Global Journal of Engineering and Technology [GJET].
ISSN: **2583-3359** (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/journal-gjet-home/

AN ENHANCED THREE-STAGE FOREGROUND ANALYSIS AND TRACKING ALGORITHM FOR BLUE SCREEN COMPOSITION

By

ABDULLAHI, Fatimah Binta[1]* and **MUHAMMAD, Sani Haliru**[2]

[1]Department of Computer Science, University of Abuja
[2]Department of Computer Science, Ahmadu Bello University, Zaria

Article History

Received: 11/04/2026
Accepted: 18/04/2026
Published: 20/04/2026

Vol – 5 Issue – 4

PP: - 27-34

Abstract

One of the most prevalent approaches to identifying video forgery is the use of blue-screen composition. However, from literature, very limited algorithms exist for detecting video forgery. An enhanced three-stage Foreground Analysis and Tracking (E3FAT) algorithm has been developed to detect blue-screen composition. The E3FAT framework operates in three phases: In the first stage, foreground blocks are taken from the target video using a Gaussian Mixture model (GMM). During the second stage, the homogeneity function is utilized to process the extracted images taken from the target video. In the final phase, forged blocks are rapidly tracked using the Discriminative Correlation Filter with Channel and Spatial Reliability (CSR-DCF) algorithm. Empirical evaluation demonstrates that E3FAT achieves a reliable detection of video manipulation, of 98.03% true positive rate and an average processing time of 95.57 seconds.

Keywords: *Blue Screen Composition, Homogeneity, Foreground Analysis, Three-Stage. Tracking algorithm*

INTRODUCTION

Modern digital devices with camera functions have made video and capturing images easy and possible. As such, the use of devices in capturing and creating images makes it difficult for fake videos and images to be traced to their sources. These devices are easily used by digital criminals to capture, edit, and distribute counterfeit videos and pictures that cannot be easily traced back to the criminals. The availability of free editing software like OpenShot, kdenlive, and Blender has contributed immensely to the ease of editing videos and images. The accessibility of this software makes it easy for videos and images to be tempered. Note that tempered videos and images may carry false information about events as well as crime scenes. False information can be posted online, which may result in social instability. Therefore, ensuring the integrity and authenticity of video content has emerged as a critical necessity, especially since videos that are displayed on the internet should not be accepted blindly without verifying and authenticating the sources.

Digital Forensics (DF) is an emerging discipline focused on verifying digital information and uncovering criminal activity (Sindhu & Meshram, 2012). It involves systematic collection, identification, extraction, and documentation of electronic evidence from various devices, which can subsequently be presented in court as legal proof (Misra et al., 2018). DF tools uses multiple categories of data, including data from devices, computer systems, mobile devices, and cloud computing. (Osho *et al.*, 2019). The majority of current research emphasizes digital image forgery detection, whereas investigations into digital video forgery remain less developed. Such studies are typically classified into active and passive forensic methodologies [30]. Active forensic methods typically rely on the incorporation of watermarks or digital signatures to safeguard and verify digital video content. Tampering with this operation usually leads to the destruction of these signals. Many of the imaging devices lack built-in signal embedding capabilities embedding functions, guaranteeing signal removal or re-embedding becomes challenging. Passive forensic approaches circumvent this limitation by requiring no auxiliary signals, relying instead on inherent video coding features and statistical properties to detect tampering. These modifications are vital indicators of video forgery detection. Video forgery techniques can be divided into inter-frame and intra-frame categories. Inter-frame forgery encompasses operations such as frame insertion, deletion, replacement, and copy-move, while intra-frame forgery parallels image forgery, targeting modifications within a single frame, such as copy-paste, logo elimination, or matting synthesis. There are several achievements in passive forensics, however, the major ones are as follows: The research performed by the Farid group from Dartmouth University United States presented some detecting methods

*Corresponding Author: ABDULLAHI, Fatimah Binta

for video forgeries detection, the authors proposed a technique that exposes digital forgeries using MPEG double compression (Wang and Farid 2006), a technique that exposes digital forgeries in an interlaced and de-interlaced video (Wang and Farid 2007a), similarly, a technique for detecting video frame replication using the gray level vector (Wang and Farid 2007b), for detecting of tampering in MPEG videos often relies on double quantization judgment, which serves as a key forensic indicator. (Wang and Farid 2009). An algorithm in (Kobayashi *et al.*, 2009) proposed video tampering that can be identified through discrepancies in noise patterns, as forged areas typically originate from different source videos that exhibit inconsistent noise characteristics. Another approach to video tamper detection has been proposed to use accumulated differential images by Zhang et al. (2009). This method detects tampering by analyzing the textural features surrounding the altered regions, thereby revealing traces of manipulation. This approach may be employed for moving objects eliminated from a stationary background. The experimental results, however, can easily be affected by trees, flowers, and plants in the environment. Another detection algorithm, a copy-paste forgery, was developed by Subramanyam and Emmanuel (2012). This method integrates HOG-based feature matching with video compression characteristics to enhance tamper detection. This algorithm was effective and had robust results against other signal-processing manipulations. The authors (Chittapur *et al*., 2014) introduced a technique that detects forged frames in video by employing mean frame comparison, enabling the identification of manipulated groups of pictures within the input video.

In D'Amiano *et al*. (2015), A new algorithm was introduced to achieve precise localization of copy-move video forgeries. Similarly, in (Bidokhti and Ghaemmaghami 2015), A passive approach for detecting copy-move video forgery in MPEG videos was introduced, in which each frame is divided into segments and the optical flow coefficient is computed for each part. Forged regions are identified when suspicious objects exhibit abnormal trends in their optical flow coefficients.

Blue screen composition has been established as a cutting-edge video forgery detection approach; only a handful of algorithms currently address this challenge. Su *et al*. (2011) examine variations in color signal correlations at object edges within tampered videos. The Prewitt algorithm was employed to detect edges, followed by the calculation of sensitive factors to highlight suspicious points. The resulting suspicious rate indicated compositing, though the method's accuracy is vulnerable to noise and dynamic foregrounds. The computational cost of this is high, the reason being that each frame requires an object segment technique (Felzenszwalb and Huttenlocher, 2004) and uses a proposed feature designed to identify suspicious points for statistical analysis. Xu et al. (2012) demonstrated that the discrepancies in quantified DCT coefficient statistics between foreground and background regions could serve as indicators of blue screen compositing. The reliability of this technique fluctuates with bit rate, achieving accuracy above 90% at best and dropping to around 70% at worst. Moreover, its applicability is restricted to the MPEG video format; in creating a tampered video, it is necessary that the two source videos come from distinct encoders. Foreground extraction relies on rough segmentation, where the separation of foreground elements from other regions must be performed manually, other than through automated processes. The authors (Mustapha *et al*., 2016) introduced a blind detection method to examine the correlation of blurring artifacts extracted from digital video. This technique successfully identified video manipulations involving chroma key compositing, with a performance metric of 91.12% true positive detection rate and 1.95%. false positives. In contrast, earlier approaches for the detection of blue screen compositing forgeries struggled to balance both accuracy and efficiency, making this proposed method a significant improvement. Existing approaches suffer from multiple drawbacks, including constraints related to video format, bit rates, encoding mechanisms, foreground segmentation algorithms, and overall video complexity (such as noise interference and non-tampered foreground elements). To overcome these shortcomings, this work introduces an Enhanced Three-stage Foreground Analysis and Tracking algorithm (E3FAT), specifically designed to identify blue screen compositing. The E3FAT can identify high accuracy and effectiveness in blue-screen compositing forgeries. The Enhanced Three-stage Foreground Analysis and Tracking algorithm (E3FAT) can accurately and efficiently detect blue screen compositing forgeries. It operates through three primary stages: The target video's foreground blocks are first taken using a GMM. Subsequently, a homogeneity function is applied to compute the resulting image, and the CSR-DCF algorithm is utilized to rapidly track and identify forged blocks within the digital video. The experiments conducted demonstrate that the proposed E3FAT algorithm not only achieves precise localization of forged regions but also demonstrates strong performance in processing speed. The paper is structured as follows: Section 2 reviews related work on blue screen compositing techniques; Section 3 details the proposed algorithm; Section 4 presents experimental results and analysis; and Section 5 concludes with final remarks. In 2011, Su et al., 2011 developed a detection method to identify blue screen compositing forgeries by leveraging edge features. This approach examines variations in the correlation between color signals along the edges of individual elements within the manipulated video. Using the Prewitt algorithm, the edges of these elements are extracted, and sensitive factors are calculated to pinpoint suspicious regions, thereby revealing potential tampering. The empirical evaluation effectively validated the detection of blue-screen composition in digital video under diverse output bit rates. Unfortunately, the accuracy of this technique was compromised by noise and other moving foreground elements. To address these shortcomings, Junyu proposed an alternative approach in 2012 for detecting blue screen compositing effects. This method leveraged differences in quality between the video's background and foreground, along with the statistical characteristics of quantified discrete cosine transform (DCT)

*Corresponding Author: ABDULLAHI, Fatimah Binta

coefficients in composite videos. The empirical evaluation result for this approach shows that the approach can successfully identify blue screen compositions in digital videos. However, the accuracy of this technique declines when different bitrate encoding schemes are applied, and its applicability is limited solely to the MPEG video format. Thus, limits the proposed approach. Similarly, the 3FAT framework proposed by Liu in 2017 detects blue-screen compositing forgeries through the extraction of foreground, detection of forged blocks, and tracking, yielding 97.3% true positives and 7.8% false negatives. Notably, the approach eliminates distractions caused by noise and other moving foreground indicators in digital video. It is versatile, functioning across any video format, bit rate, and encoding mechanism, while maintaining excellent processing speed. The technique remains limited in its ability to detect faked regions of very small sizes. Moreover, rapid background motion in digital video introduces non-ideal experimental effects, which further restrict the effectiveness and practical implementation of the technique. Shafii et al. [15] introduced a forgery detection method for blue-screen compositing, employing GMM for foreground extraction and entropy analysis for feature detection, and a subsequent tracking phase using the MOSSE algorithm efficient for tracking forged blocks within the digital video.

Experiments confirmed the method detects blue-screen forgeries with 98.02% true positives and only 1.99% false positives, even for small regions

MATERIALS AND METHODS

Building on existing literature, this paper proposed enhanced algorithm for blue-screen compositing video forgery detection. The framework comprises three stages: foreground extraction using GMM, feature detection via a homogeneity function, and forged block tracking with CSR-DCF. Figures 1 and 2 illustrate the paper framework and flowchart, respectively.

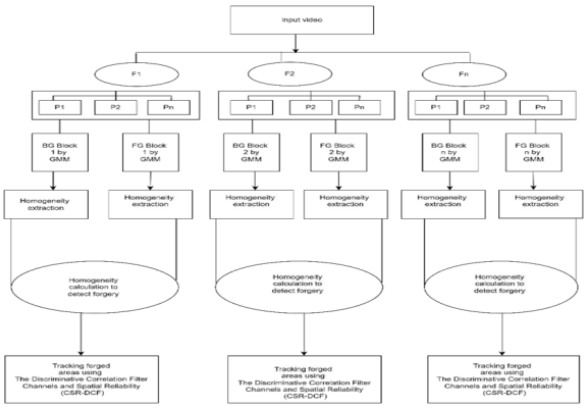


Figure 1: E3FAT Framework

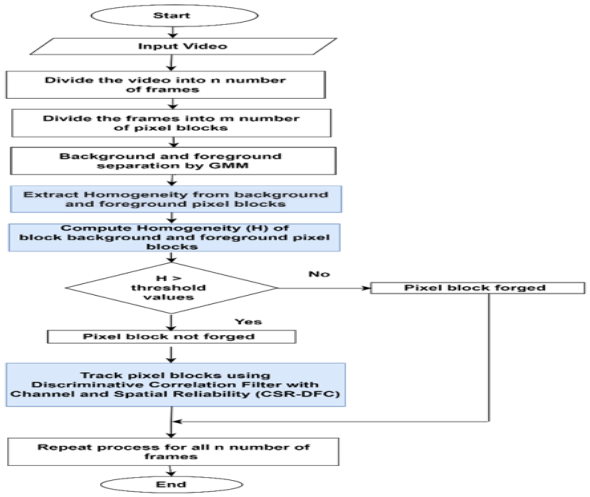


Figure 2: E3FAT Flowchart. (Muhammed et at. (2024))

A. Extraction

This section explains how video frames are broken down into pixels, with GMM used for extracting foreground elements based on temporal pixel sequences (Stauffer and Grimson, 2002).

Aslam (2017) described GMM as a probability density function formed by weighted Gaussian components, useful for background modeling and object segmentation. Stauffer and Grimson pioneered this approach, later expanded by Genovese (2013). The weighted sum of the Gaussian distributions expressed as the probability is given by equation (1).

$$P(x_t) = \sum_{i=1}^{k} w_{i,t}u_{i,t} * \eta(x_t u_{i,t} \sum t, i \quad (1)$$

where W represents the weight estimate, and k the number of distributions μ, both the average value and $\sum i, t$ is the mixture's ith Gaussian's covariance matrix at t time.

$t.n(x_t, \mu \sum,)$ According to Radi and Dugelay (2012), the Gaussian probability density function is. Obviously. The mixture's mean is provided in equation (2).

$$\mu_t = \sum_{i-1}^{k} w_{i,t}\mu_{i,t} \quad (2)$$

To improve the outcome and gain a deeper understanding of the process, the following actions were taken.

Step 1: Each input pixel is compared with the mean " μ " of the corresponding component. If the selected component's value is close enough to the input pixel's mean, then it is considered the matched component. Note the disparity between the mean and the pixel must be less.

Step 2: The Gaussian weight mean and variance are then updated to reflect the newly found pixel value for the non-matched components, and the weight "w" will decrease while the mean and standard deviation remain constant.

*Corresponding Author: ABDULLAHI, Fatimah Binta

Step 3: The components that the backdrop model would consist of will be listed. This is obtainable by setting a threshold value for the component.

Step 4: The final step involves identifying the foreground pixel. However, there will not be any pixels that will match between the foreground-designated pixels and any other element in the background.

While GMM effectively extracts foregrounds, it introduces noise. A morphological method removes these pixels before homogeneity detection, as depicted in Figure 6. This process comes before the homogeneity detection and computation phase.

B. Detection

The detection phase begins with the retrieval of relevant foreground blocks through the GMM. Its purpose is to check the manipulated target video and to locate forged blocks. A homogeneity function is computed to differentiate the foreground from the background pixel blocks. The homogeneity function computes local changes in pixel brightness within a specific neighborhood or window to determine how uniform or similar an image is. In each region, the image would be more uniform if it had a greater homogeneity value. One popular formula for computing the homogeneity function is Haralick's homogeneity measure. This co-occurrence matrix depicts the spatial associations on pairs of pixels in a picture and serves as its foundation. Where higher homogeneity levels correspond to more detailed images or videos. In addition, incoming photos, textures, or movies are described using it. To compute the homogeneity function from photos, the following procedures were followed:

The image is separated into tiny, non-overlapping sections known as blocks or tiles. The application and the required level of information will determine the block sizes. Equation 3 is used to get the homogeneity value for each block.

$homogeneity = sum(pixel\_intensity$ −mean_intensity) *2 / (block_size–1) (3)

where the following represents the pixel's intensity value inside the block.

1. $pixel\_intensity$
2. $mean\_intensity$: the average intensity value for each pixel in the block.
3. $block\_size$: total number of pixels in the block.

Steps two and three are repeated for each block in the picture.

Homogeneity values are used as a threshold to identify areas where the homogeneity value differs noticeably from the surrounding areas. Here, the application and the intended level of its sensitivity are considered while finding the threshold. Here, regions with the homogeneity value above the threshold show the presence of forgery.

4. For every block, the resulting data will show its homogeneity function for the particular block. Where a greater homogeneity or uniform pixel intensities within the block is indicated by higher values, whilst greater inconsistency or heterogeneity is indicated by lower values.

C. Tracking

Tracking an object is the identification of objects in the target video's subsequent frames or figuring out where an object appears in each frame. Historically, many algorithms were proposed for locating objects. Here, a quick object-tracking technique is suggested to locate an object that resides in the target video's current frame. Numerous practical uses exist for tracking, such as traffic management, security, and surveillance. For tracking visual objects, this paper considers the CSR-DCF tracker. For the channel features and matching target templates (filters), where the probability is to be maximized to predict position X. Assuming g comprise of N_d, channels attribute of $f = \{f_d\}d_1 : N_d$ with their corresponding filters $h = \{h_d\}d_1 : N_d$

where $f_d \in Rd_w * d_{h,} h_d \in Rd_w * d_h$, The position X is estimated by maximizing the probability as presented in equation 4 below.

$$P\left(\frac{X}{h}\right) = \sum_{d=1}^{Nd} P\left(\frac{X}{f_d}\right) P(f_d) \quad (4)$$

The density $P\left(\frac{X}{f_d}\right) = [f_d * h_d]$ is assessed at X after a feature map and a learnt template are convolutional and $P(f_d)$ indicates the dependability of the channel.

Assuming the following channels with independent features, by reducing the sum of squared discrepancies in the correlation outputs channel-wise and the intended output, optimal filters are received during the stage of learning $g \in Rd_w * d_h$,

$$argmin_h \sum_{d=1}^{Nd} //f_d * h_d - g//^2 + X \sum_{d=1}^{Nd} //h_d//^2 =$$
$$argmin_h \sum_{d=1}^{Nd} (//\hat{h_d^H} diag(\hat{f_d}) - \hat{g_d}//^2 + X//\hat{h_d}//^2 \quad (5)$$

The operator in equation (5) and Parseval's theorem yield the equivalence. $\hat{a} = vec(f[a])$ has been transformed into a column vector using the Fourier transform, i.e., $a \in R^{D*1}$, with, $D = d_w d_h$, diag (a) forms a D x D diagonal from a and $(.)^H$ is a Hermitian transpose. By equating the complex gradient of equation (4) concerning each channel zero, the minimization of equation (5) provides a closed-form solution. This approach has boundary faults since it assumes all pixels are equally dependable for filter learning and input circularity.

Dataset

Ten short videos used by Liu et al. (2018) for blue screen acquisitions retrieved from YouTube made up the dataset. Table 1 gives a summary of the data set, including the number of frames in each video. The videos were uniformly reduced to 640 x 360-pixel sizes.

(1)

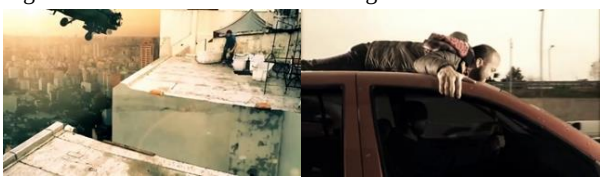
(2)

*Corresponding Author: ABDULLAHI, Fatimah Binta

(3) (4)

(5)

Figure 3 Frames Taken from Five Original Videos



(6) (7)

(8) (9)

(10)

Figure 4 Frames Taken Out of Five Fake Videos

RESULTS AND DISCUSSION

Table 1 presents a summary of the data set for the 10 videos together with their number of frames and their respective sizes.

Table 1: Classification of Video Dataset

Video datasets	Size (MB)	Number of Frames
Video 1	4.49	102
Video 2	21.4	474
Video 3	4.87	181
Video 4	12.8	339
Video 5	8.67	305
Video 6	20.3	317
Video 7	10.7	384
Video 8	17.5	407
Video 9	3.85	130
Video 10	31.3	474

The performance evaluation of these techniques was measured for all frames in 10 videos in the dataset. We evaluate the proposed E3FAT technique with True Positive Detection Rate (TPR), as this represents the acceptable standard for video-related detection and algorithms. Equation (6) is the mathematical representation of TPR, respectively.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

Here, TP: number of authentic videos correctly identified as authentic, TN: number of forged videos correctly identified as forged, FP: number of authentic videos that are incorrectly identified as forged, and FN: number of forged videos that are incorrectly identified as authentic. Tables 2 and 3 present the performance evaluated on frames from each of the 10 videos in the study's dataset. For every video, the study calculates the TPR and the FPR. A TPR with a higher value and a lower FPR (minimizing FP while maximizing TP) is generally better. The reason this performance accuracy rate was utilized is because of its effectiveness for the proposed technique, as this is a benchmark metric used for related video detection and algorithm tests. Tables 2 and 3 show the TPR and FPR results from the video datasets. The TPR shows that Shafii *et al.* (2021) and the E3FAT both produce better TPR in 5 out of the 10 videos. For PFR results in Table 3, the E3FAT produces better FPR in 6 out of the 10 videos.

Table 4 presents the performance evaluation of the running time in seconds. Figure 4 shows the average performance accuracy.

Table 2: TPR results on Original Videos

Test Videos	Size (MB)	Number of Frames	Su (2011) TPR (%)	Liu (2017) TPR (%)	Shafii *et al.*, (2021) TPR (%)	E3FAT TPR (%)
Video 1	4.49	101	90.80	97.50	97.80	**98.42**
Video 2	21.4	473	91.90	98.20	**99.37**	97.81
Video 3	4.87	180	92.70	98.04	97.57	**98.03**
Video 4	12.8	338	90.20	95.00	96.90	**98.20**
Video 5	8.67	304	90.90	96.40	97.79	**98.01**
Video 6	20.3	316	91.30	97.20	**98.98**	98.17
Video 7	10.7	383	92.50	96.40	97.15	**98.01**
Video 8	17.5	406	93.50	97.20	**98.44**	98.05
Video 9	3.85	129	94.00	96.10	**98.27**	98.15
Video 10	31.3	473	97.20	97.40	**97.98**	97.49
Average			92.00%	97.05%	98.02%	**98.03%**

*Corresponding Author: ABDULLAHI, Fatimah Binta

Table 3: FPR results on Original Videos

Test Videos	Size (MB)	Number of Frames	Su (2011) FPR (%)	Liu (2017) FPR (%)	Shafii *et al.*, (2021) FPR (%)	E-3FAT FPR (%)
Video 1	4.49	101	2.80	2.40	2.20	**2.00**
Video 2	21.4	473	2.32	2.22	0.63	1.90
Video 3	4.87	180	3.32	2.65	2.44	**2.10**
Video 4	12.8	338	3.80	2.80	3.10	**1.80**
Video 5	8.67	304	2.95	2.44	2.21	**2.20**
Video 6	20.3	316	2.56	2.00	1.02	1.80
Video 7	10.7	383	2.10	2.98	2.94	**1.95**
Video 8	17.5	406	1.99	1.75	1.56	1.75
Video 9	3.85	129	1.78	1.64	1.73	2.05
Video 10	31.3	473	2.45	2.30	2.02	**1.85**
Average			2.61%	2.3%	1.99%	**1.97%**

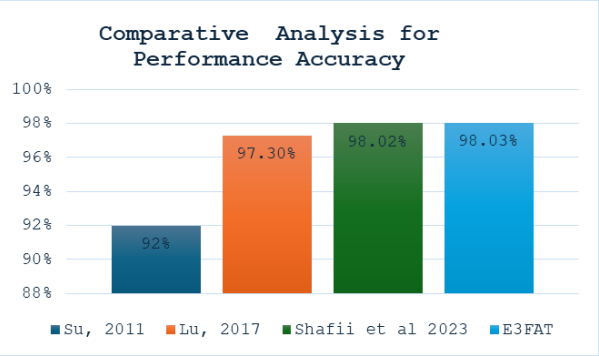


Figure 5: Average Performance Accuracy of the models

Table 4: Performance Evaluation of Running Time (secs) with Existing Studies

Videos	Su, 2011	Lui, 2017	Shafii et al, 2023	E3FAT
Video 1	2001.72	1257.91	262.16	**40.25**
Video 2	7090.96	4456.07	928.67	**199.45**
Video 3	1482.27	931.48	194.13	**124.96**
Video 4	222.31	139.71	**29.13**	147.24
Video 5	1533.16	963.46	200.79	**125.29**
Video 6	5238.82	3292.15	686.10	**67.29**
Video 7	442.41	278.12	**57.94**	118.45
Video 8	3042.31	1911.83	398.44	**84.38**
Video 9	2311.08	1452.32	302.67	**35.52**
Video 10	2132.91	1340.35	279.34	**150.88**
Average	2067.32	1299.13	270.75	**95.57**

The result for the computational time comparison and performance accuracy of the proposed E3FAT detection techniques with (Su, 2011), (Liu, 2017), and (Shafii et al, 2023) is presented. The empirical results shown in Table 2 demonstrate that the E3FAT detection technique outperformed the existing techniques with a lower running time of an average of 95.57 seconds; Shafii et al. (2021) had 270.75 seconds, Lui (2017) had 1299.13 seconds, and Su (2011) had 2067.32 seconds, respectively. Figure 3 presents the result for performance accuracy. From Figure 3, the proposed E3FAT algorithm produces an average accuracy rate of 98.03%, Shafii et al. (2021) produced 98.02%, Lui (2017) had an average accuracy rate of 97.30%, while Su (2011) produced 92%**.** The comparative results for the E3FAT technique and the other existing techniques show that E3FAT and Shafii et al (2023) recorded a higher performance accuracy value than Su (2011) and Lu (2017), respectively.

CONCLUSION

An improved three-stage foreground algorithm is proposed for blue-screen forgery detection. The framework employs GMM for extraction, homogeneity functions for detection, and CSR-DCF for tracking. Experimental evaluation confirms its effectiveness, yielding a true positive rate of 98.03% and an average processing time of 95.57 seconds. The results indicate that all the algorithms presented were able to detect forgeries with high accuracy. However, the proposed E3FAT and the Shafii et al. (2021) algorithms have the highest average TPR of 98.03% and 98.02%, whereas Su (2011) and Lui (2017) have 92% and 97.30%, respectively. In terms of the performance running time, the proposed E3FAT algorithm outperforms all the other three algorithms with an average time of 95.57 seconds.

CONFLICT OF INTEREST

The authors declared no conflict of interest.

REFERENCES

1. **Mustapha A. B, Ainuddin, W.A.W, Mohd, Y. I. I, Suleman, K, Kim-Kwang, R. C.** (2016) Chroma key background detection for digital video using statistical correlation of blurring artifact, Digital Investigation, Vol19, Pages 29-43, ISSN1742-2876
2. **Bidokhti A, Ghaemmaghami S** (2015), Detection of regional copy/move Forgery in MPEG videos using Optical flow. The International Symposium on Artificial Intelligence And Signal Processing (AISP), pp. 13-17
3. **Muhammad, S. H, Abdullahi, F.B., Mustapha, A.B, Suleiman, N.** (2024) Blue Screen Forgery Detection on Double-Compressed Videos Using Enhanced 3-Stage Foreground Algorithm, SuleLamido University Journal of Science & Technology Vol. 8 No. 2 pp.96-111 https://doi.org/10.56471/
4. **Candes EJ, Tao T** (2006) Near optimal Signal recovery from Random Projections: Universal

*Corresponding Author: ABDULLAHI, Fatimah Binta

Encoding Strategies. IEEE Trans Inf Theory 52(12):5406–5425

5. **Chen W, Yang G, Chen R, Zhu N** (2011), Digital video passive forensics for its authenticity and source. J Communication 32(6):77–182
6. **Chittapur, G.B., Murali, S., Prabhakara, H.S., Anami, B.S.** (2014). Exposing Digital Forgery in Video by Mean Frame Comparison Techniques. In: Sridhar, V., Sheshadri, H., Padma, M. (eds) Emerging Research in Electronics, Computer Science, and Technology. Lecture Notes in Electrical Engineering, vol 248. 557–562 Springer, New Delhi https://doi.org/10.1007/978-81-322-1157-0_57
7. D'Amiano, L., Cozzolino, D., Poggi, G., and Verdoliva, L. (2015), Video forgery detection and localization based on 3D patch match," *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, Turin, Italy, 2015, pp. 1-6, doi: 10.1109/ICMEW.2015.7169805.
8. Diaconis P, Freedman D (1984) Asymptotics of graphical projection pursuit. Ann Stat:793–815
9. Dibyendu M (2013) Multiresolution-based Gaussian mixture model for background suppression. IEEE Trans Image Process 22(12):5022–5035
10. Felzenszwalb PF, Huttenlocher DP (2004) Efficient Graph-based image segmentation. Int J Computer Vision 59(2):167–181
11. Jordan A (2002) On discriminative vs. generative classifiers: a comparison of logistic regression and Naïve Bayes. Adv Neural Inf Process Syst 14(1):841
12. Kobayashi M, Okabe T, Sato Y (2009) Detecting video forgeries based on noise characteristics, Advances in Image and Video Technology. Springer, 306–317
13. Li F, Huang T (2013) Video copy-move forgery detection and localization based on structural similarity. In: Farag A, Yang J, Jiao F (eds) Proceedings of the 3rd International Conference on Multimedia Technology (ICMT 2013). Lecture Notes in Electrical Engineering, Springer, Berlin, Heidelberg, vol 278, pp. 63–76
14. Otsu N (1979) A threshold selection method from gray level histogram. IEEE Trans Syst Man Cybernet 9(1):62–66
15. Porter T, Duff T (1984) Compositing digital images, Computer Graphics Proceedings, Annual Conference Series. ACM SIG-GRAPH, New York: 253–259
16. 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
17. Shujia Y, Lijun J, Shaohui D, Ling Z, Chunyu Y, Wenhao Z (2012) Power line image segmentation and extra matter recognition based on improved Otsu algorithm. IET Image Process 6(4):426–433
18. Smith AR, Blinn JF (1996) Blue screen matting. Computer Graphics and Interactive Techniques:259–268
19. Stauffer C, Grimson W (1999) Adaptive background mixture models for real-time tracking, 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2(3):246–252
20. Su Y, Han Y, Zhang C (2011) Detection of blue screen based on Edge Features, Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International. 469–472
21. Subramanyam AV, Emmanuel S (2012) Video forgery detection using HOG features and compression properties, 2012 I.E. 14th International Workshop on Multimedia Signal Processing (MMSP). 89–94
22. Vincent L (1994) Fast opening functions and morphological granulometries, Conference on Image Algebra and Morphological Image Processing. 253–267
23. Wang W, Farid H (2006) Exposing digital forgeries in video by detecting double MPEG compression, Proceedings of the 8th workshop on Multimedia and Security. ACM 37–47
24. Wang W, Farid H (2007a) Exposing digital forgeries in interlaced and deinterlaced video. IEEE Transactions on Information Forensics and Security 2(3):438–449
25. Wang W, Farid H (2007b) Exposing digital forgeries in video by detecting duplication, Proceedings of the 9th workshop on Multimedia & security. ACM 35–42
26. Wang W, Farid H (2009) Exposing digital forgeries in video by detecting double quantization, Proceedings of the 11th ACM workshop on Multimedia and Security. ACM 39–48
27. Wang Z, Bovik AC, Sheikh HR (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
28. Wright J, Yang AY, Ganesh A, Sastry SS, Ma Y (2009) Robust face recognition via sparse representation. IEEE Trans Pattern Anal Mach Intell 31(2):210–227
29. Xu J, Yu Y, Su Y, Dong B, You X, (2012) Detection of Blue Screen Special Effects in Videos International Conference on medical physics and biomedical engineering. Phys Procedia 33:1316–1322
30. Zhang K, Zhang L (2012) Real-time compressive tracking. Computer Vision - ECCV 2012:864–877
31. Zhang J, Su Y, Zhang M (2009) Exposing digital video forgery by ghost shadow artifact, Proceedings

*Corresponding Author: ABDULLAHI, Fatimah Binta

of the first ACM workshop on Multimedia in forensics. ACM 49–54

32. Zhou L, Wang D (2008) Digital image forensics. Beijing University of Posts and Telecommunications Press, Beijing, pp 8–13

*Corresponding Author: ABDULLAHI, Fatimah Binta