Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 15 (2020) pp. 144-152

Tempo Temporal Forgery Video Detection Using Machine Learning Approach

Govindraj Chittapur[1], S. Murali[2] and Basavaraj Anami[3]

[1] Department of Computer Applications,
Basaveshwar Engineering College, Bagalkot 587102, India
gbcmc@becbgk.edu

[2] Department of computer science& Engineering,
Maharaja Institute of Technology, Belavadi,srirangpatna tq Mandya 571477, India
murali@mitmysore.in

[3] Department of Computer Science& Engineering,
KLE Institute of Technology, Hubli 580030, India
anami_basu@hotmail.com

Abstract: This research paper explore a new way of detecting video forging between frames and intraframes by referring to the correlation coefficient using a frame continuity relationship. For any given video set, a groundbreaking technique called the "Spatio Temporal copy" produces video forgery detection using a machine learning method based on the continuous correlation between the conjugative sequences and the group of frames from the forgery video. The proposed forgery detection algorithm aims to identify the sequence groups forged intermediately by referring to the SVM classifier. Changing in the video sequence can result in a different fingerprint than collected initially, either at the spatial or at the temporal levels. Awareness of the statistical features that add frame continuity is the foundation for developing our algorithm to identify the video forgery detection that creates the duplicate. In the sequential continuity of the forged structures, we successfully identified the copy-move and copy delete frames, combining spatial and temporal fingerprints in an orderly and systematic approach. By referring the forensic standard data sets such as SULFA, VTD, and REWIND, we have tested and obtained high accuracy results with prominent researchers in the forensic video area

***Keywords*: Spatio-temporal, video-forgery, SVM, machine learning, forensic data set,**

I. Introduction

Video content today can be easily edited by people with video editing tools such as Movie Maker, Adobe Premiere Pro, Avidemux, After Effects, and Adobe. Given the benefits of those devices, some community abuse them and recreate video events, add or erase video frame sequences to suppress evidence. The issue involves checking the reliability and credibility of inspection videos, particularly when they are used as vital sources of evidence in court. Confirmation systems can be achieved partly using surveillance tools, widely used to monitor crimes.

Digital footage recorders, particularly inspection cameras, are widely available in this technology-oriented world at any location that generates massive amounts of multimedia content. Also, The passion for technology in the younger generation increased mobile devices and video cameras and increased the amount of digital content collected and used for techno-social communication.

Digital videos also provide significant forensic evidence in various technological, legal, medical, and surveillance applications that make these applications highly dependent on the integrity of the visual material presented in such videos. The growing use of digital images in our everyday lives has also led to an increased usage of easy-to-use and affordable tools for video editing that improves digital video visual content. A person can, however, easily use such web editing tools to make unauthorized changes to digital content, known as forgery, creation it difficult to locate full trust in the integrity of such digital content.

For proof of evidential support, digital videos are their believable source of information for that it is essential to ensure that the visual content of a video under scrutiny has not been distorted post-production and is a credible representation of reality

Video forgery is very easy to perform, but without any advanced technology, it is challenging for a human eye to detect such forgeries. Monitoring and mobile video are very quickly generated. They are prone to forgery because it can be easily counterfeited by simply removing or inserting suitable frames from or in the respective images for the lack or presence of specific objects in the picture. This video is then used as false evidence—this reconstruction. The technology needed to detect such manipulated videos also demands significant improvements with the increased probability of such malicious operations.

Authenticity can not be taken for granted because digital videos have been distorted. This is definitely accurate, though, that editing a composite video requires time and is more complicated than editing a single frame. Not all video

falsification is equally as important; it could be less essential to alter celebrity video images than to change the video recording of crime in advance. The alterability of footage, though, undermines our collective understanding of dependable and trustworthy credibility. As modern video editing technology becomes rapidly advanced, a forensic technique becomes urgently required for the identification of video falsification. The following types of video manipulation can occur depending on the context in which manipulation is performed. Related tempering field scenario as shown in Fig 1 as (A) manipulation of the space domain (B) manipulation of time-domain (C) manipulation of space-time,

Figure 2(b) Shows a spatially manipulated video created from real footage of Figure 2(a) As shown in Figure 2(c), a falsifier may tame source videos by disrupting the frame by manipulation of pixel frames spatially. Sequence by replacing objects, inserting frames, and by deleting video files, and thereby generating momentarily disrupted videos. Finally, Figure 2(d) helps a forger to manipulate videos in a combination of both the spatial and the manipulate pixel bit within the video frame or via video frames (that is, a group of adjacent structures) as well as disrupting the frame sequence and creating spatially distorting videos.

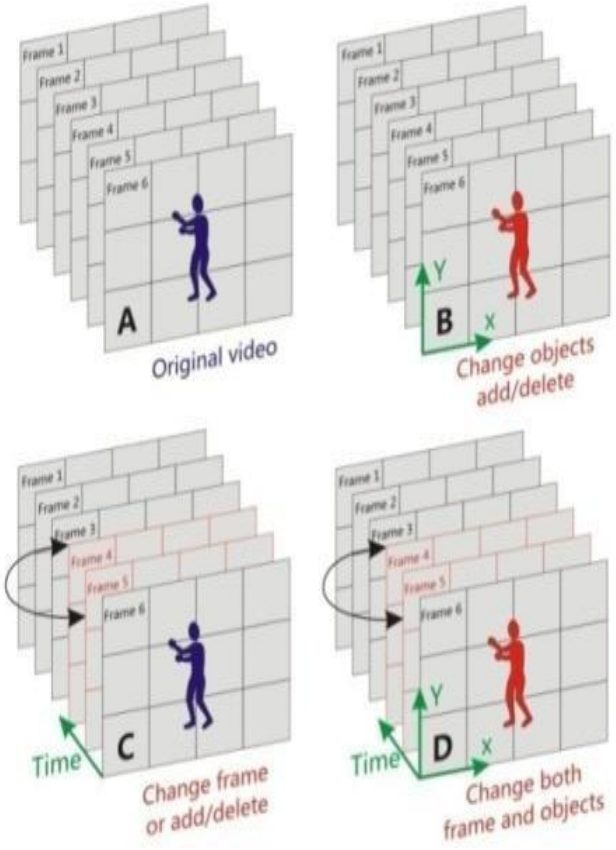

Fig 1. Scenario of Tempering Domain

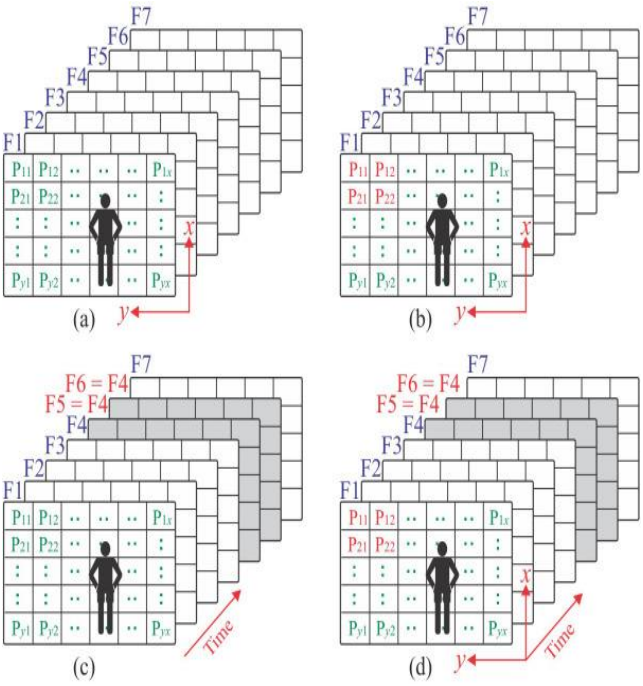

Fig 2. Different domain of forensic forgery video with reference as (a) set of Picture frames extracted from video(b) changes in the spatial features (c) changes in the temporal features (d) changes in Spatio-temporal features

II Literature survey

The literature survey revealed that significant contributions to the detection of video falsification were found, and researchers developed and suggested various video forensic methods for the detection of video forging using active and passive strategies. The following section discusses several influential contributions in the video forgery detection field.

Different methods to detect the presence of inter-frame forgery in the video sequence have been suggested in the literature. Such forgeries are usually done by first converting the video into a series of frames, then deleting, inserting, and replicating specific frames. Whenever a video is saved, some compression inevitably leads to double compression after a doctoral video is manipulated. Some significant prominent contributions in inter-frame forgery suggest by sondos M. Fadl as residue pointe[1] Extract the residue data from a video stream of each frame. Then spatial, along with temporal energies, are subjugated to exemplify data flow, and anomalous points identify phony frames. Noise ratios of original and forged frames are predictable to differentiate insertion from replication attacks. Similarly, motion residue-based work has been proposed by authors [2] to identify the forgery region in forgery video.

Hemani Sharma et al. [3][6],[10]., analyze and review the different classification and graph approaches used for video forgery detection.

Nugroho Satriyanto et al. [4]., projected a method based on locale video fake detection using the Gaussian mixture model for their suggestion. Jamimamul Bakas et al., [5] notice forgery based technique on double compression in MPEG videos and find the exact region of interference within the frames

Sanjay et al., [7] invented an object movement based on displacement paths is based on the optical flow inconsistency,

which considers picture motion for recognition and identification of clone. Using Dynamic Time Warping (DTW) matching algorithm to detect the cloned entity, the displacement paths are finally compared among themselves.P. Karthikeyan et al. [8,]., proposed a combination of mpeg2 and optical flow based forged scene detection.

Jayashree Kharat[9],[11]proposed frame duplication identification method using The 2-stage algorithm is suggested to identify doubtful frames and to extract their features and compare them with other frames in an examination video to build a decision. Scale-Invariant SIFT key points are used as an evaluation function.

III. Data set design issues

Using SULPA[13], REWIND[14], CVIP[15], and YTD[16] helped for copy-move and copy-paste tampering operations, we usually referred to it as copy-create video forgery, generating a data set from foreshadowed data set. We use the forensic dataset for testing and training using Support Vector Mchine(SVM) to classify forgery and unique by setting the parameter. In the following section explaining about the essential characteristics of the forensic dataset for the proposed implementation of copy create video forgery detection using machine learning approach.

Surrey University Library for forensic analysis (SULFA)[13]: It includes authentic and fake video files accessible via the University of Surrey website. Some 150 videos are obtained from various camera sources, including Fujifilm S2800HD, Nikon S3000, and CanonSx 220. Each video has a length of around 10 seconds, 320 into 240, and 30 frames per second resolution. All videos have time and space features. Figure 3 displays the SULFA[13] video gallery schematic view used for the proposed experiment.

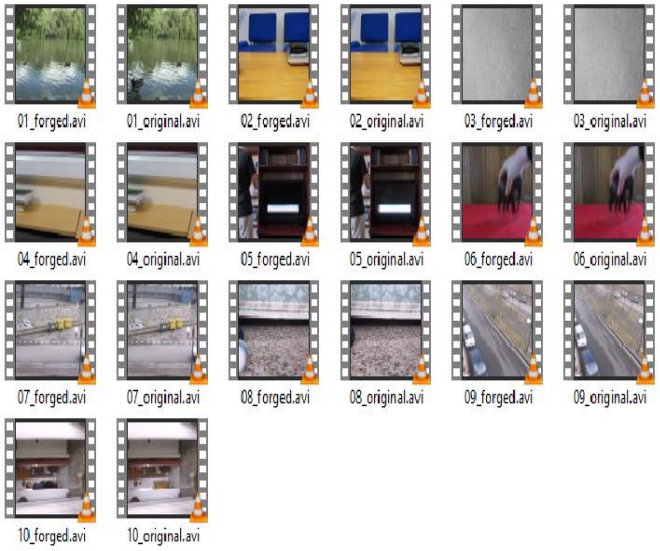

Fig 3: Schematic view of SULFA Dataset

Reverse engineering OF audiovisual content data (REWIND) [14]: This dataset consists of 20 SULFA videos: ten authentic and ten fake. Through route has a motion of 320x240 pixels and a frame rate of 30 fps. Single recorded sequences with a low-end device. They were all compacted in the initial frames in an uncompressed format (RV24, 24 bit RGB). To suit the entire device efficiently to the same level, they have all migrated to one file format in YUV (4:2:0). The percent scheme view of the lossless testing video gallery for our experiment is shown in Figures 4 to Fig 6.

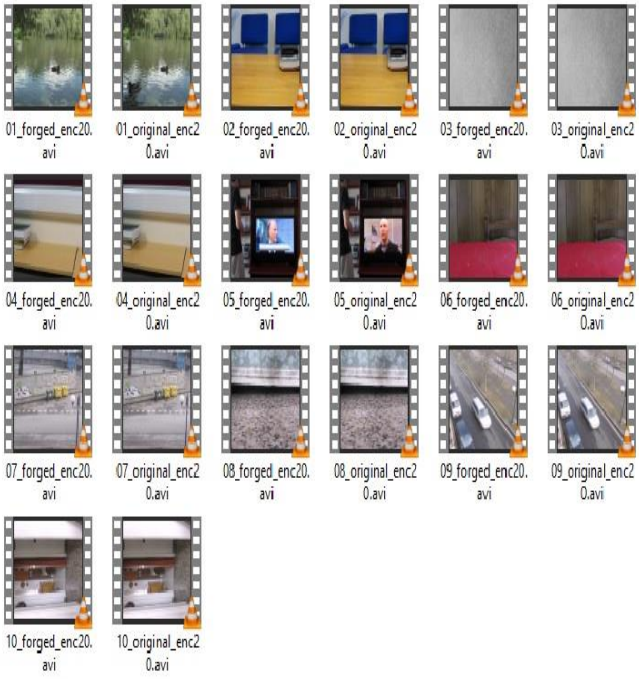

Fig 4: Schematic view Of REWIND dataset at quality factor set at 10

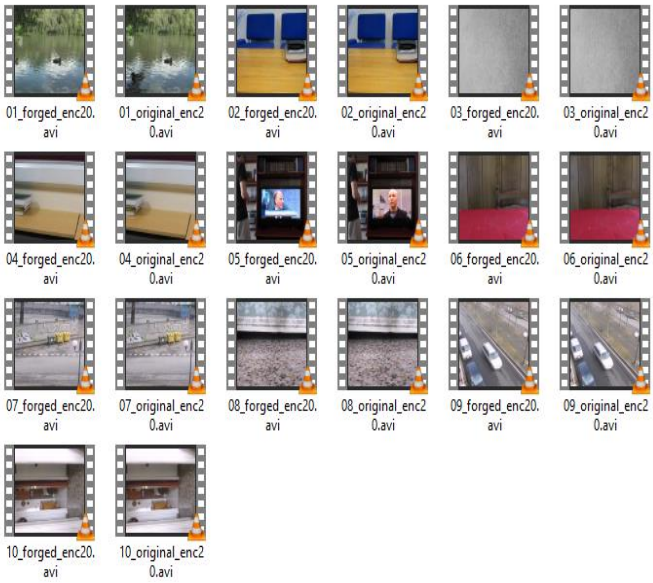

Fig 5: Schemetic view Of REWIND dataset at quality factors as 20

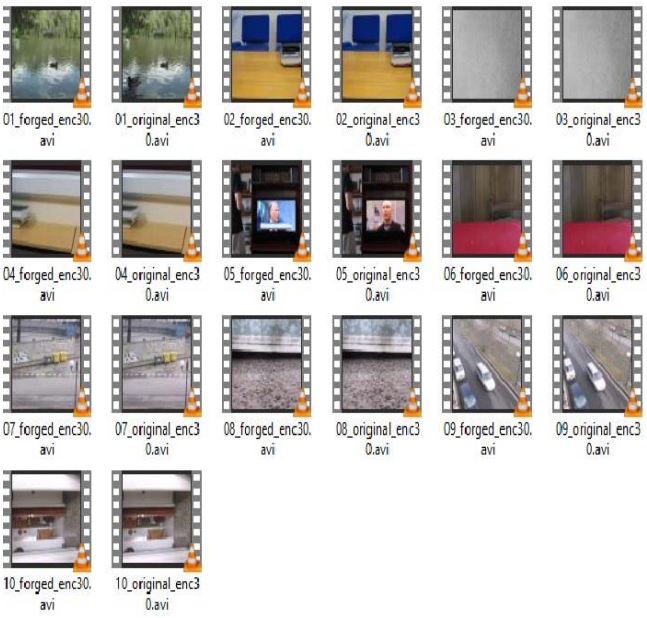

Fig 6: Schemetic view Of REWIND dataset at quality factors as 30

Video Tempering Data Set (VTD) [15]: The VTD, which focuses on the video manipulation of videos, consists of 33 16-size videos with a standard high-definition resolution of 30 fps. The original data set was divided into several unmodified segments with moving copies and pasting. We use the standard datasets above to construct a custom video to monitor the time-tempering video transformations on our proposed algorithm for manipulation and observation. A representative set of VTD set, as shown in Fig 7.

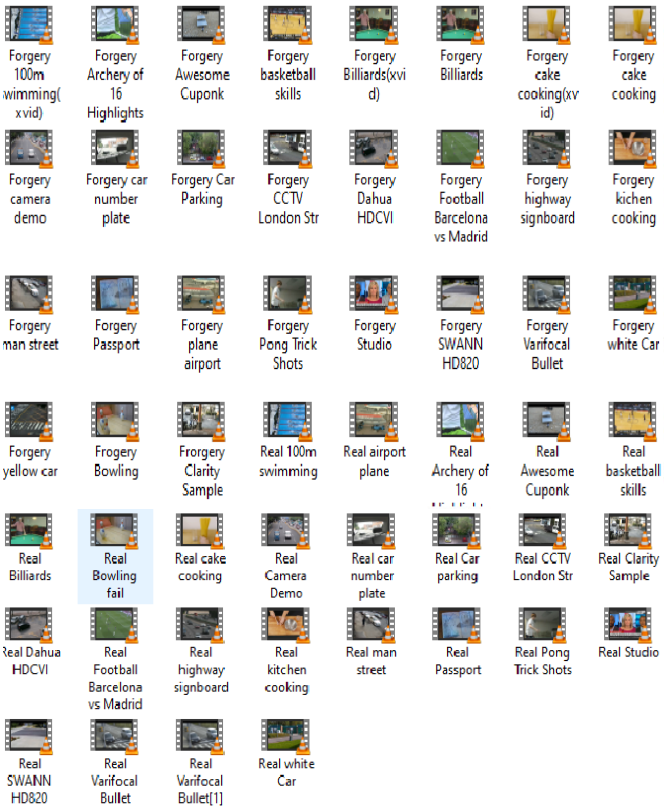

Fig 7. Representative video dataset gallery from VTD dataset

Computer Vision and Image Processing Group (CVIP) [16]: The Collection contains 160 videos from 6 original files. Manipulated videos are achieved by choosing a video frame object and recording a number of pictures. The copied object is cloned to another portion of the same video after potential transformations. The representative video forensic set is as shown in Fig.8.

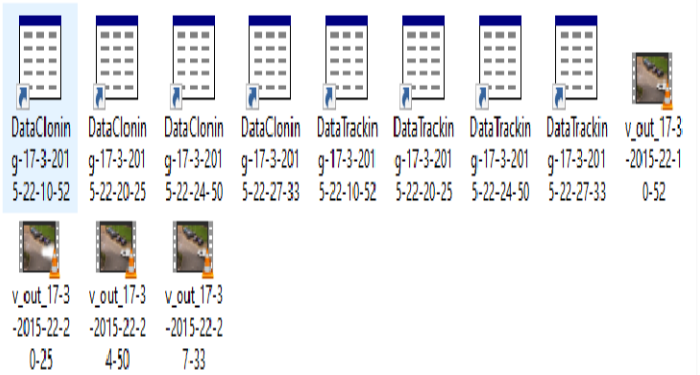

Fig 8. A representative group from CVIP for forgery detection using brightness features.

By considering above mentioned forensic dataset with reference of time as a feature space consider for design and implementing our proposed algorithm.

IV. Frame work and Algorithm for temporal tempering copy create algorithm

The fundamental principle of the proposed method is that variations of gray sequence correspondence coefficients are natural. Copying variations will also have anomalous values. Next, we examine the differences in the gray value correlation coefficients between sequential video frames and use SVM to distinguish between original videos and forgery. Our approach is evaluated in a massive analysis and the findings indicate that this is a way of understanding high precision and accuracy,

In a video that was not disturbed with traces, the similarity of the material similarity between distant frames is relatively weak. In contrast, the next photos have high content. The gray value of the frame is also easier to characterize video content reflecting the characteristics of the color and brightness and distribution level of the picture frame. We propose a technique based on the gray-value intercourse association coefficient. Fig. 5 defines the structure of discontinuity characteristics in the alleged video between different frame similarities.

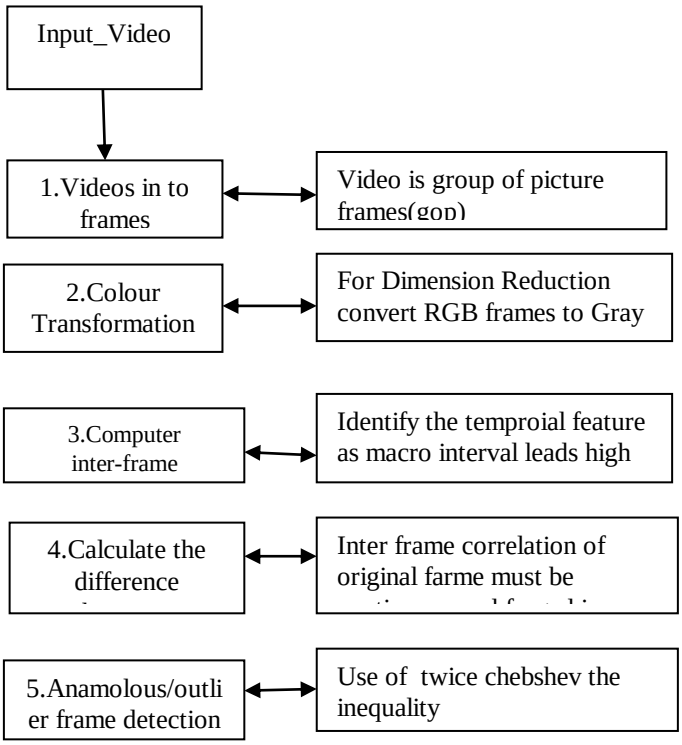

Fig 9. Stepwise representation of Framework of proposed work at Preliminary Level Investigation

1 Investigation of Preliminary Level:

Framework for the detection of video discontinuity characteristics from forensic data to identify an anomalous point The framework and details of the method to identify discontinuity content are as shown in fig.9.

Also, we would know that the checked video is either faked or manipulated at the first level of the inquiry, now we are still investigating at the second level. By adding or removing the checked video, we can recognize the manipulated collection of the sequence.

2. Secondary Level Investigation:

Upon analyzing the visionary of the video, we suggest forensic detection of copy-create film forgery by referring to the regular forensic forgery data set, as mentioned in the dataset design section.

For each outer frame, we find a predefined neighborhood, and all picture frames are alienated into non-overlapping blocks within that neighborhood. Next, we calculate the association between two respective blocks that belong to each pair of subsequent frames in this neighborhood (blocks in two frames at the same relative position). Here, too, the correlation is measured for outlier detection by computing the Pearson Correlation, which is supported by the 3ÿrule. We suggested a difference in the coefficient of correlation, which was followed by a technique for classifying original videos and generating images. The Gray Value effectively illustrates video information features content. For a frame-tampered image, gray values will be significantly modified at the manipulated stage. The structure is shown in Fig 10.

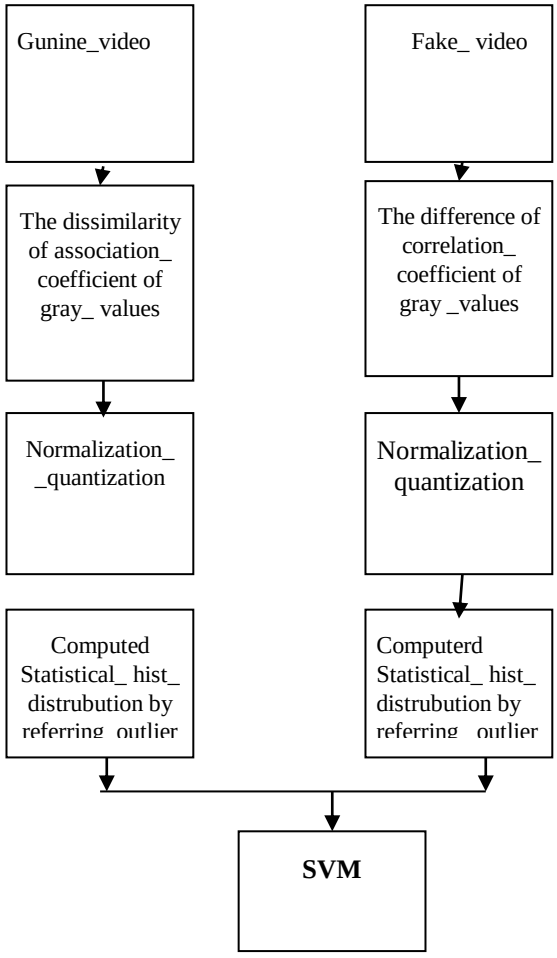

Fig. 10. Frame in this neighborhood (blocks in two frames at the same relative position). Here, too, the correlation is measured for outlier

V. Results

The results of these experiments on the forensic approach to video forgery detection using correlation differences are discussed in this section. The set of data used for the evaluation is broken down into three parts. For the experimental method, the use of three separate data sets is based on three objectives.

The first explanation is to use the planned data set to replicate these experiments to learn how copying, using the correlation coefficient, can effectively detect a forgery in a digital picture. The second explanation is to use the video data set by generating qualified copies in videos to determine the robustness of this proposed technique. The third interpretation is to check this technique to identify forgeries of compressed images.

These goals have been met. The results presented in this section indicate that variations in statistical correlation were effectively used to copy the detection of forgery in digital images.

Figures 11 to 18 shows the result that the copy produces forgery detection using difference in correlation. For the 20 test

videos from proposed forensic dataset, the correlation difference between interframe frame-blocks. Here we present a representative sample result from the video tested

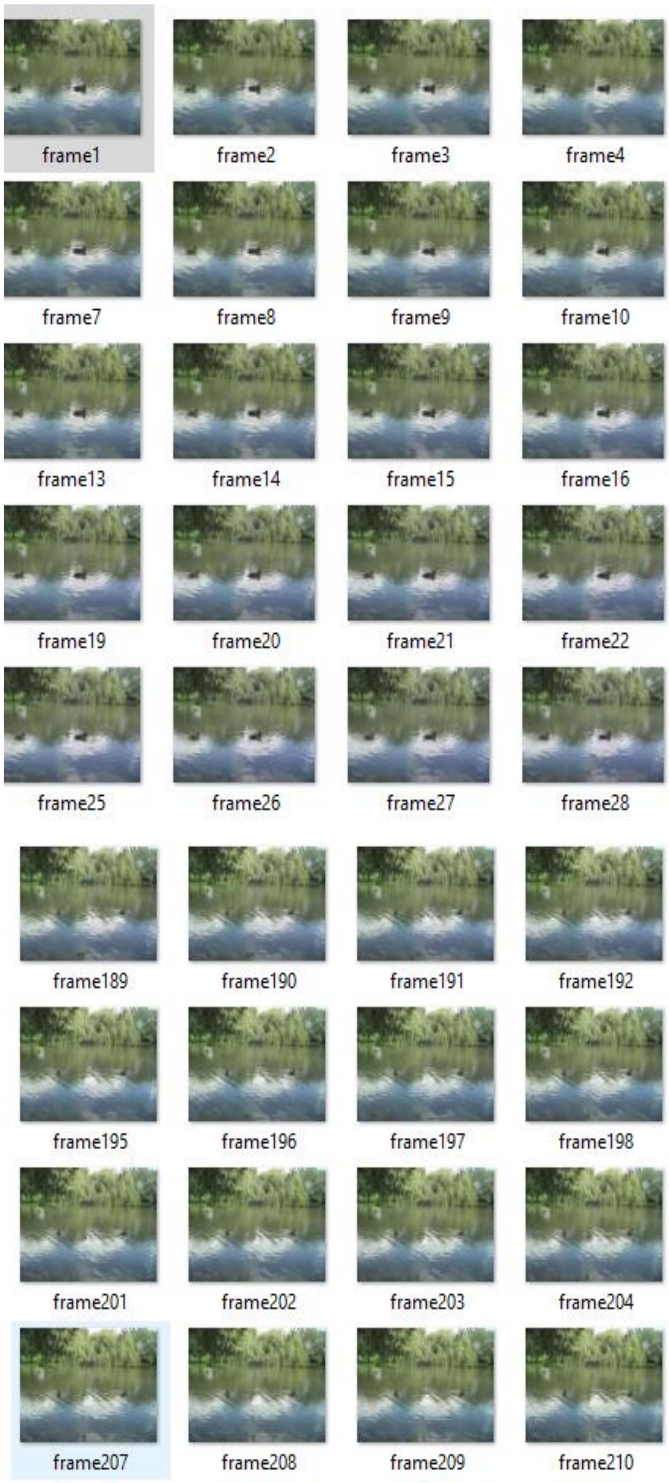

Fig11: Tested video is converted into a group of picture frames from the representative tested video set from SULFA dataset

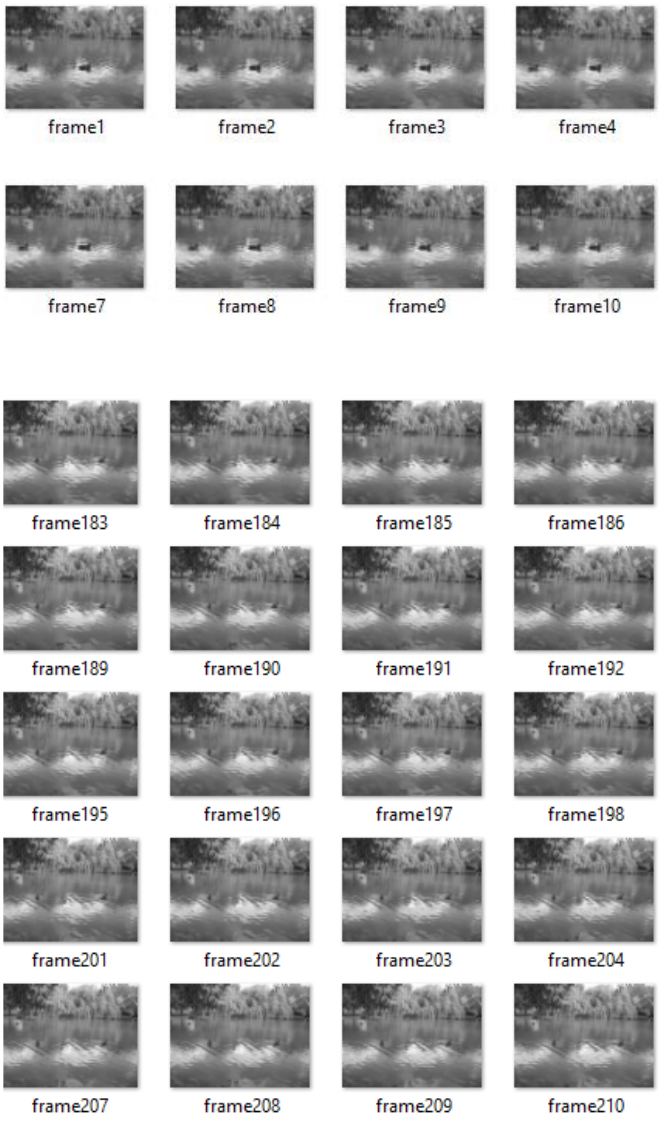

Fig 12: Preliminary Level Investigation result by converting a group of picture frames by applying the colour transformation. From sulfa tested video gallery.

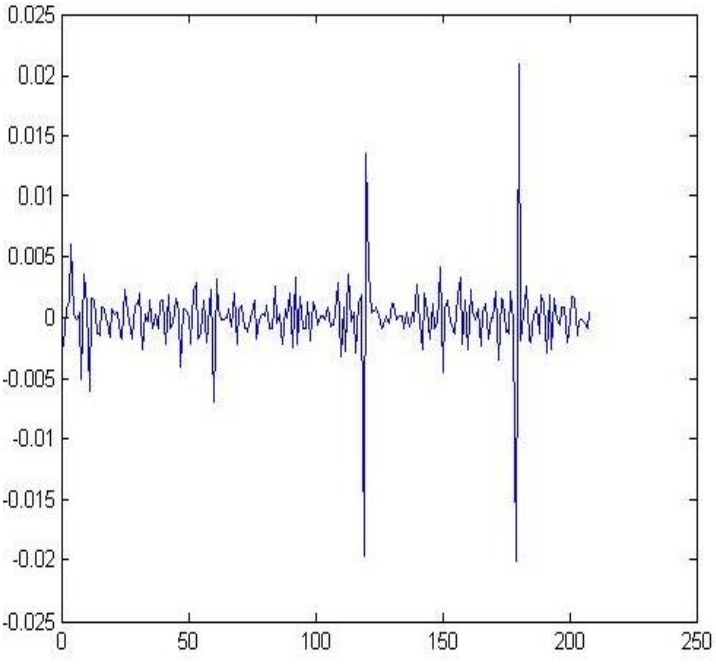

Fig 13: Extraction Of Timing parameter of correlation coefficient from the Sulfa dataset.

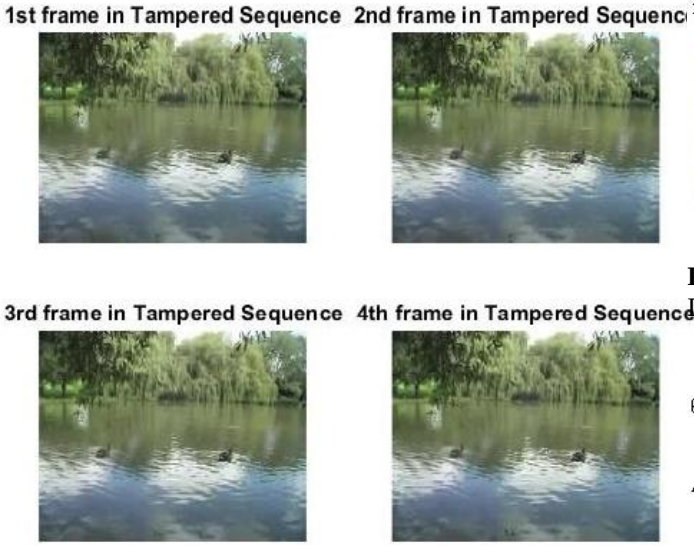

Fig14: Sequence of Tempered Forged identified by the proposed algorithm.

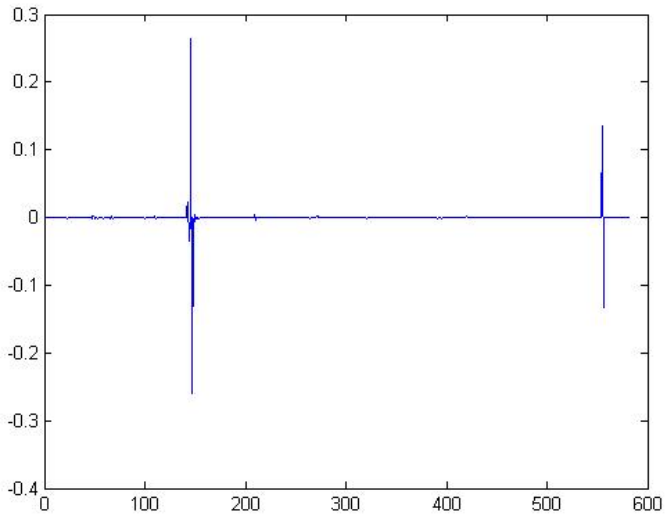

Fig 15: Extraction Of Timing parameter of correlation coefficient from the REWIND dataset.

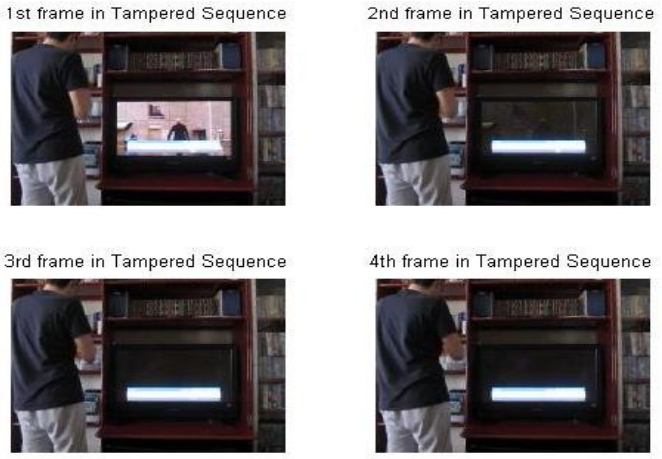

Fig16. The resultant forged sequence identified in REWIND Dataset

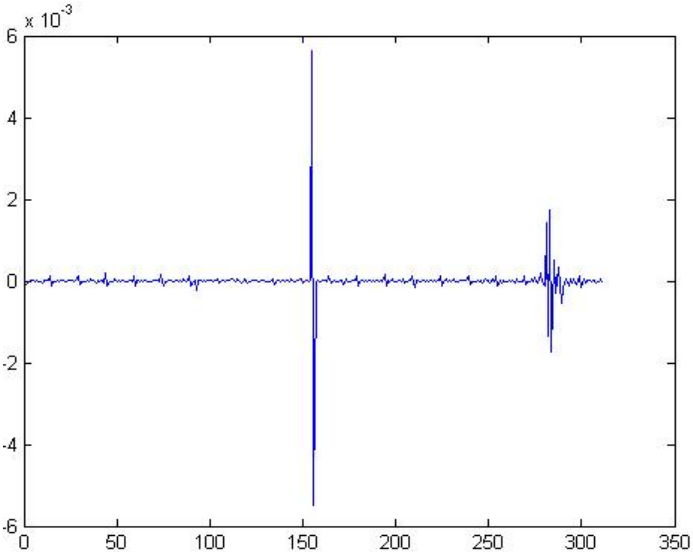

Fig 17. Extraction Of Timing parameter of correlation coefficient from the other Proposed Dataset.

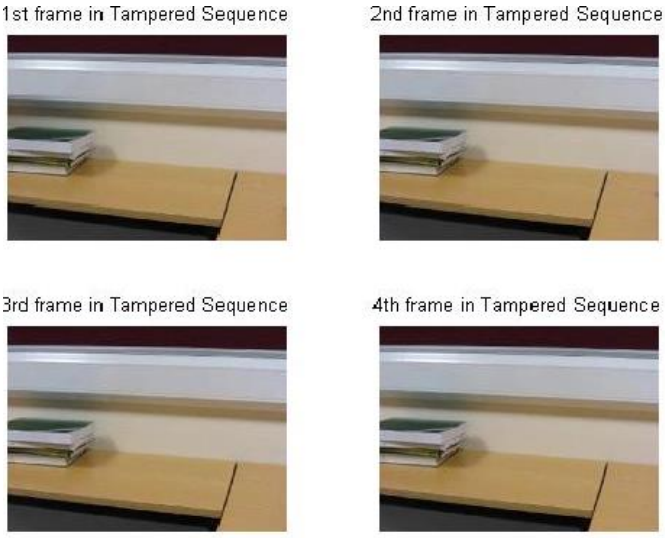

Fig18. The resultant forged sequence identified in the proposed dataset

This technique is capable of discerning whether a video has been altered. The classification accuracy between guanine and picture frame inserted forgeries is, as predicted, more significant than that of frame-deleted forgeries. Nevertheless, even the distinction accuracy between guanine and 25-frame-deleted forgeries is 95.22%, which is the experiment's lowest level.

We then seek to identify them from guanine to various kinds of forgeries. The efficient outcome, too. The precision is 97.75%. Motivated by this, we are further attempting to identify frame-inserted forgeries and picture frame-deleted falsification. We distinguish the TWENTY-FIVE frame-inserted videos and TWENTY-FIVE frame-deleted videos, as well as the ONE HUNDRED frame inserted videos and the ONE HUNDRED frame-deleted videos using the same process.

VI. Conclusions

To detect and recognize forged forging interframes between conjugative forged copy sequences, we proposed an innovative method that creates video forgery based on the difference between frames and correlation, by referring the SVM classification as a learning machine. While the inter-frame forgery recognition series maintains among the most daunting problems, it persists in the detection of video forgery. With that approach, the central theme of complexity and redundancy is reduced in videos by the massive size of their color transformation techniques between different framesets. The suggested forensic copy-creating technique used to check the relationship of the interframe between the video sequence frame set by referencing the I-frame relationship between two conjugative frame classes. By considering the standard picture, the forgery data collection, such as the SULFA and Sysu-Obj-Forge datasets, has achieved good accuracy and precession. The rate of performance is above 90%, depending on the average value of the training sample.

Acknowledgment

We thank the management and research community of B.V.V.Sanga's Basaveshwar Engineering College (Autonomous) Bagalkot and Maharaja Research Foundation, Maharaja Institue of Technology Mysore for providing infrastructure, ethical and moral support towards research activity in their campus.

References

[1] Fadl, S. M., Han, Q., & Li, Q. (2019). Inter-frame forgery detection based on differential energy of residue. IET Image Processing, 13(3), 522–528. doi: 10.1049/iet-ipr.2018.5068.

[2] SaddiqueM., AsgharK., Bajwa, U. I., Hussain, M., Aboalsamh, H. A., & Habib, Z. " Classification of Authentic and Tampered Video Using Motion Residual and Parasitic Layers." IEEE Access, 8, 56782–56797. doi: 10.1109/access.2020.2980951.

[3] H. Sharma, N. Kanwal, and R. S. Batth, "An Ontology of Digital Video Forensics: Classification, Research Gaps, and Datasets," 2019 International Conference on Computational Intelligence and Knowledge-Economy, Dubai, United Arab Emirates, 2019, pp. 485-491, doi: 10.1109/ICCIKE47802.2019.9004331.

[4] J. Bakas, R. Naskar, and A. K. Bashaboina, "MPEG Double Compression Based Intra-Frame Video Forgery Detection using CNN" 2018 International Conference on Information Technology, Bhubaneswar, India, 2018, pp. 221-226, doi: 10.1109/ICIT.2018.00053.

[5] S. Kaur and A. K. S. Kushwaha, "A Comparative study of various Video Tampering detection methods" *First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, 2018, pp.418-423,doi:10.1109/ICSCCC.2018.8703277.

[6] Al-Sanjary, O. I., Ahmed, A. A., Jaharadak, A. A. B., Ali, M. A. M., & Zangana, H. M. " Detection clone an object movement using an optical flow approach " 2018 IEEE Symposium on Computer Applications and Industrial Electronics(ISCAIE). doi: 10.1109/iscaie.2018.8405504.

[7] Karthikeyan, P. and Bhavani, R. and Rajinigirinath, D. and Priya, R., "Automatic Forged Scene Detection in Advanced Video Using Combined Mpeg-2 and Optical Flow Features "International Journal of Advanced Research in Engineering and Technology (IJARET), 11 (2), pp 246-258, 2020.

[8] Kharat, J., Chougule, S. A passive blind forgery detection technique to identify frame duplication attack. Multimed ToolsAppl **79,** 8107–8123(2020).doi.10.1007/s11042-019 -08272-y.

[9] Huang, C. C., Lee, C. E., & Thing, V. L. (2020). A Novel Video Forgery Detection Model Based on Triangular Polarity Feature Classification. International Journal of Digital Crime and Forensics (IJDCF), 12(1), 14-34. doi: 10.4018 /IJDCF .2020010102

[10] Saddique, M "Spatial Video Forgery Detection and Localization Using Texture Analysis of Consecutive Frames." Advances in Electrical and Computer Engineering, vol. 19, no.3, 2019, pp.97–108., doi:10.4316/aece.2019.03012.

[11] Wang, Q., Li, Z., Zhang, Z., & Ma, Q. " Video Inter-Frame Forgery Identification Based on Consistency of Correlation Coefficients of Gray Values. " Journal of Computer and Communications, 02(04), 51–57. doi: 10.4236/jcc.2014.24008

[12] Govindraj Chittapur, S. Murali, S., Prabhakara, H. S., and Basavaraj Anami "Exposing Digital Forgery in Video by Mean Frame Comparison Techniques." LectureNotes in Electrical Engineering Emerging Research in Electronics, Computer Science and Technology, 557–562. doi: 10.1007/978-81-322-1157-0_57

[13] Qadir, G., Yahaya, S., & Ho, A. (2012). Surrey University Library for Forensic Analysis (SULFA) of video content. IET Conference on Image Processing (IPR, 2012). doi: 10.1049/cp.2012.0422

[14] Bestagini, P., Milani, S., Tagliasacchi, M., & Tubaro, S. (2013). "Local tampering detection in video sequences." 2013-IEEE 15th International Workshop on Multimedia Signal Processing (MMSP). doi: 10.1109/mmsp.2013.6659337

[15] Omar Ismael Al-Sanjary, Ahmed Abdullah Ahmed, Ghazali Sulong, "Development of a video tampering dataset for forensic investigation, Forensic Science International," Volume 266,2016, Pages 565-572, ISSN 0379-0738,https://doi.org/10.1016/j.forsciint.2016.07.01

[16] (n.d.). Retrieved from http://www.diid.unipa.it/cvip/?page_id=48#CMFD

Author Biographies

Mr. Govindraj Chittapur is a research scholar in the department of computer science and engineering at Maharaja Institute of Technology Mysore. at presently, he is working as an Assistant professor in the department of computer applications Basaveshwar Engineering College, Bagalkot. He did his MSc. Technology by research from PES institute of technology under the university of Mysore.MCA degree from Jayachamarajendra College of Engineering and Technology presently known it as JSS Technological University Mysore. He polished more than 30 international and national conferences and journals. He has also contributed reviewer, Editorial Board Member of Springer journal, and AIRCCE publication journals. He also has an active member of the Board of Study and Board of Examination in Basaveshwar Engineering College, Bagalkot. He has a resource person for technical symposium, webinar, and faculty development programmers across India. His primary research interest is Image and Video Forensic, Machine learning, Data Science, and Image Processing.

Dr. Murali S. is a well-known professor in computer science and Engineering and Expert in computer Vision, multimedia forensics, Digital Image, and Video Processing, Data analytics and Business processing, Machine Learning, and Data Science. Presently he is President of Maharaja Education Trust Mysore and working as professor in the department of Computer Science and Engineering Maharaja Institute Of Technology Mysore. He has more than 25 years of Academic teaching experience in Computer Science and Information Science engineering. He served as both Academic and Management responsibilities various colleges of different universities. He has worked key positions of universities such as sand member, Bos Chairman, and Board of Examination positions.

Dr. Murali S. significant research contribution to the field of computer vision and multimedia forensics. He published more than 200 research papers in reputed international journals and conferences. For his social and technological contributions different societies are awarded.

Dr. Basavaraj Anami. He is a well known Indian professor and expert in computer science and engineering. He is currently Principal of KLE Institute of Technology Hubli, Karnataka, India's revered educational institution. He has comprehensive 32-year teaching experience in computer science. Dr. Basavaraj Anami started his career as a lecturer at Basaveshwar Engineering College, Bagalkot, due to his keen interest and passion for teaching. Prof Anami is a Ph.D. in Computer Science from Mysore University (2003) and IIT Madras postgraduate (1986). He graduated from Dharwad University in 1981 in Electrical Engineering. Apart from current research, Dr. Anami has played a critical role in curriculum design at several universities. He is currently Chair of Studies Committee, Visvesvaraya Technological University, and Belagavi. His research interests are image processing, voice processing and artificial intelligence. He has about 65 research papers published in various journals and conferences in India and abroad. Dr. Anami is a board member for many respected newspapers and has chaired several regional and international conferences.