VIDEO DUPLICATE AND FORGED FRAME DETECTION USING TWO-FOLD OPTICAL FLOW AND CORRELATION

A.Raja Jinu [1], C.K.Suryaraj [2]

[1]*PG student, Department of ECE, Ponjesly College of Engineering, Nagercoil,Tamil Nadu, India.*

[2]*Assistant Professor, Department of ECE, Ponjesly College of Engineering, Nagercoil,Tamil Nadu, India.*

ABSTRACT

Video compression technologies were frequently employed to minimize the enormous size of video data. However, because of lossy reduction, it also generates unpleasant visual artifacts. Compression methods like H.264 and HEVC were used to minimize the memory space and bandwidth due to the growing volume of video data available through the Internet. Many compression artifact elimination methods have been presented to produce artifact-free pictures in the previous decades to acquire good quality images/videos on the decoding side. The research uses a two-fold video authenticating system that detects and locates both frame replication and frame forging in videos. A Lucas-Kanade-based Optical flow detection technique is designed for compression as well as artifact minimization to enhance the performance of compressed videos. The technique divides each video outline into suspicious and accurate parts initially. As a result, every part records an optical stream coefficient. During video forgery identification, feature extraction, matching, and sorting are also employed. The efficiency of the proposed technique is demonstrated by significant test findings on the Mpeg4 standard database. Manually constructed filtering and sparse coding-based approaches have already been suggested as solutions to resolve such problems.

Keywords: *Video compression, Optical flow, Lucas-Kanade algorithm, Forged frame detection, Correlation*

1. INTRODUCTION

Digital video communications is a fast-changing industry, particularly because of the advances in video coding. As a result of this improvement, a wide range of video applications have emerged, including videoconferencing, High-Definition Television (HDTV), including the transmission of real-time video through multimedia[1]. The demand for such media has skyrocketed as a result of the introduction of multimedia applications; yet, storing and manipulating it in its raw state is exceedingly expensive, which considerably doubles transmission time and memory costs [2]. If an analog video stream is digitized, it could use up to 165 Mbps of bandwidth. Typically surveillance systems rarely have to join the networks with some other data-intensive applications, and uncompressed video data transmission via digital networks necessitates the highest bandwidth [3]. To solve such difficulty, video compression methods were developed to lessen the number of bits necessary to encode digital

Video data while retaining appropriate fidelity as well the video quality. The compressing ratio measures its capacity to complete the task. The higher the compressing ratio, the lower the bandwidth consumption [4].

Images are data intensive that include a lot of redundancies, which could be reduced by using a transformation with such a reversible linear stage to de-correlate the image input pixels. To comprehend video formats, one must first comprehend video features and how certain features were employed to define the framework [5]. A video is a series of images that are exhibited in chronological directions. A frame is a name given to every one of these images. Video compressing techniques won't encode every one of the data within the video; several of the features will be missed since, one cannot detect minor modifications inside the frames, such as a slight alteration in color [6]. Conventional methods can be reversed in some cases. It is a fundamental need for several applications which demand excellent quality.

Video forgery is now much simpler, while video content validation becomes more complex. As a result, the source and authenticity of footage may no longer be assumed [7]. Video forensics has become highly relevant for such purposes, particularly while digital video information has been used for legal purposes [8]. How believable audio-visual personation is created in front of the camera is through recognition of staged video containing natural ballistic trajectories. Digital video forgery could yield a variety of shapes; Figure 1 depicts the traditional interpretation. Inter-frame and intra-frame video forging techniques have been easily categorized. The phrases inter- and intra-frame are used to differentiate temporal from spatial forging. Inter-frame forging is done at the sequence level: separate frames' pixels are unaffected, however, the sequence as anentire is altered [9].

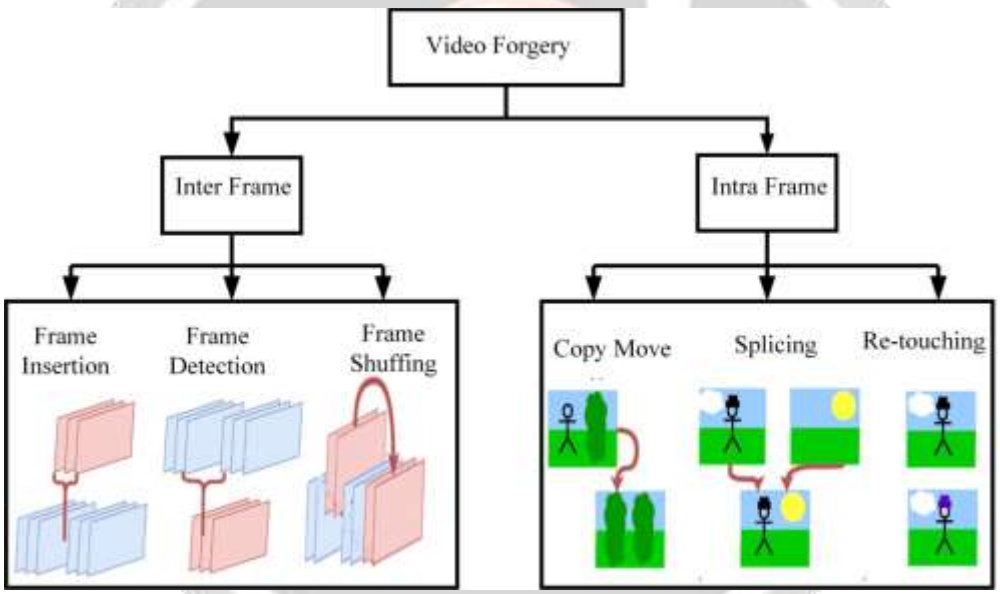

Fig -1: Various video forgery types

Intra-frame forging is done at the pixel level: specific spatial regions are changed, but the changes are time-correlated to create a plausible forged region. In mainstream media, there are video clips of fraudulently manipulated content that are remarkably effective in disseminating fabrication across social networking sites. Conventional inter-frame tampering, which hides modifications, can reorganize events and even eliminate or replace them from the chronology, however, its content-altering consequences were limited [10]. Retouching temporally or spatially up-scaled content, or adding global filters to increase perceptual quality, could change the appearance of content by affecting each pixel in a video sequence. Retouching could be used in specific areas as well. Intra-frame forging as well as some other objects forgeries that include in-painting, as well as motion transfer, can change content and context. Finally, it is possible to create synthetic movies or synthetic regions. In contrast to past animations, today's synthetic content appears to be convincingly realistic [11].

The availability of digital video as well as digital image modifying software has made reliable authentication of multimedia content difficult. Even a beginner can quickly erase an element from a video sequence, add an element from some other video file, or integrate an element created by a graphics program designer because of current manipulation techniques and the continuous multimedia development [12]. It's getting harder to tell the difference between a genuine video and one that's been tampered with. The rest of the

section represents the recent literature of existing work on video forgery detection and video compression, followed by the proposed methodology, results and discussions and finally the conclusion.

2. RELATED WORKS

The study recommends the passive strategy of combining the Neighborhood Binary Angular Pattern (NBAP) also the Polar Cosine Transform (PCD) having the GoogleNet framework for detection and localizing multiple counterfeits in the video.The pre-processing technique separates frames from input videos and converts them from a three dimension RGB color space to a 2-Dimensiongray level area. PCT and NBAP techniques are used for the extraction feature. The collected features will be placed on an already trained GoogleNet model to detect video fraud. Both intra-frames, as well as inter-frame forgery, could be detected using the recommended approach in the video. Also, although the video is subject to distortion exposure, the recommended approach is strong enough to tolerate multiple duplicates in the video. With multiple fake identities, the forecast accuracy reaches a high percentage. Experiential results further reveal that the recommended approach resists noise addition and is not affected by the length or video background of the GOP framework. The operating time of the recommended technique is also calculated and it is significantly shorter than the current modern approaches. Despite all efforts, the recommended method for watching real-time video is not particularly effective [13].

Another study [14] provides a passive blind technique for detecting frames and partial duplication in images using two separate approaches. By measuring the correlation between sorting and finding the average characteristics of every video frame, the technique identified these three types of copy-moved frame copies in the images. The study examined the creation of irregular and regular areas within the similar frame in other stages, as well as the creation of one or more series frames of the same video from another frame in the same area. Because of the tiny variation in pixel intensities in the copied area and the excellent connection with the original area, it's difficult to identify this copy-move forgery. The suggested system's second technique has recognized these copy-moved areas duplicating forgery in videos by finding the mistake with a threshold procedure and calculating the similarity among areas of two frames or inside the damaged frame. These research findings reveal that the recommended technique is more predictive and time-consuming than the most recent algorithms with acceptable performance. This technique is difficult to use for large sets of datasets.

A histogram-based technique is described in [15], which is computationally efficient and improves the accuracy of the classification. It generates histograms from frames with system properties represented using the local binary pattern (LBP). The histogram cross-sectional comparison tool is used to estimate the histogram similarities of neighboring LBP index frames. The variations between suchneighboring metric factors offer useful forgery detection indicators, which were then normalized and measured toward creating a constant-length feature vector. It increases the usefulness of the provided method for variable-length films by making it accessible. SVM classifier with RBF kernel is used for training and validation. Interframe forgery such as incorporation, identification and duplication can all be detected using this technique. Experimental findings show that high detection performance can effectively identify various types of inter-frame video fraud. There is also a comparison with existing interframe duplication identification techniques. This method can give erroneous results for large volumes of data.

The study [16] provides an effective approach for locating 'suspicious' frames also then localizing the CMF in the frame called VFDHSOG, which is dependent upon Histograms of the secondary order gradients. After getting a binary image of a frame, the correlation coefficients of the HSOG features are computed to detect a 'suspicious' frame. The Surrey University Library for Forensic Analysis (SULFA), SYSU-OBJFORGED databases, and Video Tampering Database (VTD) are used to evaluate performance. SULFA contains video streams of various grade levels, such as q10, q20, and so on, all of that reflect greater compression. Both inter and intra-frame forgeries are available in the VTD database. The SYSU dataset includes assaults such as rotating and scaling. With the capability to differentiate assaults like scaling up/down and rotational, the total accuracy is high. This process is complex for computing multiple attacks.

The passive approach to video fake identification described is dependent upon the correlation consistency among entropy-coded frames. The study uses an entropy-based system property that includes two-dimensional multiscale entropy (MSE2D) as well as two-dimensional distribution entropy (DistrEn2D).The system has four steps and can detect multiple forgeries in videos. Pre-processing is the initial stage. The texture feature was taken from the video frames in the second step. Then, to identify multiple forgeries, the inter-frame correlation stability amongst entropy-coded frames is evaluated.Numerous forgeries were located in the video utilizing conflicting point detection in the final stage. An observational result reveals that the recommended

approach (using MSE2D and DistREn2D features) works best in detecting forgery in videos. This approach is not suitable for complicated forgeries videos [17].

Region duplicating forgeries is a widespread sort of video tamper, and typical approaches for detecting video tampering are useless and inefficient for fabricated videos against complicated backdrops. The study introduces a unique video forgery identification approach to address this problem. The input video streams are first gathered from the Sondos databases and SULFA (Surrey University Library for Forensic Analysis). Furthermore, the gathered video sequences are subjected to a spatiotemporal mean approach to produce background data having a range of moving objects for successful video counterfeit identification. The GoogLeNet framework is then used to identify the feature vectors, which is followed by extracting features.Next, usingCollaboration (UFS-MSRC) and Multi-Subspace Randomization with feature selection technique, the discriminative feature vectors that minimize trained time and enhance prediction accuracy. Lastly, the Long-Term Memory (LSTM) system is used to identify duplicates in various video sequences. In the SULFA and Sondos databases, the UFS-MSRC with the LSTM model achieved high accuracy, respectively, proving that the results obtained were better than the models with video forgery identification. It takes more time for processing the training sets and needs more memory [18].

3. PROBLEM STATEMENT

The technology utilized in the existing system is quite complex, and the number of errors made is enormous. The video quality has suffered as a result of the compressing procedure. The class of methods examines a visual property that includes pixel grey levels, image textures, noise and color modes properties to discover frame correlation. While using noise-based techniques, including MPEG-2 or H.264, the effectiveness of singular value decomposition (SVD), grey value, as well as histogram differences will suffer because of noise or filtering, although noise-based methodologies would suffer substantially while using conventional coding such as MPEG-2 or H.264.

4. PROPOSED METHODOLOGY

The two-fold detection procedure aids in determining the frames' consistency and correlation. The first method is to identify the forged frame using a feature matching technique, while the other method is to identify the duplicated frame using a Lucas Kanade-based optical flow method. The suggested system takes a video sequence in a suitable format as input. The frames should be first taken from the video sequence. Pixel blocks have been used to break video frames. Separate the grayscale image into overlapped blocks of a similar size. The DCT is applied to every block from left to right, top to bottom. Every DCT square block's Gaussian RBF kernel PCA-based features are retrieved. As a result, using a threshold-based region matching method, the feature matching and the sorting procedure is completed to identify the forged frames. Furthermore, the DCT split frames have been further examined using a Lucas-Kanade based Optical Flow method to determine the variation between two successive frames to find the duplicated frame. The correlation coefficient, which analyses the correlation of direct pixels in two frames is used to characterize the resemblance of frame images. To generate the compressed result, the copied and forged frames were removed from the original video file. The process of the proposed technique is depicted in Figure 2.

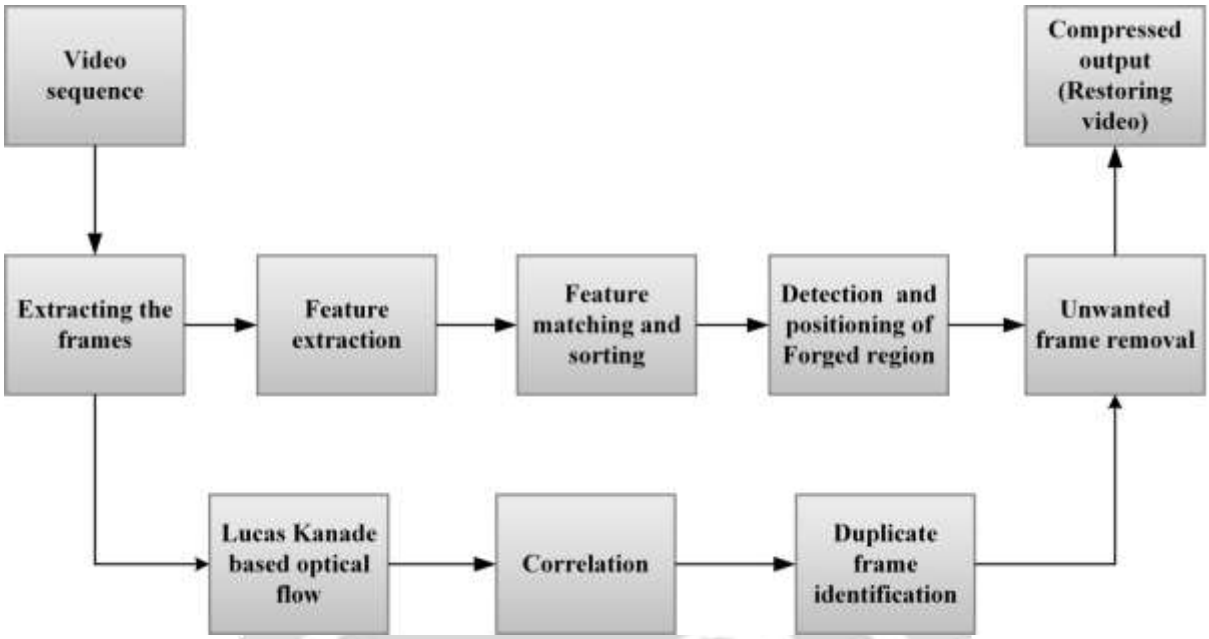

Fig -2: Compression and detection process

4.1 FEATURE MATCHING AND SORTING

Using a search distance method, feature matching finds equivalent features from two similar photos. With one image serving as the source and the other as the target, the feature matching approach has been used to both detect and retrieve and transfer characteristics from the source to the target image. After that, all of the photographs with similar features are sorted [19].

To identify the forged frames, a threshold-based region matching approach is being used during the feature matching and sorting phase. The reasoning for the threshold-based region matching is owing to the characteristics of counterfeited images that were subjected to post-processing processes; the chances of their being identical in terms of characteristics are almost non-existent. The forgery detection goal is to locate duplicated areas with a similarity measure across regions (feature vectors) lesser than a specific threshold with non-overlapping duplicated areas.

The shift distance criteria are utilized to address the first condition of Forgery detection, which is the matching among non-overlapping blocks. Considering (l_a,m_a) and (l_b,m_b) as the top left corner coordinates of the two blocks indicated by the features vectors f_a and f_b, respectively.

$$\forall\sqrt{(l_a-l_b)^2+(m_a-m_b)^2}\geq n_t \tag{1}$$

It is considered that those feature vectors for resemblance index computation to achieve the secondary condition of the Forgery detection when the two feature vectors satisfy the above eqn. (1). The Euclidean distance is used in this case and it is shown in Eqn. (2).

$$D(f_a, f_b)=\sqrt{\sum_{i=1}^{10}(f_{ai}-f_{bi})^2}<D_t \tag{2}$$

The technique generates a black map image with the portions that are judged for the duplication to be highlighted as the expected outcome to display the outcome of forgery detection.

4.2 LUCAS-KANADE ALGORITHM

The range of perceived motion speeds of brightness patterns in videos is known as optical flow (OF), and that could reveal a lot about the image spatial layout and object variation range. These have been frequently used in multimedia processing including computer vision fields, such as picture target tracking, segmentation, mosaic

creation, face coding and so on, due to their highly descriptive motion information. The most extensively utilized approaches for OF calculation in image sequences were differential techniques. The Lucas-Kanade Optical Flow is a sparsely computed Optical Flow using a local least square calculation. OF vectors generated using the Lucas-Kanade approach have been frequently employed due to their quick computation, ease of application, and resistance to noise [20].

In Lucas-Kanade OF fields, an instance of a video sequence is shown, together with the movement variation vectors of the relevant pixel among subsequent frames. The Optical Flow depicts the differences or resemblance of frames in video sequences that reveal the intricacies of motion variations in every frame. The correlation coefficient is used to represent the Optical Flow resemblance among frame images. The Lucas Kanade OF vector OFi is split into two figures: OLi in the L direction and OMi in the M direction, for two neighboring frames *Im* and i+1.N-1 OF vectors would be retrieved from a video of N frames and the correlation coefficients amongst each two Optical Flows could be determined. In an original movie, the correlation coefficients among each of the two OFs are modest since the OF records the movement change information of every equivalent pixel among multiple adjacent frames; the correlation coefficients between different OFs are comparatively low. However, in videos there will be a high connection between source frame OFs and replicated frame OFs due to copy-move forgery.

Consider an Image $Im(l,m)$. For smaller motion, the new image can be represented using Eqn. (3).

$$H(l,m) = \mathrm{Im}(l+a, m+b) \tag{3}$$

Where (a,b) represents the displacement of the pixel.

Solving this equation using Taylor's Expansion, the Lucas-Kanade equation (4) is obtained.

$$\begin{bmatrix} \sum Im_l Im_l & \sum Im_m Im_m \\ \sum Im_l Im_m & \sum Im_m Im_m \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = - \begin{bmatrix} \sum Im_l Im_t \\ \sum Im_m Im_t \end{bmatrix} \tag{4}$$

5. RESULT AND DISCUSSION

Initially, the input video is read from the folder. The video is then divided into the number of frames and as shown in figure 3.

Fig -3: Video frames

The optical flow is analyzed by comparing the correlation of each pixel in the frame with one another. It is shown in figure 4.

Fig -4: Correlation of each pixel in successive frame

The corners of the objects in the frames are found and then the values are partially differentiated in x and y directionsconcerning time. It is represented in figure 5.

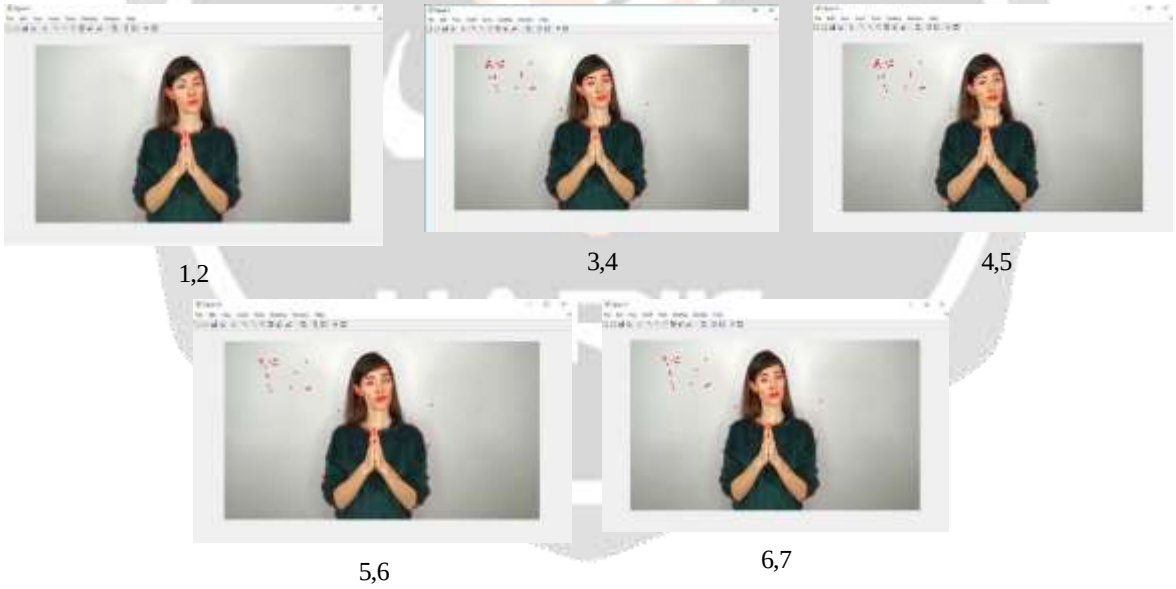

Fig -5: Determination of corner objects in successive frame

The forged frame detected using the feature matching mechanism is shown below in figure 6.

Fig -6: Detected forged frame

5.1 PERFORMANCE EVALUATION

The accuracy with which tampered portions of a video may be detected, i.e. pixel level efficiency determines an algorithm's usefulness. Tpos are successfully identified forged videos, Fpos are original videos that have been wrongly identified as forged, Tneghas forged images that have been incorrectly identified as actual videos, and Fneghave forged videos that have been falsely ignored. The following formulas are used to calculate Accuracy, Precision, Recall, and F-measure. Precision demonstrates the possibility that an identified forgery is fully a forgery; Recall estimates the proportion in which a forged video is observed and F1 score calculates the total effectiveness. Accuracy demonstrates the percentage of correct identification of forged frames, Precision has shown the possibility to a detected forgery is a forgery, Recall shows the possibility that a forged video is identified and F1 score represents the total effectiveness.

$$Accuracy(A) = \frac{T_{pos} + F_{pos}}{T_{pos} + F_{pos} + T_{neg} + F_{neg}} \tag{5}$$

$$\Pr ecision(P) = \frac{T_{pos}}{T_{pos} + F_{pos}} \tag{6}$$

$$\mathrm{Re}\,call(R) = \frac{T_{pos}}{T_{pos} + F_{neg}} \tag{7}$$

$$F - score = \frac{2PR}{P + R} \tag{8}$$

Table 1: The existing and proposed method'sperformance metrics

Method	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
SVM	96.68%	-	-	-
Coarse matching	-	82%	98%	84%
CNN	92.44%	92.54%	92.32%	92.43%
Optical flow	-	91.3%	93.2%	92.3%
Proposed	98.46%	98.82%	99.1%	98.24%

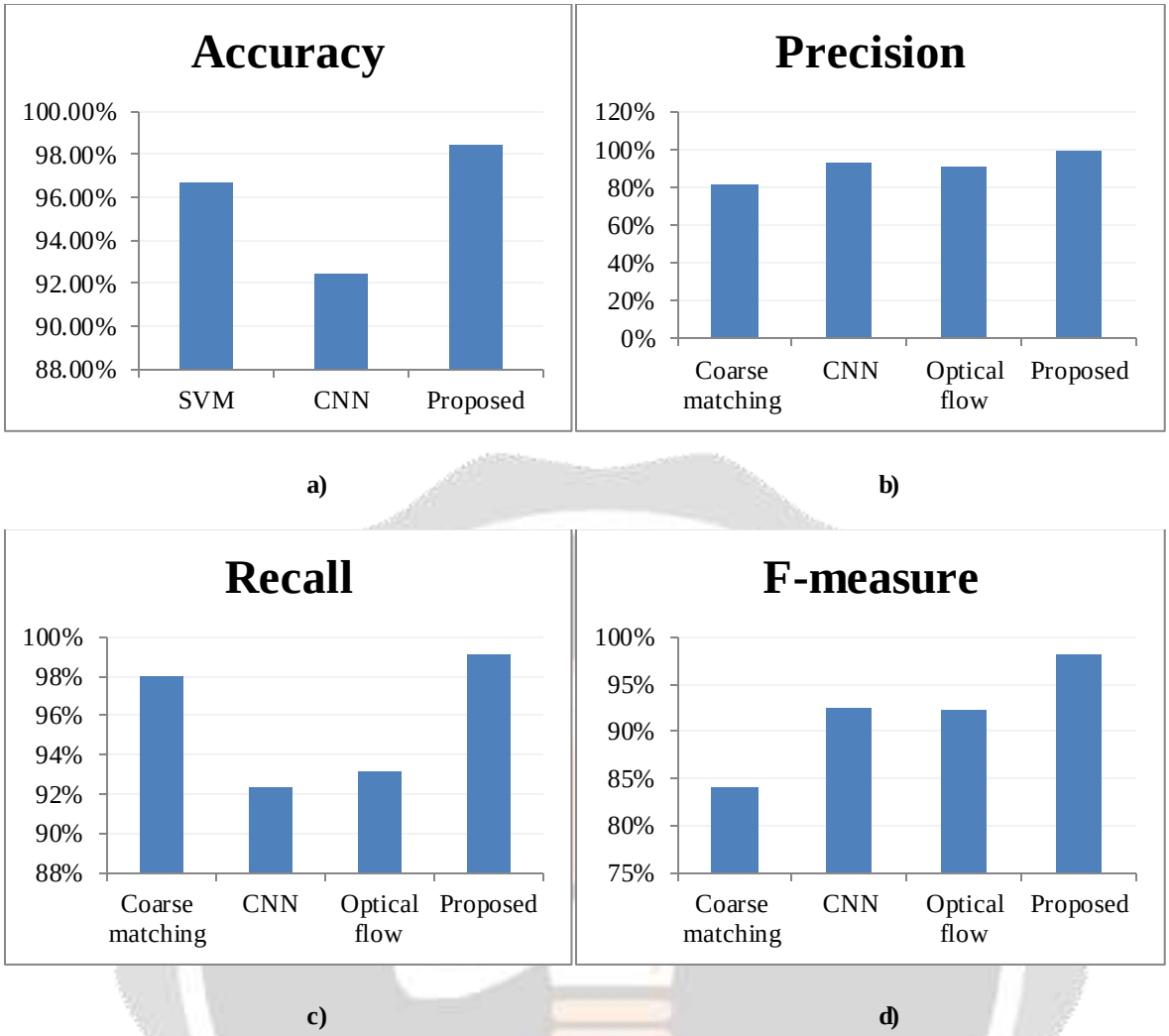

Fig -7: Comparison of a) Accuracy, b) Precision, c) Recall, d) F-measure

Table 1 and figure 7 represent the performance comparison of the existing methods like SVM, Coarse matching, CNN, Optical flow method,and proposed DCT+Lucas-Kanade optical flow mechanism in terms of accuracy, precision, recall, and F-score. It shows that the proposed method has higher accuracy of 98.46% as well as higher precision, recall and F-score valuecompared with the existing methods.

Table 2: Comparison of bitrate savings of the existing and proposed methods

Methods	Bitrate Savings
Backward Adaptive pixel-based fast Predictive Motion Estimation (BAPME)	3.78%
Background-modeling-based adaptive prediction (BMAP) method	1.13%
2D Markov Process	3.8%
Luca Kennedy (Optical Flow)	3.4%
Proposed	3.95%

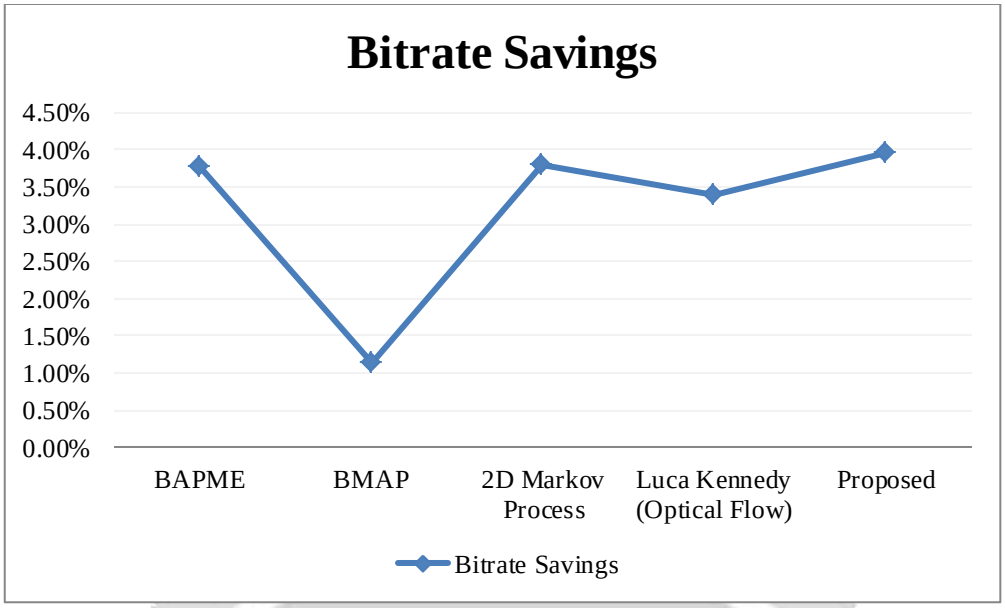

Fig -8: Comparison of existing and proposed methods in terms of bitrate savings

Table 2 and figure 8 represents the performance comparison of the existing methods like BAPME, BMAP, 2D Markov process, Luca Kennedy Optical flow mechanism, DCT-motion compensation method and proposed DCT+Lucas-Kanade optical flow mechanism in terms of bitrate savings. It shows, the suggested method has highest bitrate savings of 3.95% compared to existing techniques.

5.2 DISCUSSION

For computer vision-based devices, the technique includes a two-fold detection methodology. It demonstrates how to regulate video compression levels so that automated analyzers could examine the generated video and improve its detection effectiveness by conserving the areas of the scene which are more likely to generate significant material. The method is based on using a rapid objectness metric to compute correlation and consistency. This method's computational power makes it suitable for use in a real-time video coding process. Tests show that the approach beats H.265 in terms of speed and coding efficiency and that it may be used in a variety of video domains, including surveillance and web videos.

6. CONCLUSION

The study describes a new method for video compression based on hybrid optical flow and correlation, as well as a method for video fraud detection based on feature matching and sorting. Moreover, the proposed method somehow doesn't suffer from blocking artifacts or pixelation, resulting in much more visually appealing videos. The video output offers good performance and quality, and also a high compression ratio. The most latest video compression attempts have centered upon scalable video coding. The fundamental goals of an ongoing scalable video coding study were to accomplish compression effectiveness, flexibility (bandwidth scalability) and/or simplicity. Every scalable video coding method seeks tradeoffs on the three aspects of the contradictory nature of effectiveness, flexibility and complexity. Developers of video services must select a scalable video coding scheme that achieves the desired flexibility and efficiency at a reasonable cost and level of complexity. In terms of future research, devising implied flow without real bits consumption, including such decoder-side flow derivation or frame interpolation and extrapolation is an intriguing issue. Presently residue and intra-coding utilize the same system, which might be worth further examination for network simplicity. It's also crucial to extend the system to more complicated video data sets like 3D video and spectral video.

7. REFERENCES

[1] P. Ranganathan *et al.*, “Warehouse-scale video acceleration: co-design and deployment in the wild,” in *Proceedings of the 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, Virtual USA, Apr. 2021, pp. 600–615. doi: 10.1145/3445814.3446723.

[2] S. Kumar, Y. Badiyani, and S. Chaudhuri, "DeepQuantizedCS: Quantized Compressive Video Recovery using Deep Convolutional Networks," in *Proceedings of the 27th ACM International Conference on Multimedia*, Nice France, Oct. 2019, pp. 2396–2404. doi: 10.1145/3343031.3350965.
[3] H. He, Y. Gao, Y. Zheng, and Y. Liu, "Intelligent Power Grid Video Surveillance Technology Based on Efficient Compression Algorithm Using Robust Particle Swarm Optimization," *Wirel. Power Transf.*, vol. 2021, pp. 1–12, Dec. 2021, doi: 10.1155/2021/8192582.
[4] S. Pandit, P. K. Shukla, A. Tiwari, P. K. Shukla, M. Maheshwari, and R. Dubey, "Review of video compression techniques based on fractal transform function and swarm intelligence," *Int. J. Mod. Phys. B*, vol. 34, no. 08, p. 2050061, 2020.
[5] L. Jing, X. Yang, J. Liu, and Y. Tian, "Self-supervised spatiotemporal feature learning via video rotation prediction," *ArXiv Prepr. ArXiv181111387*, 2018.
[6] C.-Y. Wu, N. Singhal, and P. Krahenbuhl, "Video compression through image interpolation," in *Proceedings of the European conference on computer vision (ECCV)*, 2018, pp. 416–431.
[7] P. Johnston and E. Elyan, "A review of digital video tampering: From simple editing to full synthesis," *Digit. Investig.*, vol. 29, pp. 67–81, 2019.
[8] B. O. Beatrice O. Akumba, A. Aamo Iorliam, S. Agber, E. O. Okube, and K. D. Kwaghtyo, "Authentication of Video Evidence for Forensic Investigation: A Case of Nigeria," *J. Inf. Secur.*, vol. 12, no. 02, pp. 163–176, 2021, doi: 10.4236/jis.2021.122008.
[9] K. Sitara and B. M. Mehtre, "Digital video tampering detection: An overview of passive techniques," *Digit. Investig.*, vol. 18, pp. 8–22, 2016.
[10] K. Sitara and B. M. Mehtre, "Anti-Forensics for Image and Video Tampering: A Review," *Cryptogr. Inf. Secur.*, pp. 799–827, 2018.
[11] P. Johnston and E. Elyan, "A review of digital video tampering: From simple editing to full synthesis," *Digit. Investig.*, vol. 29, pp. 67–81, 2019.
[12] M.-H. Maras and A. Alexandrou, "Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos," *Int. J. Evid. Proof*, vol. 23, no. 3, pp. 255–262, 2019.
[13] N. A. Shelke and S. S. Kasana, "Multiple forgery detection and localization technique for digital video using PCT and NBAP," *Multimed. Tools Appl.*, pp. 1–29, 2021, doi: https://doi.org/10.1007/s11042-021-10989-8.
[14] G. Singh and K. Singh, "Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 11527–11562, 2019, doi: https://doi.org/10.1007/s11042-018-6585-1.
[15] M. Kaur and others, "Texture Feature Analysis for Inter-Frame Video Tampering Detection," in *Proceedings of International Joint Conference on Advances in Computational Intelligence*, 2022, pp. 305–318. doi: https://doi.org/10.1007/978-981-19-0332-8_22.
[16] P. S. Raskar and S. K. Shah, "VFDHSOG: Copy-Move Video Forgery Detection Using Histogram of Second Order Gradients," *Wirel. Pers. Commun.*, pp. 1–38, 2021, doi: https://doi.org/10.1007/s11277-021-08964-5.
[17] N. A. Shelke and S. S. Kasana, "Multiple forgeries identification in digital video based on correlation consistency between entropy coded frames," *Multimed. Syst.*, pp. 1–14, 2021, doi: https://doi.org/10.1007/s00530-021-00837-y.
[18] N. Girish and C. Nandini, "Inter-frame video forgery detection using UFS-MSRC algorithm and LSTM Network," *Int. J. Model. Simul. Sci. Comput.*, p. 2341013, 2022, doi: https://doi.org/10.1142/S1793962323410131.
[19] G. Singh and K. Singh, "Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 11527–11562, 2019.
[20] A. SB and P. V. Deepa, "COPY-MOVE FORGERY DETECTION IN VIDEO FORENSICS USING OPTICAL FLOW FOR COARSE-TO-FINE DETECTION".