Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Blue Screen Forgery Detection on Double-Compressed Videos Using Enhanced 3-Stage Foreground Algorithm

Sani Haliru Muhammad[1], Fatimah Binta Abdullahi[2*], Mustapha Aminu Bagiwa[3], Nura Sulaiman[4]
Dept. of Computer Science, Ahmadu Bello University, Zaria, Nigeria.
kurfisanihaliru@gmail.com, zeeh429@gmail.com,mstphaminu@yahoo.com, nuwair68@gmail.com

Abstract

Background: *Blue Screen Composition is one way to carry out video forgery detection using simple and affordable video editing software. The availability of this video editing software has made it extremely easy for criminals to use different videos from different sources.* ***Aim:*** *Detecting this type of video forgery must be investigated. Although several techniques have been proposed in the literature to address the problem of blue screen forgeries. However, the accuracy of these techniques reduces when the resulting forged video is compressed twice.* ***Method****: In this work, an improved three-phase foreground and background technique for detecting blue screen manipulation in double-compressed video is proposed. The proposed enhanced detection technique comprises of extraction, detection, and tracking phase. In the extraction phase, a Gaussian Mixture Model (GMM) is used to extract foreground elements from a target video. The detection phase seeks the use of a homogeneity function where a description of the image, is extracted and computed from the target video. The tracking phase used the Discriminative Correlation Filter with Channel and Spatial Reliability (CSR-DCF) algorithm to fast-track the forged blocks of a digital video.* ***Results****: The result of the experiments demonstrates that the proposed detection technique can effectively detect video manipulation using the Blue Screen composition. Even when the forged regions are compressed twice, the technique was able to detect the presence of manipulation with a true positive rate of 98.03%, a false positive rate of 1.97%, and an average running time of 49.72 seconds.* ***Conclusion****: This research outcome can verify the authenticity of a digital video.*

Keywords: *Blue Screen, Composition, Homogeneity, Foreground, Tracking, Double Compression*

1. Introduction

There is a great increase in the production and usage of internet accessible devices (computer sets, laptops, among many others). These internet accessible devices use a large amount of data when, connected to the internet. To this, the internet is considered as the base of cybercrime. This is where digital forensics comes in. Digital forensics (DF) is a new field when compared to other forensic fields in the sciences. The role of DF in science is to examine and fish out crime (Sindhu and Meshram, 2012). DF is a process of collecting, identifying, extracting, and documenting electronic evidence from different electronic devices that can be used in a court of law as legal pieces of evidence (Alhassan et al, 2018). The investigation process depends on the DF tool which is to extract effective and efficient data. There are several types of data to which the DF tool can be applied to device data, computer devices, mobile devices, cloud computing, etc. (Osho et al, 2019).

Digital Forensic (DF) tools are applied to solve computer crimes such as phishing, money laundering, bank fraud, and child exploitation. The DF tool is designed to collect and recover original files from internet

Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

accessible devices (Sachdeva et al, 2020). DF tools are categorized into six classes, they are computer forensics, network forensics, live forensics, operating system forensics, database forensics, and mail forensics.

Digital video forgeries are extremely dangerous because it may often be quite challenging to tell the difference between an authentic and a manipulated movie unless one has special training to spot them. The rise of digital video forgery can be traced to the development of video editing software which was initially created to improve digital content.

As time moves on, the increase and availability of this low cost and user-friendly content editing software have led to or resulted in the negative use of it by dubious individuals. Since the software is not expensive, people can easily get access to it and use it to make unauthorized changes to video content which can alter the originality of such items.

To fight against unauthorized digital video forgery, digital video forgery forensics was created. As earlier mentioned, digital video forensics includes tools that help to determine whether the content of a given digital video is genuine or not (Kingra et al, 2016). Victims of digital video forgery may suffer monetary loss or reputational damage. Forgery attacks on digital videos are categorized into two, they are: 'inter-frame' and 'intra-frame' forgeries as shown in Figure 1.

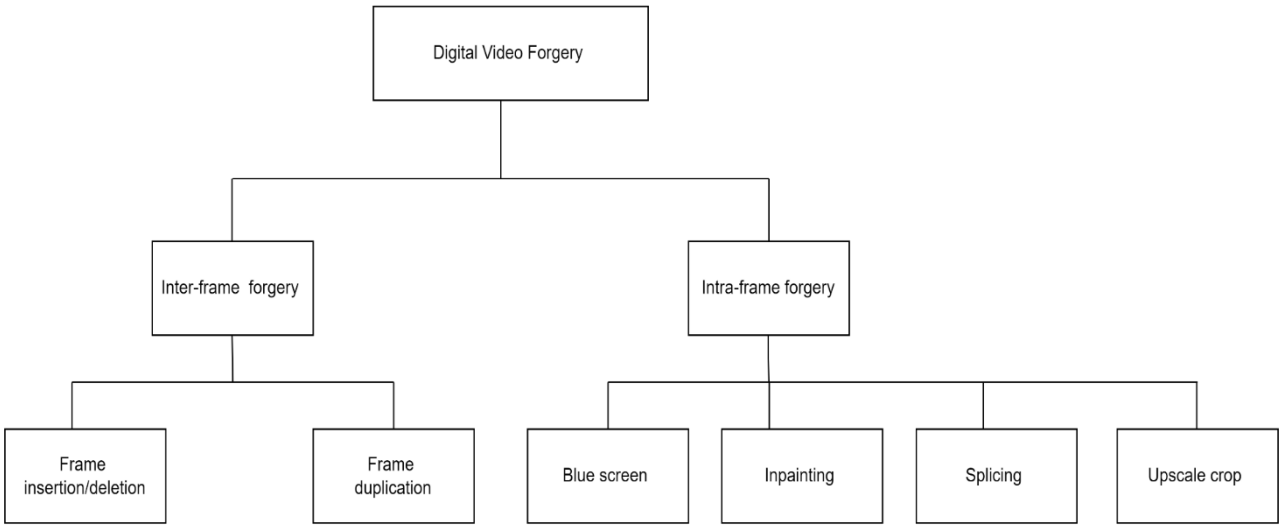
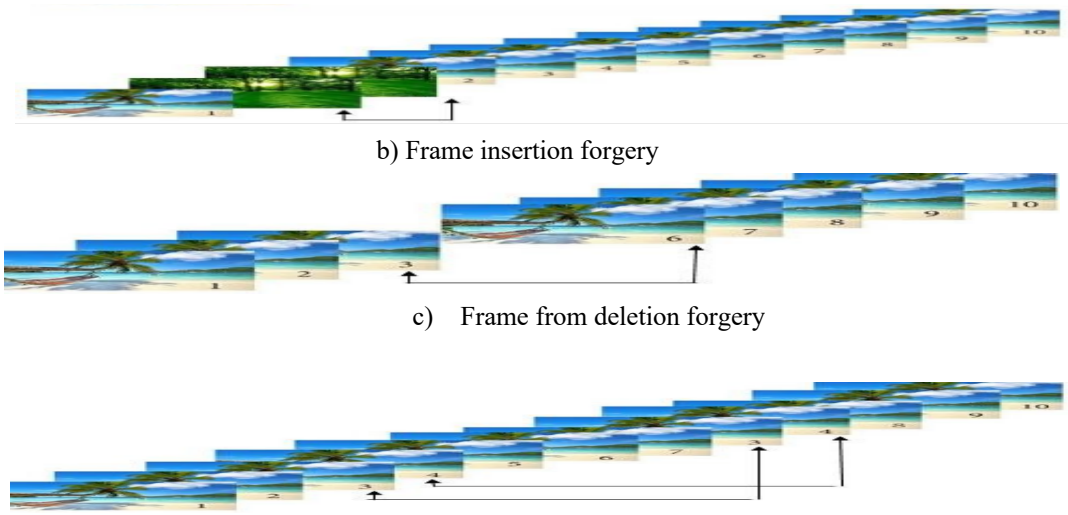


Figure 1: Types of Video Forgery Attacks (Joshi and Jain, 2015).

Inter-frame video forgery involves the adding or removing of a key object or objects from a video frame by maliciously altering, deleting, or copying some frames of the video sequence (Naskar, 2018). This type of forgery is illustrated in Figure 2.

a. Original video sequence

Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng



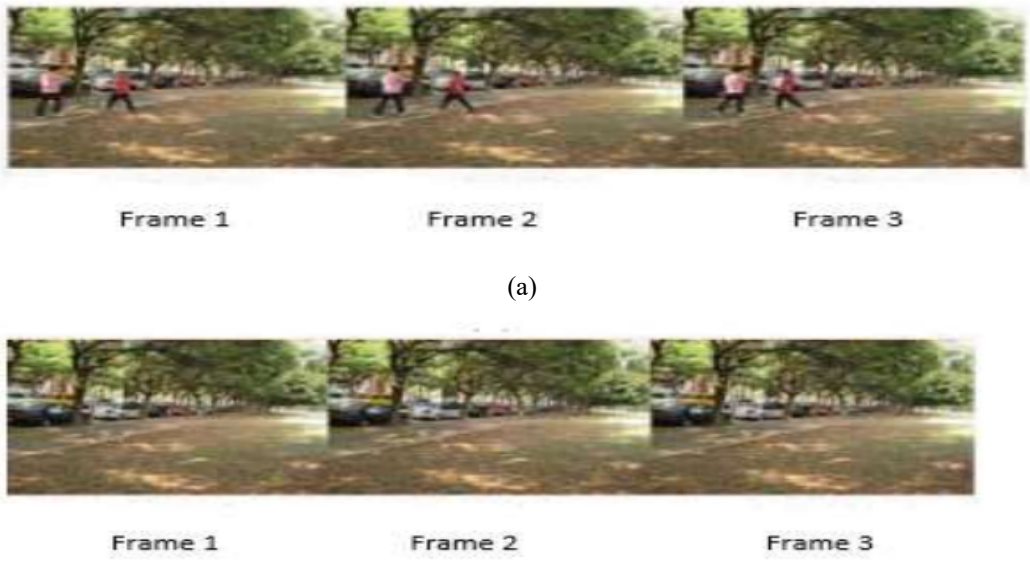
b) Frame insertion forgery

c) Frame from deletion forgery

d) Frame duplication forgery

Figure 2: Inter-frame forgeries type. (Shafii et al, 2021)

Intra-frame video forgery involves the altering some parts of the video frames by the criminal/attacker. An example of this kind of tampering is inpainting (Saxena et al, 2016) and splicing (Joshi and Jain, 2015) of the video forgery as shown in Figure 3.



(a)

(b)

Figure 3: Video Inpainting Intra Frame Forgery Type.

(a) Source video frame. (b) inpainted video frame (the two persons in the original video are removed from the original video frame after the altering of the video).

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Digital video processing software makes it relatively easy for criminals to easily create fake videos (for example, using a blue screen). Blue screen video forgery is a technique that extracts the foreground element from a video frame that has a consistent blue or green background colour and then inserts the foreground element into another video with a normal background. This technique allows criminals to use video editing tools to create false scenarios using blue screen composition, which undermines the reliability and validity of video recordings that are used as evidence in courtrooms. This problem is becoming more serious every day, as the tools for these forgeries are now available in commercial software, not just in research labs.

2. Related Works

Xu et al (2012) introduced a new way of identifying videos that have been altered with blue screen effects that create quality differences between foreground and background before re-compression. They use the inconsistencies in the statistical distribution of quantized DCT coefficients, between the foreground and the background to reveal the digital tampering. The results demonstrate that the proposed algorithm can detect blue screen manipulation with 88% accuracy. Bagiwa et al (2016)

suggest the blurring artifacts as a feature to detect video manipulation caused by the chroma key. The blurring artifacts were obtained from the video frame background and foreground blocks, and their correlation was calculated to measure the degree of blurring correlation amplitude for each block. The experiments show that the proposed technique can reliably detect the existence of tampering on a video using a chroma key. The result produced a true positive detection of 91.12% and a false positive detection of 1.95%. Liu (2018) introduced a brand-new foreground analysis and tracking (3FAT)-based video forgery detection system for blue screen compositing. The technique involves three stages, they are foreground block extraction, forged block detection, and tracking of the forged block. The experimental results showed a true positive detection rate of 97.3% and a false negative detection rate of 7.8%. The method eliminates any foreground movement or other distracting noise in the digital footage. Su et al (2019) suggest a novel way to identify videos that have been altered by using blue screen technology. They first segment a video scene into different objects and find their edges with the Prewitt algorithm. Then they extract the green components of the objects to create detection signals and compute sensitivity factors to detect suspicious edge points for each object. If the sensitivity factor is higher than a threshold, then the object is composited. The experiments demonstrate that the technique can accurately detect various types of videos with 92% accuracy. Kohli et al (2019) developed a spatial-temporal CNN to locate the forged area in a fake video. The used techniques consist of two stages: the first stage involves the detection of forged frames using the proposed temporal CNN, and the second stage involves localizing the forged area in some way using the proposed spatial CNN. To distinguish between forged and double compress frames, the first stage CNN is used, and the second stage CNN is used to localize the tampered region in a forged labelled frame. The method employed at this frame is capable of 98.94%. Su et al (2019) suggested a brand-new counterfeit detection method that uses video foreground removal to spot fake frames. The approach first calculates the energy factor (EF) of each frame. Then, to identify the falsified frames, a technology called an adaptive parameter-based visual background extractor (AVIBE) is created to identify the uncertain areas. The experimental results showed that the suggested technique outperforms existing ones in terms of computational accuracy, resilience, and efficiency. Results of the suggested algorithm for detecting accuracy are 93.17% and 86.58%. Shah et al (2020) proposed Inception Residual Network architecture based CNNs to identify picture and deep fakes' forgery detection. Using the Inception Resnet V2 architecture, the approach successfully constructed an image forgery detection system with a 91% accuracy rate for deep fakes. Ferreira et al (2021) described a collection of real and altered images and videos that used ML techniques (CNN and SVM) to identify altered

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

multimedia content. A suggested classification dataset of 40,000 images, comprising of both faces and objects, where used as the
data. Deep fake manipulation, splicing, and coy move were found. The rate of success in identifying photographs that have been altered is 99.68%, while the rate for films is 84.15%. Shafii et al (2021) proposed blue screen video forgery detection and localization utilizing an improved 3-stage foreground method. The method entails three steps: extraction of the foreground block, identification of the forged block, and tracking of the forged block. According to the experimental findings, the method has a true positive detection rate of 98.02% and a false negative detection rate of 1.99%. Mehrjardi et al, (2023) proposed a comprehensive review of image forgery types, benchmark datasets, evaluation metrics in forgery detection, traditional forgery detection methods, discovering the weaknesses and limitations of traditional methods, forgery detection with deep learning methods, as well as their performance was presented. Raj and Bakas (2023), present a motion residual and Deep Learning based forensic approach to identify object-based forged frames in surveillance videos. Firstly, the motion residuals are computed from the video sequences to extract the video forgery footprints, which are generated due to the manipulation operations. Secondly, the computed motion residuals are fed to the VGG-16 network for detecting authentic and forged frames in a surveillance video. Table 1 presents work on the topic, with each describing its proposed methods and findings.

Table 2: Summarized Literature Review

Authors	Title	Method	Findings
Xu et al., (2012)	Detection of Blue Screen Special effects in Videos	Discrete Cosine Transform (DCT).	The experiments demonstrate that the proposed technique can effectively detect blue screen manipulation with 88% accuracy. They plan to lower the false positive rate and find more features suitable for video encoders to expose digital forgeries which remain an open problem.
Bagiwa et al., (2016)	Chroma key background detection for digital video using statistical correlation of blurring artifact	Statistical correlation of Blurring Artifacts	The experiments show that the proposed technique can reliably detect the existence of tampering on a video using a chroma key, with a true positive detection of 91.12% and a false positive detection of 1.95%.
Lui et al., (2018)	A novel video forgery detection algorithm for blue screen compositing based on 3-stage foreground analysis and tracking	3-Stage foreground analysis and tracking (3FAT)	The experimental results showed a true positive detection rate of 97.3% and a false negative detection rate of 7.8%. However, the technique is incapable of detecting

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

			forged regions of small sizes.
Kohli et al., (2020)	CNN-based localization of forged region in object-based forgery for HD videos.	spatial-temporal CNN	The method employed at this frame is capable of 98.94% accuracy. Future efforts may be expanded to enhance the effectiveness of suggested post-processing attacks.
Shah et al., (2020)	Detecting video inter-frame forgeries based on convolutional neural network model.	phase-correlation	Particularly interesting is the localization of the forgery position in the video, which has above 99.9% accuracy. Future studies will focus on detecting forgeries in movies and complicated forgeries such as inpainting.
Shafii et al., (2021)	Blue Screen Video Forgery Detection and Localization using an Enhanced 3-Stage Foreground Algorithm.	3-Stage foreground analysis and tracking (3FAT)	According to the experimental findings, the method has a true positive detection rate of 98.02% and a false negative detection rate of 1.99%. However, the proposed method was not tested on double-compressed videos, which will be the focus of this work.
Mehrjardi et al., (2023)	A survey on deep learning-based image forgery detection	Survey on forgery detection based on deep-learning methods.	The survey can be helpful for a researcher to obtain a deep background in the forgery detection field.
Raj & Bakas (2023)	Detection of Object-Based Forgery in Surveillance Videos Utilizing Motion Residual and Deep Learning	Motion Residual and Deep Learning	The paper identifies object-based forged frames in surveillance videos.

From the above reviewed related literature, it was discovered that the difficulties associated with detecting Blue Screen composition in digital video persist. Even though several algorithms have been proposed to detect this type of video forgery, the existing algorithms seems inadequate and can be improved on by enhancing the accuracy on recompressed videos. The proposed algorithm focuses on detecting double-compressed video forgery in blue screen composition technology.

Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

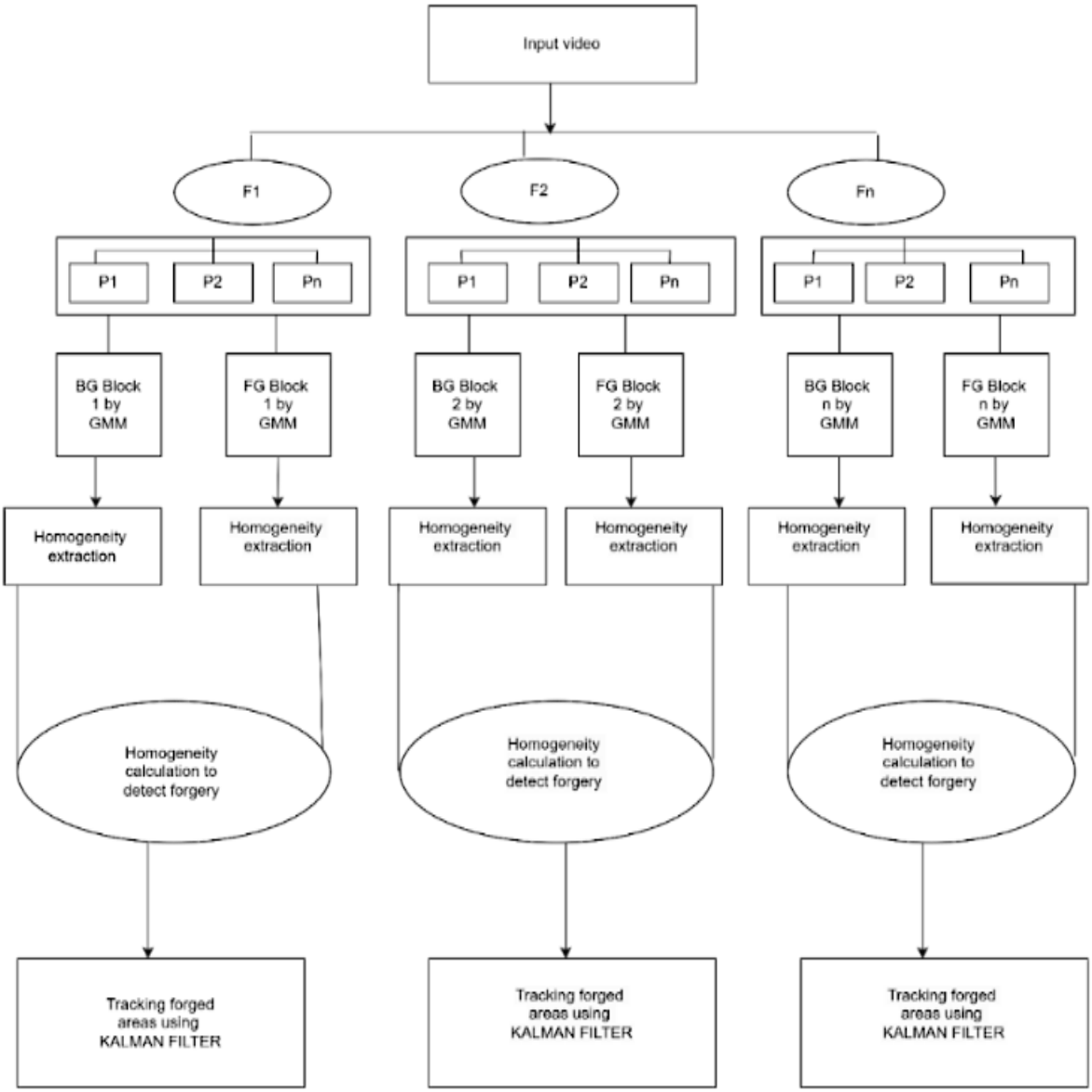
3. Materials and Methodologies

The proposed research work focuses on addressing the detection problem of blue composition in double compressed digital videos. To address this problem an enhanced blue screen video detection forgery technique is proposed. The foreground components of the target video will be extracted using the Gaussian Mixture Model (GMM) approach.

To identify the tampered region in the target video, the homogeneity function will be utilized to measure the amount of detail in the target video after the meaningful foreground elements have been extracted from it.

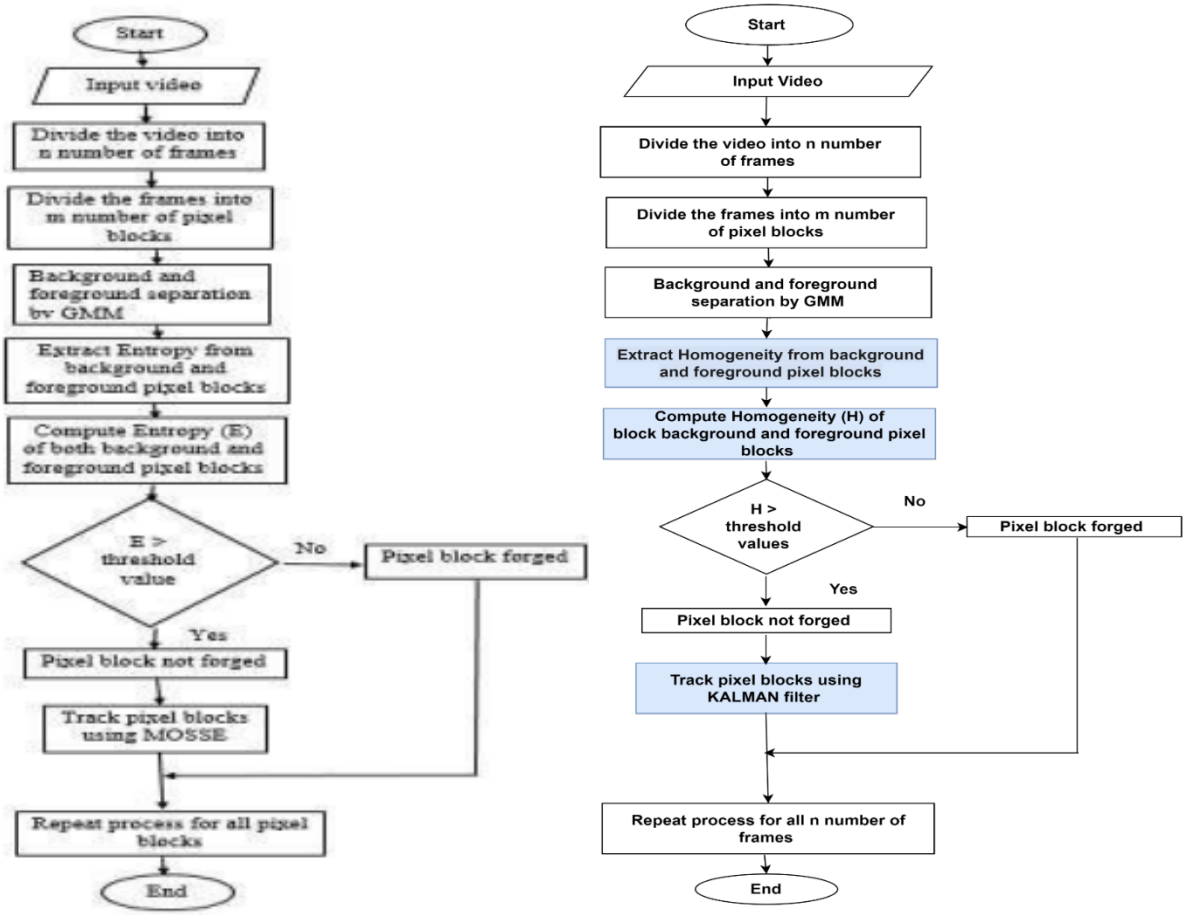
In the final step, items in the altered frame of the target video will be tracked using a rapid search target object tracking technique that is based on the Discriminative Correlation Filter with Channel and Spatial Reliability (CSR-DCF) object tracker model. This research aims to improve the accuracy of the existing detection technique by developing an improved digital video blue screen composition detection technique based on an enhanced 3-stage foreground algorithm for double compressed videos.

The framework and flowchart are shown in Figure 4 and Figure 5 respectively. The proposed enhanced detection technique is explained in three phases extraction, detection, and tracking.



Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Figure 4; Proposed Enhanced Blue Screen Forgery Detection Framework



(a) (b)

Figure 5: (a) Existing Blue Screen Forgery Detection Flowchart and (b) Proposed Blue Screen Forgery Detection Flowchart

3.1 Extraction

The video is divided into frames and further divided into pixels. The extraction process discovers the foreground element. In this stage, the pixel blocks from the video frames are categorized as either foreground or background pixels. The foreground component of the current frame is extracted using a Gaussian Mixture Model (GMM). The values of a specific pixel over time are referred to as the pixel process in GMM. The pixel process is a temporal series of pixel values Stauffer and Grimson (2002). The Gaussian Mixture Model (GMM) is a parametric probability density function that is the weighted sum of Gaussian component densities Aslam (2017). The GMM is the most widely used technique for creating a background model for the segmentation of moving objects from a background. Stauffer and Grimson introduced the GMM technique which uses a statistical model that is made up of a combination of Gaussian distributions so that it can effectively cope with multi-modal background. Mariangela Genovese also discussed GMM in 2013.

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

4. Equation (1) specifies the weighted sum of the weighted Gaussian distributions that determine the likelihood of witnessing the current pixel.

5. $$p(x_t) = \sum_{i=1}^{k} w_{i,t} * \eta(x_t, u, \sum) \quad (1)$$

6. 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 i[th] Gaussian in the mixture at time t. $t.\eta(X_t, \mu, \sum)$ is the Gaussian probability density function (Fradi and Dugelay, 2012). $\sum_{i=1}^{k}(w_{i,t}) = 1$. The mean of such a mixture is given in equation (2)

7. $$u_t = \sum_{i=1}^{k} w_{i,t}\, u_{i,t} \quad (2)$$

8. The following steps were adopted to understand the process better and achieve a better result.

9. *Step1:* Each input pixel will be 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 will be considered as the matched component. For a component to be matched, the difference between the pixel and the mean must be less when compared to the component's standard deviation.

10. *Step 2:* The Gaussian weight mean, and the standard deviation (variance) will be updated to reflect the newly obtained pixel value for non-matched components, the weight 'w' decreases, whereas the mean and the standard deviation stay the same.

11. *Step 3:* Components that would be part of the background model would be identified. This was achieved by applying a threshold value to the component weight 'w'.

12. *Step 4:* In the final step, the foreground pixel will be determined. The pixels that would be identified as foreground will not match with any other components to determine the background.

13. Gaussian Mixture Model is an efficient technique for foreground extraction, but it said to have some kind of noise. Therefore, the end, the morphological operation will be used to remove the unwanted noisy pixels.

(a) Background element (b) Foreground element

Figure 6: Screenshot of the frame Segmentation Using GMM.

3.2 Detection

After the first phase, which involves the extraction of meaningful foreground blocks using a Gaussian Mixture Model method, the next stage 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 paper, the homogeneity function is used as a feature to extract the foreground from the background in each pixel block. The homogeneity function measures the similarity or uniformity of the image by calculating local variations in pixel intensities within a given neighbourhood or window. The higher the homogeneity value, the more uniform the image would be in a particular region. It is also used to

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

describe the texture of input images or videos. Haralick's homogeneity measure is one common formula used for computing the homogeneity function. It is based on the co-occurrence matrix, which is a statistical representation of spatial relationships between pairs of pixels in an image. Therefore, higher homogeneity values indicate higher image or video details. The following will be the steps that will be taken to extract homogeneity function from the images:

1. The image will be divided into small, non-overlapping regions which is called tiles or blocks. The size of the blocks will depend on the application and the desired level of detail.
2. For each block, compute the homogeneity value using the following formula:
   homogeneity = sum ((pixel_intensity - mean_intensity) ^2) / (block_size – 1) (3)

   where:

   pixel_intensity is the intensity value of the pixel within the block.
   mean_intensity is the mean intensity value of all the pixels within the block.
   block_size is the total number of pixels within the block.

3. Repeat step 2 for all the blocks in the image.
4. Threshold the homogeneity values to identify regions with a significantly different homogeneity value compared to the surrounding regions. The threshold can be determined based on the application and the desired level of sensitivity.
5. Regions with a homogeneity value above the threshold may indicate the presence of a forgery.
6. The resulting values for each block will represent the homogeneity function for that block.

Higher values will indicate higher homogeneity or uniformity of the pixel intensities in the block, while lower values will indicate greater variability or heterogeneity.

3.3 Tracking

Object tracking in digital video involves locating an object in the successive frames of a target video or detecting the position of an object in each frame of a video. Many different algorithms have been developed for tracking over the years. In this phase, a fast object tracking algorithm

will be proposed to successfully find an object in the current frame of the target video. Tracking has many real-life applications in security, surveillance, traffic control, and more. In this study, a Discriminative Correlation Filter with Channel and Spatial Reliability (CSR-DCF) tracker is adopted for object visual tracking. Trackers based on the discriminative correlation filter method (DCF) have shown excellent performance in all standard benchmarks. Discriminative correlation methods learn a filter with a pre-defined response on the training image. The proposed CSR-DCF approach restricts the correlation filter to the parts suitable for tracking, improving the search range and performance for irregularly shaped objects. Channel reliability weights calculated in the constrained optimization step of the correlation filter learning reduce the noise of the weight-averaged filter response. The standard formulation of DCF uses circular correlation which allows for efficient implementation of learning by Fast Fourier transform (FFT). However, the FFT requires the filter and the patch size to be equal, which limits the detection range. Due to the circularity, the filter is trained on many examples that contain unrealistic, wrapped circularly shifted versions of the target. These windowing problems were recently addressed by state-of-the-art approaches of Lukežic. et al (2017) who propose zero-padding the filter during learning and introduce 16309 spatial regularizations to penalize filter values outside the object boundaries. Both approaches train from image patches larger than the object and thus increase the detection range. However, the published DCF methods assume that the target shape is well approximated by an axis-aligned rectangle. For irregularly shaped objects or those with a hollow centre, the filter eventually learns the background, which may lead to drift and failure. The same problem arises for rectangular objects in the case of occlusion. The Lukežic. et al (2017) methods both suffer from this problem. The CSR-DCF, or Discriminative Correlation Filter with Channel and Spatial Reliability, is a tracking method that overcomes the limitations of circular shift and rectangular shape assumptions. The spatial reliability map adapts the filter support to the part of the object

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 8 No. 2 [Dec, 2024], pp. 96-111
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

suitable for tracking, enabling an arbitrary search range. The spatial reliability map is estimated using the output of a graph labelling problem solved efficiently in each frame. An efficient novel optimization procedure is derived for learning a correlation filter with the support constrained by the spatial reliability map since the standard closed-form solution cannot be generalized to this case. Channel reliability is the second novelty introduced by the CSR-DCF tracker. The reliability is estimated from the properties of the constrained least-squares solution to filter design. The channel reliability scores are used for weighting the per-channel filter responses in localization. The spatial and channel reliability formulation is general and can be used in most modern correlation filters, such as those using deep features Spatial Constrained correlation filters.

Given a set of N_d channel feature of $f=\{f_d\}_{d=1:N_d}$ and corresponding target templates (filters) $h=\{h_d\}_{d=1:N_d,}$ where $f_d \in R^{w_{d\,x}\,d_h}$, $h_d \in R^{d_{w\,x}\,d_h}$ the position X is estimated by maximizing the probability

$$p(x/h)=\sum_{d=1}^{N_d} p(x/f_d)p(f_d) \tag{4}$$

The density $p(x/f_d)=\left[f_d * h_d\right]^{(x)}$ is the convolution of a feature map with a learned template evaluated at X and $p(f_d)$ is a prior reflecting the channel reliability.

Following we assume independent feature channels. Optimal filters are obtained at the learning stage by minimizing the sum of squared differences between the channel-wise correlation outputs and the desired output.

$$g \in R^{d_{wx}\,d_h}, \quad \frac{\arg\min}{h}\sum_{d=1}^{N_d}\| f_d * h_d - g \|^2 + x\sum_{d=1}^{N_d}\| h_d \|^2 = \frac{\arg\min}{h}\sum_{d=1}^{N_d}\left(\| \hat{h}_d^{\,H}\, diag\left(\hat{f}_d\right)\right) - \hat{g}_d \|^2 \lambda \| \hat{h}_d \|^2 \tag{5}$$

4. Results

The summary of the dataset is presented in Table 2 showing each video with the total number of frames.

Table 2 Classification of Video Datasets

Video	Name	Number of frames
1	Duck	102
2	Ball	474
3	Book	181
4	Elephant	339
5	Cotton	305
6	Bridge	317
7	Skyscraper	384
8	Well	407
9	Car	130
10	Airplane	474

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 1 No. 1 [June, 2020], pp. xx-yy
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

The proposed detection technique was evaluated on all the frames from each of the 10 videos in the dataset. The performance of the technique was measured using True Positive Detection Rate (TPR) and False Positive Detection Rate (FPR), which are the common standards of video-related detection and algorithm. TPR and FPR are mathematically represented by equations (6) and (7), respectively.

$$TPR = \frac{TP}{(TP+FN)} \quad (6)$$

$$\boldsymbol{FPR = \frac{FP}{(FP+TN)}} \quad (7)$$

In the given context, TP refers to the number of True Positive detections, FN refers to the number of False Negative detections, FP refers to the number of False Positive detections, and TN refers to the number of True Negative detections. For each video, we calculated the true positive rates (TPR) and false positive rates (FPR). The results were then compiled into Table 3 and histograms were plotted and presented in Figures 7 & 8. Similarly, the running time result for Blue Screen Forgery Detection on 10 Test Videos using Double Compressed Videos is presented in Table 4 and a histogram was plotted and presented in Figure 9.

Table 3: Comparative Analysis of Blue Screen Forgery Detection on 10 Test Videos

Test Video	**Size (MB)**	**Number of Frames**	**Shafii *et al.*, (2021) TPR (%)**	**Shafii *et al.*, (2021) FPR (%)**	**E-3FAT TPR (%)**	**E-3FAT FPR (%)**
Video 1	0.350	102	97.00	1.90	**98.42**	2.00
Video 2	2.08	473	96.80	2.20	**97.81**	**1.90**
Video 3	0.465	181	96.90	2.10	**98.03**	2.10
Video 4	1.75	339	96.40	2.50	**98.20**	**1.80**
Video 5	1.0	305	96.60	2.30	**98.01**	**2.20**
Video 6	3.28	317	97.20	1.80	**98.17**	1.80
Video 7	1.05	384	96.70	2.15	**98.01**	**1.95**
Video 8	1.28	407	96.30	2.40	**98.05**	**1.75**
Video 9	0.409	130	97.10	1.85	**98.15**	2.05
Video 10	3.28	474	96.50	2.05	**97.49**	**1.85**
	Average		96.50	2.05	**98.03**	**1.97**

Sule Lamido University Journal of Science & Technology Vol. 1 No. 1 [June, 2020], pp. xx-yy
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Table 4; Comparative Analysis of Running Time (secs)

Test Video	Ref. (Shafii., 2021)	E-3FAT (Proposed)
Video 1	1.23	20.39
Video 2	5.00	44.18
Video 3	2.80	56.79
Video 4	4.25	83.88
Video 5	4.10	25.71
Video 6	3.99	44.19
Video 7	4.49	41.79
Video 8	4.54	30.12
Video 9	1.88	14.73
Video 10	5.84	135.39
Average	3.812	49.72

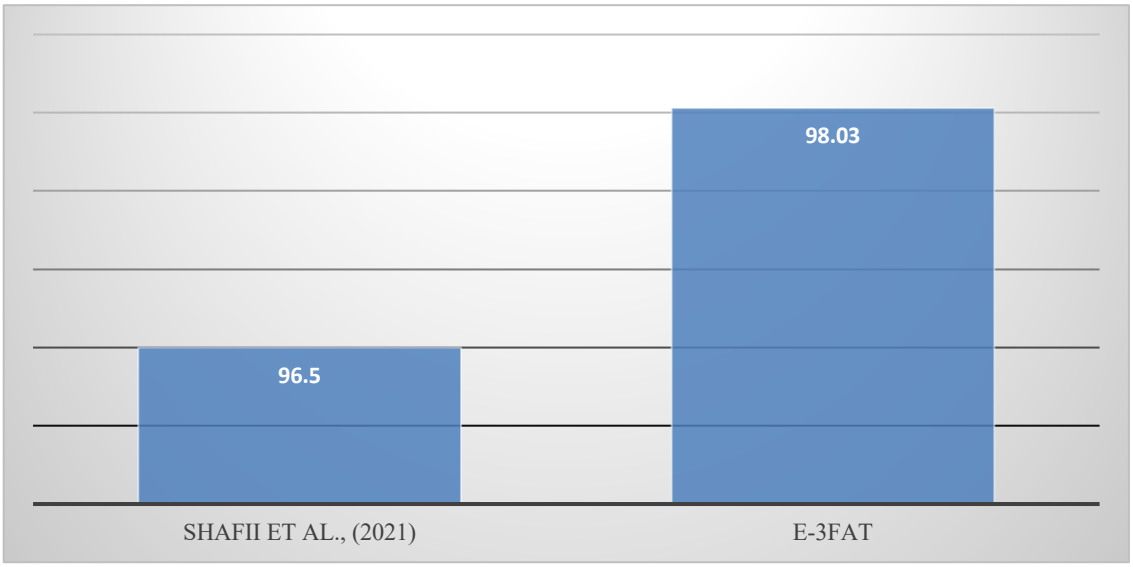


Figure 7: Comparative Analysis of Average TPR Performance Accuracy

Sule Lamido University Journal of Science & Technology Vol. 1 No. 1 [June, 2020], pp. xx-yy
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

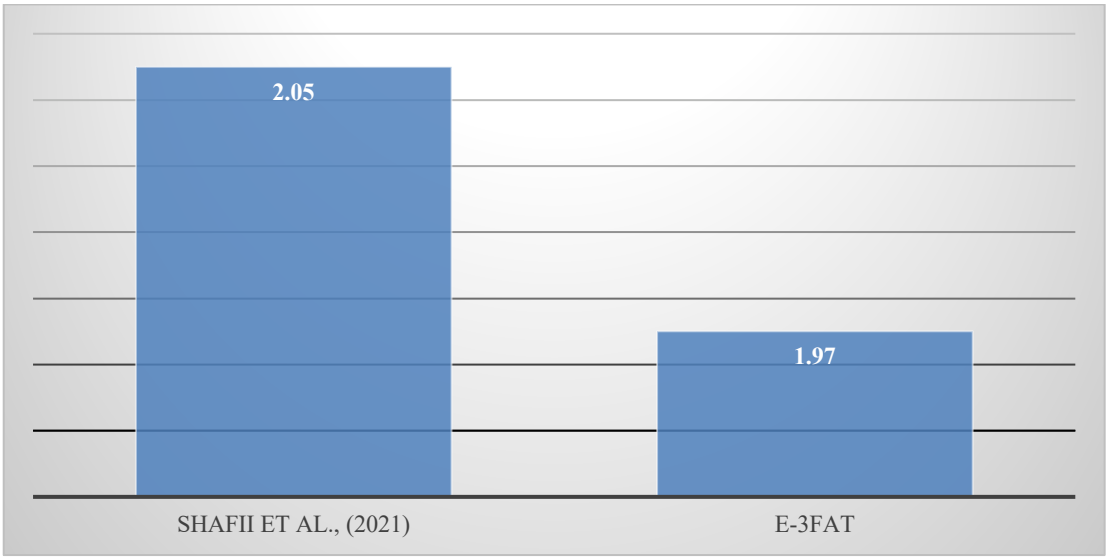


Figure 8: Comparative Analysis of Average FPR Performance Accuracy

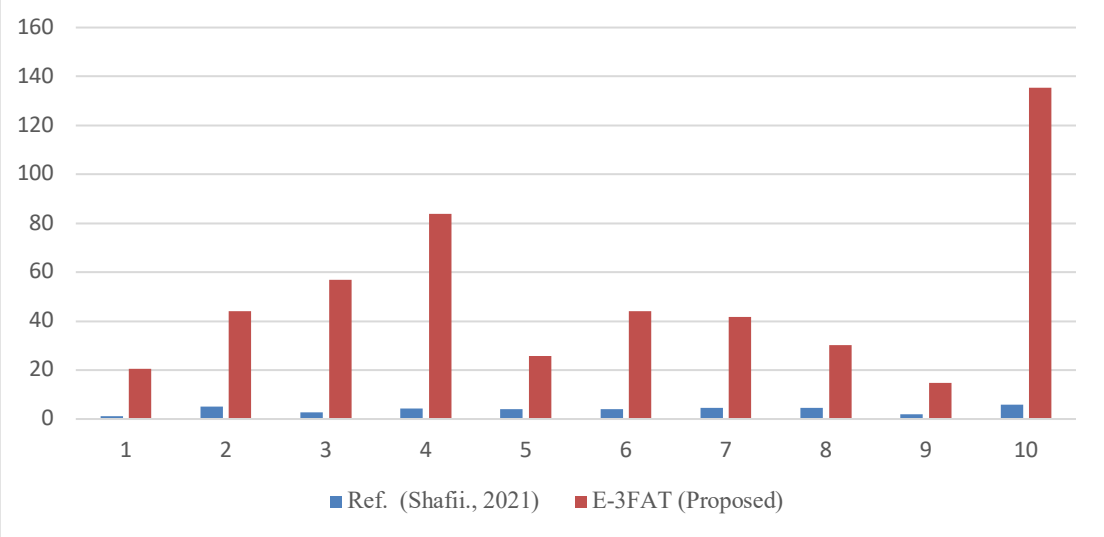


Figure 9: Comparative Analysis of Running time (secs)

5 Discussion

This section compares the experimental results of the proposed detection technique with existing blue screen detection techniques proposed by Shafii et al (2021). The comparison is based on two metrics: Table 3 presents the performance accuracy and Table 4 the running time. From Table 3, the results show that the E-3FAT technique performed better than the existing technique in 10 out of the 10 video datasets for the TPR and 6 out of the 10 video datasets in the case of FPR respectively, the best accuracy rate is in bold font. The performance accuracy rate was used to evaluate the efficiency of the proposed technique, as this is the most common standard used for video-related detection and algorithm evaluation. Table 4 presents the experimental results on the

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

running time. From the results presented the existing detection technique for blue screen forgery records a lower running time in 10 out of the 10 results as compared to the proposed technique.

Figures 7 and 8 present the average performance accuracy of the proposed blue screen detection technique using the same video dataset. The accuracy rate was used to evaluate the efficiency of the proposed technique, which is the most common standard of video-related detection and algorithm evaluation. The performance accuracy of the proposed technique is displayed above, with a higher accuracy of True Positive Detection Rate (TPR) of 98.03% and False Positive Rate of 1.97% compared to existing techniques with a True Positive Rate of 96.5% and False Positive Rate of 2.05%. A classifier with a higher TPR that maximizes true positives is better. The experimental results indicate that video compression does not affect our proposed detection technique. However, the results show that the performance of existing techniques drops when the video is compressed twice. Figure 9 presents the running time result. From the result presented, it can be observed that the existing technique for blue screen forgery took less computation time compared to the proposed E-3FAT detection technique. In each experiment, the existing technique consistently obtained a lower running time in all ten (10) videos.

6 Conclusions

Blue screen composition is a common method of digital video forgery. However, detecting this type of forgery is becoming increasingly important to digital forensic investigators due to advances in digitalization. There are only a few algorithms that have been proposed to detect manipulation in digital video through blue screen composition. We propose an Enhanced 3-stage Foreground Algorithm for Blue Screen Video Forgery Detection on double compressed videos to address this. The proposed technique consists of three phases: extraction, detection, and Discriminative Correlation Filter with Channel and Spatial Reliability (CSR-DCF) tracker object tracking. In the extraction phase, foreground elements in a digital video are extracted using GMM. In the detection phase, the homogeneity function is calculated as a descriptive feature. In the last phase, a Discriminative Correlation Filter with Channel and Spatial Reliability (CSR-DCF) tracker object tracking algorithm is used to study the tempered frame and track the block of subsequent frames. From the findings, the proposed detection technique could detect video manipulation using blue screen composition even when the forged regions were compressed twice. The true positive detection rate was 98.03%, and the false positive detection rate was 1.97%. This is an improvement over the earlier techniques which had a true positive detection rate of 96.05%, and a false positive detection rate of 2.05%.

Acknowledgment

The authors acknowledge Shafii Kasim and Musa Nura for their insight during the early stages of the research.

References

Alhassan, J. K., Oguntoye, R. T., Misra, S., Adewumi, A., Maskeliūnas, R., and Damaševičius, R., (2018) "Comparative evaluation of mobile forensic tools," in Advances in Intelligent Systems and Computing, 2018, vol. 721, pp. 105–114. doi: 10.1007/978-3- 319-73450-7_11*., Engineering, and Informatics (MEI).* Orlando, Florida, United States of America, 9-18.

Bagiwa, M. A., Wahab, A. W. A., Idris, M. Y. I., Khan, S.& Choo, K. K. R. (2016). Chroma key background detection for digital video using statistics correlation of blurring artifact. *Digital Investigation*, *19*, 29-43

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).*

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Dhaka, Bangladesh: IEEE.

Ferreira, S., Antunes, M., & Correia, M. E. (2021). A dataset of photos and videos for digital forensics analysis using machine learning processing. *Data*, *6*(8),87. https://machinelearningspace.com/object-tracking-python

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

Kingra, S., Aggarwal, N., & Singh, R. D. (2016). Video Inter-frame forgery detection: A survey. *Indian journal of science and technology*, *9*(44), 1-9.

Kohli, A., Gupta, A., & Singhal, D. (2020). CNN-based localization of forged region in object-based forgery for HD videos. *IET Image Processing*, *14*(5), 947-958.

Liu, Y., Huang, T., & Liu, Y. (2018). A novel video forgery detection algorithm for blue screen compositing based on 3-stage foreground analysis and tracking. *Multimedia Tools and Applications*, *77*(6), 7405-7427.

Lukežic, A., Vojír,T., Zajc,L.C., Matas, J., and Kristan,M., (2017) "Discriminative Correlation Filter with Channel and Spatial Reliability," *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, USA, 2017, pp. 4847-4856, doi: 10.1109/CVPR.2017.515

Mehrjardi, F. Z. Ali, M. L., Mohsen S. Z., Razieh S., (2023) "A survey on deep learning-based image forgery detection", Pattern Recognition, Volume 144, 2023, 109778, ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2023.109778

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

Naskar, J. B. (2018). A Digital Forensic Technique for Inter–Frame Video Forgery Detection Based on 3D CNN. *International Conference on Information Systems Security. ICISS2018, Lecture Notes in Computer Science, vol 11281.*Springer, Cham.

Raj, M., & Bakas, J. (2023*).* Detection of Object-Based Forgery in Surveillance Videos Utilizing Motion Residual and Deep Learning*. In: Molla, A.R., Sharma, G., Kumar, P., Rawat, S.(eds) Distributed Computing and Intelligent Technology. ICDCIT 2023. Lecture Notes in Computer Science, vol 13776,* pp.141-148. *Springer, Cham. https://doi.org/10.1007/978-3- 031-24848-1_10*

Osho, O., Mohammed, U.L., Nimzing, N.N., Uduimoh, A.A, & Misra, S (2019) "Forensic Analysis of Mobile Banking Apps," in Computational Science and Its Applications – ICCSA, pp. 613–624.

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

Sachdeva, S., Raina, B.L., Sharma, A., (2020) "Analysis of Digital Forensic Tools," J Computational Theoretical Nanoscience, vol. 17, no. 6, pp.2459–2467, Sep. 2020, doi:10.1166/jctn.2020.8916

Shafii, K., Bagiwa, M. A., Obiniyi, A. A., Sulaiman, N., Usman, A. M., Fatima, C. M., & Fatima, S. (2021). Blue Screen Video Forgery Detection and Localization Using An Enhanced 3-Stage Foreground Algorithm. *FUDMA Journal of Sciences*, *5*(2), 133-144

Shah, Y., Shah, P., Patel, M., Khamkar, C., & Kanani, P. (2020). Deep Learning model-based Multimedia forgery detection. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC)* (pp. 564-572). IEEE.

Sindhu, K.K, and B. B. Meshram (2012), "Digital Forensics and Cyber Crime Datamining," Journal of Information Security, vol. 03, no. 03, pp. 196–201, doi: 10.4236/jis.2012.33024.

Su, Y., Han, Y., & Zhang, C. (2019). Detection of Blue Screen Based on Edge Features *6th IEEE Joint International Information Technology and Artificial Intelligence Conference.* Chongqing, China: IEEE.

Xu, J., Yu, Y., Su, Y., Dong, B., & You, X. (2012). Detection of blue screen special effects in videos. *Physics Procedia*, *33*, 1316-1322.