IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

Real-Time Image Forgery Detection through Machine Learning

Waship W[1] and Dr. H. Jayamangala[2]

PG Student, Department of Computer Applications[1]

Assistant Professor, Department of Computer Applications[2]

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

22304258@vistas.ac.in and jayamangala.scs@velsuniv.ac.in

Abstract: *Digital Image Forgery can be done by deceiving the digital image to mask some meaningful or important data of the image. It is usually difficult to spot out the manipulated region of the original image. To sustain the uprightness and legitimacy of the image, the detection of forgery in the image is mandatory. Acclimation of the modern way of life and advancement in photography gadgetry has made exploitation of digital image easy with the help of image editing software. Therefore, it is crucial to detect such image forgery operations in the images. The image forgery detection can be done based on object removal, object addition, and unusual size modifications in the image. Images are one of the powerful media for communication. In our project we have used algorithms such as Copy Move Technique (CMT) as existing and Multi Support Vector Machine (MSVM) as proposed systems and both will be compared in terms of accuracy*

Keywords: Image Forgery, Digital image, CMT, MSVM

I. INTRODUCTION

Forgery is an illegal means of manipulating images or documents without prior access. Images are tampered for different reasons either to create false evidence or to earn money in an illegal way. A pictorial representation of an image conveys much better ideas than the words of a human. Due to the progression in digital technology, images are processed using several tools like Adobe Photoshop, GIMP and Corel Paint Shop and they ended up with a threat for the authenticity of digital images. Generally, image manipulations are of two types a) Allowed manipulation b) Malignant manipulation.

Allowed or incidental manipulations are the ones which never alters the semantic sense of information and are acceptable by any authentication system.

II. LITERATURE SURVEY

1. X. Zhang, Support Vector Machines, 01 2017, pp. 1214–1220.

Support vector machines use the kernel trick to perform linear classification while implicitly mapping inputs into feature spaces of high dimension. The main goal of the SVM is to help classify data in most of the statistical problems presented to machine learning experts. Understanding the correct position of data points on the hyper plane makes it possible to apply the SVM effectively. Support vector machines provide solutions to real problems in a wide range of applications. A main application is text and hypertext categorization, which reduces the requirement for labelled training in transductive and inductive settings. The classification of images is another major area employing SVMs. The SVM is believed to achieve the highest search accuracy compared to traditional query refinement techniques.

2. H.-J. Lin, C.-W. Wang and Y.-T. Kao, "Fast copy-move forgery detection", *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188-1975, 2009.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

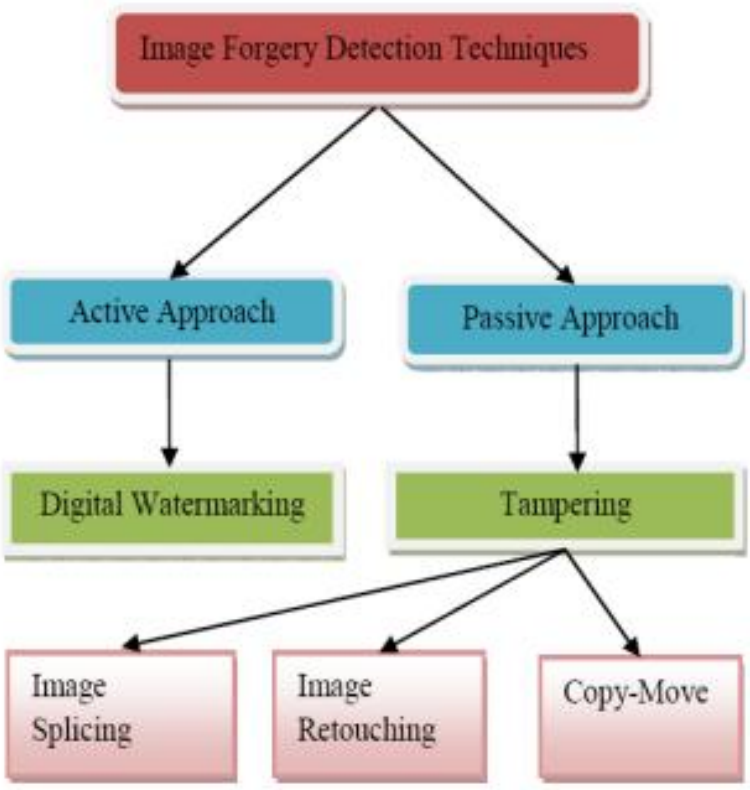
Copy-move forgery is the most common tamper which consists in copying one part of an image and then pasting in another part of the same image. Copy-move forgery detection (CMFD) is probably one of the most active research fields in blind image forensics. A large number of CMFD methods have been reported in the literature

3. K. B. Meena and V. Tyagi, "Image Splicing Forgery Detection Techniques: A Review," Springer Nature Switzerland AG 2021

DNNs can autonomously learn an extensive number of features. Over the past few years, a variety of image forgery detection methods have been proposed, for detecting image forgery, where many of which relied on deep learning

III. METHODOLOGY SECTION

To detect an ideal hyper plane for different distinct examples in a high dimensional space is the main process of the SVM. To fulfil this model there is more than one hyper plane. This process depends upon the bolster vector with the information that lies nearest on the closed surface and coordinating with the ideal choice surface. It performs classification by planning the input vectors into a high dimensional space and constructing the hyperplane to separate the data. This strategy is mainly used to solve a quadratic programming problem and non-convex, unconstrained minimization problem. The SVM is the most effective method in the classifier process.



MODULES:

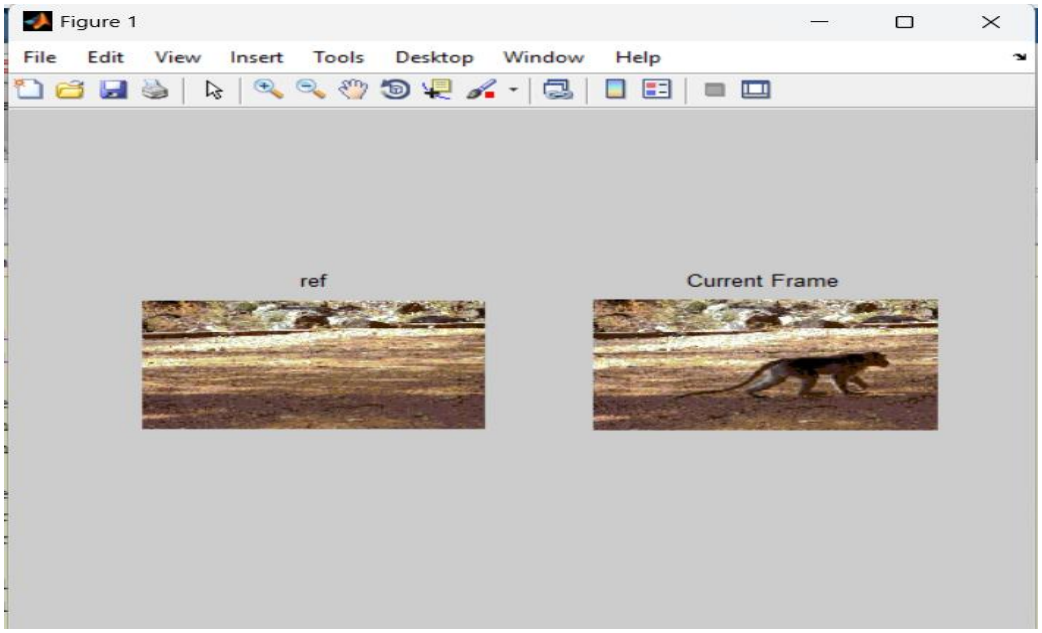
1) Face Detection Module:

This module is responsible for detecting human faces in real-time webcam feeds. It utilizes computer vision techniques and deep learning algorithms to identify faces accurately, regardless of their orientation or position in the frame.

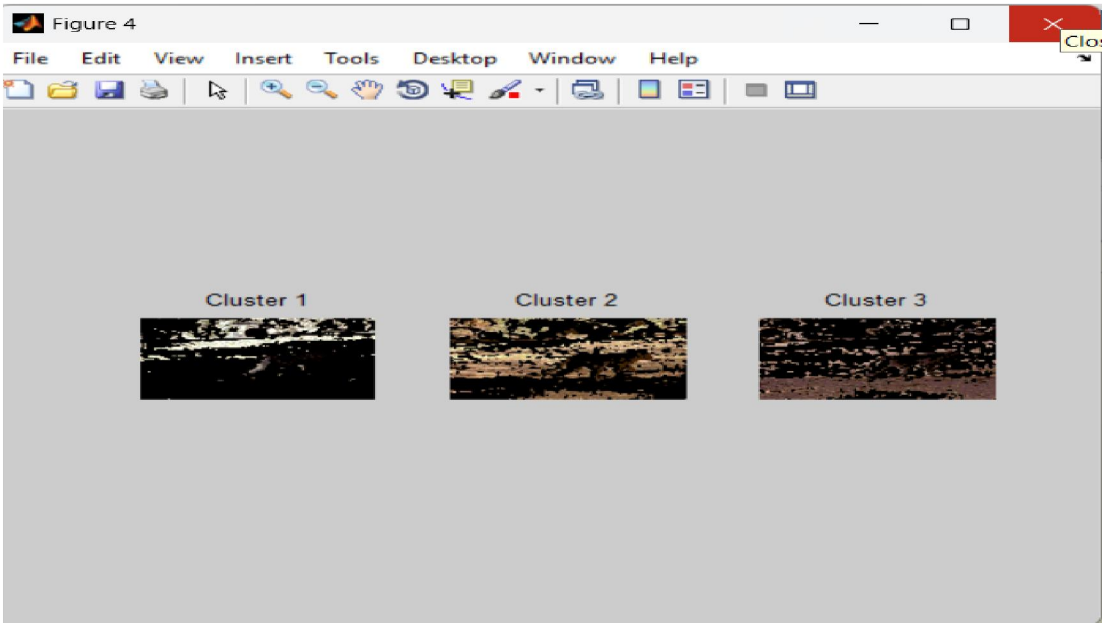
IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

2) Face Recognition Module:
Once the faces are detected, this module is responsible for recognizing and identifying individuals based on their facial features. It employs machine learning models, such as deep neural networks, to create unique face templates during the training phase. During live recognition, it matches the detected faces against these templates to identify individuals.
3) Data Preprocessing Module:
This module is involved in preprocessing the training data to ensure its quality and suitability for the face recognition algorithm. It may include tasks such as data augmentation, normalization, and cropping to improve the robustness and accuracy of the recognition process.
4) Training Module:
The training module is responsible for the initial setup of the system. It captures facial images of individuals, extracts facial features, and builds the face templates used for recognition. This process involves training machine learning models on the collected data to create a reliable and accurate face recognition model.
5) Web Interface Module:
The web interface module is built on Flask, a web framework in Python. It provides the user interface for administrators and users to interact with the system.
6) Attendance Recording Module:
This module handles the attendance recording process. When a user clicks on the "Take Attendance" button in the web interface, the system activates the face recognition module to identify individuals in the live webcam feed. Once recognized, it records their attendance in the database, along with the timestamp.
7) Database Module:
The database module is responsible for storing and managing attendance data, face templates, and other relevant information. It ensures data integrity, fast retrieval, and secure storage.

IV. SAMPLE SCREEN SHOTS



IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731



V. CONCLUSION

The proposed scheme for the detection of image forgery uses feature point extraction and morphological operation. It can divide the forged region by indicating the affected pixel. The algorithm used in the proposed experiment can achieve good performance under various challenging conditions such as geometrical transform and JPEG compression. Hence the system is providing an accurate and efficient result in detecting copy-move forgery without the help of any pre-existing data set for the forged image.

REFERENCES

[1]. A.C. Popscu, and H.Farid, "Statistical Tools for Digital Forensics" ,in Proc.The 6th international workshop on information hiding ,Toronto, Canada 2019.

[2]. Shivani Thakur, RamanpreetKaur, Dr. Raman Chadha,JasmeetKaur, "A Review Paper on Image Forgery Detection In Image Processing", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278- 0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2019), PP 86-89

[3]. DevanshiChauhan, DipaliKasat, SanjeevJain, VilasThakare, "Survery on KeyPoint based Copymove Forgery Detection Methods on Images", science direct volume 85, 2019.

[4]. Ali Qureshi, M., and M. Deriche. "A review on copy move image forgery detection techniques." IEEE, 2019.

[5]. Qazi, Tanzeela. "Survey on blind image forgery detection."IET, 2019.

[6]. M. Qiao, A. Sung, Q. Liu and B. Ribeiro,"A novel approach for detection of copy-move forgery," Fifth International Conference on ADVCOMP (Advanced Engineering Computing and Applications in Sciences, 2019.

[7]. X. Zhang, Support Vector Machines, 01 2017, pp. 1214–1220.

[8]. H.-J. Lin, C.-W. Wang and Y.-T. Kao, "Fast copy-move forgery detection", *WSEAS Transactions on Signal Processing*, vol. 5, no. 5, pp. 188-1975, 2009

[9]. K. B. Meena and V. Tyagi, "Image Splicing Forgery Detection Techniques: A Review," Springer Nature Switzerland AG 2021.

[10]. Abhishek and N. Jindal, "Copy move and splicing forgery detection using deep convolutional neural network, and semantic segmentation," Multimedia Tools and Applications (2021), Springer, 2021