FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 5 No. 2, June, 2021, pp 133 - 144
DOI: https://doi.org/10.33003/fjs-2021-0501-526

BLUE SCREEN VIDEO FORGERY DETECTION AND LOCALIZATION USING AN ENHANCED 3-STAGE FOREGROUND ALGORITHM

SHAFII, K., BAGIWA, M. A., OBINIYI, A. A., SULAIMAN, N., USMAN, A. M., FATIMA, C. M, FATIMA, S.,

Department of Computer Science, Ahmadu Bello University, Zaria

Corresponding author’s email: kasimshafii@gmail.com Phone: 08038813795

ABSTRACT

The availability of easy to use video editing software has made it easy for cyber criminals to combine different videos from different sources using blue screen composition technology. This, makes the authenticity of such digital videos questionable and needs to be verified especially in the court of law. Blue Screen Composition is one of the ways to carry out video forgery using simple to use and affordable video editing software. Detecting this type of video forgery aims at revealing and observing the facts about a video so as to conclude whether the contents of the video have undergone any unethical manipulation. In this work, we propose an enhanced 3-stage foreground algorithm to detect Blue Screen manipulation in digital video. The proposed enhanced detection technique contains three (3) phases, extraction, detection and tracking. In the extraction phase, a Gaussian Mixture Model (GMM) is used to extract foreground element from a target video. Entropy function as a descriptive feature of image is extracted and calculated from the target video in the detection phase. The tracking phase seeks to use Minimum Output Sum of Squared Error (MOSSE) object tracking algorithm to fast track forged blocks of small sizes in a digital video. The result of the experiments demonstrates that the proposed detection technique can adequately detect Blue Screen video forgery when the forged region is small with a true positive detection rate of 98.02% and a false positive detection rate of 1.99%. The result of this our research can be used to ensure the authenticity of a digital video especially when such video is presented as evidence in a legal case.

Keywords: Blue Screen, Composition, Entropy, Foreground, Tracking.

INTRODUCTION

The use of digital devices such as smart phones and tablets which are embedded with cameras has made it easier for digital criminals to easily capture, edit and distribute fake videos without leaving visible clues is easily accomplished, thereby causing confusion in the society. Tampered digital videos may carry false information about events or a crime scene, spread very fast through the network and confuse the public which undoubtedly has certain impact on social stability. Thus, the ability to ensure the integrity and authenticity of video contents is challenging as videos being displayed cannot be accepted blindly anymore.

Digital forensic was initially used as a synonym for computer forensics and is considered as a branch of forensic science which encompasses the recovery or regaining and investigating of fact or evidence found in digital devices often related to computer crimes. (Babenko, 2009) (Mark, 2002) (Carrier, 2003). Digital forensics is also referred to digital forensic science. The fast growth in computer related crimes which has led to high increase in digital forgeries has caused law enforcement agencies to begin establishing specialized personnel to handle the technical aspects of digital investigation.

Intentional alteration or modification of digital video contents for fabrication is referred to as Digital Video Forgery. Digital Video forgery can briefly be manipulating a video in such a way that changes are made in its content perceptually. Different types of video forgeries such as frame insertion/deletion/replication, copy-move and blue screen exist which can be carried out on digital videos. Digital video forgery can be divided into two parts inter frame forgery and intra frame forgery. Detecting these forgeries aims at exposing and scrutinizing the concealed facts about a video. The detection techniques primarily fall into two methods based on their approaches; active approaches and passive approaches. The active approach requires the pre-embedding of additional information which degrades the performance of the video to certain extents at the time of its creation. While the passive approach aims at extracting internal features of a video and analyzing them for different forgery detection. No pre-embedding of additional information (Chennamma, 2015).

Digital video forgeries are very dangerous because often, it is very difficult to recognize a fake video unless one is trained to identify such forgeries, it is very difficult to differentiate between an original and a tampered video. In such cases, the victims of these acts may suffer from financial loss and loss of reputation as a consequence of digital video forgery.

Forgery attacks on digital videos are categorized into two (2), the inter frame and the intra frame forgeries as shown in figure 1.

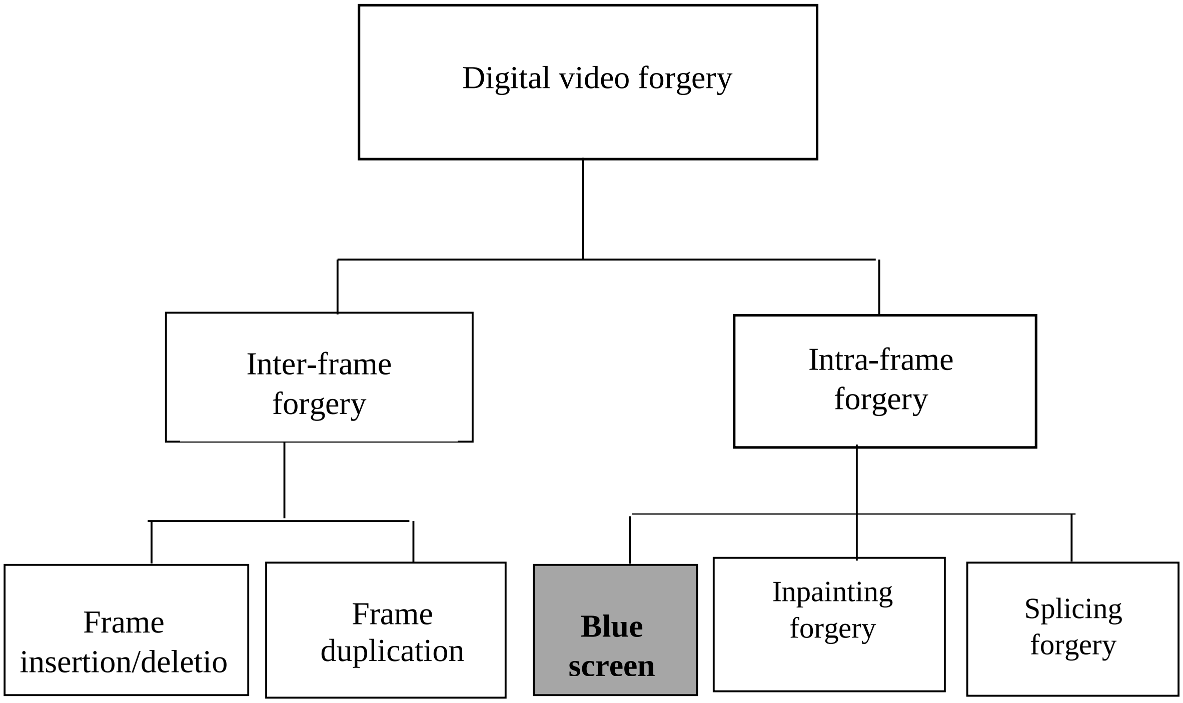
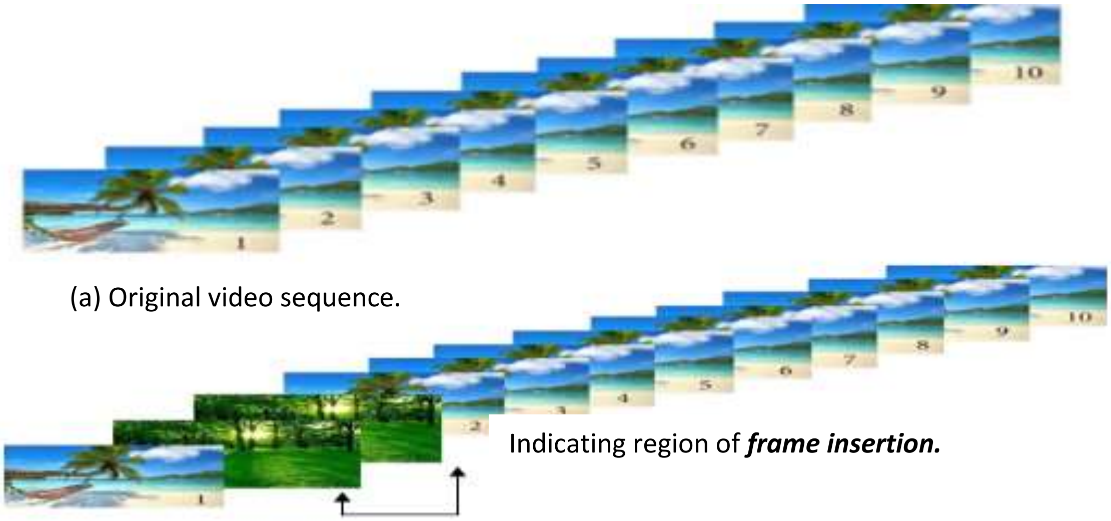


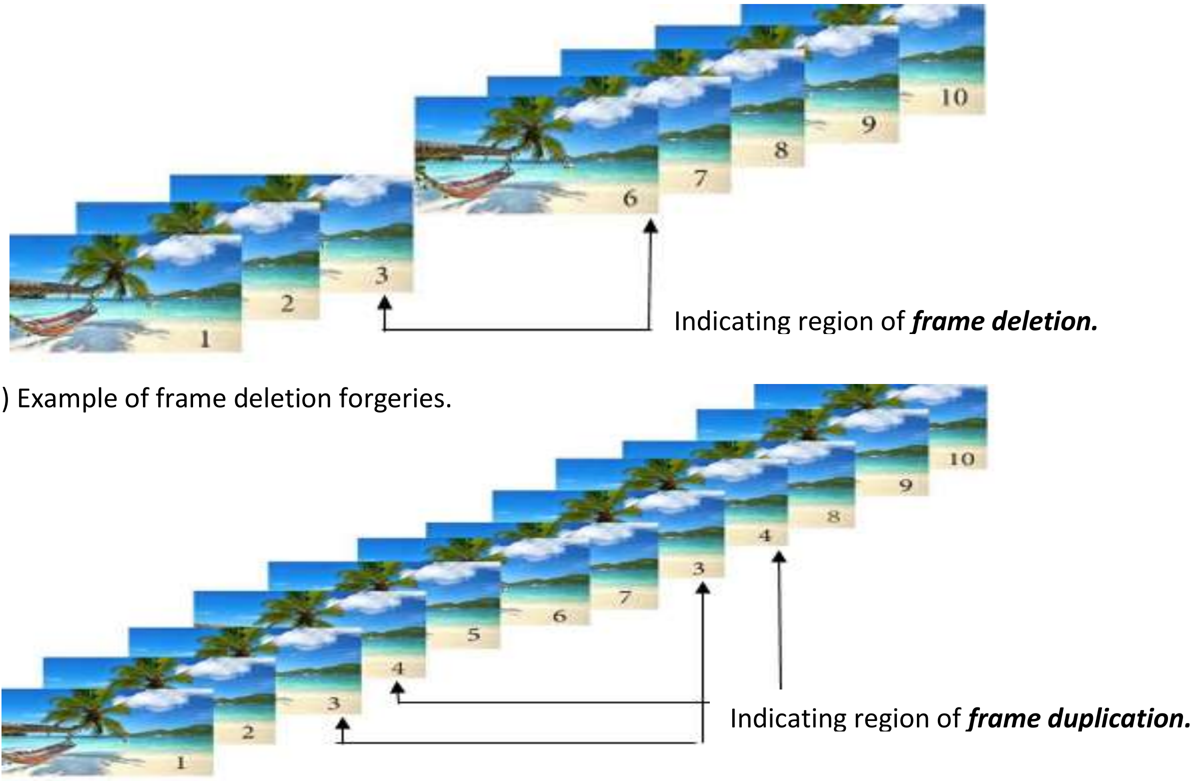
Figure 1: Video Forgery Categories.

In Inter-frame video forgery, the criminal/attacker intelligently introduces or remove an important object or objects to or from a video frame either by inserting, deleting or duplicating selected frames of the video sequence maliciously thereby, producing a tampered video (Naskar, 2018). This type of forgeries is illustrated in figure 2.


(a) Original video sequence.

Indicating region of ***frame insertion.***

(b) Example of frame insertion forgeries.

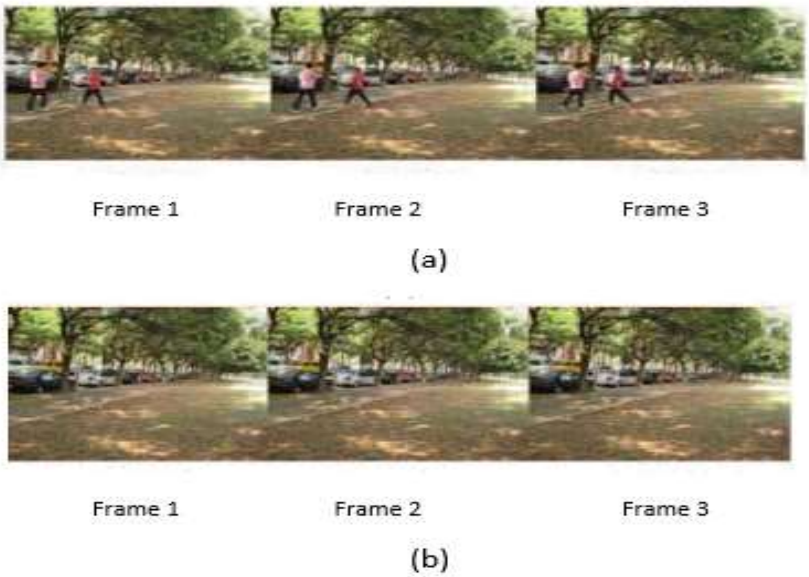

1
2
3
6
7
8
9
10
Indicating region of ***frame deletion.***
1
2
3
4
5
6
7
3
4
8
9
10
Indicating region of ***frame duplication.***

(c) Example of frame deletion forgeries.

(d) Example of frame duplication forgeries.

Figure 2: Inter frame forgeries type.

In intra frame video forgery, the frame is partially manipulated by the criminal/attacker. Example of this type of tampering includes, inpainting (Saxena, 2016) and splicing (Joshi, 2015) video forgery etc as shown in figure 3.

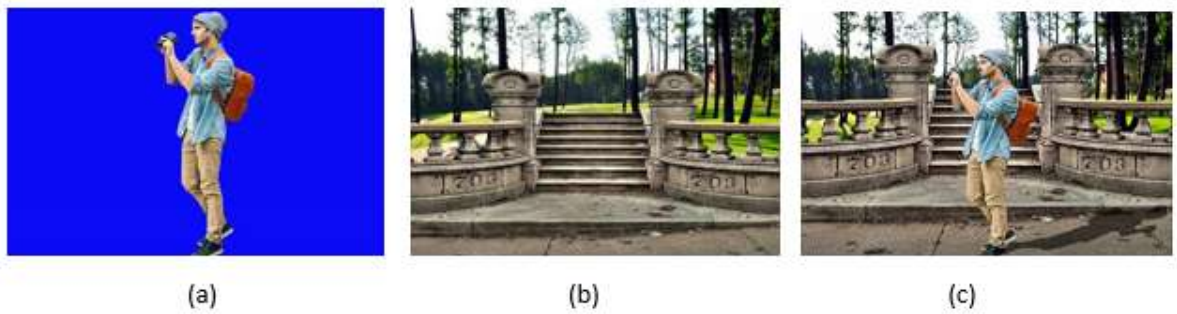


(a) Source video frame. (b) inpainted video frame (people removed from the source video frame indicating object removal)

Figure 3: Video Inpainting Intra Frame Forgery Type.

The fact that a criminal or a novice can use video editing tools to digitally manipulate videos to create non-existing situations using video editing software to forge videos (Blue screen as an example) threatens to diminish the credibility and value of video recordings presented as evidence in court independently of the fact whether the video is in digital or analog form. As one can expect, the situation will only get worse as the tools needed to perform these forgeries will move from research labs to commercial software. Blue screen composition is one of the methods of doing digital video forgery. Blue screen matting and composition involves extracting the foreground element from a particular video frame usually with a consistent background color of blue or green and embedding the foreground element into another video with a normal background.

Blue screen composition is a technique used for combining two images or two video frames together by replacing a color or a color range in one frame with that from another frame. The technique is often used in news casting, motion pictures or film industries to replace a scene's background by using a blue or green screen as the initial background and placing the anchor or the actor in the foreground. An example is shown in figure 4.



(a) A photographer standing with a constant blue color as background. (b) A video with normal background. (c) A composited video frame

Figure 4: An Example of Blue Screen Video Composition.

Despite the fact that the need for the detection of digital forgeries has been recognized by the research community, very few publications are available in detecting video compared to detecting image because, it's difficult to detect as a video sequence consist of set of images. Furthermore, a video sequence has both temporal and spatial distribution resulting in a huge data as compared to a single image.

Related Work

(Su, 2011) developed a detection technique for blue screen composition based on edge features. This blue screen detection technique explore the changes of the correlation between the color signals on the edge of individual element in the altered digital video using the Prewitt algorithm to find the edges of individual element thus, calculating sensitive factors to find out suspicious region in a tampered video. The experimental result for this detection technique successfully detect blue screen composition in digital video with different output bit rates. Unfortunately, the accuracy of this technique is easily affected by noise and other moving foreground.

(Junyu, 2012) proposed an approach for detecting special effects of blue screen composition. The approach is based on the different qualities between the video foreground and background and statistical features of the quantized discrete cosine transform (DCT) coefficient in the composited videos. The experimental result for this approach shows that the approach can successfully detect blue screen composition in digital videos. However, the accuracy of the technique decreases with different bit rate encoding and the technique can only be applied to MPEG video format only. Thus, limits the proposed approach.

(Bagiwa, 2016.) Presented a Chroma key background detection for digital videos designed to analyze the statistical correlation of blurring artifact in digital videos. This Chroma key detection technique is elaborated in three main stages namely, the pre-processing, feature extraction and the post-processing. The technique can adequately detect Chroma key forgery in a manipulated digital video with a true positive detection rate of 91.12% and a false positive detection rate of 1.95%.The experimental result of the technique shows that it cannot adequately satisfy accuracy and reliability of the system at the same time.

(Liu, 2017.) proposed a novel video forgery detection algorithm for blue screen compositing based on 3-stage foreground analysis and tracking (3FAT). The technique consist of three stages namely, extraction of the foreground block, detection of the forged block and lastly, tracking of the forged block. The experimental result revealed that the technique has true positive detection rate of 97.3% and a false negative detection rate of 7.8%. The technique rule out the distraction of noise and other moving foreground element in digital video. The technique can be applied to any video format, bit rate, encoding mechanism and execute very well in terms of speed. However, the technique is incapable of finding forged regions of small sizes. Furthermore, fast velocity movement of background element in a digital video causes non ideal experimental effect which also limits the implementation of the technique.

Proposed Detection Technique

The research work focuses on addressing detection problem of Blue Screen composition in digital videos for small forged region sizes. To address this problem, an enhanced blue screen video forgery detection and localization is proposed and the technique framework and flowchart are shown in Figure 5 and Figure 6 respectively. The proposed enhanced detection technique is explained in three main phases of extraction, detection and tracking.

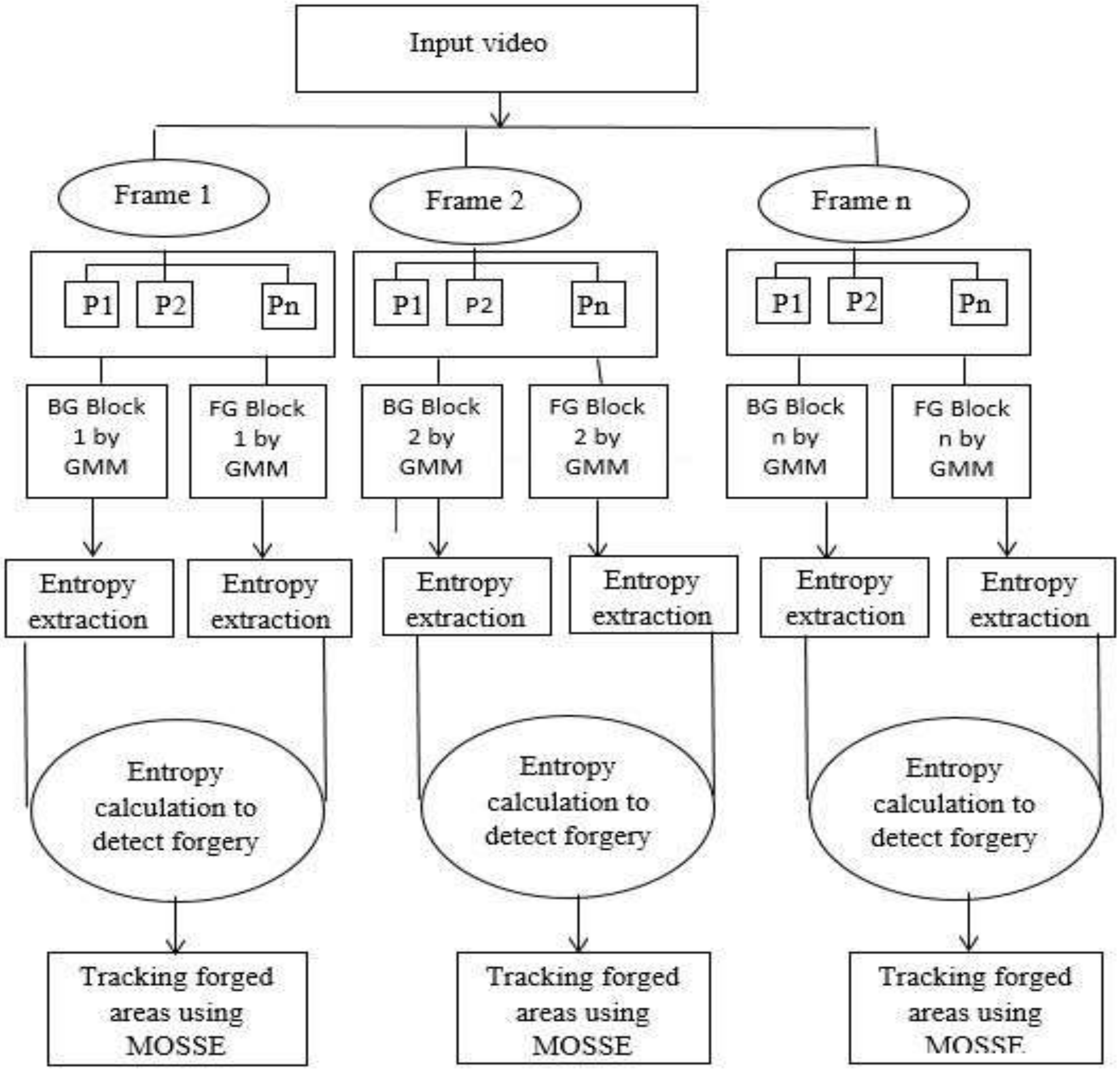


Figure 5: Proposed Enhanced Blue Screen Forgery Detection Framework

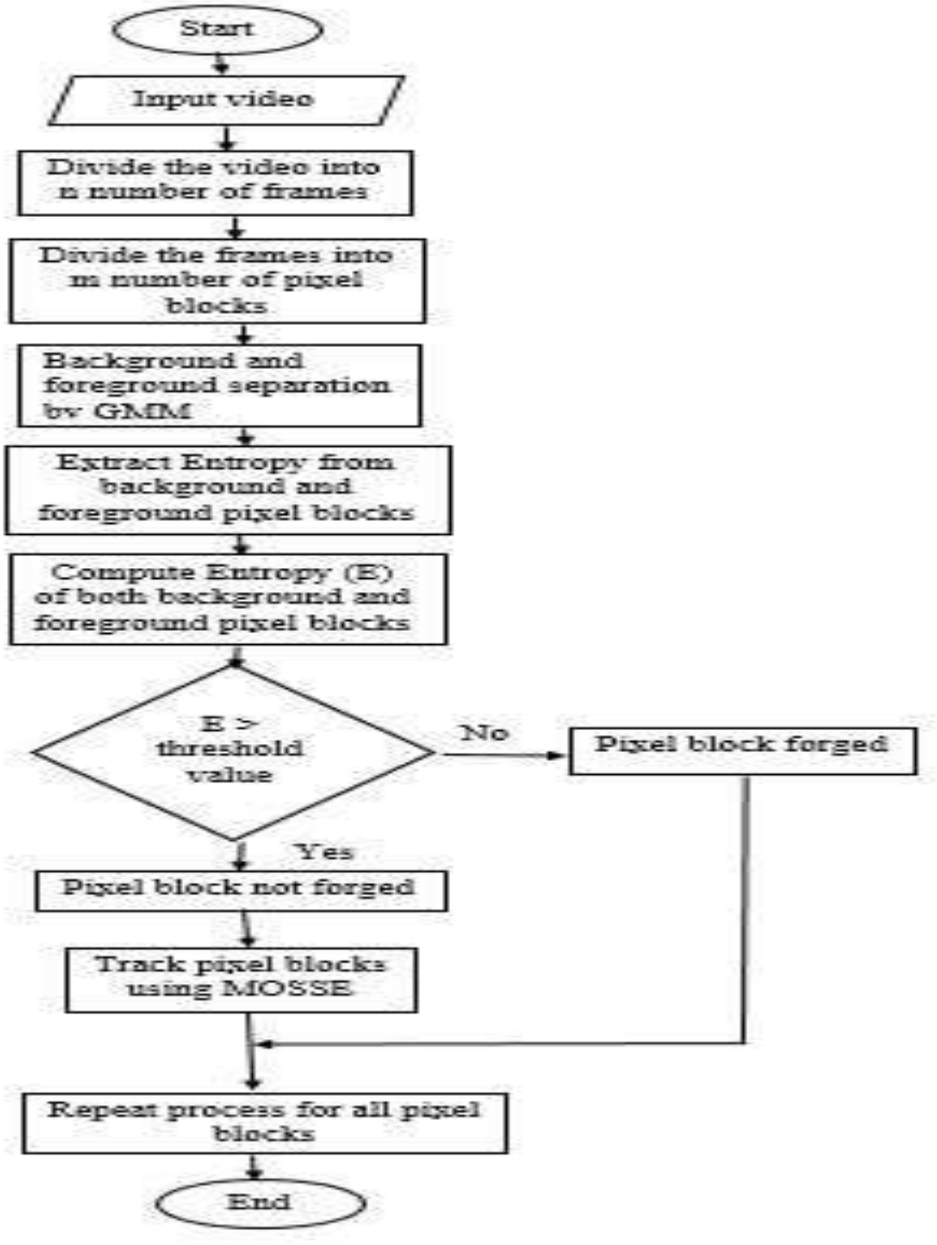

Start
Input video
Divide the video into n number of frames
Divide the frames into m number of pixel blocks
Background and foreground separation by GMM
Extract Entropy from background and foreground pixel blocks
Compute Entropy (E) of both background and foreground pixel blocks
E > threshold value
No
Pixel block forged
Yes
Pixel block not forged
Track pixel blocks using MOSSE
Repeat process for all pixel blocks
End

Figure 6: Proposed Enhanced Blue Screen Forgery Detection Flowchart.

Extraction

The video is divided into number of frames and then further sub divided into pixel of blocks. The extraction phase here, segment the foreground and background elements.

This phase provides a classification of the pixel blocks from video frames into either foreground or background pixel. In this phase, a Gaussian Mixture Model (GMM) is used to extract foreground element and background element of the current frame. In GMM, the values of a particular pixel over time is termed as ‘pixel processes. The pixel process is a time series of pixel values (Mariangela, 2013) (Stauffer, 2002)

Gaussian Mixture Model (GMM) is a parametric probability density function which is a weighted sum of Gaussian component densities (Nazia, 2017). Gaussian Mixture Model is basically one of the most popular technique to construct the background model for segmentation of moving objects from background. GMM algorithm was proposed by Stauffer and Grimson which target to effectively deal with multi-modal background by using a statistical model composed by a mixture of Gaussian distribution. (Mariangela, 2013). The probability of observing the current pixel is defined by a sum of weighted Gaussian distribution given in equation (1).

$$P(\chi_t) = \sum_{i=1}^{K} w_{i,t} * \eta(\chi_t, \mu_{i,t}, \sum_{i,t}) \qquad (1)$$

Where K is the number of distributions,$w_{i,t}$ is an estimate of the weight, $\mu_{i,t}$ is the mean value and $\sum_{i,t}$ is the covariance matrix of the ith Gaussian in the mixture at time t.$\eta(\chi_t, \mu, \sum)$ is the Gaussian probability density function. (Fradi, 2012) Obviously, $\sum_{i=1}^{K}(w_{i,t}) = 1$.

The mean of such mixture is given in equation (2)

$$\mu_t = \sum_{i=1}^{K} w_{i,t}\, \mu_{i,t} \qquad (2)$$

The following steps is adopted for better understanding of the process in order to achieve better result.

Step 1: Each input pixel is compared with the mean "μ" of the associated component. If the value of the input pixel is close enough to a chosen component's mean, then that component is considered as the matched component. For a component to be matched, the difference between the pixel and the mean must be less than when compared to the component's standard deviation.

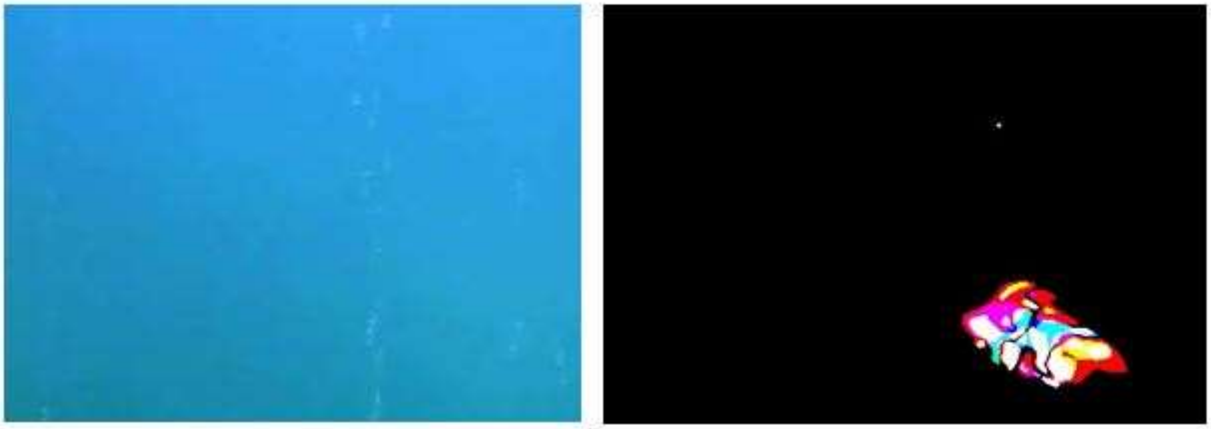
Step 2: The Gaussian weight mean and the standard deviation (variance) are updated in order to reflect the new obtained pixel value. Otherwise, for non-matched components, the weight 'w' decreases whereas the mean and the standard deviation stay the same.

Step 3: Components that are part of the background model will be identified. This is achieved by applying a threshold value to the component weight 'w'.

Step 4: In the final step, the foreground pixel is determined. The pixels that is identified as foreground does not match with any other components determined to be the background.

Gaussian Mixture Model is an efficient technique for foreground extraction but it has some kind of noise. Therefore, at last, morphological operation is used to remove unwanted noise pixels.

Figure 7 below shows the screenshot of frame segmentation using GMM where the background element and the foreground element are separately extracted from the target video in the extraction stage before entropy detection and calculation takes place in the next stage.



(a) Background element

(b) Foreground element

Figure 7: Screenshots of Frame Segmentation using GMM.

DETECTION

After the first phase which involves the extraction of meaningful foreground blocks using a Gaussian Mixture Model method, next is the detection phase. The main aim of the detection phase is to determine whether the target video has undergone tampering and thus, differentiate the tampered block from the original blocks in the target video.

In this work, we use entropy function as a feature extracted from the target video foreground and background in each pixel block. Entropy (E) of a digital video or image is a statistical measure of the degree that expresses the randomness of grey levels (colors) in an image or video. Entropy is seed to evaluate the number of details in an image or video and characterize the texture of an input image or video. Therefore, higher entropy means higher image or video details.

The entropy function of an image is computed in equation (3)

$$E = -\sum_{i=0}^{n-1} P_{(x,y)} \log_b P_{(x,y)}$$

Where:

N is the number of grey levels (256 for 8bits images), $P_{(x,y)}$is the probability of a pixel having grey level at (x,y) coordinates, b is the base of the logarithm function.

From the above equation, it is observed that the entropy of a digital image is a sum of terms that depend on the probability of occurrence of grey level of pixels. Thus, its value will not only depend on $P_{(x,y)}$but also on the quantity of gray levels present in the image. This entropy characteristic denotes that it is a nontrivial function to analyze its values when several images are compared that do not have the same quantity of grey levels. However, we are interested in knowing maximum function of the entropy under the conditions in which grey levels have a fixed number.

A structural comparison based Entropy is applied to measure the similarity between the foreground blocks and background blocks. For each foreground block, we extract the adjacent background block of the same size. For example, say X is a foreground block, then Y is the corresponding background block of X.

After the similarity analysis, a threshold value θ is set to differentiate between normal foreground blocks and the forged foreground blocks. If the Entropy value for a particular foreground is higher (greater) than θ, then the foreground block is a normal block, otherwise, the foreground block is a forged block.

Tracking

Many different algorithms have been developed for tracking over time. In this phase, a fast object tracking algorithm is proposed and our main goal is to successfully find an object in the current frame in the target video. Object tracking in digital video involves locating an object in successive frame of a target video or the process of detecting the position of an object in each frame of a video. Tracking has many real life applications in security, surveillance, traffic control etc. In this phase, we propose to adopt the use of Minimum Output Sum of Squared Error (MOSSE) for the object visual tracking.

Minimum Output Sum of Squared Error is a form of optimized correlation output filter that can be used for tracking. Other examples of robust tracking techniques includes, Fragment-based Robust Tracking (Adam, 2006), Incremental Visual tracking (David A, 2008) Stuck Structured Output Tracking with Kernels (Hare, 2015), locally Order less Tracking (S. Oron, 2015), Multiple Instance Learning Tracking (Babenko, 2009) among others. MOSSE tracker operates at a higher fps (450 fps and even more), very easy to implement and is as accurate as other complex trackers and much faster (Hare, 2015).

To perform tracking using Minimum Output Sum of Squared Error (MOSSE) technique, the following preprocessing steps were used.

i. A template in the object with a dimension of $2^n X2^n$ is cropped from the frame of the target video.

ii. The template which is obtained in the previous step is converted from its color to a grey scale image.

iii. Thirdly, a log transformation is then performed on the obtained template in the second step using equation (4)

$$\mathrm{g}(x.y) = \ln[F(x.y)] \qquad (4)$$

Where, x and y are the pixel values of output and input images respectively. The log function is applied to reduce lighting effects and enhance contrast. Thus, making high contrast features available for the filter to initialize on.

iv. Fourthly, the pixel values of the template obtained above are normalized to get a mean of zero and a normal of one. This normalization helps in reducing the effect of change in illumination and maintaining consistency in illumination between different frames of the target video.

v. Finally, the template obtained from above is changed from the spatial domain to the Frequency domain.

The preprocessing steps is briefly explained using the flow chart in figure (8) below.

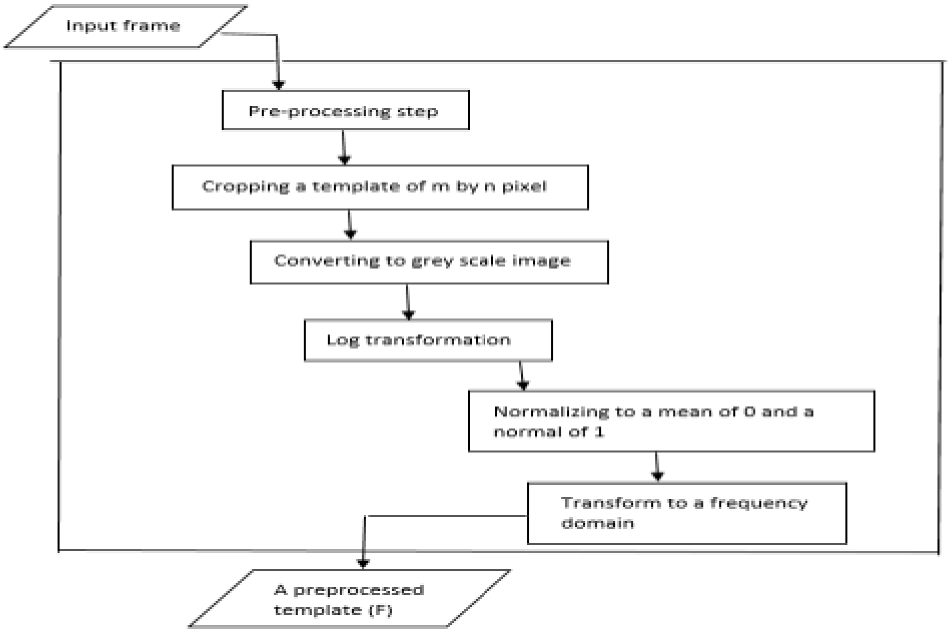

Input frame
Pre-processing step
Cropping a template of m by n pixel
Converting to grey scale image
Log transformation
Normalizing to a mean of 0 and a normal of 1
Transform to a frequency domain
A preprocessed template (F)

Figure 8: A Flow Chart Showing Preprocessing Steps.

The Minimum Output Sum of Squared Error (MOSSE).

The following steps were performed for a successful Minimum Output Sum of Squared Error (MOSSE) tracker:

Step one: The investigator clicks on the center of the object which provides the tracker with the x and y coordinates for the center of the object in the first frame of the target video.

Step two: A pixel template is cropped from the first frame of the video with the center as the x and y coordinate obtained from the step above.

Step three: The new template obtained from above is preprocessed and transformed to Frequency domain thereby retrieving F. The preprocessed steps are shown in figure 7.

Step four: A synthetic target G is created. The equation to generate the synthetic target image is presented in equation (5).

$$g(x.y) = \sum e - \frac{(x - x_i)^2 + (y - y_i)^2}{\sigma^2}$$

Where g_i is the synthetically generated image, x and y represent the location of pixels in an image, x_i and y_i represent the location of the center of the object to be initialized on. The radius of the peak is represented byσ.

Step five: F and G values are substituted for values of F_1 and G_1 respectively to compute N_1 and D_1 for the first frames of the target video.

Step six: Steps one to five are repeated for the next six (6) consecutive frames.

Step seven: The final N_1 and D_1 obtained from previous step is used to compute the filter.

Step eight: The tracker proceeds to the eighth frame of the target video and retrieve a tracking window.

Step nine: The previous step is used to track the object in the consecutive frames of the video with the location of the tracking window fixed at one position. The object can be tracked as long as the entire object remain inside the tracking window.

Experimental Results and Analysis

The summary of the dataset is presented in Table 1 showing each video with the total number of frame.

Table 1 Classification of Video Dataset

Video	Name	Number of frames
1	Duck	208
2	Ball	327
3	Book	317
4	Elephant	260
5	Cotton	272
6	Bridge	303
7	Skyscraper	166

8	Well	128
9	Car	179
10	Aero plane	100

The videos were cropped to 640×360 pixel sizes for uniformity

The performance of this method was measured on all the frames from each of the 10 videos in our dataset. Our enhanced detection technique is evaluated base on True Positive detection Rate (TPR) and False Positive detection Rate (FPR) which are the common standard of video related detection and algorithm. Equation (6) and (7) are the mathematical representations of TPR and FPR respectively.

$$TPR = \frac{TP}{(TP + FN)}$$

$$FPR = \frac{FP}{(FP + TN)}$$

Where, TP is the number of True Positive detections, FN is the number of False Negative detections, FP is the number of False Positive detections, and TN is the number of True Negative detections.

In each video, we computed the true positive rates (TPR) and false positive rates (FPR) and the results were summarized in Table 1 and histogram was plotted and presented in Figure 9.

Table 2: Experimental Result of Blue Screen Forgery Detection on 10 Test Videos.

Test Video	**Number of Frames**	**TPR (%)**	**FPR (%)**
Video 1	208	97.80	2.20
Video 2	327	99.37	0.63
Video 3	317	97.57	2.44
Video 4	260	96.90	3.10
Video 5	272	97.79	2.21
Video 6	303	98.98	1.02
Video 7	166	97.15	2.94
Video 8	128	98.44	1.56
Video 9	179	98.27	1.73
Video 10	100	97.98	2.02

Average 98.02% 1.99%

Comparison of the Proposed Technique with the Existing Work

The performance of this technique is presented as compared with existing Blue screen detection technique proposed in the work of (Liu, 2017.) using the same video dataset. The result obtained from the comparison is presented in Table 2.

Comparative Analysis for Running Time

Table 3: ***Comparative*** **Analysis** ***for Running Time (Secs)***

Test Video	**Ref** **(Su Y. 2011.)**	**Ref.** **(Liu Y. 2017)**	**E-3FAT** **(Proposed)**
Video 1	2001.72	1257.91	262.16
Video 2	7090.96	4456.07	928.67
Video 3	1482.27	931.48	194.13

Video 4	222.31	139.71	29.13
Video 5	1533.16	963.46	200.79
Video 6	5238.82	3292.15	686.10
Video 7	442.41	278.12	57.94
Video 8	3042.31	1911.83	398.44
Video 9	2311.08	1452.32	302.67
Video 10	2132.91	1340.35	279.34

The result of the CPU running time comparison between our proposed detection techniques with that of (Liu, 2017.) and (Su, 2011) for blue screen forgery indicated that our proposed detection technique records a lower CPU running time

Comparative Analysis for Performance Accuracy

Figure 9 shows the performance accuracy using the same video data set. The accuracy rate is used to evaluate the efficiency of our proposed blue screen detection technique which is the most common standard of video related detection and algorithm evaluation.

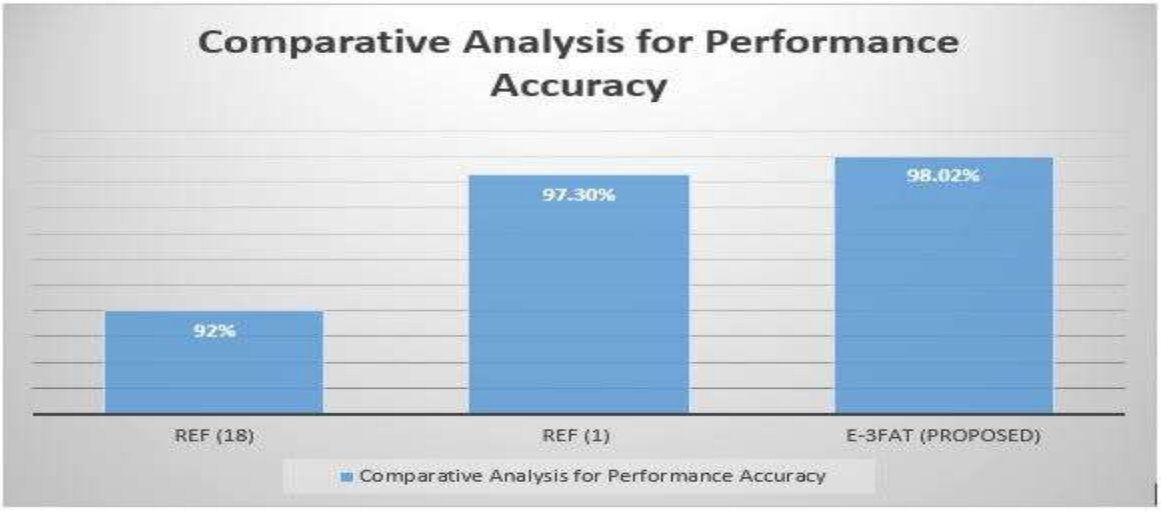


Figure 9: Comparative Analysis for Performance Accuracy

The result of the comparison between the proposed technique and (Liu, 2017.)for Blue Screen video forgery indicates that our proposed technique recorded a higher performance accuracy value and can adequately detect blue screen forgery in small region sizes.

CONCLUSION

Blue screen composition is one of the most common process of digital video forgery. However, the detection of this type of forgery is becoming more important to digital forensic investigators due to advance in digitalization today in our society. Only few algorithms have been proposed to adequately detect the presence of manipulation in digital video through blue screen composition.

To this effect, we proposed an Enhanced 3-Stage Foreground Algorithm for Blue Screen Video Forgery Detection and Localization. The proposed technique consists of three phases of namely, extraction where foreground elements in a digital video is extracted using GMM, The second phase is the detection phase where entropy function as a descriptive feature is calculated. In the last phase, MOSSE object tracking algorithm is used to study the tempered frame and track the block of subsequent frames. The performance of the proposed technique was compared with other techniques of blue screen proposed. The proposed technique is more accurate than that of the earlier ones with TPR of 98.02%.The proposed detection technique recorded a success in small forged region detection. Further research may focus on increasing the detection accuracy of Blue Screen video forgery detection

REFERENCE

Adam, A., Rivlin, E, & Shimshon, I. (2006). Robust Fragment-based Tracking using the Integral Histogram. 2006 *IEEE Computer Society Conference on Computer Vision and pattern Recognition(CVPR'06). New York, NY, USA, USA:IEEE.*

Babenko, B, Yang, M.-H, & Belongie, S. (2009) Visual tracking with online Multiple Instance Learning, *2009 IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA:* IEEE.

Carrier, B. (2003). Digital Forensic Eximination and Analysis Tools. *International Jornal of Digital Evidence.*

Chennamma, S.K. (2015), A SURVEY ON VIDEO FORGERY DETECTION *International Journal of Computer Engineering and Applications Volume IX, Issue II.*

David A. Ross, J. L.-S.-H. (2008). Incremental Learning for Robust Visual Tracking. *International Journal of Computer Vision May 2008, Volume 77, Issue 1–3, pp 125–141*. Springer.

Fradi, H., & Dugelay, J.-L. (2012). Robust Foreground Segmentation Using Improved Gaussian Mixture Model and Optical Flow. *2012 International Conference on Informatics, Electronics & Vision (ICIEV).* Dhaka, Bangladesh: IEEE.

Hare, S., Golodetz, S., Saffari, A., Vineet, V., & Cheng, M.-M. (2015). Struck: Structured Output Tracking with Kernels. *IEEE Transactions on Pattern Analysis and Machine Intelligence (Volume: 38 , Issue: 10 , Oct. 1 2016).* IEEE.

Joshi, V., & Jain, S. (2015). Tampering Detection in Digital Video - A Review of Temporal Fingerprints Based Techniques. *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom).* New Delhi, India.: IEEE.

Junyu Xu, Y. Y. (2012). Detection of Blue Screen Special Effects in Videos. *2012 International Conference on Medical Physics and Biomedical Engineering.* Elsevier B.V. Selection and/or peer review under responsibility of ICMPBE International Committee.

Mariangela Genovese, E. N. (2013). FPGA Implementation of Gaussian Mixture Model Algorithm for 47fps Segmentation of 1080p Video. *Journal of Electrical and Computer Engineering*.

Mark Reith, C. C. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*.

Mustapha Aminu Bagiwa, A. W.-K. (2016.). Chroma key background detection for digital video using statistical correlation of blurring artifact. *Digital Investigation (2016), doi: 10.1016/j.diin.2016.09.001.*

Naskar, J. B. (2018). A Digital Forensic Technique for Inter–Frame Video Forgery Detection Based on 3D CNN. *International Conference on Information Systems Security. ICISS 2018. Lecture Notes in Computer Science, vol 11281.* Springer, Cham.

Nazia Aslam, a. V. (2017). Foreground detection of moving object using GMM. *International Conference on Communication and Signal Processing, April 6-8, 2017, India.* India: IEEE.

S. Oron, A. B.-H. (2015). Loaclly Orderless Tracking. *International Journal of Computer Vision January 2015, Volume 111, Issue 2, pp 213–228*.

Saxena, S., Subramanyam, A., & Ravi, H. (2016). Video Inpainting Detection and Localization using Inconsistencies in Optical Flow. *2016 IEEE Region 10 Conference (TENCON).* Singapore, Singapore.: IEEE.

Stauffer, C., & Grimson, W. (2002). Adaptive background mixture models for real-time tracking. *Proceedings. 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (Cat. No PR00149).* Fort Collins, CO, USA, USA: IEEE.

Su, Y., Han, Y., & Zhang, C. (2011). Detection of Blue Screen Based on Edge Features. *2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference.* Chongqing, China: IEEE.

Yuqing Liu, T. H. (2017.). A novel video forgery detection algorithm for blue screen compositing based on 3-stage foreground analysis and tracking. *Multimed Tools Appl DOI 10.1007/s11042-017-4652-7*.