{\text{Total number of forged images in test sample}} \\
\text{Specificity} &= \frac{\text{Total TN Images}}{\text{Total TN Images} + \text{Total FP Images}} \\
&= \frac{\text{Total TN Images}}{\text{Total number of authenticate images in test sample}}
\end{aligned}$$

Table 1. Rule set of proposed forgery classification system

SIFT-PCA	SURF-PCA	ORB	ORB-PCA	Decision
L	L	L	L	L
M	M	M	M	M
H	H	H	H	H
L	L	L	M	L
L	L	M	L	L
L	M	L	L	L
M	L	L	L	L
L	L	L	H	L
L	L	L	L	L
L	H	L	L	L
M	L	L	L	L
M	M	M	L	M
M	M	L	M	M
M	L	M	M	M
L	M	M	M	M
M	M	M	H	M
M	M	H	M	M
M	H	M	M	M
H	M	M	M	M
H	H	H	L	H
H	H	L	H	H
H	L	H	H	H
L	H	H	H	H
H	H	H	M	H
H	H	M	H	H
H	M	H	H	H
M	H	H	H	H

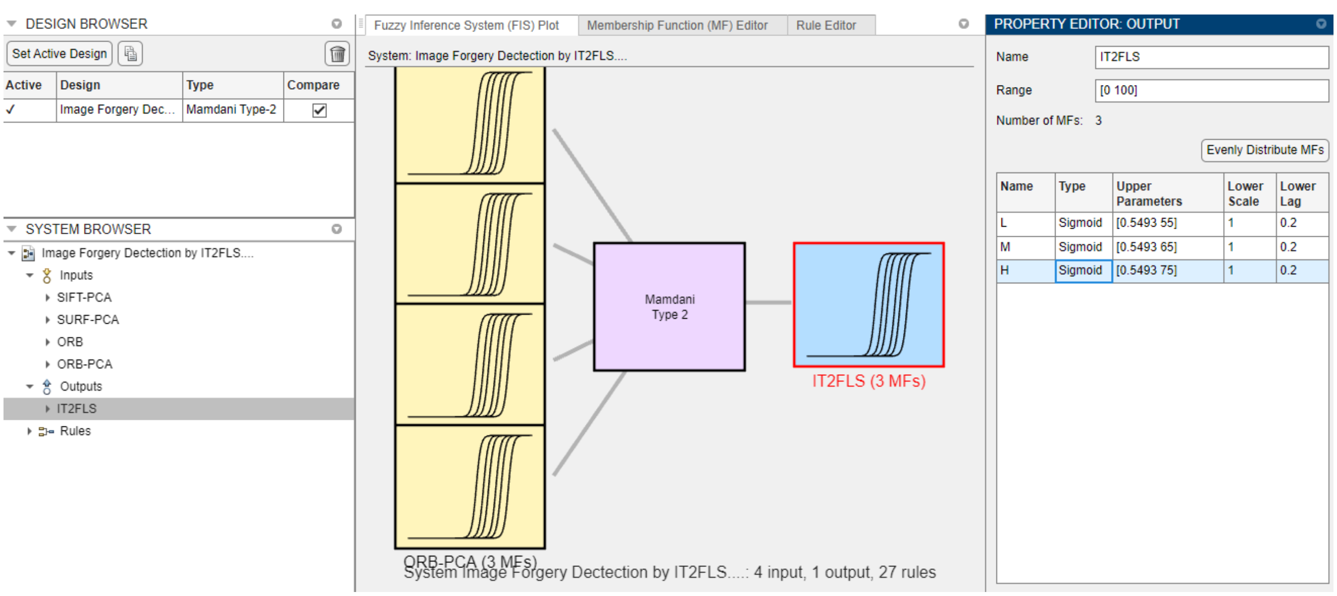
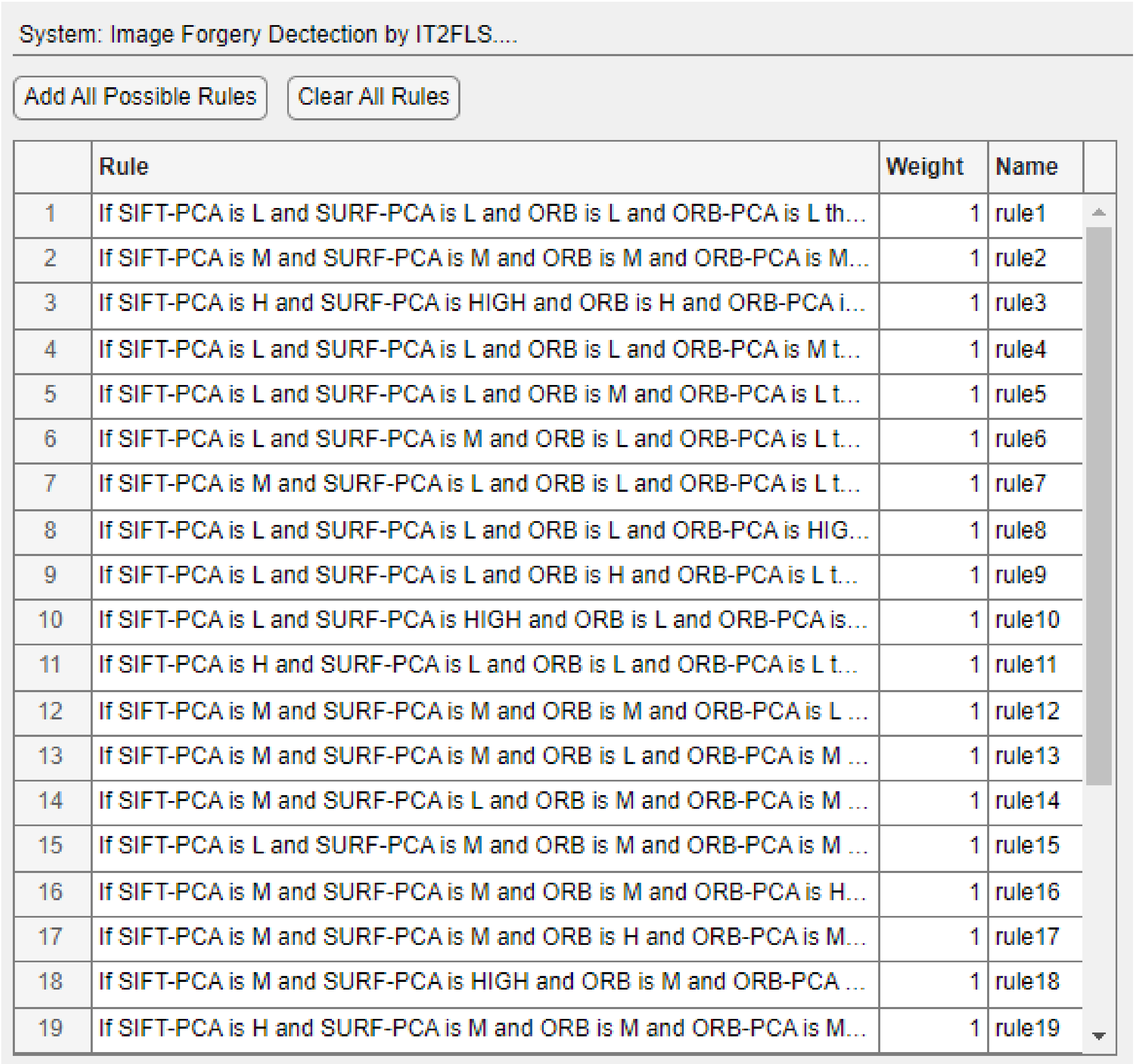


Fig 2. Designing Fuzzy Inference System Variables


System: Image Forgery Dectection by IT2FLS....

Add All Possible Rules | Clear All Rules

	Rule	Weight	Name
1	If SIFT-PCA is L and SURF-PCA is L and ORB is L and ORB-PCA is L th...	1	rule1
2	If SIFT-PCA is M and SURF-PCA is M and ORB is M and ORB-PCA is M...	1	rule2
3	If SIFT-PCA is H and SURF-PCA is HIGH and ORB is H and ORB-PCA i...	1	rule3
4	If SIFT-PCA is L and SURF-PCA is L and ORB is L and ORB-PCA is M t...	1	rule4
5	If SIFT-PCA is L and SURF-PCA is L and ORB is M and ORB-PCA is L t...	1	rule5
6	If SIFT-PCA is L and SURF-PCA is M and ORB is L and ORB-PCA is L t...	1	rule6
7	If SIFT-PCA is M and SURF-PCA is L and ORB is L and ORB-PCA is L t...	1	rule7
8	If SIFT-PCA is L and SURF-PCA is L and ORB is L and ORB-PCA is HIG...	1	rule8
9	If SIFT-PCA is L and SURF-PCA is L and ORB is H and ORB-PCA is L t...	1	rule9
10	If SIFT-PCA is L and SURF-PCA is HIGH and ORB is L and ORB-PCA is...	1	rule10
11	If SIFT-PCA is H and SURF-PCA is L and ORB is L and ORB-PCA is L t...	1	rule11
12	If SIFT-PCA is M and SURF-PCA is M and ORB is M and ORB-PCA is L ...	1	rule12
13	If SIFT-PCA is M and SURF-PCA is M and ORB is L and ORB-PCA is M ...	1	rule13
14	If SIFT-PCA is M and SURF-PCA is L and ORB is M and ORB-PCA is M ...	1	rule14
15	If SIFT-PCA is L and SURF-PCA is M and ORB is M and ORB-PCA is M ...	1	rule15
16	If SIFT-PCA is M and SURF-PCA is M and ORB is M and ORB-PCA is H...	1	rule16
17	If SIFT-PCA is M and SURF-PCA is M and ORB is H and ORB-PCA is M...	1	rule17
18	If SIFT-PCA is M and SURF-PCA is HIGH and ORB is M and ORB-PCA ...	1	rule18
19	If SIFT-PCA is H and SURF-PCA is M and ORB is M and ORB-PCA is M...	1	rule19

Fig 3. Fuzzy Rules

3 Results and Discussion

The suggested method is implemented on the CASIA 2.0 [https://www.kaggle.com/datasets/divg07/casia-20-image-tampering-detection-dataset] standard dataset. This dataset includes 7,492 genuine and 5,123 altered color images, with dimensions ranging from 240×160 to 900×600 pixels. MATLAB R2023a (9.14.0.2206163) software, equipped with 4GB of RAM and an Intel Core i3 processor, was utilized. To implement interval type-2 fuzzy logic, we employed the MATLAB fuzzy logic toolbox. Ultimately, the IT2FLS classifier's key points matching operation was executed to detect copy-move forgery.

The efficiency of the suggested method is evaluated by examining features such as specificity, precision, and accuracy. This method is verified on a set of 100 images from the CASIA 2.0 dataset. Table 2 displays the results of the comparison.

The statistical significance testing of proposed technique is performed in the following steps:

Here $n = 5,\ \overline{X} = 70.293,\ \mu_0 = 78.8,\ s = 50.754$

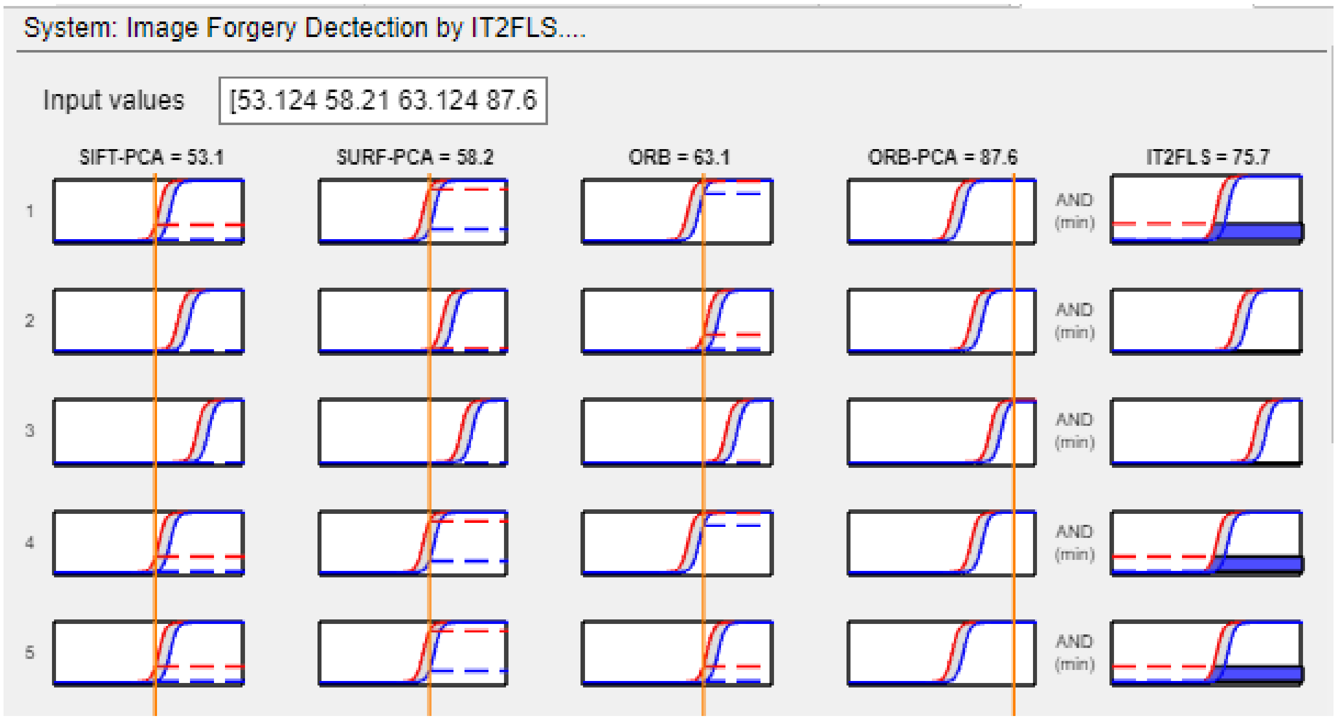


Fig 4. Output Specificity by IT2FLS

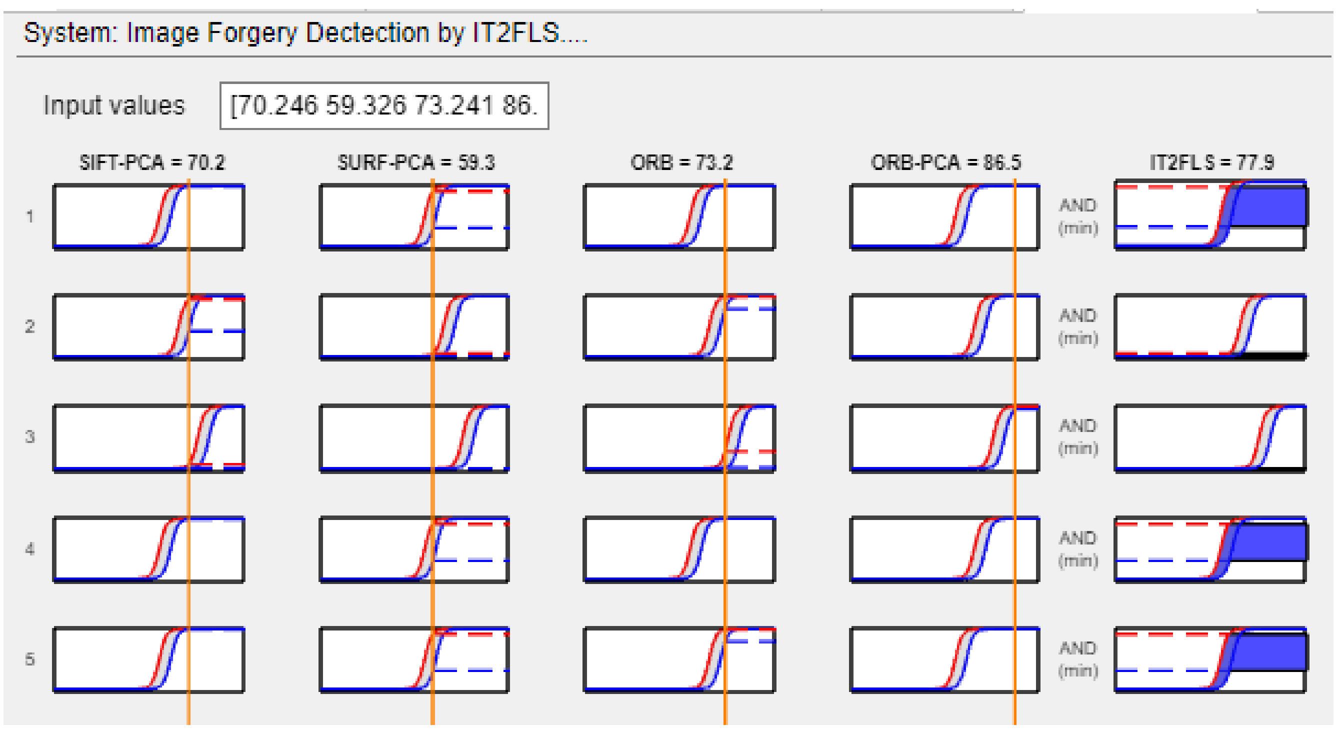


Fig 5. Output Precision by IT2FLS

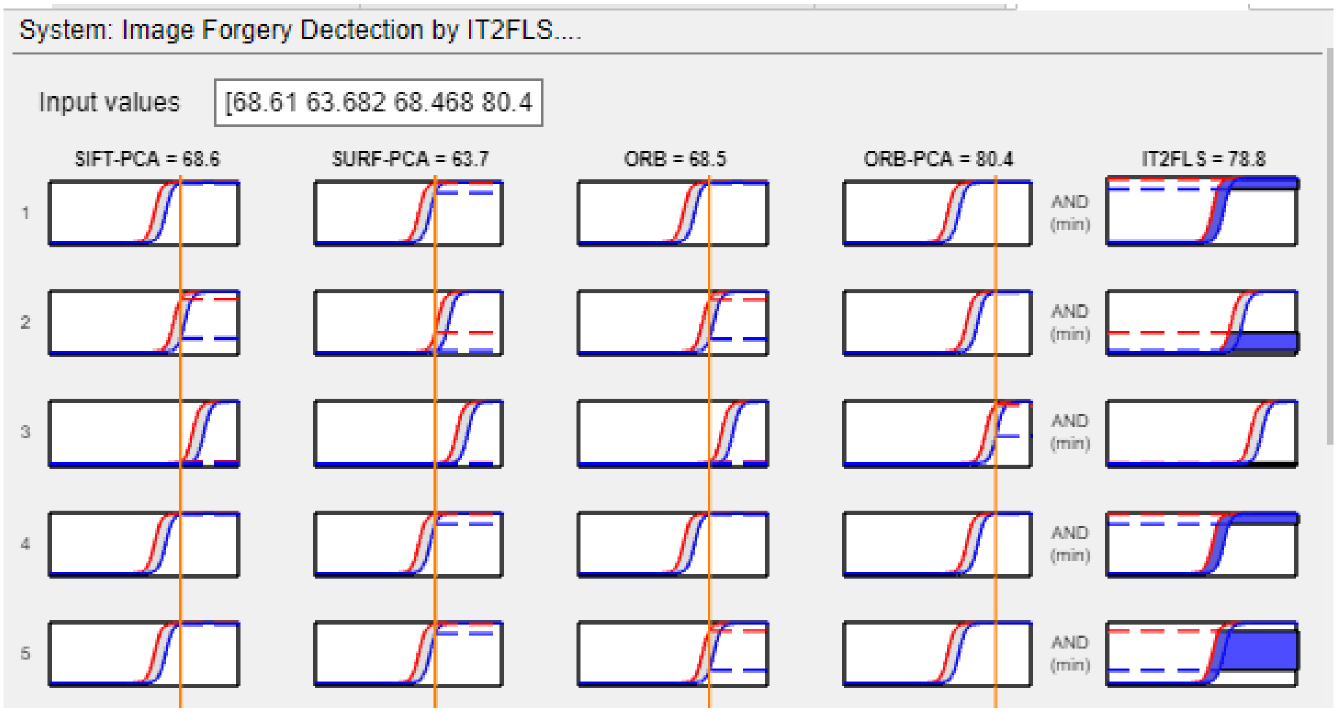


Fig 6. Output Accuracy by IT2FLS

Table 2. Comparative Results of Proposed Approach

Techniques	Specificity	Precision	Accuracy
SIFT-PCA	53.124	70.246	68.610
SURF-PCA	58.210	59.326	63.682
ORB	63.124	73.241	68.468
ORB-PCA	87.624	86.510	80.412
Average	65.5205	72.33075	70.293
IT2FLS	75.7	77.9	78.8

Step 1: Null Hypothesis (H_0): $\mu = 78.8$ [Accuracy obtained from IT2FLS]
Step 2: Alternate Hypothesis (H_1): $\mu \neq 78.8$
Step 3: Test Statistics: Under H_0 test statistics is given by, $t_{cal} = \frac{\overline{X}-\mu_0}{\frac{s}{\sqrt{n}}}$
Therefore $t_{cal} = \frac{\overline{X}-\mu_0}{\frac{s}{\sqrt{n}}} = \frac{70.293-78.8}{\frac{50.754}{\sqrt{4}}} = -0.3352$

$$|t_{cal}| = 0.3352$$

Step 4: Level of Significance (α): Assume 5%= 0.05
Therefore, degree of freedom $d_f = n-1 = 5-1 = 4$

$$|t_{tab}| = 2.776$$

Step 5: Comparison and Decision: Since $|t_{tab}| > |t_{cal}|$
Since it is not significant, so null hypothesis (H_0) is accepted and alternate hypothesis (H_1) is rejected.

In Table 2, specificity, precision and accuracy obtained from IT2FLS are higher than the average specificity, precision and accuracy obtained from different methods. In table 3, performance of proposed method is compared with previous results obtained from different methods and it is observed that the proposed method gives more accurate result than most of the existing methods.

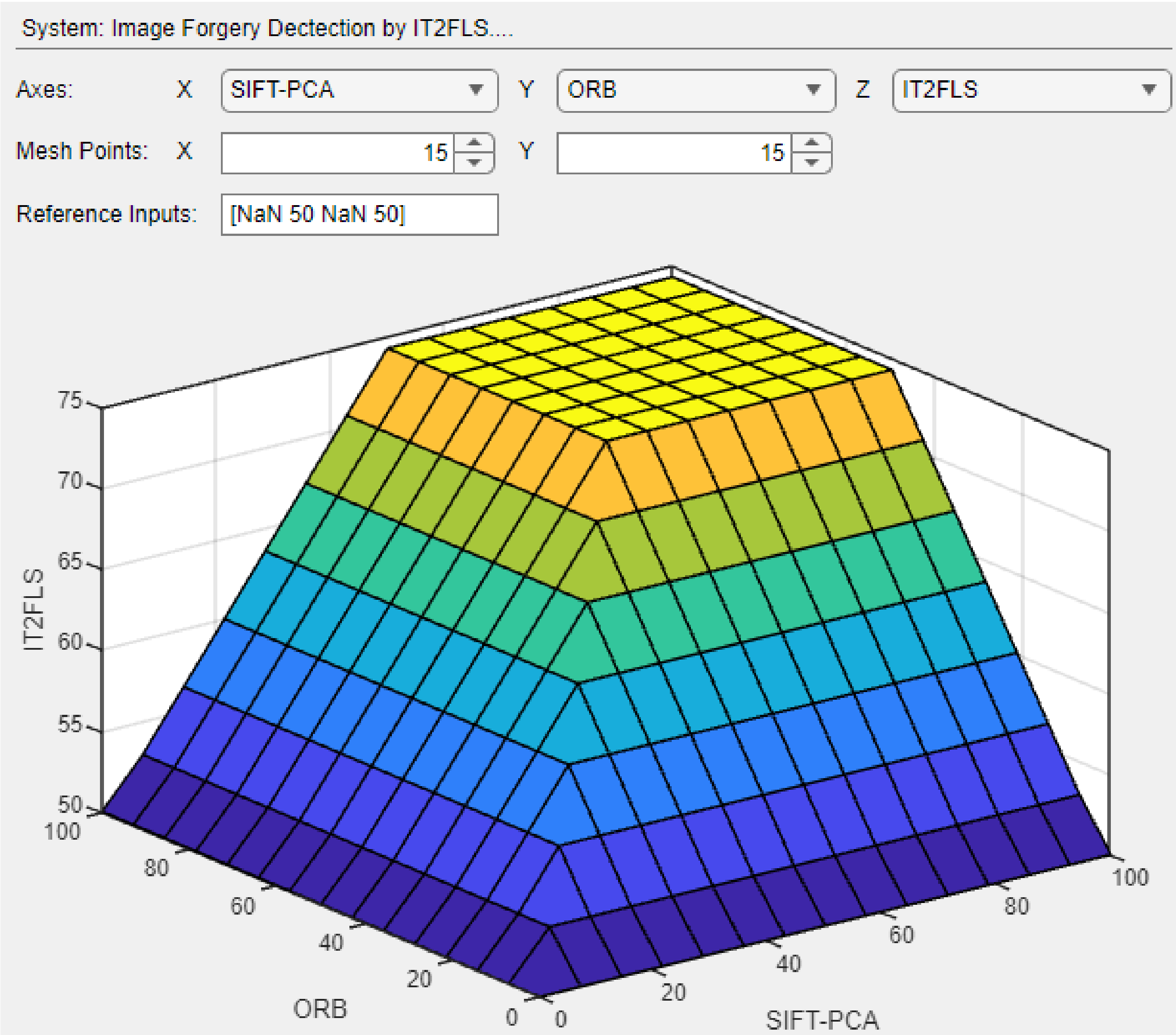


Fig 7. 3D Output

Table 3. Comparison of Performance with Previous Results

Techniques	Accuracy
Rossler et al. [28], [29]	72.2%
Nguyen et al. [28], [30]	53.3%
Li and Lyu [28], [31]	75.5%
Wu et al. [28], [32]	76.65%
Peng et al. [26]	88.4%
IT2FLS	78.8%

4 Conclusion

This study presents a novel approach utilizing block and IT2FLS methodologies to detect image forgery. The IT2FLS is employed to combine various algorithms and obtain a unified output. The outcome obtained from IT2FLS is higher than the average outcome obtained from different techniques. It has been observed that the outputs generated from different image forgery detection techniques have differences, so the decision-making process becomes complicated. To address this complication, the fusion of interval type-2 fuzzy logic with existing image forgery detection techniques presents an appropriate combination for obtaining a combined outcome. The proposed method is compared with some existing methods. There are some limitations of type-2 fuzzy logic as it works well for generalized image forgery detection, but it is not suitable for localization of forged image compared to other recent methods. In the future, combining Interval Type-2 Fuzzy Logic Systems (IT2FLS) with other soft computing methods like Intuitionistic Fuzzy Logic (IFL) can provide significant developments in image forgery detection and localization. Although the footprint of uncertainty is a useful tool for modeling uncertainty in IT2FLS, IFL provides an additional level of precision by including into account degrees of membership, non-membership, and hesitation. In regions of the image that are unclear or of poor quality, this combination enables more sophisticated decision-making, improving the system's ability to distinguish between tampered and real areas. Future hybrid models can attain improved accuracy, adaptability to noise, and more reliable localization of forged regions by utilizing the advantages of both frameworks.

References

1) Ignatov A, Kobyshev N, Timofte R, Vanhoey K, Gool LV. WESPE: Weakly Supervised Photo Enhancer for Digital Cameras. 2018.
2) Zhao G, et al. An Augmented Reality Based Mobile Photography Application to Improve Learning Gain, Decrease Cognitive Load, and Achieve Better Emotional State. *International Journal of Human–Computer Interaction*. 2023;39(3):643–658. https://doi.org/10.1080/10447318.2022.2041911.
3) Farid H. *Photo Forensics*. 2016.
4) Cao G, Zhao Y, Ni R. Forensic estimation of gamma correction in digital images. 2010.
5) T MN, Sekhar LC, M IS. Image Forgery Detection Using Deep Learning Techniques - A Review. 2023. https://ijsrst.com/IJSRST523101125.
6) Elaskily MA, Elnemr HA, Dessouky MM, Faragallah OS. Two stages object recognition based copy-move forgery detection algorithm. *Multimed Tools Appl*. 2019;78(11):15353–15373. https://doi.org/10.1007/s11042-018-6891-7.
7) Elaskily MA, Alkinani MH, Sedik A, Dessouky MM. Deep learning based algorithm (ConvLSTM) for Copy Move Forgery Detection. *IFS*. 2021;40(3):4385–4405. https://doi.org/10.3233/JIFS-201192.
8) Parveen A, Khan ZH, Ahmad SN. Block-based copy–move image forgery detection using DCT. *Iran J Comput Sci*. 2019;2(2):89–99. https://doi.org/10.1007/s42044-019-00029-y.
9) Pukale PDD, Kulkarni PVD. IMAGE FORGERY DETECTION AND LOCALIZATION USING DEEP LEARNING. *Journal of Emerging Technologies and Innovative Research (JETIR)*. 2024;11(1). https://www.jetir.org/papers/JETIR2401179.pdf.
10) Singh R, Verma S, Yadav SA, Singh SV. Copy-move Forgery Detection using SIFT and DWT detection Techniques. 2022.
11) Meena KB, Tyagi V. A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms. *Multimed Tools Appl*. 2020;79(11–12):8197–8212. https://doi.org/10.1007/s11042-019-08343-0.
12) Wang C, Zhang Z, Zhou X. An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features. *Symmetry*. 2018;10(12):706. https://doi.org/10.3390/sym10120706.
13) Lađević AL, Kramberger T, Kramberger R, Vlahek D. Detection of AI-Generated Synthetic Images with a Lightweight CNN. *AI*. 2024;5(3):1575–1593. https://doi.org/10.3390/ai5030076.
14) Mahmood T, Nawaz T, Irtaza A, Ashraf R, Shah M, Mahmood MT. Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images. *Mathematical Problems in Engineering*. 2016;2016:1–13. https://doi.org/10.1155/2016/8713202.
15) Abbas MN, Ansari MS, Asghar MN, Kanwal N, O'Neill T, Lee B. Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks. 2021.
16) Isnanto RR, Zahra AA, Santoso I, Lubis MS. Determination of the Optimal Threshold Value and Number of Keypoints in Scale Invariant Feature Transform-based Copy-Move Forgery Detection. *International Journal of Electronics and Telecommunications*. 2020;p. 561–569. https://doi.org/10.24425/ijet.2020.134013.
17) Khan SA, et al. Visual User-Generated Content Verification in Journalism: An Overview. *IEEE Access*. 2023;11:6748–6769. https://doi.org/10.1109/ACCESS.2023.3236993.
18) Zhang Z, Zhang Y, Zhou Z, Luo J. Boundary-based Image Forgery Detection by Fast Shallow CNN. 2018.
19) Abbas MN, Ansari MS, Asghar MN, Kanwal N, O'Neill T, Lee B. Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks. 2021.
20) Qazi EUH, Zia T, Almorjan A. Deep Learning-Based Digital Image Forgery Detection System. *Applied Sciences*. 2022;12(6):2851.
21) Abidin ABZ, Majid HBA, Samah ABA, Hashim HB. Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review. 2019.
22) Shirsho MH, Rana MM, Akhter J, Rahaman ASMM. Enhancing Image Manipulation Detection through Ensemble ELA and Transfer Learning Techniques. *IJCDS*. 2025;18(1):1–12. https://doi.org/10.12785/ijcds/1571015807.
23) García-Gutiérrez A, Gonzalo J, Rubio C, Corvino MM. Estimating Landfill Landslide Probability Using SAR Satellite Products: A Novel Approach. *Remote Sensing*. 2024;16(9):1618.
24) Lin SD, Wu T. An integrated technique for splicing and copy-move forgery image detection. 2011.
25) Stamm MC, Liu KJR. Forensic detection of image manipulation using statistical intrinsic fingerprints. *IEEE TransInformForensic Secur*. 2010;5(3):492–506. https://doi.org/10.1109/TIFS.2010.2053202.
26) Peng J, Liu C, Pang H, Gao X, Cheng G, Hao B. GP-Net: Image Manipulation Detection and Localization via Long-Range Modeling and Transformers. *Applied Sciences*. 2023;13(21):12053.

27) Fu G, Zhang Y, Wang Y. Image Copy-Move Forgery Detection Based on Fused Features and Density Clustering. *Applied Sciences*. 2023;13(13):7528. https://doi.org/10.3390/app13137528.
28) Zanardelli M, Guerrini F, Leonardi R, Adami N. Image forgery detection: a survey of recent deep-learning approaches. *Multimedia Tools and Applications*. 2023;82:17521–17566. https://doi.org/10.1007/s11042-022-13797-w.
29) Rossler A, Cozzolino D, Verdoliva L, Riess C, Thies J, Niessner M. FaceForensics++: Learning to Detect Manipulated Facial Images. 2019.
30) Nguyen HH, Yamagishi J, Echizen I. Capsule-forensics: Using Capsule Networks to Detect Forged Images and Videos. 2019.
31) Li Y, Lyu S. Exposing DeepFake Videos By Detecting Face Warping Artifacts. *arXiv*. 2018. https://doi.org/10.48550/ARXIV.1811.00656.
32) Wu Y, Abd-Almageed W, Natarajan P. BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization;vol. 11210. 2018.