International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

Digital Image Forgery Detection Using SURF and ORB Technique

Jyoti Yadav, Nilima Dongre

Submitted: 24/11/2023 **Revised**: 28/12/2023 **Accepted**: 07/01/2024

Abstract: Copy-move forgery involves duplicating part of an original image and pasting it elsewhere within the same image to disguise manipulations. Detecting such forgeries is crucial for verifying image authenticity. This research explores keypoint-based approaches for copy-move detection, specifically SURF and ORB. SURF (Speeded Up Robust Features) identifies interest points using the Hessian matrix and describes them with Haar wavelet responses. ORB (Oriented FAST and Rotated BRIEF) uses FAST keypoint detection and binary BRIEF description for efficiency. After extracting SURF and ORB features, SVM and EM classifiers categorize images as forged or genuine. Performance is evaluated using accuracy, precision, recall and F1 score. Results demonstrate ORB+SVM and ORB+EM outperform SURF+EM on all metrics. This highlights ORB's advantages over SURF for copy-move detection when paired with SVM or EM. ORB provides faster feature extraction and description leading to better classification. In conclusion, keypoint methods like ORB show promise for copy-move forgery detection. ORB's efficiency and discriminative power, combined with SVM or EM classification, can effectively identify image manipulations. This research provides valuable insights into optimal feature extraction and machine learning techniques for enhanced forgery detection.

Keywords: *Copy move forgery, Block based, SURF algorithm, ORB algorithm, SVM and EM algorithm*.

1. Introduction

Digital images are becoming increasingly important in many applications, but the ease of photo editing software has also enabled damaging image manipulations. Motivations for image tampering include hiding or adding information, enhancing quality, and creating composites from multiple images. While these manipulations may seem minor, any type of forgery can be deceptive.The ability to seamlessly alter digital images raises major security concerns, as manipulations are typically imperceptible. Many forensic methods now exist to assess image integrity and detect tampering like splicing, which covertly changes or removes key elements.

There are three main categories of digital image forgery, detectable through image content analysis:

- Copy-Move: In copy-move forgery, part of the original image is copied and pasted to a new location within the same image, creating a manipulated result.
- Image Splicing: Image splicing involves rearranging and combining multiple images to construct a new fabricated image.
- Image Retouching: Image retouching is a more subtle technique that enhances aspects of an image while preserving the original look of the subject. It is less intrusive than other forgery methods.

As a consequence of these sophisticated manipulation techniques, the need for reliable methods to detect and verify the authenticity of digital images has become crucial.

1.1 Problem Definition

Both the traditional block-based approach and keypoint-based approach have certain limitations, as outlined below:

- In copy-move forgery detection, existing algorithms can only identify the largest copied region in tampered images containing multiple copied areas, leaving smaller copied regions undetected.
- Most algorithms fail to detect small copied regions, leading to potential oversight of crucial tampering.

Ramrao Adik Institute of Technology,

D.Y. Patil Vidyapeeth,

Nerul, Navi Mumbai

jyotee_yadav@yahoo.in, nilima.dongre@rait.ac.in

● Current algorithms can only identify duplicate regions larger than the block size. If the duplicated area is smaller, the algorithm fails to detect the forgery.

● There is presently no algorithm capable of detecting multiple copied regions pasted in various areas of the same image, complicating identification of sophisticated forgeries.

In light of the shortcomings observed in existing systems, our proposed approach aims to address these challenges. The design of our proposed system is carefully crafted to effectively tackle these limitations. The problem definition for our proposed system includes the following objectives:

● To develop a system that can effectively handle tampered images with multiple copied regions, not limited to just the largest regions.

● To create a system that can successfully detect forgeries where the duplicate region may be smaller than the block size.

● To design a system capable of detecting multiple copied regions skillfully pasted into different areas of the same image, enhancing detection of sophisticated forgeries.

2.Related information

The primary goal of this research paper is to detect copy-move type image forgeries, which are relevant in various applications like criminal evidence systems or portraying crowded scenes using sparse populations. The authors propose a novel method that surpasses previous approaches in efficiency and reliability [5].

The paper introduces an image matching algorithm called L-SURF, building on SURF and ORB algorithms. The process involves image enhancement via the Laplacian operator, feature point detection through SURF, rotation-invariant binary feature description using ORB, and precise feature matching using Hamming distance and Lowe's approach. Experiments show L-SURF's remarkable ability to address issues like brightness sensitivity and lack of scale invariance in ORB, leading to significant improvements in matching accuracy [6].

Furthermore, the paper explores specific forgery detection techniques for copy-move and splicing. The authors employ match points after SIFT and SURF feature extraction. For splicing detection, they extract edges from YCbCr components' integral images, apply GLCM, and form feature vectors fed to an SVM classifier. Results indicate faked parts are distinctly visible when plotting parameters are 4 or 5 [7].

Another contribution is a forgery detection technique using illuminant color. The improved method leverages ML classifiers with feature extraction techniques (HOG, GLCM, SIFT). Classifiers identify attributes and determine image authenticity. By removing image texture and gradient attributes, the classifier is effectively trained [8].

Additionally, the paper presents techniques for detecting contrast enhancement and copy-paste forgery. Contrast enhancement detection relies on contrast calculation and is robust to JPEG compression. For copy-paste detection, a DCT-based feature extraction method efficiently detects small, medium, and large forged regions. The proposed contrast enhancement algorithm proves robust against post-processing, overcoming limitations of previous approaches [9].

A. COPY MOVE FORGERY DETECTION

Here is a brief overview of digital image forgery detection technology:

Digital image forgery detection techniques can be classified into two main categories - active and passive:

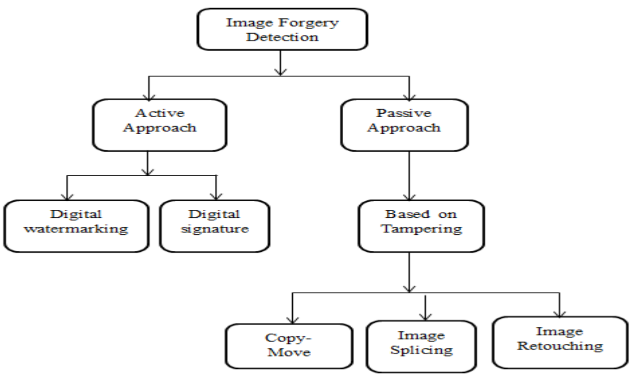

Fig.1 Taxonomy of Image forgery detection technique.

Active Techniques

Digital Watermarking:

Watermarking proactively embeds verification data within the image itself. A watermark signal is created by the source and encoded into the image through subtle modifications to the pixels. This produces a watermarked image that contains the hidden verification data. Later, the recipient analyzes the image to extract and verify the watermark. If the extracted watermark does not match the original, it indicates the image has been tampered with. The watermark is designed to be spread throughout the image in a way that makes complete removal difficult. Although some image degradation may occur, the watermark allows for at least partial recovery of the original image contents. Overall, watermarking enables tamper detection through embedded verification data.

Digital Signatures:

Signatures work by extracting unique innate features of the pristine image that can function as a fingerprint. The signature is generated by applying a hash function or message digest algorithm to properties of the original image, like its color histogram. During verification, this signature generation process is repeated on the image being authenticated. By comparing the new signature to the original, the image can be verified. Matching signatures provide a compact way to authenticate images without embedding any data.

Passive Techniques

Image Splicing Detection:

Splicing creates composite forgeries by copying content from multiple images and pasting together. Sometimes, these manipulations can be identified through visible irregularities between spliced regions. This includes differences in lighting, noise patterns, edge sharpness, camera characteristics, compression artifacts, etc. Passive splicing detection analyzes these inherent image properties to reveal inconsistencies indicative of tampering. No watermarks or signatures are used, just the image itself.

Block-based Methods:

Here, the image is divided into overlapping blocks which are each analyzed for anomalies. The blocks are often converted to an alternate domain like DCT or DWT using frequency transforms. By analyzing the frequency coefficients, quantization artifacts, noise residues, etc., tampered blocks can be identified. Block-based methods allow precise localization of manipulated regions within the image. They are robust against compression and noise addition.

Keypoint Methods:

Interest points known as keypoints are extracted to represent salient image regions. Keypoint detectors like SIFT, SURF, and ORB identify these keypoints. Feature descriptors are then created for each keypoint based on the surrounding pixel patterns. Matching descriptors reveals duplicated regions from copy-move forgeries, even if operations like scaling or rotation were applied. Keypoints provide robustness to common transformations.

3.Proposed Methodology

The proposed technique utilizes a dataset of high-resolution images containing realistic copy-move forgeries. Using a standardized dataset enables comparative benchmarking of results. The key steps are feature extraction, classification, and performance evaluation. For feature extraction, interest points known as keypoints are identified in the images along with descriptive feature vectors using two methods - SURF and ORB. SURF (Speeded Up Robust Features) relies on the Hessian matrix to detect keypoints at locations with large determinant of Hessian values. The descriptors are generated using Haar wavelet responses within the keypoint neighborhood, providing robustness to image transformations. ORB (Oriented FAST and Rotated BRIEF) offers an efficient alternative to SURF, using FAST keypoint detection and adding an orientation component based on intensity centroids. The descriptors are computed using the BRIEF (Binary Robust Independent Elementary Features) algorithm on image patches rotated according to the keypoint orientation. This makes ORB features invariant to rotation. After extracting SURF and ORB feature vectors, machine learning algorithms categorize them as belonging to forged or genuine image regions. The classifiers used are Support Vector Machines (SVMs) and Expectation-Maximization (EM). SVMs find optimal decision boundaries for classification while EM handles latent variables and estimates model parameters via maximum likelihood. Finally, the accuracy, precision, recall, and F1-score are computed to quantify the performance of each combination of feature extractor and classifier. Comparative evaluation determines the optimal techniques for copy-move forgery detection on this dataset.

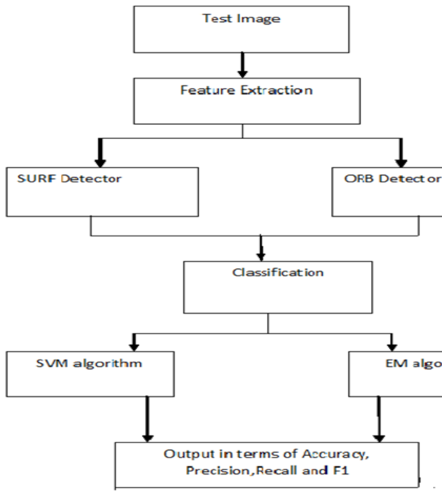

Fig.2 Flow diagram of the proposed methodology

1. Integral Images for Efficient Summation: The concept of integral images, also known as summed area tables (SAT), was introduced by Viola and Jones. An integral image allows fast computation of the sum of pixel values within a rectangle in the original image. The value at point (x,y) in the integral image represents the sum of pixels within the rectangle from the origin to (x,y).

2. Hessian Matrix for Interest Point Detection: SURF utilizes the Hessian matrix for its superior performance in identifying interest points like blobs and corners. Interest points are located where the determinant of the Hessian matrix is maximized. For an image point (x,y) at scale σ, the Hessian matrix H(x,σ) is defined.

3. Description of Interest Points: SURF constructs a scale space pyramid with Gaussian filters instead of image reduction. Extrema of the determinant values in the pyramid are found by comparing a point to its 26 neighbors, identifying interest points and scales. A square region around each point is divided into 4x4 sub-regions. The Haar wavelet response along x and y directions is calculated. These responses are weighted by the interest point values using a Gaussian, forming the description.

4. In summary, integral images allow efficient summation, the Hessian matrix detects robust interest points, and the wavelet responses describe the neighborhood around each interest point. Together these methods enable the SURF algorithm to reliably identify and describe key image features.

ORB uses FAST for keypoint detection and BRIEF for descriptor extraction.

The FAST algorithm is able to quickly detect interest points or corners in an image by examining the intensity values of pixels in a neighborhood around each candidate point. The key steps of the FAST corner detection process are:

1. Select a pixel p in the image to test whether it is a corner. Let Ip be the intensity of this pixel.

2. Choose a threshold value t for brightness comparison against the surrounding pixels. This threshold determines how much brighter or darker the surrounding pixels need to be compared to p in order to indicate a corner.

3. Consider a circular ring of 16 pixels around the candidate pixel p. This ring defines the neighborhood region to examine.

4. Check if there is a contiguous set or arc of n pixels (e.g. n=12) in the ring that are all significantly brighter than Ip+t or significantly darker than Ip-t.

5. If such a set exists, then p is marked as a potential corner since there is a high contrast arc-shaped area passing through its neighborhood.

6. To speed up the detection, perform an initial test on just 4 pixels in the ring at locations 1, 9, 5 and 13. If p fails this initial test, it cannot be a corner.

7. Candidate pixels passing the first test are further analyzed by checking all 16 pixels in the full ring to confirm the presence of a high contrast arc.

8. Final corners are output once all candidate pixels in the image have been examined.

By using this two stage test process, FAST is able to rapidly discard non-corners and only apply the full arc test to potential corner points. This acceleration makes FAST quick and efficient for finding distinct corners in images. This accelerated segment test approach efficiently filters corners. Only candidates passing the initial four-pixel test undergo the full segment test. This FAST keypoint detection localizes interest points rapidly. ORB leverages FAST's accelerated corner detection to quickly identify keypoints. BRIEF then provides a binary descriptor for each keypoint for matching. Together, they comprise an efficient feature detection and description method.

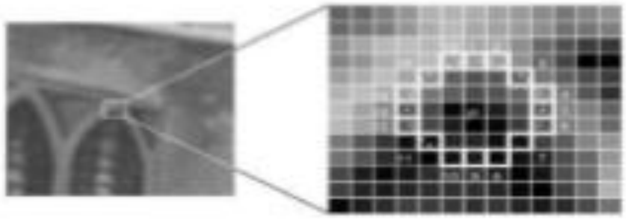

Fig.3 FAST Corner Detector

A. **BRIEF:** The BRIEF descriptor is in the form of a bit string that represents a description of an image patch p constructed from a set of binary intensity tests. Consider a smoothed image patch p, a binary test τ is defined by:

$$\tau(p; x, y) = \begin{cases} 1 : p(x) > p(y) \\ 0 : \ p(x) \leq p(y)1) \end{cases} \qquad (1)$$

where p(x) is the intensity of p at point x. A feature is defined as a vector of n binary tests.

3A. SVM (Support Vector Machine): Support vector machines (SVMs) offer a powerful supervised machine learning approach for tackling both classification and regression predictive modeling problems. By nonlinearly mapping input data into a high-dimensional feature space, SVMs can convert complex nonlinear relationships between attributes and targets into simpler linear ones. This allows them to construct optimal separating hyperplanes between classes in the transformed space. SVMs achieve this nonlinear mapping through the use of mathematical functions called kernels. Instead of needing to compute the full high-dimensional coordinate representation, kernels allow efficient computation of inner products between mapped data points. Common kernel functions include polynomials and radial basis functions.

A key advantage of the kernel-based approach is that SVMs can learn complex nonlinear decision boundaries in the original input space by finding a linear boundary in the high-dimensional kernel-induced feature space. This principled technique of embedding data into a higher-dimensional space and constructing linear models can handle inherently nonlinear classification and regression tasks. As a result, SVMs demonstrate excellent generalization performance across many problem domains, from computer vision and natural language processing to bioinformatics and earthquake prediction.

For copy-move image forgery detection, SVMs can leverage their nonlinear modeling capabilities to accurately discern forged from authentic image regions based on metadata, noise patterns, and other extracted features. The rich feature representation achieved through kernels helps SVMs construct optimal nonlinear decision boundaries even for difficult cases where classes are not straightforwardly linearly separable in the original feature space. This allows SVMs to effectively handle the complexity of copy-move forgery detection.

3B. EM Algorithm: The EM (Expectation-Maximization) algorithm offers an elegant iterative approach to finding locally optimal maximum likelihood estimates of parameters in probabilistic models containing latent variables or missing data. It alternates between an expectation (E) step and a maximization (M) step.

In the E-step, the expected value of the log-likelihood function is computed given the current parameter estimates, incorporating expected values for any latent variables based on the observed data. This handles missing data by taking the expectation over the latent variable distribution.

The M-step then maximizes this expected log-likelihood to find improved parameter estimates. Numerical optimization techniques are employed to maximize the log-likelihood function's expected value with respect to the parameters.

These two steps are repeated in an iterative fashion, with each iteration guaranteed to increase the log-likelihood. The algorithm converges when the log-likelihood improvement falls below a specified threshold.

A key advantage of EM is its conceptual simplicity and ease of implementation. By iteratively taking the expectation of latent variables and maximizing expected log-likelihood, it provides a straightforward mechanism for handling missing data problems.

However, the algorithm is guaranteed to converge only to a local rather than global maximum. It also exhibits slower convergence than methods like gradient descent. Multiple random restarts can improve the chances of finding a better optimum.

4.Experimental results

Results and Analysis of Feature Extraction and Classification

This study utilized the MICC-F600 dataset of digital images as input for copy-move forgery detection. Two key feature extraction methods were applied on these images - SURF and ORB:

SURF (Speeded Up Robust Features) detects interest points based on the Hessian matrix and describes them using Haar wavelet responses to characterize the neighborhood.

ORB (Oriented FAST and Rotated BRIEF) uses FAST corner detection to find keypoints and generates efficient binary descriptors with BRIEF.

After extracting features using SURF and ORB, two machine learning algorithms categorized the images as either forged or genuine:

SVM (Support Vector Machine) constructs optimal nonlinear decision boundaries for classification.

EM (Expectation-Maximization) handles latent variables to estimate model parameters and classify data.

The results obtained from combining these feature extractors and classifiers are analyzed in the following sections using key metrics - accuracy, precision, recall, and F1-score.

Comparative evaluations determine optimal combinations of feature detection and machine learning techniques for copy-move forgery identification. The experiments demonstrate the effectiveness of keypoint-based approaches, especially ORB, for accurately detecting image manipulations.

In summary, this study provides valuable insights into advanced feature extraction and classification methods for copy-move forgery detection in digital images. The analysis and results showcase promising techniques.

Fig.4 Input image or Original image

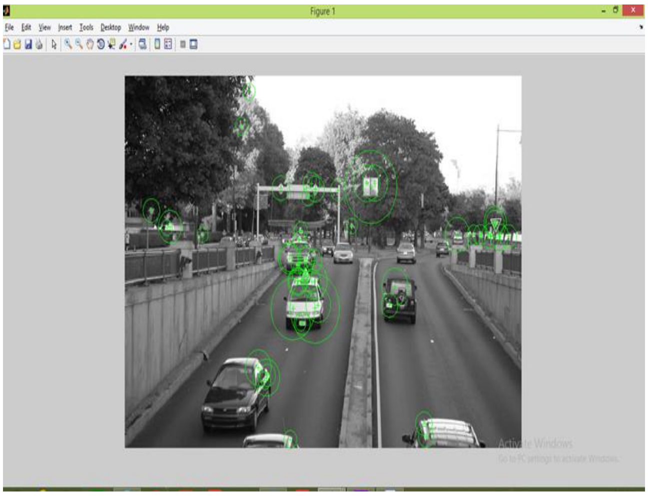

Fig.5 Key-point or Feature extraction of input image.

Fig.6 Forged Image

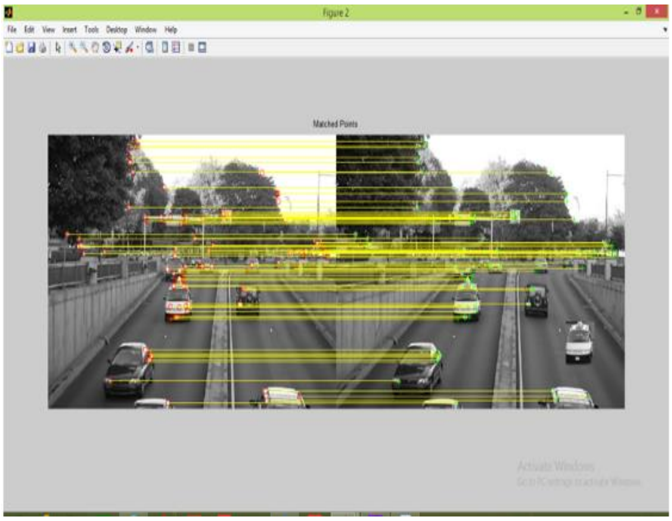

Fig.7 Copy-Move detection using SURF

Classification results in terms of precision, accuracy, recall, and F1 for test images or data sets using SVM RBF kernels and EM algorithms. Identified in the following table.

Table 1. Classification Result of feature extraction using SURF+SVM

F1	Recall	Precision	Accuracy	Input image	Method
81.0	82.2	81	90.6	Six hundred	SURF+SVM
79.04	79.23	79.16	89.4	Four fifty	SURF+SVM
72.76	72.77	72.13	80.0	Three hundred	SURF+SVM

Record ORB descriptor used for MICC-F600 feature extraction. The results of feature extraction using the ORB descriptor is as shown below.

Fig.8 Input image

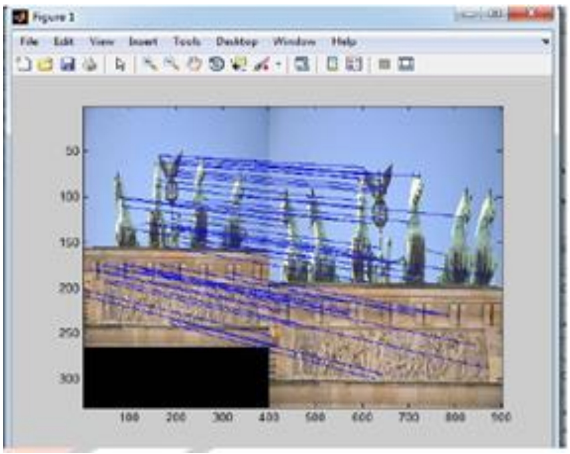

Fig.9 Input image and processed image

Figure 10 illustrates the performance of the ORB descriptor for copy-move forgery detection under rotations, scaling, and orientation changes. The first column shows the original image before manipulation. In the second column, the forged image has the plane region copied, rotated, scaled, and transformed to a different orientation. The third column displays the recognition results using ORB feature matching to detect the duplicated regions. Despite the rotations, scaling, and orientation changes, ORB is able to correctly identify the manipulated plane area in the forged image. This demonstrates ORB's robustness to common image transformations applied during copy-move forgeries. By extracting oriented and scale-invariant features, ORB can reliably match keypoints between the original and forged images to reveal duplicated content, even under affine distortions. The results highlight ORB's strengths for copy-move forgery detection, including efficient feature computation, robust keypoint orientation assignment, and binary string descriptions that are resilient to image manipulations. This makes ORB well-suited for identifying copy-move forgeries created through a variety of transformations.

Table 2: Accuracy, Precision, Recall and F1 for ORB descriptor with SVM and EM algorithm.

F1	Recall	Precision	Accuracy	Input image	Method
86.9	88.67	84.78	90.0	Six hundred	ORB+SVM
84.4	86.8	83.4	92	Four fifty	ORB+SVM
89.7	90.4	87.9	94	Three hundred	ORB+SVM
83.3	87	83.07	88	Six hundred	ORB+EM
81.22	84.9	82.4	88	Four fifty	ORB+EM
89.78	90.3	88.99	94.8	Three hundred	ORB+EM

4.1 COMPARISON BETWEEN SURF + SVM, ORB + SVM AND ORB + EM

Performance Evaluation and Comparison

The effectiveness of image forgery detection systems is evaluated using performance metrics including accuracy, precision, recall, and F1 score. Quantitative results for each metric are presented in Tables 1 and 2, and illustrated graphically.

The first graph shows a comparative analysis of accuracy achieved by the SURF+EM, ORB+SVM, and ORB+EM implementations. The x-axis plots accuracy percentage, while the y-axis lists the systems. SURF+EM attained approximately 91% accuracy, ORB+SVM around 89%, and ORB+EM about 92%.

This demonstrates ORB+EM performs slightly better than SURF+EM in terms of accuracy, and both outperform ORB+SVM. The visual graph compares accuracy across systems, an essential evaluation metric for image forgery systems.

Similarly, the other graphs provide visual comparisons of precision, recall, and F1 score for the different methods. Together, these quantitative results and graphical analyses evaluate the relative performance of the feature extraction and classification techniques based on key metrics. They highlight that ORB paired with EM achieves the best overall performance in detecting image forgeries on the dataset.

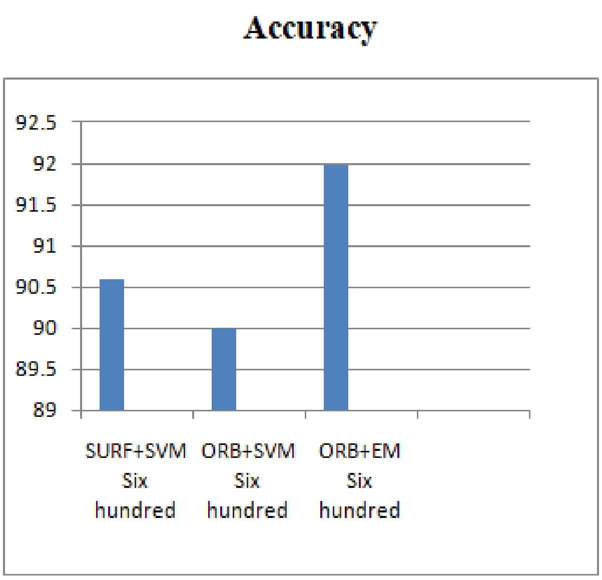

Fig.10 Comparative representation of Accuracy

Precision

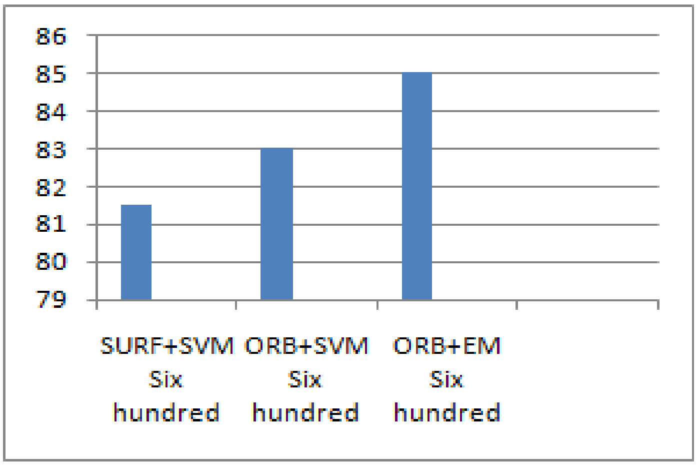

Fig.11 Comparative representation of Precision.

Recall

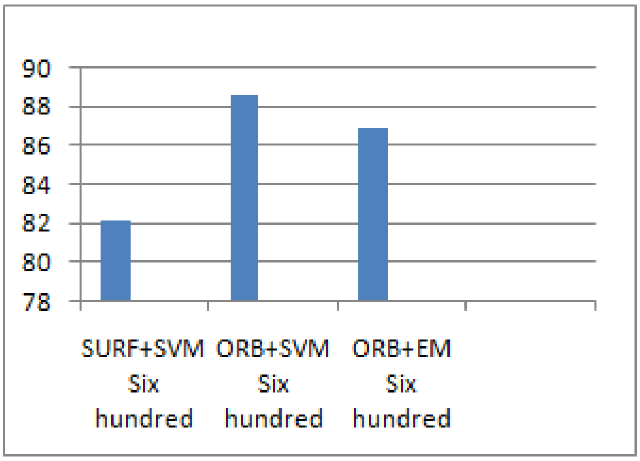

Fig.12 Comparative representation of Recall.

F1

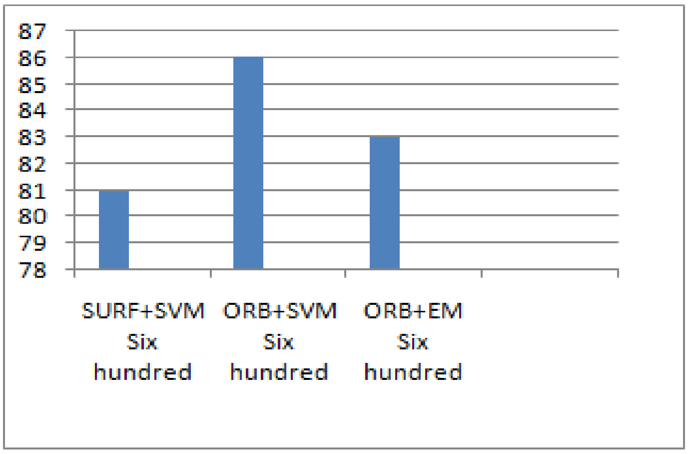

Fig.13 Comparative representation of F1.

Quantitative comparison of SURF+SVM, ORB+SVM, ORB+EM

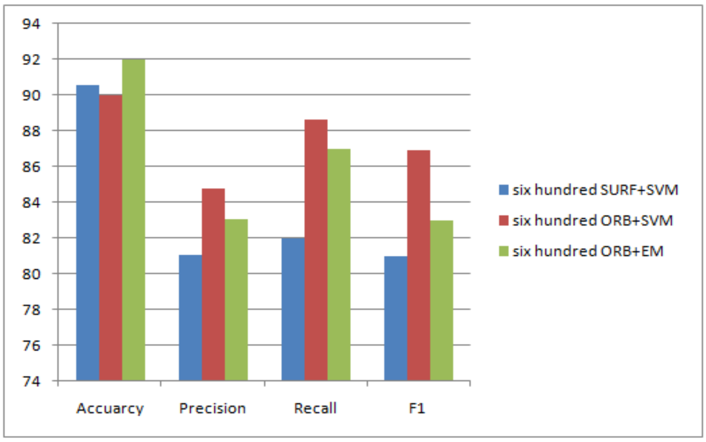

Fig.14 Comparison graphs of implemented techniques.

5.Conclusin

This work covers advanced digital image processing techniques that play critical roles in image forgery detection and feature extraction. Digital watermarking has emerged as an effective approach for embedding and verifying information in digital images. It involves creating a watermark and encoding it into the image to provide a means of checking authenticity and detecting manipulations. Block-based methods are powerful for identifying different forgery types like copy-move and splicing by dividing the image into blocks and analyzing forged areas. Keypoint-based methods like SURF detect interest points based on the Hessian matrix and Gaussian filters to reveal tampered regions.

Support Vector Machines (SVMs) enable effective image classification through linear and nonlinear decision boundaries to handle separable data. The Expectation-Maximization (EM) algorithm is essential for characterizing features from methods like ORB and SURF to evaluate performance accuracy. Our novel approach combines ORB with EM and SVM for copy-move forgery detection. Although SURF can identify keypoints, it is computationally expensive. ORB provides faster feature detection and description. Our experiments demonstrate ORB's superiority over SURF in accuracy, precision, recall, and F1 score. Thus, ORB is more efficient for detecting and describing salient points in copy-move forgery.

In summary, the advanced image processing and machine learning techniques discussed make valuable contributions to forgery detection and authentication. By enhancing the reliability of image verification, these methods ensure integrity across diverse applications like security, forensics, and content verification. The innovations in this field are critical for establishing authenticity in the digital age.

References

[1]. Haipeng Chen, Xiwen Yang, and Yingda Lyu "Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm." Digital Object Identifier 10.1109/ACCESS. 2020.297480 (2020).

[2]. Meena, K. B., and Tyagi, V. "A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-019-08343-0(2020).

[3]. Qiyue Lyu, Junwei Luo, Ke Liu, Xiaolin Yin, Jiarui Liu, Wei Lu," Copy Move Forgery Detection based on double matching", J. Vis. Commun. Image Represent. 76, 103057. doi:10.1016/j.jvcir. (2021).

[4]. Muzaffer, G., Ulutas, G., and Ustubioglu, B. "Copy Move Forgery Detection with Quadtree Decomposition Segmentation," in 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, July 7–9, 2020, 208–211. doi:10.1109/tsp49548.2020.9163516 (2020).

[5]. Tahaoglu, G., Uluas, G., and Ustubioglu, B. (2021). "A New Approach for Localization of Copy-Move Forgery in Digital Images," in 2021 44th International Conference on Telecommunications and Signal Processing (TSP), Brno, Czechia, July 26–28,

2021, 183–186. doi:10.1109/tsp52935.2021.9522680 (2021).

[6]. Shobhit Tyagi, Divakar Yadav “ForensicNet : Modern CNN-based Image Forgery Detection Network”, https://doi.org/10.21203/rs.3.rs-1802559/v1(2022).

[7]. Liang Xiu-jian and Sun He “Deep Learning Based Image Forgery Detection Methods” DOI: 10.32604/jcs.2022.032915 (2022). 31 Digital Image Forgery Detection Using SURF And ORB Technique

[8]. Kang Hyeon Rhee,” Generation of Novelty Ground Truth Image Using Image Classification and Semantic Segmentation for Copy-Move Forgery Detection”.Digital Object Identifier 10.1109/ACCESS.2021.3136781.(2021).

[9]. Khalid M. Hosny , Akram M. Mortda , Mostafa M. Fouda , And Nabil A. Lashin ” An Efficient CNN Model to Detect Copy-Move Image Forgery”, Digital Object Identifier 10.1109/ACCESS. 2022.3172273(2022).

[10]. Esteban Alejandro Armas Vega , Edgar Gonzalez Fernandez , Ana Lucila Sandoval Orozco , Luis Javier Garcia Villalba,” Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression”, Digital Object Identifier 10.1109/ACCESS.2020.2964516(2020).

[11]. Nhan Le and Florent Retraint,” A Statistical Modeling Framework for DCT Coefficients of Tampered JPEG Images and Forgery Localization”, Digital Object Identifier 10.1109/ACCESS. 2022.3188299 (2022).

[12]. Kalyani Kadam, Swati Ahirrao, Ketan Kotecha, And Sayan Sahu, “Detection and Localization of Multiple Image Splicing Using MobileNet V1”, Digital Object Identifier 10.1109/ACCESS. 2021.3130342.(2021)..

[13]. Anh-Thu Phan-Ho and Florent Retraint, “A Comparative Study of Bayesian and Dempster-Shafer Fusion on Image Forgery Detection”, Digital Object Identifier 10.1109/ACCESS.2022.3206543 (2022).

[14]. A-Rom Gu, Ju-Hyeon Nam And Sang-Chul Lee , “FBI-Net: Frequency-Based Image Forgery Localization via Multitask Learning With Self-Attention”, Digital Object Identifier 10.1109/ACCESS. 2022.3182024(2022).

[15]. Savita Walia , Krishan Kumar , Munish Kumar , And Xiao-Zhi Gao, And Sang-Chul Lee , “Fusion of Handcrafted and Deep Features for Forgery Detection in Digital Images”, Digital Object Identifier 10.1109/ACCESS.2021.3096240(2021)