IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMAGE FORGERY DETECTION WITH BLOCK MATCHING SVD EXTRACTION

Ms. SUJEETHA,M.E[1]., PRAMOTH.S[2], MUTHUVEL.K[3], KARTHIK.S[4]

1ASSISTANT PROFESSOR, 2,3,4 UG STUDENTS

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MAHENDRA ENGINEERING COLLEGE, TAMILNADU, INDIA

ABSTRACT

Image block matching is the main step of duplicated region detection for exploring copy-paste image forgery. Several manipulations have been made in images due to high powerful tool evolvement. A copy and move forgery may occur in images where they cannot be easily. The image are get analyzed particularly for the region where the image get forged. The region of the image get copy and paste will be known with the proposed Gaussian RBF kernel PCA. High computational time in this step is one of the most important problems to find similar regions. This paper presents a block based digital image watermarking scheme that is dependent on the mathematical technique of singular value decomposition (SVD). Traditional SVD watermarking already exists for watermark embedding on the image as a whole. In the proposed approach, the original image is divided into blocks, and then the watermark is embedded in the singular values (SVs) of each block separately. Furthermore, we determine performance of proposed algorithm based on time complexity function.

Keywords: SVD Extraction, Image forgery & Digital watermarking

INTRODUCTION

1.1 COPY AND MOVE FORGERY

Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content, and detecting forgeries will only increase. Detection of malicious manipulation with digital images (digital forgeries) is the topic of this paper. In particular, we focus on detection of a special type of digital forgery – the copy-move attack in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. In this paper, we investigate the problem of detecting the copy-move forgery and describe an efficient and reliable detection method. The method may successfully detect the forged part even when the copied area is enhanced/retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG. The performance of the proposed method is demonstrated on several forged images.

1.2 IMAGE PROCESSING SOFTWARES

Nowadays, with the wide availability of powerful and easy-to-use image processing softwares, even a nonprofessional can tamper with an image without leaving any trace detectable by the human vision system. Consequently, the integrity of digital images can no longer be presumed without further investigations. In order to regain image's credibility especially when it comes to sensitive data such as evidences in court of law, news items, medical records to name but few, reliable techniques must be developed to examine the integrity and/or authenticity of digital images.

Generally, these techniques are divided into two major categories: the active methods on one hand and the passive/blind methods on the other hand. The drawback of the first category is the requirement that certain information is embedded into the image either during its creation or before its broadcasting to the public. Digital watermarking belongs to this category [1]. The inserted information can be used either to detect the source of an image or to detect possible modifications of an image. On the contrary, passive / blind methods do not require any prior information to be embedded into the digital image. They work with the assumption that any forgery, even if not visible with naked eyes, would modify the intrinsic statistics of the original image. Copy-move forgery belongs to this category [2]. As mentioned previously, this kind of forgery is mostly used to hide a specific object or area in the original image.

1.3 FORGERY DETECTION

Any Copy-Move forgery introduces a correlation between the original image segment and the pasted one. This correlation can be used as a basis for a successful detection of this type of forgery. Because the forgery will likely be saved in the lossy JPEG format and because of a possible use of the retouch tool or other localized image processing tools, the segments may not match exactly but only approximately.

Thus, we can formulate the following requirements for the detection algorithm:

1. The detection algorithm must allow for an approximate match of small image segments

2. It must work in a reasonable time while introducing few false positives (i.e., detecting incorrect matching areas).

3. Another natural assumption that should be accepted is that the forged segment will likely be a connected component rather than a collection of very small patches or individual pixels.

In this section, two algorithms for detection of the Copy-Move forgery are developed – one that uses an exact match for detection and one that is based on an approximate match. Before describing the best approach based on approximate block matching that produced the best balance between performance and complexity, two other approaches were investigated – Exhaustive search and Autocorrelation.

1.4 SCOPE OF THE PROJECT

With rapid advances in digital information processing systems, and more specifically in digital image processing software, there is a widespread development of advanced tools and techniques for digital image forgery. One of the techniques most commonly used is the Copy-move forgery which proceeds by copying a part of an image and pasting it into the same image, in order to maliciously hide an object or a region. In this paper, we propose a method to detect this specific kind of counterfeit. The feature vectors obtained are then lexicographically sorted to make similar image blocks neighbors and duplicated image blocks are identified using Euclidean distance as similarity criterion. Experimental results showed that the proposed method can detect the duplicated regions when there is more than one copy move forged area in the image and even in case of slight rotations, JPEG compression, shift, scale, blur and noise addition. Due to this necessitous, active approaches have restricted scope. Digital watermarking and digital signatures are some of the examples. Watermarking involves injecting a watermark which is used for the authenticity of the digital image which is indivisible from the image. On the other hand, Passive methods are the non-intrusive/blind methods and it never needs any prior information to include in the digital image. A digital image can be tampered by different attacks

like resizing, addition of noise, blurring, rotation, scaling compressing, image splicing, copy-move and many more.

1.5 PROJECT DESCRIPTION

The major motivation of the forgery in image is manipulating the image in such a way that it cannot be distinguished to the naked eye. Image manipulation has increased the demand to assess the trustworthiness of digital images when used in crime investigation, as witness of law and for surveillance purposes. In this paper, various types of image forgery and detection techniques have been explained. Initially different kinds of forgery attacks are categorized and summary of passive approach is discussed. n contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories: 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip postprocessing; 4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera. I will review several representative forensic tools within each of these categories. In so doing, I have undoubtedly omitted some worthy papers. My hope, however, is that this survey offers a representative sampling of the emerging field of image forgery detection.

1.6 ORGANIZATION OF THE REPORT

The report consists of the introduction in chapter 1 which tells about the forgery, copy and moving image and the software's used for the implementation. Chapter 2 contains the literature survey and chapter 3 consist the existing, proposed implementation of the system. Chapter 4 explains the modules with the system architecture and the chapter 5 explains the data flow system for the project continued with the result and conclusion in chapter 6. Chapter 7 contains the conclusion and future enhancement with the references and appendix.

1.7 LITERATURE REVIEW

[1] TITLE: A FAST AND ACCURATE ALGORITHM FOR COPY-MOVE FORGERY DETECTION

AUTHOR: Abdullah M. Moussa

YEAR: 2015

DESCRIPTION:

In recent years, and with the presence of many efficient image processing tools, digital image forgery has become a serious social issue. Copy-move forgery is one of the most widely used methods for image forgeries in which a part of the image is copied and then pasted to another location in the same image. This procedure is usually used to add or cover a critical part of the image. In this paper, we propose a new fast and accurate algorithm for copy-move forgery detection in digital images. In the proposed algorithm, the image to analyze is segmented into overlapping square blocks with a predefined side length, each one of the blocks is split into equally spaced k subblocks. The sum of pixel intensities of each sub-block is used to form a k-dimensional vector with the help of sliding window and such vector is used as a feature for each block. The resulting features of all blocks are stored in a KD-tree. The block corresponding to each node in the KD-tree is checked with the block corresponding to the nearest neighbor of this node. If the correlation between such blocks is above a prespecified threshold, the two blocks are considered as clones. Experimental results and comparisons with a state of the art method show that the proposed algorithm is fast and accurate.

[2] TITLE: A SURVEY OF COPY-MOVE IMAGE FORGERY DETECTION TECHNIQUES

AUTHOR: Kanagavalli.N, Latha.L

YEAR: 2017

DESCRIPTION:

Digital images are in used widely in recent years and for multiple purposes. The information will be shared through newspapers, magazines, internet, or scientific journals. It is used as a strong proof against various crimes and as evidence used for various purposes. With the appearance of means of image processing and editing tools, creating or transform images has become simple and available. There are many types of image forgery, one of the most important and prominent type is called copy-move forgery in which a part of the image is copied and pasted into the same image with the aim of hiding something important or showing a false scene. This paper surveys different types of digital image forgeries and forgery detection methods. The survey has been done on existing techniques for forged image.

[3] TITLE: IMPROVING SURF BASED COPY-MOVE FORGERY DETECTION USING SUPER RESOLUTION

AUTHOR: Mejren Mohammad Al-Hammadi, Sabu Emmanuel

YEAR: 2016

DESCRIPTION:

In recent years, keypoints-based features, such as speeded up robust features (SURF), capture the attention of researchers in the area of image copy-move forgery detection. They are fast to compute and are quite robust to most interprocessing and post-processing operations. However, they will fail to detect the forgery if not enough keypoints are detected, and that is the case when the forgery size is small. A small size forgery is possible if the object is far away from the camera, or if the image is scaled down as a post-processing step. In this paper, our focus is on detecting forgeries of small size using an improved SURF based copy-move forgery detection (CMFD) method. Our method improves keypoints detection by preprocessing the image using a single image super resolution (SISR) algorithm. The proposed approach has been evaluated and compared against original SURF through a comprehensive set of experiments using a dataset of small size forgeries. Experimental results indicate that our method outperforms SURF especially when the forgery size is small

[4] TITLE: MODIFIED MULTI-SCALE FEATURE EXTRACTION FOR COPYMOVE FORGERY DETECTION BASED ON CMFD-SIFT

AUTHOR: Mohammed Ikhlayel, Mochamad Hariadi, I Ketut Eddy Pumama

YEAR: 2018

DESCRIPTION:

The copy-move attack is a more common method in digital tampering. When copy-move forgery image occur, many important objects add or remove from the image. In order to implement forensic of the images, In the literatures many methods of copy-move forgery detection (CMFD) have been improved. The different approaches of CMFD featurebased was prosed in recent years. but, still more place to enhancement performance further. the problem of Many methods are suffering insufficient matched key points, but forgeries performance on the mirror transformed, then many feature-based methods when the forged region is of uniform texture it might hardly expose the tempering. In this paper we proposed a now scheme. In this scheme the criteria of block and keypoint features will integrate to gather in a new scheme, then multiple copy-move regions or objects will be work very well and especially when regions and objects are different sizes and contain both detailed textures and smooth.

SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

Copy-move forgery is one of the most commonly used manipulations for tampering digital images. Keypoint-based detection methods have been reported to be very effective in revealing copy-move evidence due to their robustness against various attacks, such as large-scale geometric transformations. However, these methods fail to handle the cases when copy-move forgeries only involve small or smooth regions, where the number of keypoints is very limited. To tackle this challenge, we propose a fast and effective copy-move forgery detection algorithm through hierarchical feature point matching. We first show that it is possible to generate a sufficient number of keypoints that exist even in small or smooth regions by lowering the contrast threshold and rescaling the input image. We then develop a novel hierarchical matching strategy to solve the keypoint matching problems over a massive number of keypoints. To reduce the false alarm rate and accurately localize the tampered regions, we further propose a novel iterative localization technique by exploiting the robustness properties (including the dominant orientation and the scale information) and the color information of each keypoint. Extensive experimental results are provided to demonstrate the superior performance of our proposed scheme in terms of both efficiency and accuracy.

2.2 FEASIBILITY STUDY

Preliminary investigation examine project feasibility, the likelihood the system will be useful to the organization. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging old running system. All system is feasible if they are unlimited resources and infinite time. There are aspects in the feasibility study portion of the preliminary investigation:

- Technical Feasibility
- Operation Feasibility
- Economical Feasibility

2.2.1 Economic Feasibility

A system can be developed technically and that will be used if installed must still be a good investment for the organization. In the economical feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs.

The system is economically feasible. It does not require any addition hardware or software. Since the interface for this system is developed using the existing resources and technologies available at NIC, There is nominal expenditure and economical feasibility for certain.

SYSTEM DESIGN

3.1 PROPOSED SYSTEM

Image and visual process have been updated where the digital image will be the information sources. The ambition behind the image content forgery is to perform the manipulations in a way, making them hard to reveal through the naked eye, and use these creations for malicious purposes. In recent years, an exciting field, digital image forensics, has emerged which finds the evidence of forgeries in digital images. The main objective of our system is to develop the identification of the image forgery system using multiple key point extraction system. The Key points will identify and detect the region of where the image get forged whether any extra features are get added are they are removed. The copy and move forgery detection will detect the images which are getting edited. Thus the user can easily identify the images which are forged and they will not share the to any other one. The image are get analyzed particularly for the region where the image get forged. The region of the image get copy and paste will be known with the proposed Gaussian RBF kernel PCA. To present various aspect of image forgery detection; To review some late and existing procedures in pixel-based image forgery detection; To give a comparative study of existing procedures with their advantages and disadvantages.

3.2 MODULES

- Image Acquisition
- Gray scale Conversion
- Block extraction SVD
- Gaussian Kernel PCA
- Block Matching
- Duplicate Region Detection

MODULE DESCRIPTION

3.2.1 Image Acquisition

The rapid progress in colorization technologies has enabled colorized images to be visually indistinguishable from natural images. State-of-the-art colorization methods are already capable of misleading human observers in the subjective tests. Digital imaging or digital image acquisition is the creation of a digitally encoded representation of the visual characteristics of an object. Making an input of this created digital image is known as image acquisition. The image can be extracted with our features the digital sequences of our images. such as a physical scene or the interior structure of an object. According to our observation, the colorized images tend to possess less saturated colors, and the colorization method favors some colors over others, though these differences are difficult to visually detect. Since the Hue-Saturation-Value (HSV) color space separately represents the chrominance information in the hue and saturation channel, we calculate the normalized histograms (each containing 200 bins) of the hue and saturation channel in 15000 natural images and their corresponding fake colorized images, separately.

3.2.2 Gray Scale Conversion

The gray scale conversion is achieved since the computational values will be less. The gray scale conversion turns the image into black and white where the number of pixels will be very less. Here the pixel value will be 0-255 where they can be known as black and white. Instead of computing large values from the color images these computations between 0-255 reduce the complexity. A most recent work converted the color image and video to grayscale [8]. The proposed technique converted the image and video perceptually accurate. First, H-K (Helmoltz-Kohlrausch) phenomenon predicted by a chromatic lightness term that corrects perceived lightness based on the color's chromatic component. The color image converted to linear RGB by inverse gamma mapping, then transformed to CIELUV color space. Its apparent chromatic object lightness channel calculated. Lightness channel to grayscale values mapped using reference white chromatic values. Gamma mapping applied to move from a linear space to a gamma-corrected space. Local contrast increased in the grayscale image to represent better the local contrast of original image. The work carried out using CIELab and CIELuv color spaces. This two step approach a good compromise between a fully automatic technique (first step) and user control (second step) making this approach well suited for natural images, photographs, artistic reproductions as well as business graphics. The main limitation of the approach is the locality of the second step.

3.2.3 Block Extraction SVD

Image block matching is the main step of duplicated region detection for exploring copy-paste image forgery. For efficient block extraction Singular Value Decomposition (SVD) is imposed to make a block detection SVD requires data for all intervals corresponding to a time range query, and incremental SVD does not consider an arbitrary time range. SVD is a powerful numerical analysis tool for matrices computation. SVD is a one way decomposition algorithm and is optimal matrix decomposition in a least square sense. The size of the input matrix considered can be either square or rectangle. · It is a method for transforming a set of correlated

variables into a set of uncorrelated variables. This property of SVD provides an interpretation of relationships among the original data items. The SVD is performed on the original image (F matrix)

$$F=UV^T \quad (5.1)$$

Where U and V are the diagonal feature of the extracted block

The original image is divided into blocks using the diagonal features extracted. Each object with the combination of the pixel are get blocked with the given SVD

The watermark (W matrix) is added to the SVs of the original matrix.

$$D=S+kW \quad (5.2)$$

The SVD is performed on the new modified matrix (D matrix)

$$D=U_wS_wV_w{}^T \quad (5.3)$$

The watermarked image (Fw matrix) is obtained by using the modified matrix (Sw matrix).

$$F_w=US_wV^T \quad (5.4)$$

The proposed SVD based watermarking scheme in which the watermark is added to the SVs of the whole image or a apart of it [3]. A single watermark is used in this scheme which may be lost due to attacks. To avoid this disadvantage, we propose an approach in which , the original image is segmented into blocks and the watermark is added to the SVs of each block in a modified manner.

3.2.4 Gaussian Kernel

In other words, the Gaussian kernel transforms the dot product in the infinite dimensional space. The infinite dimensional space is converted into a Gaussian function of the distance between points in the data space. If two points in the data space are nearby then the angle between the vectors that represent them in the kernel space will be small.

- For an image block $Br(x, y)$ of size $h \times w$, where x, y are 0, 1, 2, . . . , $N - 1$, we decompose the block $Brc(x, y)$ in terms of 2D SVD basis function. The result occurs in the form of a coefficients matrix $C(p, q)$ of size $h \times w$ that contains the SVD coefficients:
- In our implementation, a Gaussian RBF kernel function is chosen, which is defined by the mapping function : [0,∞) → R.
- The dimensionality of matrix MKPCA can be reduced to NC where π is the Gaussian kernel parameter.
- Using this parameter the PCA based difference are analyzed with the computed features.

However, this approach cannot provide fast query speed for a long time range due to heavy computations induced by the reconstruction and the following SVD. The goal of Stitched-SVD is to efficiently stitch the SVD results in the query time range by avoiding reconstruction and minimizing the numerical computation of matrix multiplication. Feature extraction reduces dimensionality with minimal loss of information by (linear or nonlinear) projection of D-dimensional vector onto d dimensional vector (d < D). n image analysis area, there are several types of feature extraction: frequency domain feature, transform-based feature, spatial domain feature, statistical feature, histogram and color feature, texture feature, edge feature. Each method has advantages and disadvantages. Hence selecting the best feature is important and it depends on system specifications. In duplicated region detection to select and evaluate the feature extraction

3.6 OUTPUT DESIGN

In this paper, image forgery detection, different kinds of image forgery techniques like Active and Passive are mentioned. The summary of various techniques that helps us to detect forgeries. To perform indistinguishable copy-move forgery, post-processing of snippet is performed. Proposed algorithm can detect forgery under post-processing operations like rotation, scaling and noise. We have applied sample images from internet which are shown in figure 4 to our algorithm and got desirable output as shown in figure 4. Proposed algorithm (SVD) has given a desirable output which is better than using PCA. SVD algorithm requires lower time than PCA in detection method. But as overlapping block size increases the total time required for detection decreases but false detection increases. In future, the proposed method can be modified or extended to detect forgery by more post-processing operations on snippet and also can be extended to detect on color image format. Forged images created with duplicated and distorted regions are visually difficult to detect. An effective and robust forensic method based on angular radial partitioning and Harris key-points is proposed. We demonstrated the effectiveness and robustness of the proposed method with a series of experiments on realistic forged images with high resolutions from two image databases: MICC-F220 and image data manipulation. The experiment results showed that the proposed method can detect duplicated and multiple regions effectively, and with high accuracy, in the presence of several geometric transformation operations including (rotation and scaling), image degradations including JPEG compression and Additive White Gaussian Noise. The proposed method can detect rotated regions in multiples of 30 degrees and different rotation angles up to 360 degrees with estimation of rotation angles between duplicated regions. A current limitation of the proposed technique is that it cannot detect the duplicate regions when distorted with blurring and illumination changes. Therefore, involving blur invariant features and multiresolution local binary pattern descriptors is part of the future work that we are exploring to improve the technique. Wefind that the CMFD is a popular research area due to the rapidly increasing numberof publications in last two and half years. Publication statistics are shown inFig. 2. In this survey paper, we classifiedthe CMFD techniques,

SYSTEM TESTING

System testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently before live operation commences. Testing is vital to the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, the goal will be successfully achieved. System Testing is a type of software testing that is performed on a complete integrated system to evaluate the compliance of the system with the corresponding requirements. System testing detects defects within both the integrated units and the whole system. The result of system testing is the observed behavior of a component or a system when it is tested. System Testing is basically performed by a testing team that is independent of the development team that helps to test the quality of the system impartial. The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

OBJECTIVES OF TESTING

- Testing is the process of executing a program with the intent of finding an error.
- A successful test is one that uncovers a discovered the error.

5.1 TYPES OF TESTING

A series of tests are performed for the proposed system before the system is ready for user acceptance testing.

- Unit testing
- Integration testing
- System testing
- Functional testing

- Performance time testing

UNIT TESTING

The first test in the development process is the unit test. The source code is normally divided into modules, which in turn are divided into smaller units called units. These units have specific behavior. The test done on these units of code is called unit test. Unit test depends upon the language on which the project is developed. Unit tests ensure that each unique path of the project performs accurately to the documented specifications and contains clearly defined inputs and expected results. A Unit corresponds to a screen /form in the package. Unit testing focuses on verification of the corresponding class or Screen. This testing includes testing of control paths, interfaces, local data structures, logical decisions, boundary conditions, and error handling. Unit testing may use Test Drivers, which are control programs to co-ordinate test case inputs and outputs and Test stubs, which replace low-level modules. A stub is a dummy subprogram.

INTEGRATION TESTING

Testing in which modules are combined and tested as a group is known as integration testing. Modules are typically code modules, individual applications, source and destination applications on a network, etc. Integration Testing follows unit testing and precedes system testing. Testing after the product is code complete. Betas are often widely distributed or even distributed to the public at large in hopes that they will buy the final product when it is release. Integration testing is used to verify the combining of the software modules. Integration testing addresses the issues associated with the dual problems of verification and program construction.

SYSTEM TESTING

System testing is a critical aspect of Software Quality Assurance and represents the ultimate review of specification, design and coding. Testing is a process of executing a program with the intent of finding an error. A good test is one that has a probability of finding an as yet undiscovered error. The purpose of testing is to identify and correct bugs in the developed system. Nothing is complete without testing. Testing is the vital to the success of the system. In the code testing the logic of the developed system is tested. For this every module of the program is executed to find an error. To perform specification test, the examination of the specifications stating what the program should do and how it should perform under various conditions.

FUNCTIONAL TESTING

It is a type of software testing whereby the system is tested against the functional requirements/specifications. Functions (or features) are tested by feeding them input and examining the output. Functional testing ensures that the requirements are properly satisfied by the application. This type of testing is not concerned with how processing occurs, but rather, with the results of processing. It simulates actual system usage but does not make any system structure assumptions.

Apart from these tests, there are some special tests conducted which are given below:

PERFORMANCE TIME TESTING

This test determines the length of the time used by the system to process transaction data. In this phase the software developed Testing is exercising the software to uncover errors and ensure the system meets defined requirements. Testing may be done at 4 levels.

- Unit Level
- Module Level
- Integration & System
- Regression

Module Level Testing

Module Testing is done using the test cases prepared earlier. Module is defined during the time of design.

Regression Testing

Each modification in software impacts unmodified areas, which results serious injuries to that software. So the process of re-testing for rectification of errors due to modification is known as regression testing. Delivery Installation and Delivery are the process of delivering the developed and tested software to the customer. Refer the support procedures Acceptance and Project Closure Acceptance is the part of the project by which the customer accepts the product. This will be done as per the Project Closure, once the customer accepts the product closure of the project is started. This includes metrics collection, PCD etc.

CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION

This paper presents a visually undetectable, robust watermarking scheme. The proposed algorithm depends on embedding the watermark into the SVs of the original image after dividing it into blocks. The experimental results show that the proposed Block-by-Block SVD-Based method gives fidelity and robustness against Gaussian noise, cropping and JPEG compression. One of the main problems in duplicated region detection is high computational time for exposing the similar blocks. In this paper we proposed a two layer block matching using two types of feature extraction namely low and high accurate features. Low accurate feature is used for grouping the blocks in first match while high accurate feature is applied in local block matching. In this method we did not focus on feature vector reduction for improving the time complexity. Due to reducing the feature vector dimension can affect robustness of the system; we used the block grouping for reducing the extra compare operations. As a result, this improves time complexity significantly. The results demonstrate that when using two layers matching, time complexity of the system is more efficient than lexicographically sorting algorithm.

6.2 FUTURE ENHANCEMENT

In future, we plan to extend our work to multilayer block matching with efficient multilayer feature extractions algorithms. The detection system will be extended to more transform domain watermarking approaches such as DWT- SVD and DCT-SVD

REFERENCES

[1] Abdullah M. Moussa , A Fast and Accurate Algorithm for Copy-Move Forgery Detection, Tenth International Conference on Computer Engineering & Systems (ICCES), 2015

[2] Kanagavalli.N , Latha.L , A Survey of Copy-Move Image Forgery Detection Techniques, International Conference on Inventive Systems and Control, 2017

[3] Mejren Mohammad Al-Hammadi , Improving SURF Based Copy-Move Forgery Detection Using Super Resolution , IEEE International Symposium on Multimedia, 2016

[4] Mohammed Ikhlayel , Mochamad Hariadi , I Ketut Eddy Pumama , Modified Multi-scale Feature Extraction for CopyMove Forgery Detection Based on CMFD-SIFT, International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), 2018

[5] N. Hema Rajini, Image Forgery Identification using Convolution Neural Network, International Journal of Recent Technology and Engineering (IJRTE), Volume-8, Issue-1S4, June 2019

[6] Qi Yan, Rui Yang,Jiwu Huang,Robust Copy–Move Detection of Speech Recording Using Similarities of Pitch and Formant, IEEE Transactions on Information Forensics and Security (Volume: 14 , Issue: 9 , Sept. 2019)

[7] Rahul Dixit, Ruchira Naskar,Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images , IET Image Processing (Volume: 11 , Issue: 9 , 9 2017)

[8] Srinivasan Ramakrishnan ; Sivasamy Nithya, Two improved extension of local binary pattern descriptors using wavelet transform for texture classification, IET Image Processing (Volume: 12 , Issue: 11 , 11 2018)

[9] Yuan Wang , Lihua Tian , Chen Li, LBP-SVD Based Copy Move Forgery Detection Algorithm, IEEE International Symposium on Multimedia (ISM), 2017

[10] Yuanfang Guo, Xiaochun Cao, Wei Zhang, Rui Wang, Fake Colorized Image Detection, IEEE Transactions on Information Forensics and Security (Volume: 13 , Issue: 8 , Aug. 2018)