European Journal of Molecular & Clinical Medicine

ISSN 2515-8260 Volume 08, Issue 02, 2021

DIGITAL IMAGE FORGERY DETECTION USING SUPER PIXEL SEGMENTATION AND HYBRID FEATURE POINT MAPPING

[1]V.Shiva Narayana Reddy
Associate Professor, Department of CSE, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India
[2]K. Vaghdevi
Department of CSE, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India
[3]Dr. Kamakshaiah Kolli
Associate Professor, Department of CSE, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India

Abstract:
In recent years, digital images have a large variety of uses and for different purposes. The most significant and common form is called digital image forgery, which uses the same image in the forgery process, and we have many kinds of image forgeries. For creating a duplicate or hiding any existing objects, a region of an image copies and paste into the same image. For a forgery with particular form, the images are tested in this paper. Images will first be split into super pixels to detect the forgery attack. Because of the high dimensional existence of the feature space, the representation of reduced dimension feature vector is achieved with the implementation of hybrid function point mapping. During the feature matching, the efficiency is also improved. In order to identify the forgery in the picture, the suggested system is successful. The proposed method therefore offers a detecting forgery with efficiency and efficacy that helps to improve the image authenticity in evidence-centered applications.

INTRODUCTION

Digital Image forensics is a field of research that seeks to verify the originality of digital images by retrieving their background content. Digital images are quickly forged by different techniques, leading to changes in their meaning and authenticity. With the enormous growth of technology, the use of the image has been expanding day by day in our daily lives. Because of this, forgery of the digital image has turned out to be increasingly straightforward and indiscoverable.

The ability to create image forgery is nearly as old as photography itself. Over a two-decade, photography is the normal and fascinating art which turned out for creating portraits and by that portrait photographers can earn money by making forgery possible by enhancing deals by retouching their photographs. Detection of image forgery has developed as an amazing study in various applications of digital image processing, image forensics, criminal investigation, biomedical technology, and computer vision, etc. Due to sophisticated software

techniques that are difficult to validate whether a picture is distorted by naked eyes, it has gained more popularity and challenge.
A high level view on forensics of digital images and its possible detection approaches is given in this chapter. The motivation to propose efficient methods of copy move forgery detection is described based on the classifier and optimization techniques. It culminates with discussion of the organization of the rest of the thesis along with its contributions.

Due to the huge development of technology, the usage of the digital image has been expanding day by day in our daily lives. Because of this forgery of the digital image has turned out to be increasingly straightforward and indiscoverable. At present technology where anything can be controlled or changed with the assistance of modern technology had started to disintegrate the authentic of images [66, 67, 68], counterfeiting and forgeries with the move to the Mega pixels, which gives a new way for forgery.

Imitation is not new to humankind but rather it is past generation issues. It was restricted to craftsmanship previously and the overall population didn't affect by composing. The ability to create image forgery is nearly as old as photography itself [23]. Over a two-decade, photography is the normal and fascinating art which turned out for creating portraits and by that portrait photographers can earn money by making forgery possible by enhancing deals by retouching their photographs [73]. Image forgery detection had gain more attention and incredible investigation in various fields such as computer visualization, image processing, biomedical tools, immoral analysis, image forensics, etc. It gained further attention and demanding due to advanced software's that become difficult to verify if naked eyes influence an image [40].

Image forensics is a well developed field that analyzes the images of specific conditions to build up trust and genuineness. It is quick and better-known domain due to several executions of real-time applications in numerous areas incorporates intelligence, sports, legitimate administrations, news reporting, medical imaging, and protection assert investigations. An image can be faked by modifying the image features characteristics such as brightness, darkness or image parameters or concealing data [23, 82].

Image forgery implies altering the digital image to some meaningful or valuable data. It can simply be described as the process of adding or removing specific characteristics from an image without any evidence of alteration and avoiding them for malicious purposes. In some cases, it is complicated to recognize the altered image part from the authenticate image. The identification of a forged image is essential for originality and to preserve truthfulness of the image. A forgery detection that endeavours the unobtrusive irregularities in the color shade of the illumination changes in images [69]. To accomplish by consolidating data from material science and statistical based illuminate estimators on image regions to separate texture and edge-based features.
Image forgery detection plays an important role in forensics to give authenticity to the image. It is extremely complex to detect the imperceptible forged image. To successfully detect forgery, any forgery establishes a connection between the forged image and the original

image. The different image forgery detection techniques [19, 63] are shown in Figure 1.2. For passive image forgery detection, a few proficient methods of forgery detection are provided. The relevant algorithms for detecting image forgery fall into one of the following categories.

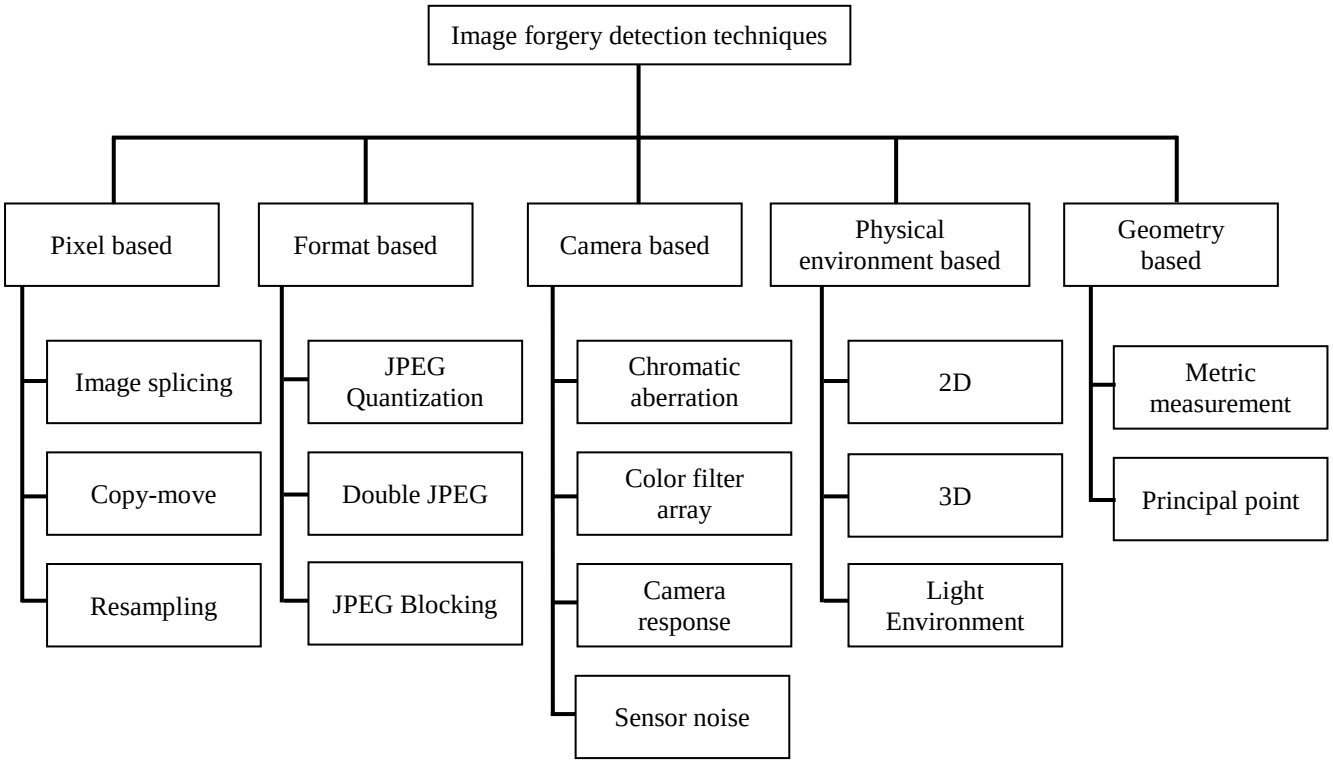

Figure 1.2: Image Forgery Detection Techniques

2. Literature

Muhammad et al. [1, 2], proposed an efficient non-intrusive Dyadic Wavelet Transform (DyWT) for copy-move forgery detection. DyWT is shifting invariant and efficiently catches the basic data about the images. At first, the image is segmented and disintegrated utilizing DyWT to create the LL and HH sub bands. The similarity measure is utilized to compare each pair segments by sub bands to distinguish the copied and pasted part. The performance parameter values demonstrate the better results with segmentation algorithm that can assist in conversion of an image into more complete objects with precision.

Ryu et al. [3], proposed a Copy-Rotate-Move (CRM) scheme using Zernike moments for minimization of JPEG compression, obscuring and additive white Gaussian noise. Additionally, this method can recognize forgery even on the rotated region since Zernike moments are logarithmically invariant to revolution. In any case, the drawback of this technique is that it is yet feeble against scaling and manipulation based on affine transform.

Fadl et al. [4], discussed the detection of forged images. The block-based matching algorithm is developed for forgery detection in which the input image is processed to achieve the authentic output with forged image. In order to establish the similarity factor and divide input data into different clusters, the k-mean clustering technique is used. Based on the procedure of feature extraction, the clustered data retrieves for differentiating the forged data and image features. The performance parameters have provided the results accurately that represent the

output image in the current class. The complexity of time can increase by 50 percent in contrary to the other current methods.

Bayram et al. [6], discuss the feature demonstration which is invariant to noise or blurring. These extracted features are further invariant to few geometric alterations includes scaling and rotation that might be connected to the copied region before pasting. Fourier Mellon Transform (FMT) is employed as feature representation and counting bloom filter to enhance the time complexity. The experimental results demonstrated that this FMT of the feature block is more vigorous to JPEG compression.

Zhao &Guo [7], proposed a robust technique to detect the copy-move forgery. The quantization of the DCT coefficients and quantization division is utilized. This method applied on each image which further divided into non-overlapping sub-blocks. By using the largest singular value, the each block's dimension with extracted feature is minimized using SVD. Based on the similarity matching, the sorting of feature vectors lexicographically and identification of forged image blocks have done by shift frequency threshold. By comparing with JPEG compression, Additive White Gaussian Noise (AWGN), and Gaussian blurring, the copy-move forgery technique is providing robust results based on the experimental analysis.

Pandey et al. [8], analyzed the video processing based copy-move forgery to distinguish the forge area of the video. This procedure utilized different pre-processing for removal of noise and classification steps to identify the forged area. The video editing software is utilized for editing the videos and duplicate moves. The relationship between video frames is assigned as special segments for simple to recognize the copy and pasted frame from another area. The SIFT algorithm is employed to form the edges in the feature extraction process. The experimental results demonstrate the proficient noise reduction processes to enhance the image quality .This method works efficiently for temporal images with efficient classification accuracy rate.

Ranjani et al. [9], proposed forgery detection by incorporating the techniques of Inverse Discrete Cosine Transform and Discrete Cosine Transform (DCT) based on row and column reduction method. The computational complexity relevant to cost, time, and the picture proficiency is diminished by this new technique. Initially, the input image is divided into grids as rows and columns. In which DCT is associated with each row and columns with the help of lines and segments and it changed into various pieces with various estimations. Finally, the copied picture gets managed from viewpoint of is confinement regard.

Li et al. [10], developed a Polar Harmonic Transform (PHT) based on block matching for copy-move forgery detection. The features extracted by PHT from the circular blocks are utilized to provide indefinite image features. These block are compared with PHT features. The input images are collected from the publicly available datasets and simulated by MATLAB. The proposed method performs robust to compression of JPEG, noise, and object rotation based on the performance results.

Ke et al., was proposed a technique of copy-move detection for determining the forgeries of image based on the identification of irregularities in variance of image noise on the immersion part of HSV shading space. From RGB color space, the conversion of image into HSV color space initially and isolated into blocks with different sizes. The forged images haphazardly trimmed at various areas from the images and white Gaussian noise was included. For image blocks that have a size of 32×32, the noise estimation is evaluated that shows the best outcomes.

Christlein et al. [11], proposed Same Affine Transformation Selection (SATS) for a rotation invariant selection whichThe benefit of the shift vectors is shared at an exclusive computational expense that has been somewhat increased. As a result, the suggested methodology unambiguously recoups the parameters of the relative change associated with the area being copied. The results show that when the copied region is rotated, SATS outperforms shift vectors, self-sufficient image size.

Davarzani et al.[12], suggested a method of detecting tampering using local binary patterns. The regions copied are recognized and the forged region is also observed in 90-degree items affected by compression of JPEG, blurring, scaling, noise or rotation. noise, blurring, JPEG compression, scaling or rotation. The input image is transformed to a gray scale and split into blocks that overlap. In order to find the features by applying the LBP operators, the Multi-resolution Local Binary Pattern (MLBP) is used on each block. The matrices of functions are sorted lexicographically and the matching blocks are identified by the strategy of the k-d tree.

K Kamakshaiah et al [16], proposed recognition of objects such as fishes has drawn more attention while submerged pictures are showing some difficulty due to their poor picture quality which also includes rough background surfaces when compared to general images. Medicines prepared from fishes help in curing different diseases to reduce the health issues in the present world (for example, rheumatism problems, gel for wounds, bandages, etc). In our proposed method we are projecting a deep neural network that supports recognition of fishes to acquire their count, species and medical usage.

Existing system

Existing Block diagram:

The following figure shows the block diagram of the existing system.

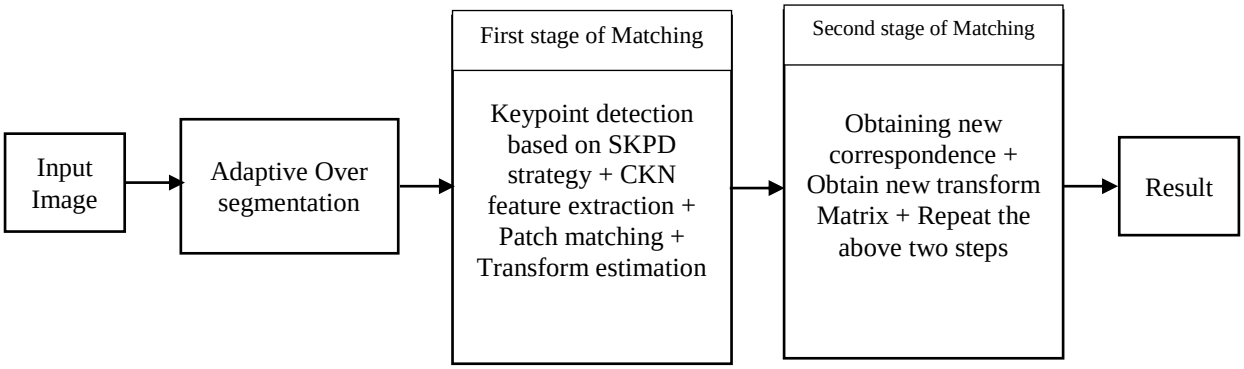

Figure 2. Existing method

3.1 Input Image:

The pre-processing is the primary step in every input image, the preprocessing methods is involve color channels that converts the gray scale image or segmentation by focusing on achieving the reduction of complexity in computation and improving the identification with precision.

3.2 Adaptive Over Segmentation:

In this paper, the algorithm of Adaptive Over-Segmentation which allows the segmentation of host image as image blocks into irregular shape of non-overlapping regions. The forgery regions can define through the matching of certain irregular and non-overlapping regions. The computational costs will reduced by the segmentation of non-overlapping than the overlapping blocking. But, the forgery area can reflect by the significant and irregular regions when compared to the normal blocks. It's difficult to evaluate the initial super pixel scale in SLIC. Different sizes of copy-move regions and host images are included and different content is available in the real-time applications of copy-move forgery detection. Different types of results in forgery detection will provide by different super pixel sizes. The super pixels of different sizes of forgery images should be blocked by different host images.

$$E_{LF} - \sum|CA_4| \tag{1}$$

$$E_{HF} - \sum_i(\sum|CD_i| + \sum|CH_i| + \sum|CV_i|), \quad i = 1,2,\ldots,4 \tag{2}$$

$$P_{LF} = \frac{E_{LF}}{E_{LF}+E_{HF}} . 100\% \tag{3}$$

$$S = \begin{Bmatrix} \sqrt{0.02 \times M \times NP_{LF}} > 50\% \\ \sqrt{0.01 \times M \times NP_{LF}} \leq 50\% \end{Bmatrix} \tag{4}$$

Several experiments are performed to look for In order to obtain good forgery detection performance, the relationship between the host image frequency distribution and the initial superpixel scale. A four-level DWT processes on the host image based on the "Haar" wavelet. By using (1) and (2), the low frequency energy or ELF and the high frequency energy or EHF can be determined respectively. The percentage of the low-frequency distribution of the PLF using (3) is determined by the low-frequency energy of the ELF and the high-frequency energy of the EHF, The initial superpixel size S can be described as (4) where the initial superpixel size is S; the host image size is M*N; and the low frequency distribution percentage is P LFF.

The host image is divided into the blocks with initial sizes using the Adaptive Over-Segmentation technique based on the provided host images. For improving the performance of forgery detection, each image can specify as an acceptable size of block which is described below.

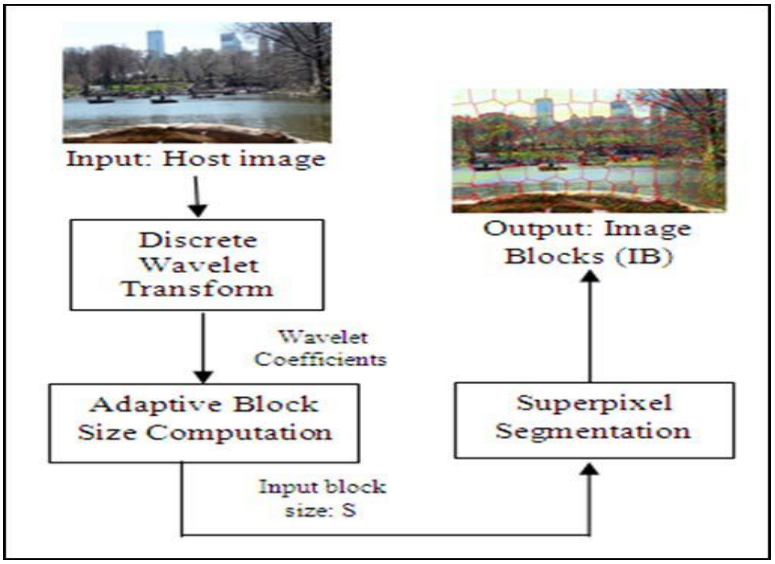

Figure 3The adaptive over-segmentation flowchart

CKN feature extraction:

The generate patch descriptors designed by the Convolution Kernel Network (CKn), and keypoint detectors can generate input patches (e.g. DoG). The special M and M' denotes the two m* m size patches, and = {1, · · ·, m}2 is the set of pixel positions. The **M** sub-patch centered with a fixed sub-patch size at position z∈ (resp. pz denotes the M 'sub-patch) is denoted by Pz. The sub-patches near the **M** border includes outside values which are discarded in execution without padding. The **M** and **M'** these are described by the convolutional Kernel.

$$K_1(M,M') = \sum_{Z,Z^1\in\Omega} \|P_z\| \|P'_{Z'}\| \, e^{-\frac{\|Z-Z'\|^2}{2\beta_1^2}} \, e^{-\frac{\left\|\bar{P}_Z-\bar{P}'_{Z'}\right\|^2}{2\alpha_1^2}} \quad (5)$$

Where, || · || denotes the L2 standard, β1 and α 1 denote Gaussian kernel smoothing parameters and p ~z:= (1/|||pz ||)pz is the L2-normalized version of the pz sub-patch, and p~ z is the L2 version of pz . Therefore a patch's feature representation is determined using the con-volutional kernel. For the kernel to be a match kernel, the choice of hyperparameters may give a tunable degree of invariance, generating hierarchical convolutionary representations.

The convolutional kernel architecture with two layers is shown in Fig. 3. For implementation and comprehensive proof, and for the ingenious nature of CKN, it's very tough to draw the theoretical roots. Based on CKN, the complete protocol of forgery detection is simple to understand besides that CKN generates the descriptors of function for patches.

Proposed System

Block diagram:

The proposed block diagram contains input image, super pixel segmentation, feature extraction and hybrid feature mapping blocks. In super pixel segmentation the entire image is divided into number of super pixel blocks and these blocks are saved. Get the features from each and every super pixel block. The feature extraction is done by using the 3 feature extraction techniques i.e. resnet, SHIFT and SURF respectively. All features are combined and get the best matching values. Map the matched pixel values and mark the forgery part of the image.

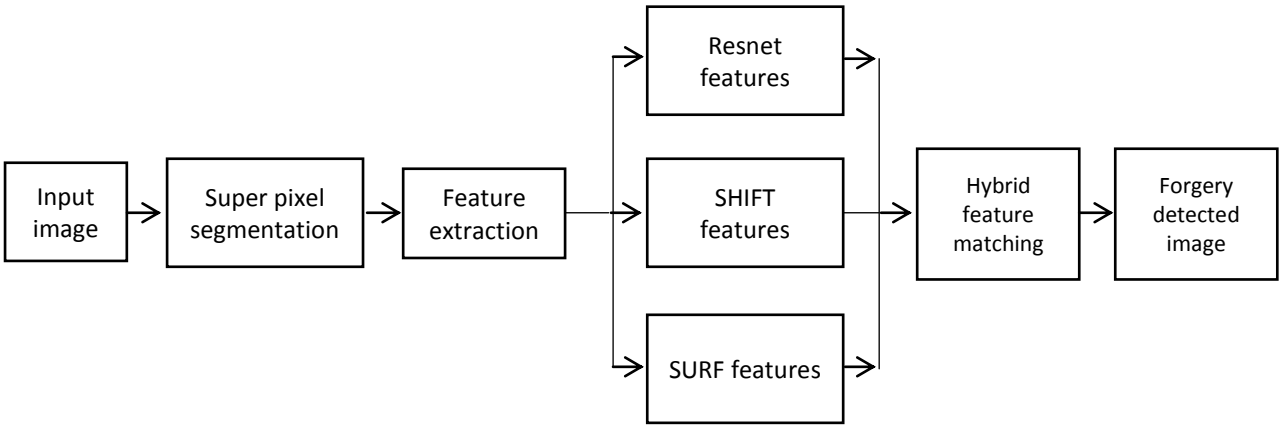

Figure 4. Proposed Block diagram

SLIC based Superpixel Segmentation

A convenient primitive is provided by superpixels that helps to determine local image features. The image's redundancy is captured by them and is reduced the subsequent image processing tasks' complexity greatly. For various applications, superpixels have been proved to be useful in object localization, body model estimation, skeletonization, image segmentation, and depth estimation. Superpixels should be produced segmentations of high quality, easy to use, and rapid to become useful. All these requirements don't met by most of the methods of state-of-the-art superpixel unfortunately. Most often, these are having drawbacks in terms of inconsistent size and shape, poor quality segmentation, high computational cost, or contain multiple difficult-to-tune parameters as demonstration. When compared to the state-of-the-art techniques, the approach in the proposed work is addressed these problems, simple, and is produced compact, high quality, and uniform superpixels nearly with more efficiency. The proposed algorithm of simple linear iterative clustering (SLIC) is performed pixels with a local clustering in the 5-D space in which the CIELAB color space's L, a, b values and the coordinates of x, y pixels are defined. The regularity and compactness in the superpixel shapes, and accommodates grayscale seamlessly including color images have been enforced by a novel distance measure. SLIC is very simple to apply and easily implemented practically as it specifies the superpixels with a desired number by only parameter. More efficient results could be obtained by SLIC than existing competing techniques as shown by the experiments of the dataset of Berkeley benchmark dataset since SLIC is producing the similar or better quality image segmentations based on the measures of under-segmentation error and standard boundary recall.

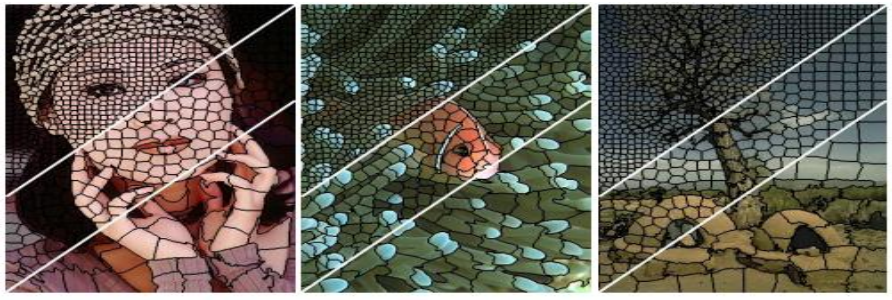

Figure 4: The superpixel segmentation algorithm, different sizes and their region boundaries.

In Fig 4, the desirable compact and highly uniform superpixels are useful for many vision tasks and those are regarding the image boundaries produced by SLIC. While swiching from pixel-based graphs to superpixels, graph-based models like Conditional Random Fields (CRF) are increased the dramatic speed but the performance can be degraded due to the loose or irregular superpixels. At the superpixel locations, SIFT extract by local features from the image that become less meaningful and discriminative when superpixels are loose or irregular and learning statistics over two or more superpixels cliques can unreliable.

SLIC segmentation algorithm

According to the image plane's proximity and similarity, superpixels are generated by the approach based on the clustering pixels. This is completed in the space with five-dimensional [labxy]. In the CIELAB color space, it is referred to the vector of pixel color and it is considered as perceptual uniform for small color distances and xy is the pixel's position. By considering an assumption of input images of sRGB, the spatial distance operates in the xy plan by relying on an image's size while limiting the maximum possible distance between two colors in the CIELAB space. It's not possible to utilize the Euclidean distance in the 5D space without any spatial distances normalization. A new distance measure that concerns the size of superpixel is introduced for cluster pixels in the 5D space. By using this measure, pixel proximity and color similarity is enforced in the 5D space that allows to create the approximate equalization of the spatial extent and their expected cluster sizes.

Algorithm

The simple algorithm of linear iterative clustering summarizes in Algorithm 1. For determining locations, it's require to move them in corresponding to the lowest gradient position in a size of 3 × 3 neighborhood based on the K regular sampling with spaced cluster centers. To decrease the chances of selecting a noisy pixel and to limit the placing them at an edge, this is considered. As mentioned in the below equation (4.2), image gradients are determined.

$$G(x,y) = ||\mathbf{I}(x+1,y) - \mathbf{I}(x-1,y)||^2 + ||\mathbf{I}(x,y+1) - \mathbf{I}(x,y-1)||^2 \quad (4.2)$$

Where $I(x,y)$ is the lab vector corresponding to the pixel at position (x,y) and $||.||$ is the L_2 norm. It is considered for both color and intensity data. With the nearest cluster center whose search area overlaps with the pixel, each pixel of image is associated. After making the association of all pixels with the nearest cluster center, a new center determines as the average labxy vector of all pixels related to the cluster. The repetition of associating the pixels with the nearest cluster center is considered and recomputing of cluster center is done until convergence.

At the process with final phase, a few stray labels may retain. The same label is included in a few pixels in the large segment's vicinity but not connected to it. The spatial proximity measure may arise as the clustering not enforcing the connectivity explicitly. The connectivity enforces in the last phase of an algorithm according to the disjoint segments relabeling with the largest labels of neighboring clusters. For segmenting of an image, this phase is taking less than 10% of required total time and it is O (N) complex.

Residual Neural Network (ResNet)

A Residual Neural Network (ResNet) is a CNN that consists of so-called residual Blocks. Such a residual block is shown once in Figure 5. A residual block works as follows: Outgoing from an input x, either the input image or the output of another Convolutional layer, is through the first convolutional layer, including batch Normalization and Activation (SReLU), given and then by the second convolutional Layer. Before the values through batch normalization and activation (SReLU) of the second convolutional layer is given the input x added and then by batch normalization and activation (SReLU) given. The first convolutional layer calculates f (x) as normal second convolutional layer, on the other hand, calculates f (x) + x. The name Residual is moving therefore, that the rest is also calculated here. The greater depth that is possible with ResNets, the result is that the gradient also through the additional connection is returned and thereby slower becomes smaller.

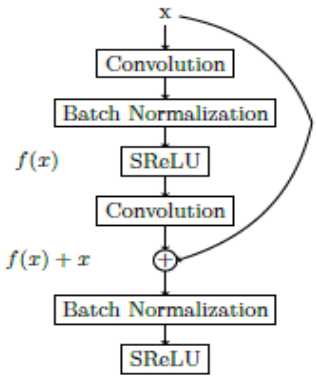

Figure 5.: Schematic representation of a residual block.

It should be noted that if one of the convolutional layers has a dimension reduction carries out (stride≥ 2), the addition is no longer possible or a dimension reduction must also be carried out here, otherwise the Dimensions no longer match. The paper uses two methods to do this presented. The first method adjusts the dimensions to each other and fills them if necessary with zeros. The second performs a projection that needs it but additional parameters. The experiments in this work use one Modification of the first method by the lambda expression lambda t: K.repeat_elements (t [:;:; :: 2; :: 2]; 2; 1) is described. Since the stride is always 2 2, every second value of the output is taken and for the number of filters that are doubled instead of being padded with zeros, the values repeated.

The CNNs in experiments 22 and 23 are ResNets. There are three in total Convolutional layer with a stride of 2 2 per network. All convolutional layers that come after a convolutional layer with stride double the number of Filters, starting with 64 filters (8 64, 8 128, 8 256, 9 512). Overall the four residual networks 34 convolutional layers.

The two ResNets of the 23rd experiment (once with 1286 classes and once with 6465 classes) have an additional link over all Convolutional layer with the same number of filters. That means, for example, that the output of the eighth convolutional layer, which is the last with 64 filters, the output of the first convolutional layer is added.

Scale Invariant Feature Transform (SIFT)

The David Lowe (1999, 2004) developed image-based matching and identification by the image descriptor is Scale Invariant Feature Transform (SIFT). For a wide range of purposes relevant to the point matching between the view-based artifacts and different views of a 3-D

scene, this descriptor and associated image descriptors are utilized in computer vision. In the image domain, the descriptor of SIFT is invariant for rotations, translations, and transformations of scaling. It is robust to the variations in illumination and to moderate the transformations. For object recognition and image matching, the descriptor of SIFT has been used in practice under real-world conditions.

The SIFT descriptor, In its original formulation, it consisted of a gray-level image method to detect the interest points where the local gradient directions statistics about image intensitives that were accumulated for describing the local image structures around each point of interest in a local neighbourhood for utilizing this descriptor to fit for corresponding values. For generating better results for different tasks like biometrics, images alignment, texture classification, and objects categorization, the descriptor of SIFT was implemented for dense grids (dense SIFT). The SIFT descriptor was also implemented from 2-D spatial images to 2+1-D spatiotemporal video and from gray to color images.

SIFT stands for Scale-Invariant Function Transform and D.Lowe, British Columbia University, first introduced it in 2004. SIFT is image size and rotation invariance.

Algorithm

SIFT is a very important algorithm. The SIFT algorithm mainly has four steps involved. One-by-one, we'll see them.

Peak range of scale-space: possible position for finding features.

Keypoint Localization: Accurately locating the keypoints of the feature.

• Orientation Assignment: Keypoint orientation assignment.

Keypoint descriptor: Defining the keypoints as a vector of high dimensions.

• Keypoint Matching

Peak Scale-space Selection

Scale-space

Only on a certain scale are real world objects important. A perfect sugar cube could view on a table. It doesn’t exist actually when the whole milky-way is stared. This artifacts with multi-scale nature is popular. And on digital images, a scale space aims to reproduce this notion.

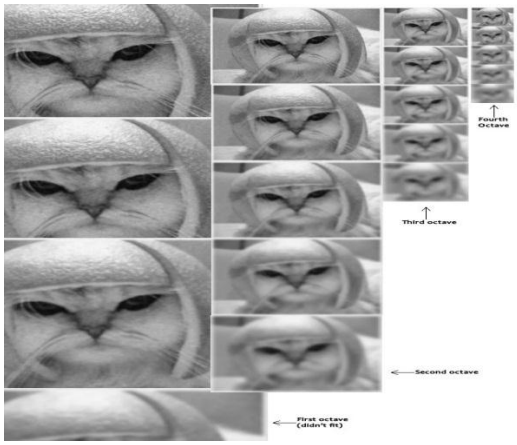

Figure 7: Scale space attempts on digital images.

An image's scale space is a function L(x,y,σ) that is generated at different scales with the input image from the convolution of a Gaussian kernel(Blurring). Scale-space is divided into octaves, depending on the size of the original image, the number of octaves and scale. So we're generating several octaves of the original photo. The image size of any octave is half the previous one.

DOG(Difference of Gaussian kernel)

We are now using those blurred images to create another collection of images, the Dierence of Gaussian (DoG). For finding interesting key points in the image, these DoG images are great. The Gaussian difference is acquired as the Gaussian blurring difference between a picture with two different σ, let it be σ and kσ. In the Gaussian Pyramid, this process is done for various octaves of the picture. It is represented in the image below:

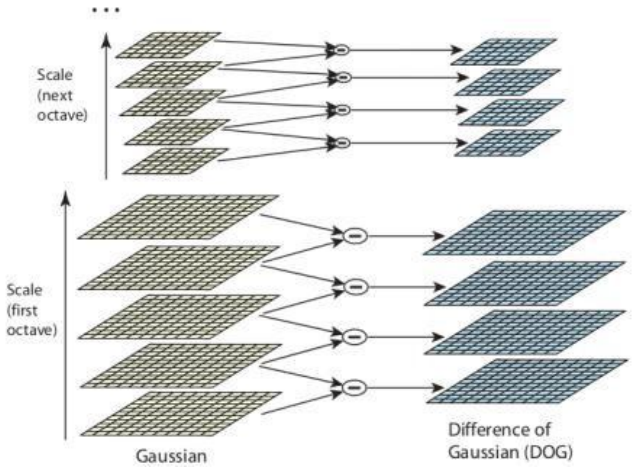

Figure 8: Scale Invariant Feature Transform building a scale space

SURF: speeded up robust features

A proprietary local feature descriptor and detector is the Speeded Up Robust Features (SURF) in the computer vision. Different types of tasks like 3D classification or reconstruction, images registration, and objects detection can be processed. The inspiration is taken from the scale-invariant function transform (SIFT) partially. When compared to SIFT, the standard version of SURF is operating fast and to be more robust than the SIFT in terms of different transformations of image.

An integer approximation of the detector determinant's Hessian blob is utilized by SURF for detection of points of interest that can determine based on a precomputed integral image with the operations of 3 integers. Around the point of interest, its feature descriptor is operated based on the response of Haar wavelet. These are also determine by considering an assistance of integral image.

SURF descriptors can be used to control objects, to recreate 3D scenes, to locate and detect the objects, people or faces, and to extract the interest points. In the United States, SURF implementation with an algorithm is proprietary. For the image rotation, an upright version of SURF (called U-SURF) is not invariant and easier to compute and more suitable for use in the application where the camera stays less or more horizontal.

For copying the original image with the Laplacian Pyramid shape or Pyramidal Gaussian, the conversion of an image into coordinates is done based on the technique of multi-resolution pyramid for creating an image with similar size that has reduced bandwidth. A spatial blurring effect known as Scale-Space is achieved on the original image and is ensured the invariance of the points of interest in scale.

To representing the image comparison and invariant similarity, the SURF (Speeded Up Robust Features) technique is a robust and fast algorithm. Based on box filters, the estimation of operators is made rapidly in the SURF approach that allows to implement in real-time applications like recognition and tracking of objects. Two phases include in SURF such as:

• Extraction of feature
• Description of feature

Results and Discussion

Experimental Results:

Figure 1 show the input which is forged.

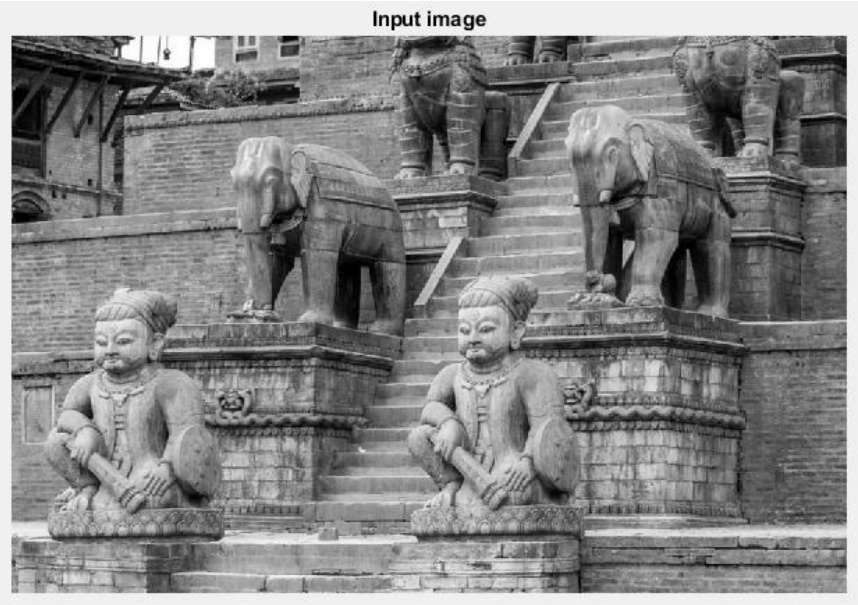

Fig.1 Input image

The figure 2 show the Super pixel segmentation result. Divide the image into approximately 600 super pixels and these super pixels are saved for further enhancement.

Figure Super pixel segmentation image

Figure 2 shows the feature point matching. By combining the resnet, shift and surf features into one local point to achieve higher accuracy to match the features in forged image

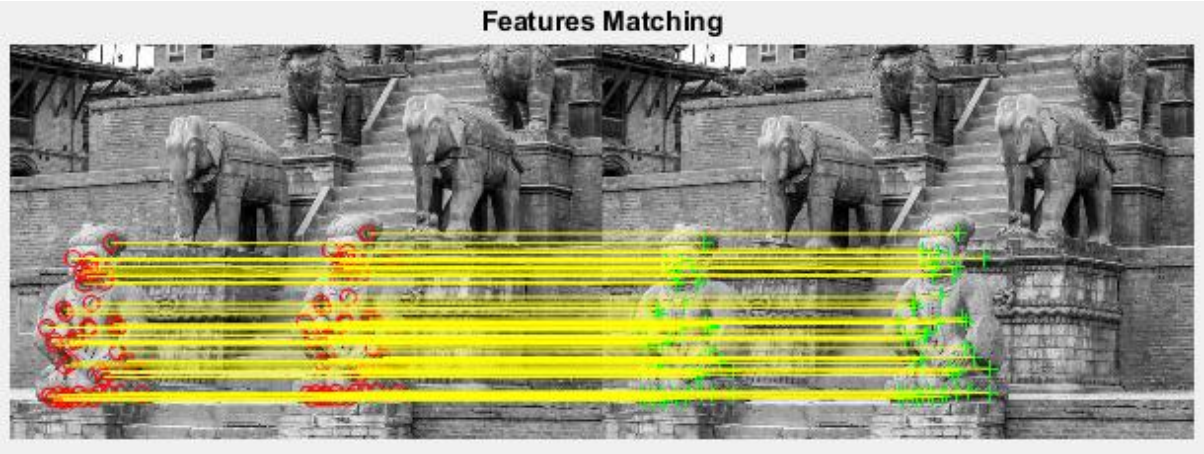

Fig 2. Feature point matching

Figure 3 show the detection of forgery part. After matching the feature points, the image is binarized and marked for showing the exact forgery part.

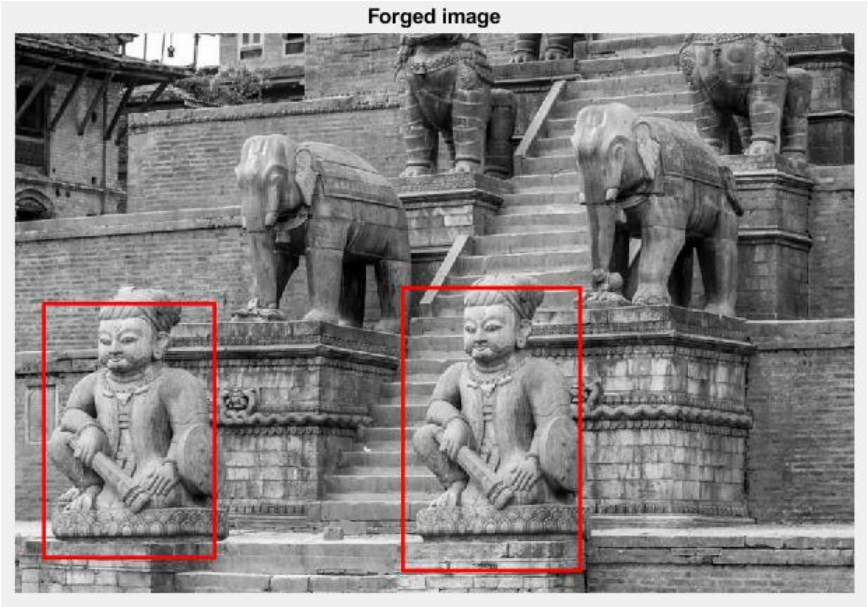

Fig 3. Forgery marked output image

Figure 4 shows the Elapsed time, which is used to calculate how much time taken the algorithm to complete the task.

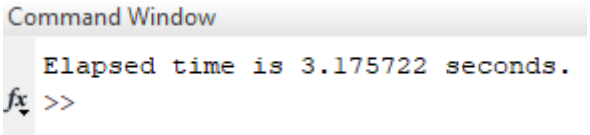

Fig 4. Elapsed time

Conclusion:

In this review, the forms discovering is focused that ensures the forgery detection in digital images. Here, the reduction of length dimension and determination of forged objects in the suspected image were concerned. For considering the similar objects in the forged image, SURF, SHIFT, and ResNet have utilized for feature extraction. From the findings, an

inference can be drawn and the proposed method marks the detected forgery picture for easier comprehension in addition to the effective detection of forgeries and locating the forged areas precisely. By comparing with the proposed method's detection efficiency based on the current standard forgery systems, the methodology findings are robust.

References:

[1] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy– move forgery in digital images," in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, Aug. 2003.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[3] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Proc. 18th Int. Conf. Pattern Recognit. (ICPR), Aug. 2006, pp. 746– 749.

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 1750–1753.

[5] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic Sci. Int., vol. 171,nos. 2–3, pp. 180–189, 2007.

[6] X. B. Kang and S. M. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Comput. Sci. Softw. Eng., Dec. 2008, pp. 926–930.

[7] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy–move forgery," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2009, pp. 1053–1056.

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2009, pp. 25–29.

[9] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, "Fast and robust forensics for image regionduplication forgery," Acta Automat. Sinica, vol. 35, no. 12, pp. 1488–1495, 2009.

[10] H. J. Lin, C. W. Wang, and Y. T. Kao, "Fast copy–move forgery detection," WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.

[11] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copyrotate-move forgery using Zernike moments," in Information Hiding. Berlin, Germany: Springer-Verlag, 2010, pp. 51–65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments,"IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1355–1370,Aug. 2013.

[13] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2011, pp. 1880–1883.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of copy– move forgery in digital images using SIFT algorithm," in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272–276.

[15] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[16] Sushma Pulidindi, K. Kamakshaiah and Sagar Yeruva, A Deep Neural Network on Object Recognition Framework for Submerged Fish Images, ISBN :978-981-15-0978-0, LNDECT, volume 37(2020), pp 443-450.