# A Robust Region Duplication Detection Scheme for Digital Video

**Mrs. Jayashree Kharat*, Dr. Sangeeta Chaugule**
*Department of Electronics Engineering, DKTE's Textile and Engineering Institute,*
*Ichalakranji, 416115, India*
**Email: jayashree2k2@gmail.com; corresponding author*

***Abstract***

*This paper addresses the intra frame forgery detection problem in digital video. In the intra frame forgery, a part of the region or an object from the frame is copied and pasted at other location in the same frame or group of frames from the same video. This work proposes hybrid algorithm developed using Scale Invariant Transform (SIFT) and Random Sample Consensus (RANSAC) to address the issue. While performing the experimentation, it is assumed that a small object is copied from the frame pasted in same as well as across the consecutive frames in the video sequence. Also, various image processing operations such as rotation, scaling, compression, flipping are applied on the forged region before pasting at other position to check the robustness of the algorithm. The experimental results show that the proposed method outperforms with respect to detection accuracy and simulation time. The observed average detection accuracy is 99.56% and the simulation time is 0.0921 sec. which is better than other methods reported in the literature.*

***Key words:*** *Video Forgery; Intra-frame Forgery; RANSAC; SIFT; Geometrical attacks.*

## Introduction

In the digital era the multimedia is playing vital role in the current affairs. In this pandemic situation, everything has become online. Almost everyone is now taking the help of online sites such as FACEBOOK, TWITTER, GOOGLE, YOUTUBE for entertainment, education, health and fitness, knowledge up gradation, information sharing, online business and many more to list. To quote the example, in INDIA there are 265 million active users for YOUTUBE onlay while for FACEBOOK the number of users is 270 million. This statistic indicates the popularity of those online sites among the society. To reduce the crime in banking, schooling and other public sectors, the government has made the CCTV compulsory. All these online information sharing tools are really very helpful for the day to day life activities of the human being. For example, a large number of educational videos with animation are available on YOUTUBE which the students can access easily to understand the complex concepts by the visualization. There are so many advantages of those sites. But this has darker side too. Unfortunately, there are cruel minds in societies which uses such sites as medium to perform the destructive things. Those people modify the contents of the video/image that coveys the important information to mislead the opinion of the society about that activity.

The people may change the objects, persons, audio clipping in the video to convey the wrong information through it. For example, in most of the times, the police take the help of CCTV footage during the investigation of the crime. But the person who is involved in crime may change the contents of the video to hide the presence of the criminal. Hence any digital media in the form of image or video cannot be treated as authentic proof as it may have undergone manipulations. Thus, it has become vital to verify the integrity of the digital information before trusting it.

The process by which the videos are modified is called as video forgery. Manipulation of the video has



ISSN: 2233 -7857 IJFGCN

become very easy due to easily available video editing software's such as Photoshop, Adobe Premier, Pro CC, and KineMaster etc. These software are freely available online and very easy to handle. Hence a novice user can use this software to edit the video.

Two types of manipulations can be done in digital video namely spatial tampering and temporal tampering. A brief information of both the types of tampering attacks is given below.

***Spatial/Intraframe tampering***

In this type, the manipulation is done at frame level. The part of object/region is copied from the frame and pasted across other successive frames of the same video. The figure 1 demonstrates the concept of spatial tampering. Figure 1 (A) represents the authentic frames of the test video in which the car is getting parked. Figure 1 (B) represents the tampered frame sequence in which the car is copied, compressed in size and pasted before the original car which visualizes as two cars are running on the road.


Figure 1 (A): Authentic Frames of videos.


Figure 1 (B): Forged Frames of videos.

Figure 1: Example of Spatial Tampering

***Temporal/Interframe tampering***

In this type, the manipulation is done on the sequence of the frames. A set of frames of video is duplicated at some other position in the same video. Figure 2 demonstrates the example of the temporal tampering. Figure 2 (A) shows the frame sequence from original video. Figure 2 (B) represents the frames from forged video in which the frame numbers 21-23 are pasted in between 5$^{th}$ and 6$^{th}$ frame location.


Figure 2 (A): Authentic Frames of videos.


Figure 2 (B): Forged Frames of videos.

Figure 2: Example of Temporal Tampering.

Video forensic is the branch of forensic science which intends to find out the techniques to detect the forgery in digital video. There are two techniques available in literature.

*Active forensic method*

In this technique the predefined symbols such as watermark, digital signatures are entrenched in the



ISSN: 2233 -7857 IJFGCN

digital video at the time of capturing. The main limitation of these techniques is that, to add the watermark, the camera with special hardware is required which is costly.

*Passive forensic method*

In this technique the characteristics of videos are studied and explored to detect the forgery. These techniques are referred as passive blind techniques, because for these techniques, the source video is not required to find the tampering. Hence these techniques are getting more popular those days.

This paper proposes the passive blind forgery scheme to identify and locate the spatial forgery in the video. The method uses the hybrid combination of SIFT and RANSAC to identify the manipulation.

The rest of the paper is organized as: section 2 takes the overview of the related methods used for region duplication detection. In section 3, proposed method is explained in detail. The simulation results and result analysis are presented in section 4. In the last section conclusion of the work and future scope is discussed.

**Related Work**

The spatial forgery detection process is similar to the image forgery detection. Only the difference is, in spatial forgery, the attack is done on the moving set of frames. Hence the algorithms used for image forgery detection can be extended to detect the spatial forgery in digital video. In image forensic two approaches are proposed namely keypoint based and block-based approach. In both the approaches, the prominent features are extracted from the image. These features are then compared to check the similarity between the features. If features are matched the corresponding image is treated as forged image. Most of the researchers have used feature point algorithms such as FFT, DCT, SURF, SIFT, DWT to extract the features from the image while for matching the features, clustering algorithms such as K-means clustering, g2nn, KD-tree etc. are used. While exploring the image copy move forgery detection problems, few researchers have considered geometrical transformation like rotation, jpeg compression, noise addition. [6-18]. Over past two decades, the image forensic has got the full attention and lots of research has been done in this field. But video forensic still is not fully explored. There are many gaps which requires to pay attention. The pioneer work in video forgery detection is done in 2007 in which authors have used correlation coefficient as feature to measure the spatial and temporal similarity between the frames of test video. As the proposed method performs frame wise comparison, the simulation time of the method is high. Also, the detection accuracy of the said method is low for the small sized forged object [19]. The next work in literature suggests block-based approach to discover the spatial and temporal forgery by Histogram of Gradient (HOG) features. The accuracy of the said method is good but the simulation time is very high. [20] The authors in [21] have used Scale Invariant Future Transform (SIFT) and K-NN clustering algorithm to detect the spatial forgery. The proposed method is tested on very limited dataset. The noise properties of spatially collocated regions of the frame are used to detect the forged area in [22]. The same concept is further explored in [23] in which inconsistencies of noise characteristics are recorded to detect the forged area. In [24], the authors have proposed block-based method which uses EMF features to find the similarity between the objects. To increase the detection accuracy, AFCT algorithm is used to remove the false matches obtained in first step of detection. In [25], the authors have used keypoint based approach to find the forged region in present frame and then spatiotemporal context learning is used to detect and locate forged area in successive frames. Further in [26], the authors have considered regular as well irregular shaped object detection. Error frame is constructed by subtracting the vectors of current and previous frames. The error frame is converted into binary frame by writing 1 for duplicate region and 0 for authentic region. To locate the duplicate region in the frame, the binary frame is ANDed with forged frame. Optical flow is used as feature in [27] to detect the forgery. The frames of the video are grouped as suspicious and innocent. Optical flow coefficient of each group is calculated.



ISSN: 2233 -7857 IJFGCN

If the secondary peaks are found in the optical flow coefficient then that segment is treated as forged. From the above discussion, it is clear that, while designing the algorithm along with detection accuracy other parameters like computational time, various geometrical transformations, position of camera, size of the region are also very important. In this paper, we suggest the algorithm to find the intra frame forgery in digital video. While addressing this issue following cases are considered:

- An object is copied from the frame and pasted at same frame as well as consecutive frames of the same video.
- Following attacks are applied on the forged region to check the robustness of the proposed method
  - Rotation
  - Scaling
  - Brightness variation
  - RGB
  - Multiple copy paste
  - Shearing
  - No transformation

**Proposed Method**

The flowchart shown in figure 3, shows the steps used to detect the region duplication forgery in video. To find the tampered area in frame of test video, first the video is transformed into frames. Then the SIFT key points of individual frame are extracted and matched to find the tampered region. Finally, RANSAC homography matching is used to remove false positive. The detailed algorithm is discussed in following sub-sections.



ISSN: 2233 -7857 IJFGCN

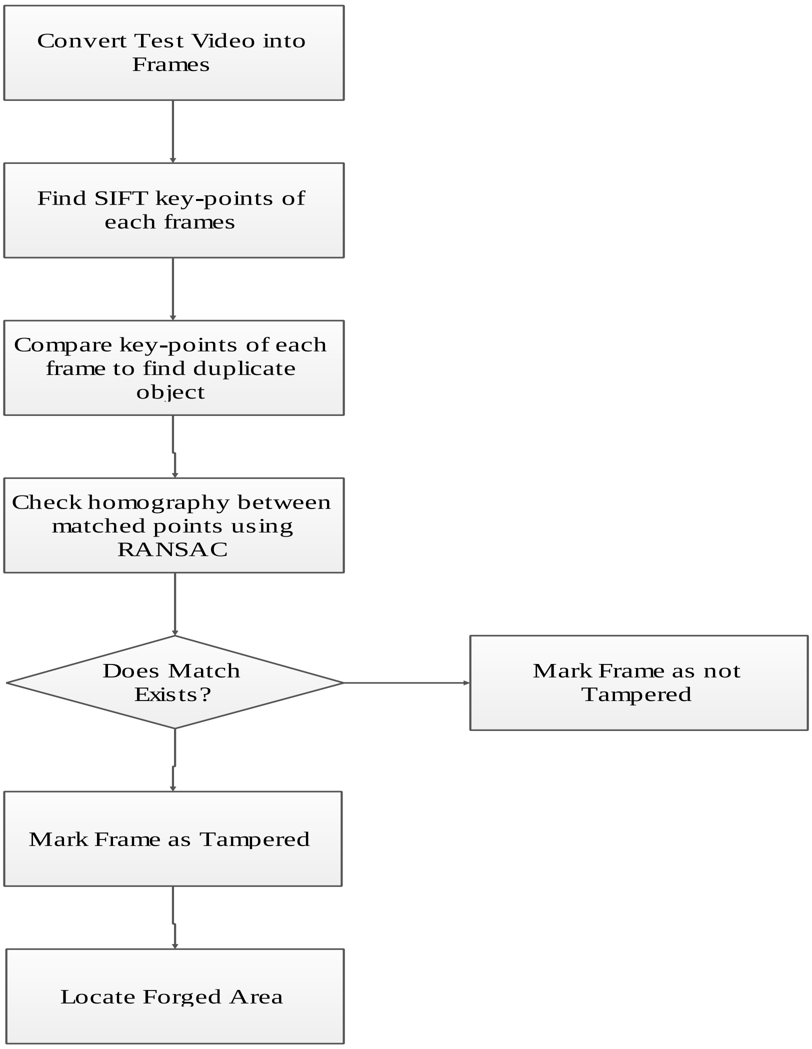


**Figure 3.** Flowchart of Proposed Method

**Scale invariant feature transform (SIFT)**

This is very popular key point-based algorithm of computer vision mostly used to detect and describe local features of the image [28].

**Process of SIFT implementation**

The SIFT algorithm is implemented in four steps which are discussed in short in following subsequent sections.

*Scale space extrema detection*

This is the first stage of calculation and used to search overall scales and image locations. The scale space images are obtained by first selecting the original image and by creating progressively blurred out images. This set of scale space (i.e. blurred images) is called as 1$^{st}$ Octave. Then, the original image is resized to half size and again blurred images are generated. This set of scale space is called as 2$^{nd}$ Octave. This process is repeated to generate octaves. The total number of octaves and scale depend on the size of the original image. In this case 5 octaves are generated. The blurring of an image is done with the help of Gaussian blur operator. This can be done as follows: The scale space of an image is defined as a function of $L(x, y, \sigma)$ this is obtained by Eq. (1), in which the input image $I(x, y)$ is convolved with variable scale Gaussian $G(x, y, \sigma)$. In this process scale space and DoG images are generated which are of great use for finding key-points.



ISSN: 2233 -7857 IJFGCN

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \qquad (1)$$

Where, * is convolution operation in x and y

$$G(x, y, \sigma) = \frac{1}{2\Pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \qquad (2)$$

$$D(x, y, \sigma) = G(x, y, k\sigma) - G(x, y, \sigma) * I(x, y) = L(x, y, k\sigma) - L(x, y, \sigma) \qquad (3)$$

Next step is to find a stable key-points. To detect stable key-points, each pixel is compared with its all neighbors. The checking is carried out for the current image, image above and below of the current image. As shown in Figure 4, let X be the current pixel and green circles are the neighbors of X. In this way, total 26 checking will be done to find the keypoint. `X` will be marked as a key-point if it is the greatest or least of all its 26 neighbors. In general, non-maxima or non-minima pixels won`t go through all 26 checking's. A few initial checking is sufficient to discard it. As lower and uppermost scales don't have enough neighbors, it becomes difficult to detect key-points for them and hence they are skipped.

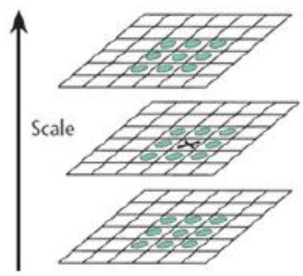


**Figure 4.** Key-point detection process

*Key-point localization*

The previous steps finalize the Stable key-points, but these key-points may lie between the pixels and we can`t access the data between the pixels. Hence there is a need to detect sub-pixel location. These sub-pixels are detected by using available pixel data with the help of Taylor series expansion given in Eq.4

$$D(X) = D + \frac{\partial D^{T}}{\partial X} X + \frac{1}{2} X^{T} \frac{\partial^2 D}{\partial X^2} \qquad (4)$$

Where, D and its derivatives are evaluated at the sample point X = (x, y, σ) T. From the above step, sufficient key-points are generated. Some of them lie on edges or some of them don 't has enough contrast. These key-points are not used as features. To discard such keypoints Harris corner detector is used. Low contrast features are removed by simply checking their intensity levels.

*Key-point descriptor*

This is the last step used to create a feature for each key-point. Around each key-point of local image, gradients are measured for each scale. These are transformed into a representation that allows for significant levels of local shape distortion and change in luminance.

**Matching between the features**



ISSN: 2233 -7857 IJFGCN

Once the SIFT features are extracted using above algorithm, the next step is of feature matching. To decide the matched pairs of features, the angle between features are compared. If this angle is less than the predefined threshold value, then these features are considered to be matched. After the many experimentation phases, the threshold we have kept is 0.65. The angle is calculated by dot product of coordinates of SIFT features.
The dot product is given as

$$a.b = |ab^T| \qquad (5)$$

Here $b^T$ stands for the b transpose. We have to check whether the nearest neighbor has angle less than distance ratio.

$$a.b = |a||b|\cos\theta \qquad (6)$$

Now apply inverse cosine transform to the dot product and match the nearest neighbor.

Though, through above procedure we get the matched pairs of key points, there are chances of getting some false matched pairs as some identical points may present in frame due to similar objects of the frame. This leads to the false positive rate means authentic region will be detected as forged region which directly affect the detection accuracy of the algorithm. To remove this false positive rate, RANSAC is used.

**Random sample consensus (RANSAC)**

RANSAC is unsupervised algorithm used for clustering. To apply RANSAC, minimum four matches are required between the clusters. Homography, H is estimated by randomly picking any four points from matched points. All the remaining matched points are transformed according to H and compared in terms of distance with respect to their corresponding matches. Distance metric used for RANSAC is as follow

$$d = \sum_{i=1}^{NUM} min\big(D(p_{ib}\ \varphi(p_{ia}: H), t)\big) \qquad (7)$$

Where $p_{ia}$ and $p_{ib}$ are the points in cluster a, b respectively. ($p_{ia}$: H) represents the projection of point $p_{ia}$ of cluster based on transformation matrix H, t is the threshold value and NUM represent the number of points. The points with distance greater than t are termed as inliers while others as outliers and are discarded. [29, 30]

**Result Discussion**

To check the performance of the proposed method, the experimentation is carried out on total 35 forged videos. The performance of the proposed method is measured in terms of two parameters namely detection accuracy and simulation time taken to detect the forged region. In this section we will discuss in detail the simulation results.

**Details of dataset**

For the experimentation, the test video data available from [] is taken. The dataset consists of forged videos with various attacks. The attacks considered in this paper are namely rotation, brightness variation, scaling, RGB, shearing, multiple and no transformation etc. Multiple attack means it is the combination of two attacks. Before pasting the object, it is modified using two attacks may be rotation plus scale down. No transformation means, the object is not modified, it is pasted as it is.
In order to check the sturdiness of the proposed method, the location of the attack in the test video is also varied. The attack is present in consecutive first 1-30 or 1-50 frames, middle 1-30 frames or last 1-20 frames. All the test videos are of varying frame size (around 100 to 560 frames per video) and



ISSN: 2233 -7857 IJFGCN

varying resolution (320*240, 1280*720, 640*780).

The table 1 explores the test video data used for the experimentation. The type of video, resolution, no of forged frame and the type of attack used are listed in detail. Total 44 test videos are used to check the performance of the proposed method.

**Performance Parameters**

To analyze the performance of the proposed forgery detection algorithm following performance parameters are used in this work.

$$Precision\ Rate = \frac{TP}{TP + FP}$$

$$Recall\ Rate = \frac{TP}{TP + FN}$$

$$Detection\ Accurcy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where, TP = Authentic is detected as Authentic
TN = Forged is detected as Forged
FP = Authentic is detected as Forged
FN= Forged is detected as Forged



ISSN: 2233 -7857 IJFGCN

| Sr. No | Test Video | Total No of frames | Forma t of Video | Size of frames | No of forged frames | Type of Attack | Details of Attack |
|---|---|---|---|---|---|---|---|
| 1. | T1R | 172 | AVI | 640X36 0 | 1 -30 | Rotation | Degree of rotation is 30 to $180^0$ |
| | T2R | 172 | AVI | 640X36 0 | 1-30 | | |
| | T3R | 259 | MP4 | 960X54 0 | 3-27 | | |
| | T4R | 259 | MP4 | 960X54 0 | 3-27 | | |
| | T5R | 101 | AVI | 960X54 0 | 1-34 | | |
| | T6R | 101 | AVI | 960X54 0 | 1-50 | | |
| | T7R | 101 | AVI | 960X54 0 | 1-47 | | |
| 2. | T1RG | 259 | MP4 | 960X54 0 | 3-27 | RGB | The amount of RGB component is varied from 20 to 60% |
| | T2RG | 259 | MP4 | 960X54 0 | 1-25 | | |
| | T3RG | 104 | AVI | 960X54 0 | 1-41 | | |
| | T4RG | 104 | AVI | 960X54 0 | 1-25 | | |
| | T5RG | 104 | AVI | 960X54 0 | 1-25 | | |
| 3. | T1S | 98 | AVI | 960X54 0 | 3-27 | Scaling | The scaling factor is 10 to 80% |
| | T2S | 259 | MP4 | 960X54 0 | 1-25 | | |
| | T3S | 259 | MP4 | 960X54 0 | 1-50 | | |
| | T4S | 167 | AVI | 640X36 0 | 1-29 | | |
| | T5S | 163 | AVI | 640X36 0 | 1-28 | | |
| | T6S | 98 | AVI | 960X54 0 | 1-25 | | |
| | T7S | 102 | MP4 | 960X54 0 | 1-35 | | |
| | T8S | 104 | MP4 | 960X54 0 | 1-55 | | |
| | T9S | 104 | AVI | 960X54 0 | 1-25 | | |



ISSN: 2233 -7857 IJFGCN

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4. | TM1 | 172 | MP4 | 640X360 | 1-15 | Multiple | Maximum two attacks are combined on the same object. |
| | TM2 | 259 | MP4 | 960X540 | 1-25 | | |
| | TM3 | 104 | AVI | 960X540 | 1-25 | | |
| | TM4 | 104 | AVI | 960X540 | 1-25 | | |
| | TM5 | 200 | MP4 | 960X540 | 1-30 | | |
| 5. | TSH1 | 172 | AVI | 640X360 | 1-20 | Shearing | The amount of trimming of the object is 10 to 50% |
| | TSH2 | 259 | MP4 | 960X540 | 3-27 | | |
| | TSH3 | 104 | AVI | 960X540 | 1-20 | | |
| 6. | TB1 | 259 | MP4 | 960X540 | 3-27 | Brightness | The amount of brightness variation is 20 to 80% |
| | TB2 | 98 | AVI | 960X540 | 1-25 | | |
| | TB3 | 100 | MP4 | 960X540 | 5-30 | | |
| | TB4 | 104 | AVI | 960X540 | 10-40 | | |
| | TB5 | 104 | AVI | 960X540 | 10-64 | | |
| 7. | TNT1 | 172 | AVI | 640X360 | 1-30 | No Transformation | The objects are copied and pasted as it is without any attack. |
| | TNT2 | 172 | AVI | 640X360 | 1-30 | | |
| | TNT3 | 172 | AVI | 640X360 | 1-30 | | |
| | TNT4 | 98 | AVI | 960X540 | 1-25 | | |
| | TNT5 | 259 | MP4 | 960X540 | 51-75 | | |
| | TNT6 | 259 | MP4 | 960X540 | 100-124 | | |
| | TNT7 | 259 | MP4 | 960X540 | 209-258 | | |
| | TNT8 | 104 | MP4 | 960X540 | 1-30 | | |
| | TNT9 | 104 | MP4 | 960X540 | 1-40 | | |
| | TNT10 | 104 | MP4 | 960X540 | 46-85 | | |



ISSN: 2233 -7857 IJFGCN

International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 3856 -3874

Table 1: Details of Dataset

**Result analysis**

The proposed algorithm successfully detects and locate the tampered area in each frame. A detailed analysis of the results in terms of detection accuracy and simulation time for the test video with respect to attack is presented in following sections.

**In terms of Detection Accuracy**

The table 2 gives the detailed result analysis of all the videos used in experimentation. The figures indicated in table 2 (a) represents the parameters like false positive, false negative, true positive and true negative for each video. These parameters are used to calculate the final performance parameters like precision rate, recall rate and detection accuracy which are stated in table 2(b).

| Sr. No | Type of Attack | Test Video | Total no of Frames | No of Forged Frames | Forged detected as Forged (TN) | Forged detected as Authentic (FN) | Authentic detected as Forged (FP) | Authentic detected as Authentic (TP) |
|---|---|---|---|---|---|---|---|---|
| 1. | Rotation | T1R | 172 | 1 -30 | 1-30 | 0 | 0 | 142 |
| | | T2R | 172 | 1-30 | 1-30 | 0 | 0 | 142 |
| | | T3R | 259 | 3-27 | 3-27 | 0 | 0 | 235 |
| | | T4R | 259 | 3-27 | 3-27 | 0 | 0 | 235 |
| | | T5R | 101 | 1-34 | 1-34 | 0 | 0 | 67 |
| | | T6R | 101 | 1-50 | 1-50 | 0 | 1 | 50 |
| | | T7R | 101 | 1-47 | 1-47 | 0 | 0 | 54 |
| 2. | RGB | T1RG | 259 | 3-27 | 3-27 | 0 | 0 | 235 |
| | | T2RG | 259 | 1-25 | 1-25 | 0 | 0 | 235 |
| | | T3RG | 104 | 1-41 | 1-40 | 1 | 0 | 63 |
| | | T4RG | 104 | 1-25 | 1-23 | 2 | 0 | 79 |
| | | T5RG | 104 | 1-25 | 1-23 &25 | 1 | 0 | 79 |
| | | T6RG | 72 | 1-30 | 1-30 | 0 | 0 | 42 |
| 3. | Scaling | T1S | 98 | 3-27 | 3-27 | 0 | 0 | 74 |
| | | T2S | 259 | 1-25 | 1-25 | 0 | 0 | 234 |
| | | T3S | 259 | 1-50 | 1-50 | 0 | 0 | 209 |
| | | T4S | 167 | 1-29 | 1-29 | 0 | 0 | 138 |
| | | T5S | 163 | 1-28 | 1-27 | 1 | 0 | 135 |
| | | T6S | 98 | 1-25 | 1-25 | 0 | 0 | 73 |
| | | T7S | 102 | 1-35 | 1-35 | 0 | 0 | 67 |
| | | T8S | 104 | 1-55 | 1-55 | 0 | 0 | 49 |
| | | T9S | 104 | 1-25 | 1-25 | 0 | 0 | 79 |
| 4. | Multiple | TM1 | 172 | 1-15 | 1-13 &15 | 1 | 0 | 157 |



ISSN: 2233 -7857 IJFGCN

| Sr. No | Type of Attack | Test Video | Total no of Frames | No of Forged Frames | Forged detected as Forged (TN) | Forged detected as Authentic (FN) | Authentic detected as Forged (FP) | Authentic detected as Authentic (TP) |
|---|---|---|---|---|---|---|---|---|
| | | TM2 | 259 | 1-25 | 1-23 | 2 | 0 | 235 |
| | | TM3 | 104 | 1-25 | 1-24 | 1 | 0 | 79 |
| | | TM4 | 104 | 1-25 | 1-23 | 2 | 0 | 79 |
| | | TM5 | 200 | 1-30 | 1-30 | 0 | 0 | 170 |
| 5. | Shearing | TSH1 | 172 | 1-20 | 1-20 | 0 | 0 | 152 |
| | | TSH2 | 259 | 3-27 | 3-10 & 12-27 | 1 | 0 | 235 |
| | | TSH3 | 104 | 1-20 | 1-20 | 0 | 0 | 84 |
| 6. | Brightness | TB1 | 259 | 3-27 | 3-27 | 0 | 0 | 235 |
| | | TB2 | 98 | 1-25 | 1-23 | 2 | 0 | 73 |
| | | TB3 | 100 | 5-30 | 5-29 | 1 | 0 | 75 |
| | | TB4 | 104 | 10-40 | 10-38 | 2 | 0 | 74 |
| | | TB5 | 104 | 10-64 | 10-64 | 0 | 0 | 50 |
| 7. | No Transformation | TNT1 | 172 | 1-30 | 1-30 | 0 | 0 | 142 |
| | | TNT2 | 172 | 1-30 | 1-27 | 3 | 1 | 142 |
| | | TNT3 | 172 | 1-30 | 1-26 | 4 | 1 | 141 |
| | | TNT4 | 98 | 1-25 | 1-25 | 0 | 0 | 73 |
| | | TNT5 | 259 | 51-75 | 51-75 | 0 | 0 | 234 |
| | | TNT6 | 259 | 100-124 | 100-124 | 0 | 0 | 234 |
| | | TNT7 | 259 | 209-258 | 209-258 | 0 | 0 | 210 |
| | | TNT8 | 104 | 1-30 | 1-30 | 0 | 0 | 74 |
| | | TNT9 | 104 | 1-40 | 1-40 | 0 | 0 | 64 |
| | | TNT10 | 104 | 46-85 | 46-85 | 0 | 0 | 67 |

Table 2 (a): Performance parameters

| Sr. No | Type of Attack | Test Video | Recall Rate (%) | Precision Rate (%) | Detection Accuracy (%) | Average Detection Accuracy (%) |
|---|---|---|---|---|---|---|
| 1. | Rotation | T1R | 100 | 100 | 100 | 100 |
| | | T2R | 100 | 100 | 100 | |
| | | T3R | 100 | 100 | 100 | |
| | | T4R | 100 | 100 | 100 | |
| | | T5R | 100 | 100 | 100 | |
| | | T6R | 100 | 98 | 100 | |
| | | T7R | 100 | 100 | 100 | |
| 2. | RGB | T1RG | 100 | 100 | 100 | 99.36 |
| | | T2RG | 100 | 100 | 100 | |
| | | T3RG | 98.43 | 100 | 99.04 | |



ISSN: 2233 -7857 IJFGCN

| | | | | | | |
|---|---|---|---|---|---|---|
| | | T4RG | 97.53 | 100 | 98.07 | |
| | | T5RG | 98.75 | 100 | 99.04 | |
| | | T6RG | 100 | 100 | 100 | |
| 3. | Scaling | T1S | 100 | 100 | 100 | 99.93 |
| | | T2S | 100 | 100 | 100 | |
| | | T3S | 100 | 100 | 100 | |
| | | T4S | 100 | 100 | 100 | |
| | | T5S | 99.26 | 100 | 99.38 | |
| | | T6S | 100 | 100 | 100 | |
| | | T7S | 100 | 100 | 100 | |
| | | T8S | 100 | 100 | 100 | |
| | | T9S | 100 | 100 | 100 | |

| **Sr. No** | **Type of Attack** | **Test Video** | **Recall Rate (%)** | **Precision Rate (%)** | **Detection Accuracy (%)** | **Average Detection Accuracy (%)** |
|---|---|---|---|---|---|---|
| 4. | Multiple | TM1 | 99.36 | 100 | 99.41 | 99.23 |
| | | TM2 | 99.15 | 100 | 99.61 | |
| | | TM3 | 98.75 | 100 | 99.04 | |
| | | TM4 | 97.53 | 100 | 98.07 | |
| | | TM5 | 100 | 100 | 100 | |
| 5. | Shearing | TSH1 | 100 | 100 | 100 | 99.87 |
| | | TSH2 | 99.58 | 100 | 99.61 | |
| | | TSH3 | 100 | 100 | 100 | |
| 6. | Brightness | TB1 | 100 | 100 | 100 | 99.00 |
| | | TB2 | 97.33 | 100 | 97.96 | |
| | | TB3 | 98.68 | 100 | 99 | |
| | | TB4 | 97.36 | 100 | 98.08 | |
| | | TB5 | 100 | 100 | 100 | |
| 7. | No Transformation | TNT1 | 100 | 100 | 100 | 99.54 |
| | | TNT2 | 97.93 | 99.3 | 98.25 | |
| | | TNT3 | 97.24 | 99.29 | 97.10 | |
| | | TNT4 | 100 | 100 | 100 | |
| | | TNT5 | 100 | 100 | 100 | |
| | | TNT6 | 100 | 100 | 100 | |
| | | TNT7 | 100 | 100 | 100 | |
| | | TNT8 | 100 | 100 | 100 | |
| | | TNT9 | 100 | 100 | 100 | |
| | | TNT10 | 100 | 100 | 100 | |

Table 2 (b): Performance parameters



ISSN: 2233 -7857 IJFGCN

The table 2 (b) represents the three important parameters used to verify the performance of the proposed method. The parameters are listed for each video of all the attacks separately. From these figures it is clear that detection accuracy of the proposed method ranges between 97 to 100%. The last column of the table denotes the average detection accuracy for each attack. The average detection accuracy for each attack is in between 99-100%. Figure 5.9 is the graphical representation of average detection accuracy for each attack. The average detection accuracy of the proposed method including all the attacks is equal to 99.56% which quite impressive as compared to other methods reported in literature.

**In terms of Simulation Time**

| Sr. No | Type of Attack | Test Video | Simulation Time (Seconds) | Average Simulation Time (Seconds) |
|---|---|---|---|---|
| 1. | Rotation | T1R | 0.119 | 0.084 |
| | | T2R | 0.057 | |
| | | T3R | 0.014 | |
| | | T4R | 0.013 | |
| | | T5R | 0.125 | |
| | | T6R | 0.124 | |
| | | T7R | 0.129 | |
| 2. | RGB | T1RG | 0.024 | 0.078 |
| | | T2RG | 0.014 | |
| | | T3RG | 0.127 | |
| | | T4RG | 0.123 | |
| | | T5RG | 0.123 | |
| | | T6RG | 0.058 | |
| 3. | Scaling | T1S | 0.035 | 0.080 |
| | | T2S | 0.052 | |
| | | T3S | 0.049 | |
| | | T4S | 0.060 | |
| | | T5S | 0.055 | |
| | | T6S | 0.036 | |
| | | T7S | 0.106 | |
| | | T8S | 0.128 | |
| | | T9S | 0.203 | |
| 4. | Multiple | TM1 | 0.059 | 0.27 |
| | | TM2 | 0.039 | |
| | | TM3 | 0.065 | |
| | | TM4 | 0.035 | |
| | | TM5 | 0.567 | |
| 5. | Shearing | TSH1 | 0.112 | 0.049 |
| | | TSH2 | 0.013 | |
| | | TSH3 | 0.023 | |
| 6. | Brightness | TB1 | 0.053 | 0.045 |
| | | TB2 | 0.041 | |
| | | TB3 | 0.063 | |
| | | TB4 | 0.023 | |
| | | TB5 | 0.045 | |
| 7. | No Transformation | TNT1 | 0.053 | |
| | | TNT2 | 0.053 | |



ISSN: 2233 -7857 IJFGCN

| | | | | |
|---|---|---|---|---|
| | | TNT3 | 0.053 | 0.039 |
| | | TNT4 | 0.031 | |
| | | TNT5 | 0.013 | |
| | | TNT6 | 0.015 | |
| | | TNT7 | 0.034 | |
| | | TNT8 | 0.014 | |
| | | TNT9 | 0.115 | |
| | | TNT10 | 0.017 | |

Table 3: Simulation Time

Table 3 represents the total simulation time taken by the test video to detect and locate the forgery. The time is recorded in seconds. The last column of the table represents the average simulation time recorded for all the attacks. The average simulation time required for all the test videos is 0.0921sec which is quiet less as compared to other methods reported in the literature.

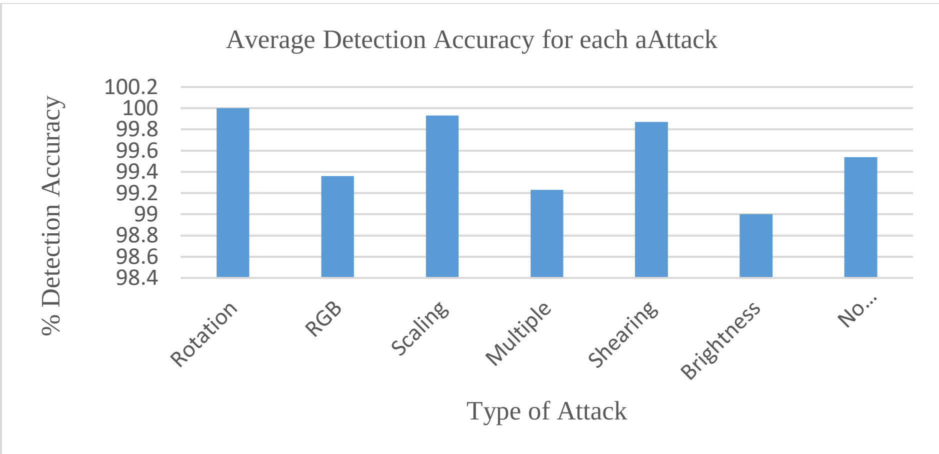


Figure 5: Graphical Representation of Detection Accuracy for all attacks

**Simulation results**

This section presents the simulation results of the proposed method. The figures (6-12) represent the pictorial form of detection results for all the mentioned attacks. While displaying the results, for each case one test video is selected. The figure (6-12) represents consecutive five frames of the test video indicating the existence of attack. The blue lines indicate the matching between original object and its copied version.

**Figure 6.** RGB attack

**Figure 7.** Rotation Attack



ISSN: 2233 -7857 IJFGCN

International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 3856 -3874

**Figure 8.** Scaling Attack

**Figure 9.** Shearing attack

**Figure 10.** Multiple attack (combination of scaling and flipping)

**Figure 11.** Brightness attack

**Figure 12.** No Transformation

The figure (6-12) clearly demonstrate that the proposed method successfully detects and locates the forged object in all the successive frames of the test video even if it has undergone the geometrical transformation. It proves the robustness of the method against various types of attacks.

**Performance analysis with respect to detection accuracy**

The table2 shows the comparative analysis of the proposed method with existing methods reported in literature in terms of detection accuracy.

| Sr. No | Author | Algorithm Used | Detection Accuracy (%) |
|---|---|---|---|
| 1 | Wang | Correlation Coefficient | 70 |
| 2 | Subrammanum | HOG Features | 89.7 |
| 3 | Su | Exponential-Fourier Moments | 93 |
| 4 | Su-Li | Modified MISIFT | 92.6 |



ISSN: 2233 -7857 IJFGCN

| | | | |
|---|---|---|---|
| 5 | Sigh | Correlation Coefficient | 96.6 |
| 6 | Proposed Method | SIFT and RANSAC | 99.56 |

**Table 4.** Performance analysis of proposed method with existing methods in terms of detection accuracy

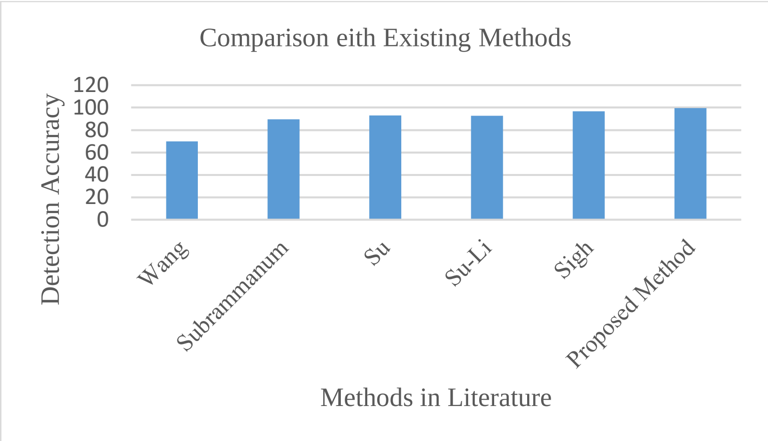


Figure 13. Bar Graph indicating the performance analysis of proposed method with existing methods**.**

From figure 13, it is clear that the detection accuracy of the proposed method is quiet high as compared to existing methods in literature highest as compared to other methods. This highlights the effectiveness of the proposed method.

**Performance analysis with respect to simulation time**

Table 5 shows the comparison of average simulation time taken by the proposed method and others existing methods to detect the region duplication forgery.

| Sr. No | Author | Algorithm Used | Simulation Time (Sec) |
|---|---|---|---|
| 1 | Wang | Correlation Coefficient | 418.833 |
| 2 | Subrammanum | HOG Features | 883.83 |
| 3 | Su | Exponential-Fourier Moments | 204.66 |
| 4 | Su-Li | Modified MISIFT | 84 |
| 5 | Sigh | Correlation Coefficient | 0.714 |
| 6 | Proposed Method | SIFT with RANSAC | 0.0921 |

**Table 5.** Comparative Analysis of proposed method with existing methods in terms of simulation time

The figures indicated in Table 5 underlines that; the total simulation time of the proposed method is very small as compared to existing method which is highly important factor for real time applications of forgery detection.

**Conclusion**

This paper presents novel region duplication forgery detection scheme in digital video which studies the attack in which the object is copied and pasted from a frame and in consecutive frames of the same



ISSN: 2233 -7857 IJFGCN

video. The sift features along with RANSAC are used to identify tampered frames and to mark the duplicated objects. In order to make the forgery operation tough to detect by naked eyes, different types of attacks such as rotation, scaling, compression, shearing are used on the forged object before pasting it at other location. The robustness, simulation time and the accuracy of detection of forged region is proved to be very great through the various experiments conducted on 35 forged videos. The average accuracy of detection is 99.56% and simulation time is 0.0921sec which is quite better than the other methods reported in literature. This paper addresses the attack in which the forged object is present in successive frames which belong to same GOP. In future, the work will be extended to locate the forged region present in the frames from different GOP

**REFERENCES**

1. H. Yin, W. Hui, H. Li, C. Lin, and W. Zhu, "A Novel Large-Scale Digital Forensics Service Platform for Internet Videos," IEEE Transactions on Multimedia, vol. 14, pp. 178-186, 2012.
2. K. Sitara, B. M. Mehtre, “Digital video tampering detection: An overview of passive techniques”, Digital Investigation 18 (2016) 8e22
3. S. Milani, M. Fontani, P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi, and S. Tubaro, “An overview on video forensics,” APSIPA Transactions on Signal and Information Processing, vol.1, 2012.
4. S. Upadhyay and S. K. Singh, “Video authentication: Issues and challenges,” International Journal of Computer Science, vol. 9, no. 1-3, pp. 409–418, 2012.
5. Pradeep K. Atrey, Wei-Qi Yan and Mohan Kankanhalli, “A scalable signature scheme for video authentication”, Springer Journal of Multimedia Tools and Applications, 34(1): 107-135, July 2007
6. T. Stütz, F. Autrusseau, and A. Uhl, "Non-blind structure-preserving substitution watermarking of H. 264/CAVLC inter-frames,” IEEE Transactions on Multimedia, vol. 16, pp. 1337-1349, 2014.
7. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A sift-based forensic method for copy-move attack detection and transformation recovery,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
8. V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches”, IEEE Transactions on information forensics and security 7 (6) (2012) 1841-1854.
9. R. C. Pandey, S. K. Singh, K. Shukla, R. Agrawal, “Fast and robust passive copy-move forgery detection using SURF and SIFT image features”, in 9th International Conference on Industrial and Information Systems (ICIIS), 2014 IEEE, 1-6, 2014.
10. Ardizzone, A. Bruno, G. Mazzola, “Copy-move forgery detection by matching triangles of key points”, IEEE Transactions on Information Forensics and Security 10 (10) (2015) 2084-2094.
11. J. Li, X. Li, B. Yang, X. Sun, “Segmentation-based image copy-move forgery detection scheme”, IEEE Transactions on Information Forensics and Security 10 (3) (2015) 507-518.
12. S. Prasad, B. Ramkumar, “Passive copy-move forgery detection using SIFT, HOG and SURF features”, in IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), IEEE, 706-710, 2016
13. W. Li and N. Yu, “Rotation robust detection of copy-move forgery,” in Proc. IEEE International Conference on Image Processing ICIP’10, 2010, pp. 2113–2116
14. T. Van Lanh, K. Chong, S. Emmanuel, and M. Kankanhalli, “A survey on digital camera image forensic methods,” in Proc. IEEE International Conference on Multimedia and Expo ICME’07,



ISSN: 2233 -7857 IJFGCN

2007, pp. 16–19.
15. X. Pan and S. Lyu, “Region duplication detection using image feature matching,” IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.
16. Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra, “A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery”, IEEE Transaction on Information Forensic and Security, Vol. 6, No. 3, September 2011.
17. Yuanman Li, Jintao Zhou, “Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching”, IEEE Transaction on Information Forensic and Security, Vol. 14, No. 5, May 2019.
18. G. Jin and X. Wan, “An improved method for SIFT-based copy move forgery detection using Non-maximum value suppression and optimized J-linkage”, Signal processing: Image Communication, 2017, doi.10.2016/j.image.2017.05.010
19. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," in Proceedings of the 9th workshop on Multimedia & security, pp. 35-42, 2007.
20. V. Subramanyam and S. Emmanuel, "Video forgery detection using HOG features and compression properties," in IEEE International Workshop on Multimedia Signal Processing, pp. 89-94, 2012
21. Ramesh Chand Pandey, Sanjay Kumar Singh and K.K. Shukla, “Passive Copy- Move Forgery Detection in Videos,” 5th International Conference on Computer and Communication Technology, ICCCT-2014, PP.301-306.
22. C.-C. Hsu, T.-Y. Hung, C.-W. Lin, and C.-T. Hsu, "Video forgery detection using correlation of noise residue," in IEEE 10th Workshop on, Multimedia Signal Processing, pp. 170-174, 2008.
23. M. Kobayashi, T. Okabe, and Y. Sato, "Detecting video forgeries based on noise characteristics," in Advances in Image and Video Technology, Springer, pp. 306-317, 2009.
24. L.Su, C. Li, Y. Lai & J. Yang, “A Fast Forgery Detection Algorithm based on Exponential-Fourier Moments for Video Region Duplication”, IEEE Transactions on Multimedia, doi.10.1109/TMM.2017.2760098.
25. L. Su, C. Li, “A novel passive forgery detection algorithm for video region duplication”, Multidimensional systems and signal processing, vol, 29, pp, 1173-1190, 2018, doi.10.1007/s11045-017-0496-6.
26. Gurvinder Singh, Kulbir Singh, “Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation”, Multimedia Tools and Applications, pp. 1-36, 2018, doi.org/10.1007/s11042-018-6585-1



ISSN: 2233 -7857 IJFGCN