Journal of Robotics and Control (JRC)
Volume 6, Issue 2, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i2.25567

Hybrid SVD and SURF-Based Framework for Robust Image Forgery Detection and Object Localization

Fallah H. Najjar [1*], Ansam Ali AbdulAmeer [2], Salman Abd Kadum [3]
[1, 3] Department of Computer Networks and Software Techniques, Technical Institute of Najaf, Al-Furat Al-Awsat Technical University, 54001, Najaf, Iraq
[1] Department of Emergent Computing, Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia
[2] Department of Intelligent Medical Systems, Biomedical Informatics College, University of Information and Communication Technology, 10001, Baghdad, Iraq
Email: [1] fallahnajjar@atu.edu.iq, [2] ansam.ali@uoitc.edu.iq, [3] salman.kadhum@atu.edu.iq
*Corresponding Author

***Abstract*—This paper presents a highly effective and reliable approach for detecting image forgery and identifying manipulated regions in digital images. The proposed method uses a combination of Singular Value Decomposition (SVD) and the Speeded-Up Robust Features (SURF) algorithm, achieving a high degree accuracy of 99.1% for revealed tampering. After an input image is initially divided parallel to partition, then is performed by SVD to extract features with remarkable discriminability, the method is valued based on independent experiments. The norms are calculated, and pixels with the same norm begin to group to identify potentially tampered areas. In order to simplify the detection process, we conduct a weighted comparison among subgroups to distinguish real structures from false ones. Once we discover a suspicious forgery area, the SURF algorithm comes into play to accurately identify the manipulated items. This process uses a keypoint detector, descriptor calculations, the match between points, and geometric checking to improve the accuracy and reliability of forgery localization. Experimental results on different image databases show that this method is effective. It exhibits advanced ability in detecting forgeries, finding objects and locating where they are in an image. Eventually, we hope this work will produce a sturdy forgery detection system and improve the accuracy of recognizing tampered regions. The proposed method is useful in digital forensics and image verification.**

Keywords—Copy-Move Forgery; Forged Object Localization; Image Processing; SURF; SVD.

I. INTRODUCTION

Copy-Move Forgery Detection is one of the most essential contents in digital image forensics, Which refers to finding and locating copy-moved areas within a digital image [1][2]. In the present digital world of counterfeit images, piracy is a significant problem [3][4]. With many image manipulation tools becoming phony devices and an inability to survive without a variety of operations occurring to rectify what would be original data, someone else's now false data [5]. It becomes clear that something must soon be done to detect localizations anywhere in the imagery [6][7]. With this operation, the region of origin has its original content removed and is stuck up in another part elsewhere on the same piece of paper. Often, this tampering is done to cover up or duplicate many items, leading to the dissemination of false information, deception, and unsanctioned use of images [8][9]. Image authentication and detection is the system that automatically finds regions in an input digital image subjected to copy-move forgery [10]. It utilizes different image processing and computer vision techniques such as feature extraction, similarity measures, and clustering [7][11]. After the image is broken into several sub-images, the system gathers the characteristic features of each block area and compares them against similar ones found among other areas [12]. Then, the exact physical location of the site under question, a duplicate patch, is localized by analyzing source-aligned images [13][14]. Investigators can, therefore, employ this localization for further investigations, such as proof of principle and quantification. Copy-Move Forgery Detection and Localization is widely used in digital forensics, copyright protection, and image authentication [15]. It is important to litigate based on doctored images, ensure objective and original presentation by journalism agencies, and maintain the reliability of visual content from any field [12][16]. Detection algorithms based on machine learning (profound learning) or pattern recognition are constantly being created and improved by researchers to respond faster than forgers as new forgery methods emerge [17][18].

However, the challenge is to attain high accuracy and efficiency in coping with various complexities (e.g., rotation/scaling/partial occlusion) [19][20]. As the digital environment continues to develop, maintaining image integrity and assuring that visual information we come across daily can be trusted is increasingly at risk [21]. Accordingly, copy-move forgery's detection and localization problem remains an open field for reducing such threats [22]. Additionally, it is crucial to handle copy-move forgeries because digital images play a vital role in numerous areas, such as legal investigations and media, where their authenticity or integrity is prone [4][23][24]. We are using Singular Value Decomposition (SVD) for classification. Meanwhile, the Speeded-Up Robust Features (SURF) is used for localization to develop a robust solution for detecting forged regions within images.

In order to overcome these challenges, our main contributions in this study are as follows: (i) hybrid SVD-SURF approach for forgery detection and localization. We propose an integrated SVD-based feature extraction and SURF-based localization framework to detect copy-move forgeries with high precision. SVD extracts robust features from image blocks, and SURF is applied to enhance localization accuracy. (ii) Improved robustness against geometric transformations and noise. Through norm-based grouping in SVD and keypoint matching in SURF, this approach enriches the ability to accept different image alterations. A typical problem in forgery detection is that the method commonly withstands the rotation, scaling, and noise encountered.

The remaining sections of the paper are structured as follows: In the second step, a comprehensive overview of related studies is presented. Thirdly, it introduces the proposed methodology in detail. Fourthly, it delves into specific results and engages in in-depth discussions. Lastly, it Encapsulates the key takeaways and conclusions drawn from the study.

II. RELATED WORKS

Raju and Nair introduced a technique founded on binary discriminant features for copy-move forgery detection. One of the methods for this is extracting these features by comparing original and forged images. These images were broken into blocks, where we calculated the mean value and standard deviation of each block. They estimate that 46-man discriminant functions based on two region-specific objects were binarized and released as binary features, irrelevant to the discrepancy between plants produced by mesh forgery of leaves [25].

Wang et al. proposed a new detection approach for Copy-Move Image Forgery. This approach depends on three main factors: deriving adaptive keypoint, Hybrid feature extraction of transform domain plus texture features. The authors identified adaptive keypoints using SLIC and KMM methods. Thus, these adaptive keypoints are very Important in Differentiating Candidate Forgeries. Furthermore, the hybrid features are based on Fast Quaternion Generic Polar Complex Exponential Transform (FQGPCET) combined with the Gray-Level Co-Occurrence Matrix (GLCM). The combination of features from the texture domain and from the transform domain improves copy-move forgery detection [26].

Kaur, N. et al. introduced an advanced deep learning-based method to detect copy-move forgeries in digital images. The proposed approach involves two main steps. First, Contrast-Limited Adaptive Histogram Equalization (CLAHE) enhances the image's contrast. This improvement allows for finding hidden features that cannot easily be observed in copy-move forgeries and enforces the overall detection process. A Convolutional Neural Network (CNN) determines whether the image is real or fake. It looks like some fake images were presented to CNN. CNN is trained on a labeled dataset, which helps it classify genuine and manipulated images easily. CLAHE is combined with poorly-trained CNN to boost hidden visualization and deep learning is involved in classifying bigger mistakes. Their proposed technique efficiently and effectively identifies copy-move forgery in digital images [27].

Kumar et al. authored a brand-new algorithm that is feature-oriented in design. Take the image, partition it into blocks, and then apply Discrete Cosine Transform (DCT) to each of these blocks. These histograms of DCT coefficients provide high-level features. Singular Value Decomposition (SVD) is carried out on these features to reduce their dimensions. Afterward, a Support Vector Machine (SVM) classifier is used to categorize the feature subspace into two classes, doctored or genuine, thus opening up the way for detecting copy-paste fakes in images with digital signatures [28].

Copy-move has been the focus of numerous digital forensic applications, and a range of methods have been proposed for its detection [29][30]. Block-based techniques like DCT and Discrete Wavelet Transform (DWT), traditional methods, partition the image into overlapping blocks to search for similarity, but they are computationally expensive and fail in the presence of distortions [31][32]. Other keypoint-based methods like Scale-Invariant Feature Transform (SIFT) and SURF can achieve high performance in terms of robustness to transformations [33][34]. However, they are less effective on smaller or significantly modified forgeries.

With extensive research on image forgery detection, most existing methods have three main deficiencies: feature extraction can bring high computational cost, similarity measurement is not rigorous enough, and clustering still needs improvement [35]. SIFT, Oriented FAST, Rotated BRIEF (ORB), and Discrete Cosine Transform (DCT) are severally circumspect. While SIFT may be immune to rotation and scaling, it is extremely expensive, smash counts time and memory and can miss small or low-contrast forgeries [36]. ORB has higher efficiency but is less accurate in handling complex transformations in the presence of varying light, and so often, it gives false positives [37].

Furthermore, the similarity measures popular in forgery detection have significant disadvantages [38]. For example, noisy areas usually afflict scores with less value because it is so sensitive to minute changes in pixels besides noise [39]. Another instance is Correlation-based matching, which can accurately detect overlapping regions of interest but becomes ineffective if changes involve rotation or scaling [40]. For this account alone, more computational resources might be demanded for manipulation so that material benefits vanish across an understandable lengthy calculation study. A further problem with correlative-based methods is their excessive demand for computational resources [40].

In this study, we introduce our proposed method that combines SVD and SURF localization to take the respective advantages of the two methods. SVD enables efficient dimensional reduction and robust feature extraction, making classification more accurate; SURF can resist familiar image transformation to locate objects accurately. The proposed hybrid method can resolve the challenges like high computational costs and transformation sensitivity encountered in existing methods, therefore providing a comprehensive solution for copy-move forgery detection.

A. Singular Value Decomposition (SVD)

In fact, SVD is a very mathematical algorithm has started to be adopted by image-processing researchers over the last few years [41]. Initially used in a range of fields, this algorithm based on SVD has quickly branched into an array of territories [40][42]. SVD will decompose any matrix into three matrices, U, S, and V (which are rotation matrices), in such a way that some fundamental properties stay unaffected. For the algebraic region of image processing, this technique functions by providing a decomposition of an (m, n) matrix to form $A = USVT$. The stability and conceptual advantages of SVD have motivated researchers to use this classic algebraic transform, as it possesses robust orthogonal matrix factorization properties in imaging [43]. However, (A) matrix can be decomposed into three constituent matrices using the SVD procedure. For any given matrix ($A \epsilon R^{\mathrm{m\times n}}$), the decomposition results in the following three matrices [44].

$$A = USV^T \tag{1}$$

Where $U \epsilon R^{\mathrm{m\times m}}$ is an m × m is an orthogonal matrix known as the left singular vector matrix, $S \epsilon R^{\mathrm{m\times n}}$ i is a diagonal matrix containing the singular values, and $V \epsilon R^{\mathrm{n\times n}}$ is an n × n orthogonal matrix, referred to as the right singular vector matrix.

SVD is applicable to matrices where $A \epsilon R^{\mathrm{m\times n}}$, where $m \geq n$. In the special instance where $m = n$, the diagonal elements of the matrix S are only non-zero positive values.

In the special instance of $m > n$, diagonal matrix S elements are descending positive values and zeros values [45]-[48].

$$AA^T = USV^T(USV^T)^T \tag{2}$$

$$AA^T = USV^TVSU^T \tag{3}$$

$$AA^T = US^TU^T \tag{4}$$

Also,

$$A^TA = (USV^T)^TUSV^T \tag{5}$$

$$A^TA = VSU^TUSV^T \tag{6}$$

$$A^TA = VS^TV^T \tag{7}$$

B. Speeded Up Robust Features (SURF)

The SURF algorithm works in three main steps- interest point detection, orientation assignment, and feature description [49]. In the end, these stages work together in order to extract some distinct features from an input image [50]. Readers are encouraged to consult this reference [51]. Even if the image is rotated or resized, our interest points in detected images are stable and work well under different conditions. These areas are critical for processes like image object recognition. Haar wavelets are the method we use to capture these points in an image, and this is a critical step in the SURF algorithm. It prepares the data in a summary for simple comparison and matching compatible knowledge between images of different datasets. This process makes SURF applicable to a number of computer vision applications [52].

III. PROPOSED SCHEME

The proposed method aims to design an effective and efficient arm for copy-move forgery detection in digital images. The scheme performs this by combining SVD for feature extraction and classification with SURF - a keypoint-based localization to improve detection accuracy in face verification while maintaining computational efficiency. The aim is to produce a robust digital forensics tool capable of identifying and interpreting altered image content regardless of complex transformations or small forgeries. The preprocessing steps of the proposed copy-move forgery detection scheme are based on three primary modules: image resizing, denoising, and changing from Red, Green, and Blue (RGB) images to grayscale. One of the first steps is to resize the image so that it has a standard dimension in processing and helps ease some computation load. Then, the image is often denoised, with ordinary filters lying in Gaussian filtering and median filtering, to erase particular noise that could affect the extracting process. Afterward, the image is encoded to grayscale by converting it from RGB while preserving basic structural information and reducing data content into one channel. In this way, we make the image more suitable for better and faster feature extraction in further forgery detection process.

Furthermore, in this method, the input image is divided into overlapping blocks and processed by SVD to extract its feature vector, then processed for norms of specific values that are used as a distinct identity value. It has a dictionary, groupDict, which will categorize the blocks by their norms. So far, so good; now, for each block processed, its norm is measured, and it is appended to a group in groupDict. After all, blocks are grouped with other similar norms. Every norm group is then subdivided. It turns out that this can be achieved by evaluating the spatial relationship between blocks using 8-adjacency (evaluates neighboring cells in a grid form) and city block distance (a metric for calculating distance based on movements through an evenly spaced grid).

These subgroups are indicators of potential forgery, bringing together blocks whose content is similar (although the correlation might be weak) and are near each other in the image. If too many of these grouped blocks or keypoints are found, the image is marked as forged, indicating a duplication. The blocks are first clustered with the help of their feature similarity, and then spatial clusters can be derived by examining 8-adjacency for city block distance. If more than a predefined threshold number of blocks or keypoints match and their spatial distribution indicates that the resemblance is intentional, you can label the image as forged. If no patterns or the number of matches below this threshold are detected, it can be a genuine image.

Moreover, a robust algorithm for detecting copy-move forgery images based on the SVD transformation and SURF

algorithm for localization is proposed. Algorithm 1 describes the steps of the proposed method.

The input image is divided into overlapping blocks. SVD is applied to each block, yielding three matrices. The norm value is computed from the diagonal matrix and sorted in ascending order. Pixels with similar norms are grouped, and groups with fewer than three members are ignored. Subgroups are formed within each group based on 8-adjacency. Subgroups with distances less than or equal to thirty are considered connected objects. Selected subgroups meeting size and distance conditions are assigned weights.

After pairwise comparisons, each subgroup obtains weight. The number of remaining subgroups for each norm is noted. Two arrays, sorted by weight and subgroup count, are created. The top six norms by weight (W1) and the top ten norms by subgroup count (W2) are selected. Forgery regions are identified if any of the following conditions are met: (i) There are at least eight subgroups in the top ten of W2, with weight greater than or equal to sixteen in the top six of W1. (ii) There are at least eight subgroups in the top ten of W2, with eight or fewer subgroups in the top six of W2.

Forgery regions are identified. In addition, the SURF algorithm is applied to localize forged objects within the identified regions:

1) Keypoints and descriptors are detected and computed on the entire image using SURF.
2) Keypoint matching between the forged and original regions is performed.
3) Geometric verification is executed, discarding false matches.
4) Forged objects are localized based on the matched keypoints and descriptors.

However, understanding the efficiency of the proposed method is crucial for practical implementation. The computational complexity of SVD is $O(n^3)$ for an image of size $n \times n$, which is mitigated by applying it to small overlapping blocks. This way, it adheres to constant factors where optimal methods are still possible and can be optimized well for large images.

Likewise, SURF carries a complexity of $O(n \log n)$, making it much faster than SIFT. The proposed method balances accuracy and computational cost, as demonstrated through comparative performance analysis across different image sizes.

However, Fig. 1. displays the proposed scheme of the proposed method.

IV. RESULTS AND DISCUSSION

In this section, we conducted a series of experiments to evaluate the proposed schemes. Initially, the proposed method was tested on RGB images sourced from the CASIA [53] and CoMoFoD [54] datasets, both of which are widely used in digital image forensics. CASIA dataset [53] contains both real and spurious images of different types, including forgery types such as splicing, copy-move, and more. The CoMoFoD dataset [54], designed especially for copy-move forgery detection, consists of different geometric transformation-based forged images in terms of rotation and scaling. Combined, these data collections form a broad and complex assessment dataset to validate the liberalism of both object detection methods over different backgrounds. The datasets contain real photos, including animals, plants, buildings, and different foods. Fig. 2 shows a sample of the images in our current proposal.

Algorithm1: Copy-Move-Forgery Detection With Localization (image)

Input: Color Image
Output: Result of Forged Image (either True or False)
Step 1: Perform Preprocessing on the image (denoising, grayscale conversion, image resizing)
Step 2: Divide the image into overlapping blocks.
Define norm(block):
Step 3: Extract features for the block using SVD transformation (norm)
Initialize groupDict as an empty dictionary.
  For each block in the image:
Step 4: Calculate the norm for the block.
Step 5: Add a block to the corresponding group in groupDict based on its norm.
  For each normGroup in groupDict:
Step 6: Create subgroups based on 8-adjacency and city block distance.
  For each subgroup in subgroups:
Step 7: Check conditions:
    A. Difference in size <= 1 pixel
    B. Distance between subgroups > threshold
  For each subgroup that meets the conditions in step 7:
Step 8: Calculate the weight for the subgroup based on conditions.
  For each normGroup in groupDict:
Step 9: Count the number of valid subgroups and sum the weights of all valid subgroups.
Define forgery Threshold = 2 for the number of subgroups and 8 for total weights
Step 10: Classify the image as a forgery if any of the following conditions are met:
  A. Number of subgroups for a norm > forgeryThreshold
  B. number of subgroups > forgeryThreshold and total weights > forgeryThreshold × 2
  If the image is classified as a forgery:
Step 11: Apply SURF algorithm for forged object localization:
  a. Distinguish keypoints and descriptors using SURF on the entire image.
  b. Match keypoints between the forged and original regions
  c. Perform geometric verification and discard false matches.
  d. Localize forged objects based on the matched keypoints and descriptors.
Return Forgery Detection Result and Localization of Forged Objects

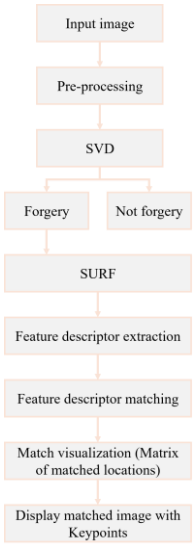

Fig. 1. Proposed schema

Fig. 2. Samples of images were collected from the CASIA dataset, left column, and the CoMoFoD dataset, right column

However, the experimental setup was conducted on a Windows 11 Pro 64-bit machine. The system is powered by an 11th Gen Intel Core i7-11800H processor with 16 CPUs at 2.30GHz and 32,768 MB of RAM. Matlab 2022 was used for experiments. The performance of the proposed algorithm was measured by using the confusion matrix and measuring the precision [55], recall, and F1 scores, which were measured by the equations (8), (9), and (10) [55]-[57].

$$\text{Precision} = \frac{T_P}{T_P + F_P} \tag{8}$$

$$\text{Recall} = \frac{T_P}{T_P + F_N} \tag{9}$$

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{10}$$

Where, TP is the true positive, TN is the true negative, FN is false negative, and FP means false positive [58].

The F1-score for the proposed method was 99.1%. This high F1 score indicates a robust ability to precisely locate duplicated and manipulated regions, ensuring that even subtle alterations do not go unnoticed. Fig. 3 shows samples of the detected forgery images.

Fig. 3. CASIA dataset image samples, left column, and the CoMoFoD dataset, right column, were detected by using the SVD algorithm

The localization of the forged object is performed using the SURF algorithm, which is highly effective in practice. It detects and locates inexact regions by matching features within the image using this algorithm. As illustrated in Fig. 4, the results illustrate that the algorithm can consistently highlight the forged object, confirming that they are robust in identifying image alterations.

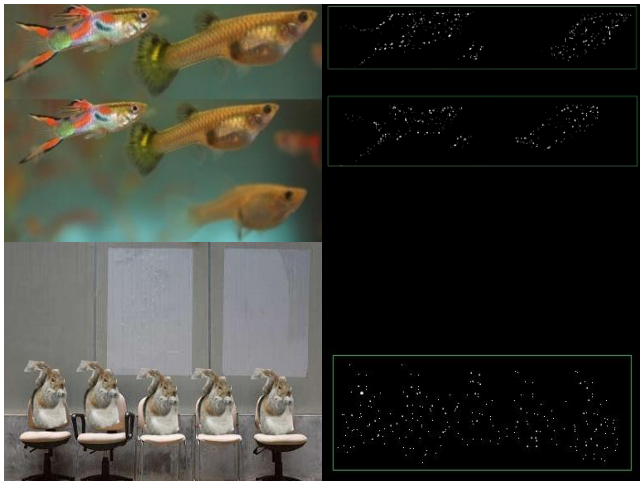

Fig. 4. The result of the SURF algorithm. The top row displays the input image, while the bottom row highlights the location of the forged object

More importantly, the proposed algorithm was tested for detecting forged images where the images contained objects scaled or rotated—considered difficult scenarios. The findings show that the algorithm can identify these cases and all other difficult images. Fig. 5. demonstrates an instance of such a scenario.

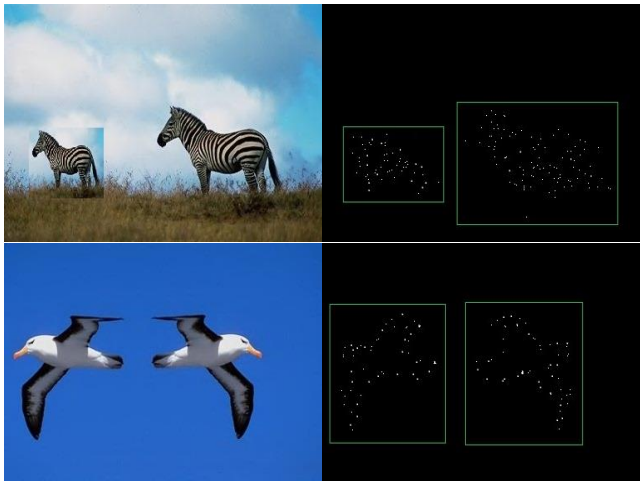

Fig. 5. Samples of images with the challenges (scaling and rotation) were detected, and the proposed algorithm localized the forged object

Compared with other methods, the proposed algorithm is shown in Table I. It is clear that the proposed algorithm is more efficient than other methods because the SVD concerns all the neighbor pixels and compares the features of the image regions.

The comparison of forgery detection methods reveals a diversity of detection in the F1-score, leading to a disparity in detection efficiency and robustness. Fu et al. [59] achieved an F1-score of 92.89%, indicating reasonably good effectiveness, but may face limitations in dealing with

complex forgery tools. Rathore et al. [60] only achieved 92.24% accuracy, revealing difficulties sustaining performance under extensive transformation. Ahmed et al. The F1-score of 95.9% for [61] seems to have better feature extraction capabilities. Tinnathi and Sudhavani [62] achieved 93.56%, representing an appropriate trade-off between efficiency and robustness. Niu et al. [63] had a 94.54% score, showing resistance to some types of forgeries but potential weaknesses in highly compressed/occluded images. Kunj and Vipin [64] obtained a comparatively greater F1-score (96.97%) but demonstrated effective computational complexity in identifying the manipulated areas.

On the lower end, Wang et al. The proposed methods [65] reported an F1-score of 82.16%, indicating issues with generalization between different forgery types. The limits of false positive reduction were shown, where Singh and Singh [66] reached only 86.81%. Diwan and Roy [67] achieved 98.56%, showing high localization accuracy but computational costs. The results showed that the proposed method outperformed all existing approaches with the highest F1-score of 99.1%. It underlies its robustness to transformations, ability to adapt to real-world conditions and efficiency in localization of tampered regions. The approach effectively overcomes the limitations of previous methods, especially in instances of intricate forgeries, noise, and geometric distortions. However, real-time performance and detecting very subtle forgeries could be improved further.

TABLE I. COMPARING THE EFFICIENCY OF DIFFERENT METHODS

Auth. Ref, Year	*Method*	*F1-Score*
Fu et al. [59], 2023	SURF, A-KAZE, and DBSCAN	92.89
Rathore et al. [60], 2020	BWT and SVD methods	92.24
Ahmed et al. [61], 2021	KS and SVD methods	95.9
Tinnathi and Sudhavani [62], 2021	AGSO / RANSAC	93.56
Niu et al. [63], 2021	SIFT / BFMI methods	94.54
Kunj and Vipin [64], 2020	FMT-SIFT methods	96.97
Wang et al. [65], 2024	Keypoint of CNN method	82.16
Singh and Singh [66], 2020	DCT and SVD methods	86.81
Diwan and Roy [67], 2024	Keypoint of CNN method	98.56
Our Study, 2025	Our Proposed SVD	99.1

V. CONCLUSION

This study proposed a new, robust methodology to detect copy-move forgery in digital images. We achieved competitive prediction accuracy using SVD feature extraction and SURF forgery localization. A significant property of the SVD is that it is tolerant to region rotation and scaling, i.e., when rotating or scaling the same region, about its centroid yields a nearly identical norm represented by the SVDs. Migration Detection by SVD: The key benefit of SVD in forgery recognition is that it identifies the touched areas using unique features taken from photographs. It resists common forgeries, decreases the dimensionality of data sets, and enables statistical analysis.

Furthermore, mathematics cannot get any better than that. When integrated with other methods, SVD improves detection accuracy and adapts easily to emerging forgery techniques. There are many other advantages of using SURF for copy-move forgery localization. However, the critical benefits like robust feature detection, invariant to scale/rotation invariance, and efficient computation make it most suited among others, which include distinctive features as well as maintain geometric verification consistency constraints that too depend on extent adaptability, although the particular threshold is needed, possible integration with series of techniques along update versions having closer real-world applicability can be a result for more research validations.

SURF helps in improving the precise identification of duplicate areas within images. Further research should follow in optimizing this algorithm for real-time processing, enhancing anti-advanced forgery pattern techniques, and including other feature extraction methods. Growing the datasets and testing against more diverse methods will be needed. In addition, developing user-friendly interfaces, robustness in diverse environmental conditions, and cross-domain applications could substantially widen its adoption and potential. These are the regions that, if addressed, will enable the proposed method to become a more complete and robust solution for copy-move forgery detection and other image integrity applications.

REFERENCES

[1] M. H. Farhan, K. Shaker, and S. Al-Janabi, "Copy–move forgery detection in digital image forensics: A survey," *Multimedia Tools and Applications*, pp. 1-33, 2024.

[2] M. H. Farhan, K. Shaker, and S. Al-Janabi, "Double Dual Convolutional Neural Network (D2CNN) for Copy-Move Forgery Detection," in *2023 15th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 439-444, 2023.

[3] C. Bhure, G. S. Nicholas, S. Ghosh, N. Asadi, and F. Saqib, "AutoDetect: Novel Autoencoding Architecture for Counterfeit IC Detection," *Journal of Hardware and Systems Security*, pp. 1-20, 2024.

[4] S. K. Narasimhamurthy, V. K. Mahadevachar, and R. K. T. Narasimhamurthy, "A Copy-Move Image Forgery Detection Using Modified SURF Features and AKAZE Detector," *International Journal of Intelligent Engineering & Systems*, vol. 16, no. 4, 2023.

[5] J. E. Kennedy, "Addressing researcher fraud: retrospective, real-time, and preventive strategies–including legal points and data management that prevents fraud," *Frontiers in Research Metrics and Analytics*, vol. 9, p. 1397649, 2024.

[6] A. Islam, C. Long, A. Basharat, and A. Hoogs, "Doa-gan: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pp. 4676-4685, 2020.

[7] M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, and Z. Habib, "Spatial Video Forgery Detection and Localization using Texture Analysis of Consecutive Frames," *Advances in Electrical & Computer Engineering*, vol. 19, no. 3, 2019.

[8] R. G. Mani, R. Parthasarathy, S. Eswaran, and P. Honnavalli, "A Survey on Digital Image Forensics: Metadata and Image forgeries," in *Workshop on Applied Computing, January 27-28, 22*, 2022, vol. 55, pp. 22-55.

[9] Z. N. Khudhair, F. Mohamed, and K. A. Kadhim, "A review on copy-move image forgery detection techniques," in *Journal of Physics: Conference Series*, vol. 1892, no. 1, p. 012010, 2021.

[10] A. S. Al-Qazzaz, P. Salehpour, and H. S. Aghdasi, "Robust DeepFake Face Detection Leveraging Xception Model and Novel Snake Optimization Technique," *Journal of Robotics and Control (JRC)*, vol. 5, no. 5, pp. 1444-1456, 2024.

[11] M. Qadir, S. Tehsin, and S. Kausar, "Detection of Copy Move Forgery in Medical Images Using Deep Learning," in *2021 International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)*, pp. 1-6, 2021.

[12] Z. N. Khudhair, F. Mohamed, A. Rehman, and T. Saba, "Detection of Copy-Move Forgery in Digital Images Using Singular Value Decomposition," *Computers, Materials & Continua*, vol. 74, no. 2, 2023.

[13] Y. Wu, W. Abd-Almageed, and P. Natarajan, "Image copy-move forgery detection via an end-to-end deep neural network," in *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 1907-1915, 2018.

[14] K. K. Thyagharajan and G. Kalaiarasi, "Pulse coupled neural network based near-duplicate detection of images (PCNN–NDD)," *Advances in Electrical and Computer Engineering*, vol. 18, no. 3, pp. 87-96, 2018.

[15] P. Deb, S. Deb, A. Das, and N. Kar, "Image Forgery Detection Techniques: Latest Trends And Key Challenges," *IEEE Access*, vol. 12, pp. 169452-169466, 2024.

[16] X.-y. Wang, C. Wang, L. Wang, H.-y. Yang, and P.-p. Niu, "Robust and effective multiple copy-move forgeries detection and localization," *Pattern Analysis and Applications*, vol. 24, pp. 1025-1046, 2021.

[17] S. U. Qureshi *et al.*, "Systematic review of deep learning solutions for malware detection and forensic analysis in IoT," *Journal of King Saud University-Computer and Information Sciences*, p. 102164, 2024.

[18] A. Ghai, P. Kumar, and S. Gupta, "A deep-learning-based image forgery detection framework for controlling the spread of misinformation," *Information Technology & People*, vol. 37, no. 2, pp. 966-997, 2024.

[19] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," *Australian Journal of Forensic Sciences*, vol. 49, no. 3, pp. 281-307, 2017.

[20] K. Asghar, M. Saddique, M. Hussain, G. Bebis, and Z. Habib, "Image Forgery Detection Using Noise and Edge Weighted Local Texture Features," *Advances in Electrical and Computer Engineering*, vol. 22, no. 1, pp. 57-68, 2022.

[21] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, vol. 178, p. 114361, 2024.

[22] C. B. Rabah. *Analysis of scanned documents for integrity and authenticity checking*. (Doctoral dissertation, Ecole nationale supérieure Mines-Télécom Atlantique; École supérieure des communications de Tunis (Tunisie)), 2021.

[23] P. Aberna and L. Agilandeeswari, "Digital image and video watermarking: methodologies, attacks, applications, and future directions," *Multimedia Tools and Applications*, vol. 83, no. 2, pp. 5531-5591, 2024.

[24] S. Mukherjee and A. K. Pal, "A hybrid SWT-SVD based multiresolution features for robust image copy-move forgery detection," *Multimedia Tools and Applications*, vol. 83, no. 16, pp. 48141-48163, 2024.

[25] P. M. Raju and M. S. Nair, "Copy-move forgery detection using binary discriminant features," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 2, pp. 165-178, 2022.

[26] X.-y. Wang, X.-q. Wang, P.-p. Niu, and H.-y. Yang, "Accurate and robust image copy-move forgery detection using adaptive keypoints and FQGPCET-GLCM feature," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 2203-2235, 2024.

[27] N. Kaur, N. Jindal, and K. Singh, "A deep learning framework for copy-move forgery detection in digital images," *Multimedia Tools and Applications*, vol. 82, no. 12, pp. 17741-17768, 2023.

[28] S. Kumar, S. Mukherjee, and A. K. Pal, "An improved reduced feature-based copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 82, no. 1, pp. 1431-1456, 2023.

[29] D. P. Timothy and A. K. Santra, "Detecting Digital Image Forgeries with Copy-Move and Splicing Image Analysis using Deep Learning Techniques," *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 5, 2024.

[30] A. Diwan, R. Mahadeva, and V. Gupta, "Advancing Copy-Move Manipulation Detection in Complex Image Scenarios Through Multiscale Detector," *IEEE Access*, vol. 12, pp. 64736-64753, 2024.

[31] A. Yadav, J. Goyal, and M. Ahmed, "Robust block-based watermarking algorithm with parallelization using multi-level discrete wavelet transformation," *Journal of Real-Time Image Processing*, vol. 21, no. 6, p. 182, 2024.

[32] S. A. Hosseini and P. Farahmand, "An attack resistant hybrid blind image watermarking scheme based on combination of DWT, DCT and PCA," *Multimedia Tools and Applications*, vol. 83, no. 7, pp. 18829-18852, 2024.

[33] D. Pennati and L. Bocchi, "Analysis of the Relationship Between Scale Invariant Feature Transform Keypoint Properties and Their Invariance to Geometrical Transformation Applied to Cone-Beam Computed Tomography Images," *Bioengineering*, vol. 11, no. 12, p. 1236, 2024.

[34] U. Diaa, "A Deep Learning Model to Inspect Image Forgery on SURF Keypoints of SLIC Segmented Regions," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12549-12555, 2024.

[35] M. M. Eltoukhy, F. S. Alsubaei, A. M. Mortda, and K. M. Hosny, "An efficient convolution neural network method for copy-move video forgery detection," *Alexandria Engineering Journal*, vol. 110, pp. 429-437, 2025.

[36] Z. Ullah, L. Qi, E. Pires, A. Reis, and R. R. Nunes, "A Systematic Review of Computer Vision Techniques for Quality Control in End-of-Line Visual Inspection of Antenna Parts," *Computers, Materials & Continua*, vol. 80, no. 2, 2024.

[37] F. Usman, C. Shi, and Y. Wang, "DRL-SLAM: Enhanced Object Detection Fusion with Improved YOLOv8," in *International Conference on Intelligence Science*, pp. 257-272, 2024.

[38] M. Verma and D. Singh, "Survey on image copy-move forgery detection," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 23761-23797, 2024.

[39] M. F. Ab Jabal, A. N. H. Abdullah, F. H. Najjar, S. Hamid, A. K. Khalid, and W. D. W. A. Manan, "A Novel Color Feature for the Improvement of Pigment Spot Extraction in Iris Images," *Journal of Image and Graphics*, vol. 12, no. 4, 2024.

[40] U. Samariya, S. D. Kamble, S. Singh, and R. K. Sonker, "A survey on copy-move image forgery detection based on deep-learning techniques," *Multimedia Tools and Applications*, pp. 1-60, 2024.

[41] A. Bilal *et al.*, "Improved Support Vector Machine based on CNN-SVD for vision-threatening diabetic retinopathy detection and classification," *Plos one*, vol. 19, no. 1, p. e0295951, 2024.

[42] A. Pyrkov, A. Aliper, D. Bezrukov, D. Podolskiy, F. Ren, and A. Zhavoronkov, "Complexity of life sciences in quantum and AI era," *Wiley Interdisciplinary Reviews: Computational Molecular Science*, vol. 14, no. 1, p. e1701, 2024.

[43] Z. N. Khudhair *et al.*, "Color to Grayscale Image Conversion Based on Singular Value Decomposition," *IEEE Access*, vol. 11, pp. 54629-54638, 2023.

[44] F. A. Khattak, I. K. Proudler, and S. Weiss, "Scalable analytic eigenvalue extraction algorithm," *IEEE Access*, vol. 12, pp. 166652-166659, 2024.

[45] N. K. El Abbadi, A. Al Rammahi, D. S. Redha, and M. AbdulHameed, "Image Compression based on SVD and MPQ-BTC," *J. Comput. Sci.*, vol. 10, no. 10, pp. 2095-2104, 2014.

[46] N. K. El Abbadi and E. J. Al Taee, "An Efficient Storage Format for Large Sparse Matrices based on Quadtree," *International Journal of Computer Applications*, vol. 105, no. 13, 2014.

[47] N. K. El Abbadi, A. Mohamad, and M. Abdul-Hameed, "Image encryption based on singular value decomposition," *Journal of Computer Science*, vol. 10, no. 7, p. 1222, 2014.

[48] A. Abdi, J.-P. Berrut, and S. Hosseini, "Explicit methods based on barycentric rational interpolants for solving non-stiff Volterra integral equations," *Applied Numerical Mathematics*, vol. 174, pp. 127-141, 2022.

[49] D. Kumar, R. C. Pandey, and A. K. Mishra, "A review of image features extraction techniques and their applications in image forensic," *Multimedia Tools and Applications*, pp. 1-102, 2024.

[50] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Computer Vision–ECCV 2006: 9th European Conference on Computer Vision, Graz, Austria, May 7-13, 2006. Proceedings, Part I 9*, pp. 404-417, 2006.

[51] A. Kumar, "SURF feature descriptor for image analysis," *Imaging and Radiation Research*, vol. 6, no. 1, p. 5643, 2024.

[52] N. K. EL Abbadi, S. A. Al Hassani, and A. H. Abdulkhaleq, "Panoramic Image Stitching Techniques Based on SURF and Singular Value Decomposition," in *International Conference on New Trends in Information and Communications Technology Applications*, pp. 63-86, 2021.

[53] J. Dong, W. Wang, and T. Tan, "Casia image tampering detection evaluation database," in *2013 IEEE China summit and international conference on signal and information processing*, pp. 422-426, 2013.

[54] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD—New database for copy-move forgery detection," in *Proceedings ELMAR-2013*, pp. 49-54, 2013.

[55] F. H. Najjar, N. B. Hassan, and S. Abd Kadum, "Hybrid Deep Learning Model for Hippocampal Localization in Alzheimer's Diagnosis Using U-Net and VGG16," *International Journal of Robotics and Control Systems*, vol. 5, no. 2, pp. 730-747, 2025.

[56] S. M. Saadi and W. Al-Jawher, "Ensemble Learning with optimum Feature Selection for Tweet Fake News Detection using the Dragonfly approach," in *2023 16th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 575-580, 2023.

[57] N. I. Ali, A. H. Soomro, S. Soomro, and A. G. Memon, "RSS Feeds Filtering from Multiple Sources Using Automated Techniques of Natural Language Processing," *The Asian Bulletin of Big Data Management*, vol. 4, no. 1, p. 250, 2024.

[58] F. H. Najjar, S. Abd Kadum, and N. B. Hassan, "Integrating Multi-scale Feature Extraction into EfficientNet for Acute Lymphoblastic Leukemia Classification," *Journal of Image and Graphics*, vol. 13, no. 1, pp. 83-89, 2025, doi: 10.18178/joig.13.1.83-89.

[59] G. Fu, Y. Zhang, and Y. Wang, "Image Copy-Move Forgery Detection Based on Fused Features and Density Clustering," *Applied Sciences*, vol. 13, no. 13, p. 7528, 2023.

[60] N. K. Rathore, N. K. Jain, P. K. Shukla, U. Rawat, and R. Dubey, "Image forgery detection using singular value decomposition with some attacks," *National Academy Science Letters*, vol. 44, pp. 331-338, 2021.

[61] B. Ahmed, T. A. Gulliver, and S. alZahir, "Blind copy-move forgery detection using SVD and KS test," *SN Applied Sciences*, vol. 2, no. 8, p. 1377, 2020.

[62] S. Tinnathi and G. Sudhavani, "An efficient copy move forgery detection using adaptive watershed segmentation with AGSO and hybrid feature extraction," *Journal of Visual Communication and Image Representation*, vol. 74, p. 102966, 2021.

[63] P.-p. Niu, C. Wang, W. Chen, H. Yang, and X. Wang, "Fast and effective Keypoint-based image copy-move forgery detection using complex-valued moment invariants," *Journal of Visual Communication and Image Representation*, vol. 77, p. 103068, 2021.

[64] K. B. Meena and V. Tyagi, "A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 8197-8212, 2020.

[65] J. Wang *et al.*, "Object-level Copy-Move Forgery Image Detection based on Inconsistency Mining," in *Companion Proceedings of the ACM on Web Conference 2024*, 2024, pp. 943-946.

[66] Priyanka, G. Singh, and K. Singh, "An improved block based copy-move forgery detection technique," *Multimedia Tools and Applications*, vol. 79, pp. 13011-13035, 2020.

[67] A. Diwan and A. K. Roy, "CNN-Keypoint Based Two-Stage Hybrid Approach for Copy-Move Forgery Detection," *IEEE Access*, vol. 12, pp. 43809-43826, 2024.