ISSN No:-2456-2165

Deep Fake Detection in Social Media Forensic Taxonomy, Challenges, Future Directions

[1]Dr.Hafiz Gulfam Ahmad Umar, [2]Muhammad Aoun, [3]Muhammad Haris Sarfraz, [4]Muhammad Farhan Ali, [5]Muhammad Younis
[1,2,3,4,5]Ghazi University CS & IT department Dera Ghazi Khan, Punjab, Pakistan

Abstract:- With the rapid growth of smartphone technology, it is now commonplace to upload & download videos as part of digital social networking. More incidents are being recorded on video than ever before, so the information on them is more valuable than ever. In this paper, we give a full review of how to get information from video content & find fakes. In this context, we look at different modern methods for detecting video fakes, computer vision & (ML) methods like (DL). We also discuss recurring resource, legal, alsotechnical issues, as well as the challenging of applying Deep learning for the task, such as the theory underpinning DL, CV, restricted, datasets, real-time processing, ML, employed with IoT-based devices. This survey also lists common video forensics analysis & investigation products. In this survey weexamine video content information extraction & counterfeit detection in detail, which, as far as we know, has not been done before.

Keywords:- *Digital Forensic, Anti Forensic, ML, DL, CV, Video forensic, video forgery.*

I. INTRODUCTION

Video content authentication has become a major issue as deep learning (DL) techniques improve & visual editing apps gain popularity. Video improvement has also garnered interest recently. De-blocking, noise reduction, & night contrast are covered. (VMF) is more vital than ever to ensure visual media accuracy & improve surveillance camera footage. Due to DL-based video forgeries & automated surveillance. Video material has been utilized as evidence in several legal proceedings worldwide. Because it's easier & more accurate to falsify recordings, video forensics is crucial for validating such evidence. Forged videos can be used to produce fake news or manipulate movie frames to mask a breach. Post-COVID workplace changes have made video communications the norm & permanently impacted how people communicate in business, banking, education, healthcare, & socially. Addressing these concerns has become more important. Communication is increasingly dependent on video authenticity. Fake videos on social media caused individuals to lose faith in the news & cease seeking the truth, according to a survey. In April 2018, BuzzFeed Video posted a video of Barack Obama talking directly the camera (BuzzFeedVideo, 2018) to demonstrate political news deception. The first 35 seconds of the clip showed Obama's face, then his statements got worse. The split-screen featuring Obama on the left & Jordan Peele, prominent US comedian, right shows how online films can be misinterpreted almost halfway through the film. AI synchronized lipsync& facial expressions. The video quickly went popular due to its quiet theme. Maras & Alex & rou (2018) discussed how Deep fake algorithms replicate movements, voices, & variations to make fake movies look authentic. As hardware & software improve, making these videos becomes easier, the writers noted. Video forensics can discover false videos & more. As the number of digital devices that can create & retain video data grows, does the need to recognize fakes & derive usable information from such data. Hence, video forensics processes video data for court evidence. Xiao said video evidence is compared to well-known photos of persons, vehicles, attire, & weaponry.

Because of their popularity, videos are everywhere. Video forensics is significant because bogus movies are more common & deep learning can extract data from videos. Because false recordings touch people's daily lives & automated video monitoring is rising, studying how to recognize them is more vital than ever. So, we will study video forensics to learn about data collection & forgery. This survey required a ten-year literature review. This review covered "video forensics," "analysis," "forgery detection," & "information extraction." Video forensics tools required much research to use. Below are our significant accomplishments. We explain image & video forensics first.

- In this article, we examine the most recent methods (ML & CV) for video forensics that have been put forth in recent years.
- We look at active & passive video forgery, frame forgery, & different methods for video forgery that use DL.
- Along with talking about how to find copy-moves, we also talk about how to get data out of videos, how to fake videos, & how to improve videos.
- We list the difficulties users & researchers in video forensics have to deal with.
- We give a discussion on several tools used in video forensics for finding evidence.

II. BACKGROUND

Combining video pictures creates a moving picture. frames. Resolution & FPS vary. A movie's resolution is its pixels per frame, while FPS is its frame rate. Videos are admissible in court. Hence, "video forging" has evolved to manipulate video material. Copy-move forgery & copy-paste fraud are prominent video faking methods. Copy-move forgeries involve moving a component of an image to hide information. Copy-move involves editing video frames and also Copy-paste forgeries change a video scene's meaning (Tembe&Thombre). Figure 2 shows copy-move forgeries. To alter videos, add, switch, or remove frames in any order. Milani e divided video forgery detection into active & passive categories. Active forgery detection

ISSN No:-2456-2165

watermarks or digitally signs videos. Pre-processing slows video clip production. As counterfeit videos cannot recover the digital signature & watermark, the video will be assumed to be fake. However, altering a movie to examine statistical correlations is a passive forgery detection strategy. The film is fake if the correlations don't match. Deep learning CNN model by Yao et al. (2017) detects object-based counterfeiting. This model uses five layers to swiftly gather high-dimensional information before pre-processing video frames, unlike typical CNN.

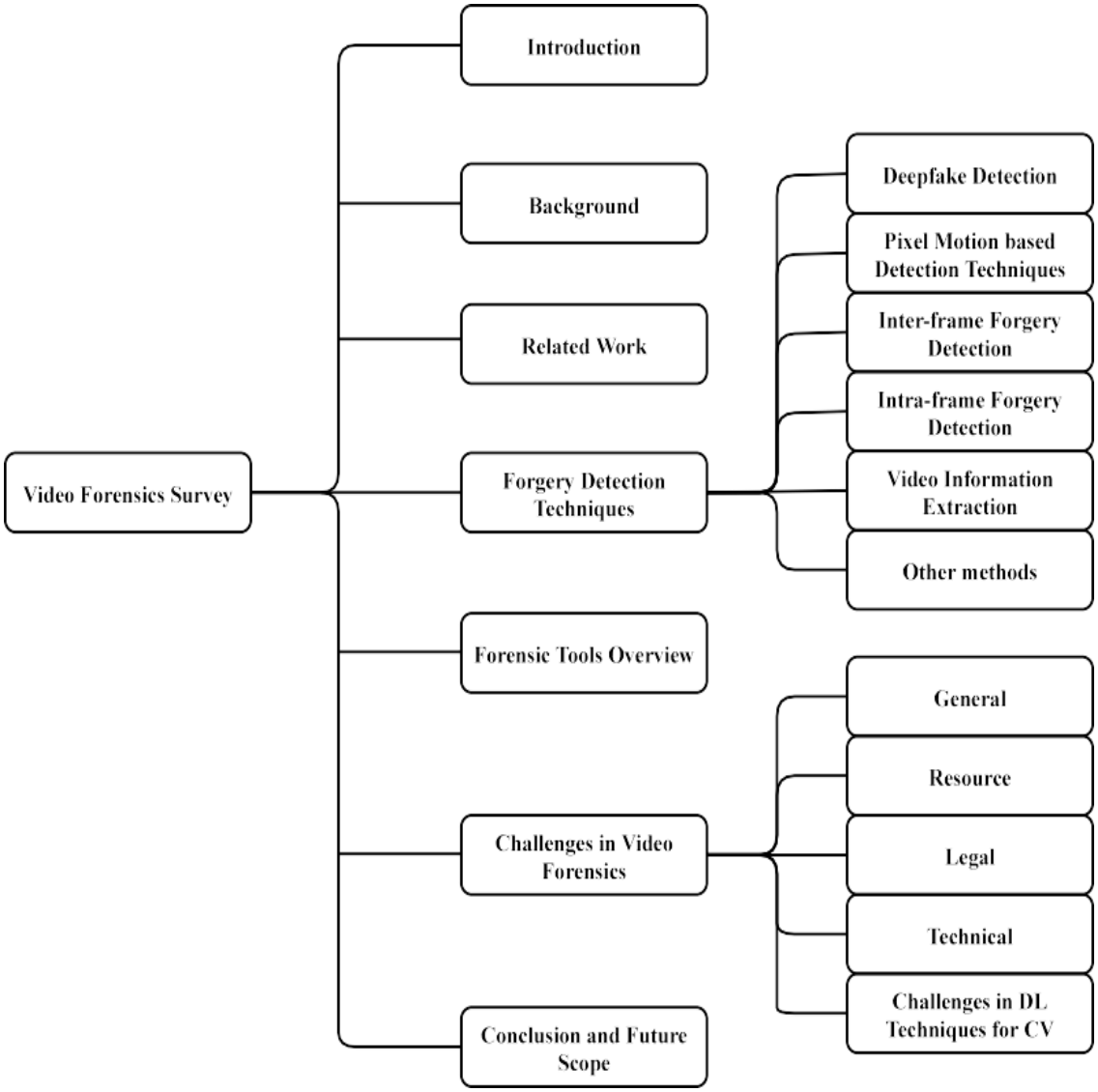

Fig. 1: Block Diagram

Xiao et al. (2019) say video forensics includes movie evidence. Face detection & key frame discovery help prosecutors find evidence in crime scene videos. Key frame extraction makes video from summary key frames of video sequences. Many communities struggle with key frame selection. video tampering detection block diagram.

III. RELATED WORK

A lot of video can be forensically examined. Video forensics research increased. Video forensics research surveys are summarized below. Shahraki et al. (2013) examined typical features & pros & cons of current video forensics software. Video forensics tool & product features were surveyed recently (Alsmirat et al., 2020). Wahab et al. examined active & passive video counterfeiting detection methods. Wahab et al. suggested improving passive video detection methods since basic distortions can be examined & identified, digital data semantics differ from digital evidence authenticity, &passive video detection systems can be improved. Complex distortions are harder to find. Kaur & Jindal's 2020b survey studied ways of video tampering that occur both between and within frames, whereas Sowmya & Chennamma's 2015 survey examined active & passive methods. Recent research have described many goods & their pros & cons. No survey included all video forensics detection methods & product information. This survey discusses connected survey article restrictions.

ISSN No:-2456-2165

Reference	DF Detection	Timeline	Published	Scope
[25]	Image/Video	2019	Arxiv	Covers how Deep fakes are made & how to find them from 2017 to 2020, but there aren't many studies from 2020.
[26]	Image	2020	Elsevier	The survey only looks at studies on how to change a person's face. It doesn't look at how to make or find deep fake videos.
[27]	Image/Video	2021	Arxiv	Along with the deep fake data sets, recent work on face synthesis, attribute manipulation, identity switch & expression Swap is addressed.
[28]	Image/Video	2021	ACM	Focuses on how different deep learning networks can be used to make & find deep fakes. Well-known structures from other subjects are also covered.
[29]	Image/Video	2021	Springer	Covers a brief overview of the tools used to make & find Deep fakes, as well as a small number of studies.
Current	Image/Video	2022	Sensors	Focuses on recentre search on how to make deep fakes & how to find them. It looks at deep fake tweets as well as images &videos. There are alot of new studies about well-known deep fake apps &methods.

Table 1: A comparison of reviews & surveys on deep fakes

IV. FORGERY DETECTION TECHNIQUE

Video forensics approaches are described here. Information extraction follows video forgery detection. Tables 4 & 5 list several of this essay's strategies with brief descriptions. Product information and video forensics in one survey. This survey examines the linked survey articles' limitations.

A. Deep fake detection

DL models made this. Auto encoders create feature maps from picture frames. Decoding another image creates the bogus image. Image 4 illustrates deep fake generation. Several algorithms use discrepancies to detect deep fake videos. Li suggested detecting deep fake films by their absence of realistic eye blinking. Li &Lyu suggested using closed-eyelid photos during the deepfake generator's training phase to eliminate this mismatch. Yang et al. did it differently. Yang et al. (2019) detected forgeries using in-depth fake films & inconsistent head orientations. Li &Lyu found no Using puppet master deep fakes or lip syncing (2018). McCloskey & Albright (2018) used generational adversarial network color artifacts to detect deep-fake pictures (GAN). According to Li &Lyu, targeting specific local regions of deepfake video frames with this technique is uncertain (2018). Someone offered Mesonet, which contained the algorithms Meso no 4 and MesoInception no 4, to identify Face-2-Face forged movies and deep false videos.. As a neural network could not identify both types of forgeries, two strategies were chosen. Li et al. Afchar's approach overfit to self-generated deep fakes, according to Li &Lyu (2018). They then used face warping artifacts to detect deep-fake films better than Mesonet. employed XcepTemporal, aIn order to recognize the temporal and spatial hallmarks of deep-fake videos, CNN architecture latent convolutional representations, bidirectional recurrent structures, and entropy-based cost functions. Pair learning and two-branch patch architecture were presented (PCNN). The first branch distinguishes between genuine and fake face patches, while the second branch, which detects deep fakes, records the differences between the face region and the non-facial region. Guarnera collected local attributes using expectation maximization for GAN modeling (EM). Wang found that neuron firing patterns finer information & feed into an external binary neural network were efficient & resistant to four well-known perturbation attacks.

Hence, most deepfake detection research uses many DL algorithms. Most study focuses on deep-fake film defects. DL models' feature extraction is used to boost performance & robustness. GAN adversarial training creates deepfakes. Fooling an algorithmic detector & iterating makes deep fakes more convincing. When they learn new detection methods, people can better avoid AI-based detection systems.

B. Pixel motion-based detection methods

To identify motion fraud, a movie is broken down into individual frames based on their pixels. To create a connection between the newly forged and original frames, Lin altered the pixel alignment of a copy-move section on a deteriorating frame. There is a spatial relationship between the authentic and false clips.. Wang suggested using ordered frames to compare frames & find more. Forgeries on static frames rendered the approach useless. Mathai predicted error notions for each unique block from each video frame using arithmetic moment descriptors. 52% of the st&ardized cross-correlation forgeries establishing threshold matches. Wu's team (2014) The velocity field showed a consistency-based strategy for detecting movie inter-frame forgeries. The velocity field consistency method calculates time-related displacements by comparing nearby video frames. Frame duplication & deletion should cause displacement. Zhang didn't find the updated location. Wang developed optical flow analysis to detect fakes. The OF is apparent brightness pattern movement velocity distribution. Unlike counterfeit processes, optical flows (OFs) vary almost continuously in movies.

Computing weight limits this strategy .Al-Sanjary developed copy-move forgery detection that analyzes optical flow fluctuation to identify harmonic movement in video frames. Al-Sanjary suggested an optical flow discrepancy-based method. Dynamic temporal warping

ISSN No:-2456-2165

(DTW) matching compares object movement displacement trajectories to find the duplicate. Zhang et al. (2016) upgraded Wu & Wang's (2014) approach (2014). The (MVP) & its variation factor were employed to detect frame deletion & duplication, with inter-frame forgeries' discontinuity points. It detected frame deletions better.

McCloskey & Albright used generational adversarial network color artifacts to detect deep-fake pictures (GAN). According to Li &Lyu, targeting specific local regions of deepfake video frames with this technique is uncertain (2018). Afchar suggested Mesonet, which contained Meso no 4 also MesoInception no 4 algorithms, to detect deep false & Face2Face forged videos. As a neural network could not identify both types of forgeries, two strategies were chosen. Li et al. Li showed that face warping artifacts could detect deep-fake films more accurately than Mesonet, although Afchar's technique overfit to those videos because it used a self-generated dataset.

Temporal and spatial characteristics of deep-fake films were identified by Chintha using XcepTemporal, a CNN architecture It uses latent convolutional representations, bidirectional recurrent structures, and entropy-based cost functions. The two-branch patch-and-pair learning architecture was presented by Li et al. (2020b) (PCNN). The face in the video is broken up into patches that are sent to the first branch, where they are analyzed to determine whether they are real or fake. The second branch then uses this information to effectively detect deep fakes by keeping track of the differences between the face region and the non-face region. Guarnera et al. (2020) used expectation maximization (EM) to extract local features for use in their GAN simulation. An external binary neural network fed neuron activation patterns that captured finer information, as discovered by Wang et al. (2020), was both effective and resilient to four well-known perturbation attacks.

C. Detecting interframe forgeries

Inter-frame manipulation involves copying, adding, or removing frames in a movie (Kaur & Jindal, 2020b). It may replicate or reorder video frames, making it a counterfeit. "Frame duplication" here indicates copying. & pasting frames from one video into another. Inter-frame video fraud detection methods & datasets. Inter-frame video forgeries involve duplicating, relocating, or splicing a video .Sharma developed & deployed multiple algorithms for detecting fraudulent & cloned videos. Wang &Farid's 2007 video had non-overlapping frames. The frames appeared in the same order throughout the video. 2010 saw more residue features & cross-modal subspace transformation methods.

Many scholars used (PSNR) to calculate movie motion (Khammar, 2012). This was used to check for editing. Wang &Farid (2006) found 3-D ballistic motion in movie flights, indicating that gravity affects the object's journey. Stamm employed motion prediction error to detect video frame additions & deletions, while Conotter targeted moving objects with geometric video. Some writers suggest counterfeit detection using MPEG compression techniques. Wang &Farid (2006) found static & temporal distortions in twice-compressed videos. Bakas used the prediction footprint variation (PFV) pattern to identify outlier P-frames. Fadl et al. (2020a) employed HOG to detect inter-frame forgeries. Grabb's test found irregularities using correlation coefficients. Motion energy images (MEIs) detected duplicate & scrambled frames. Fadl et al. (2020b) detected frame duplication by taking average shot time. The Gray Level Co-Occurrence Matrix extracts features from feature vectors to detect frame duplication by comparing surrounding vectors (GLCM). Kaur & Jindal (2020a) employed a complete convolutional neural network to identify faked frames using frame spatial & temporal correlation. Inter-frame forgeries have been detected using various methods. Most experiments employ REWIND. Researchers often discover counterfeits using frame optical flow. REWIND dataset accuracy is 89%.

ISSN No:-2456-2165

Reference	Year	Technique	Dataset	Input	Best result
Rezendeet al. [22]	2016	Resnet 50	Tokudaetal[50]	images	Acc 94.05%
Senguret al.[23]	2017	AlexNet, VGG16	NUAA[61], & CASIA-FASD [62]	images	94.01%
Khodabakhsh etal.[26]	2018	CNN	Fake face in the wild	Fine details fromhigh passfilters	99.40%
Marraet al. [49]	2020	Incepti onV3, LSTM	Video from multiple websites	Videos	99.60%
Lietal. [28]	2021	CNN	Private Data	image	94.00%
Lietal.[59]	2022	CNN	UADFV, Deepfak E	Videos	89.55%

Table 2: Survey methodology summarized work

D. Othermethods

Ulloa used two Convolutional Nural Network-based models to detect video manipulation in colorized & original images. Huang et al. (2017) detected bogus frame insertions using multi-level subtraction. They used video features such distinct objects not moving between frames, the same light direction, & the same pixel intensity to be computationally efficient. These details determined video frame addition. A redesigned Human Activities Database gave Huang et al. 93.66% accuracy. If the detection criteria change quickly, this strategy will provide more false positives. Kono et al. (2019) demonstrated convolutional LSTM, a new DL method that used video spatial & temporal components to identify forgeries. The authors developed a wide forgery detection system after realizing previous algorithms focused on specific forgeries.

They trained the model using CDnet2014 & hosting side flicks & found it insufficient. So, despite technological constraints, targeting specific types of forgeries was more successful. Su used exponential Fourier moment to identify duplicate video sections (EFM). This method divides frames into many overlapping patches. These patches tracked & searched for counterfeit locations throughout the video. 93.1% accuracy. This method only works for area duplication, not other frauds. Zhao et al. (2018) proposed histogram matching for forgery detection. When properly gathered, this method reportedly detects 99% of movies. This strategy works best without abrupt scene shifts. FFT is used to quickly learn & find altered visual data.

Tools	Link&Features
Deep Face Lab	https:///ohgithub.com/iperov/DeepFaceLab. –Cuttraining timeby3hours. –Better performance for adapting to poses &expressions. Sharp features of the face, like the eyes &teeth. –Helpsimprovethequalityofimagesbysupportinglargedatasetswithupto100kimages. –Allows lip manipulation, head replacement,do-aging,&othersimilarthings.
FSGAN	https://github.com/YuvalNirkin/fsgan. Face switching and reenactment can be applied on any two faces, even new ones. Change both your position & how you feel[57].
Disco Face GAN	https://github.com/microsoft/DiscoFaceGAN. –Makes pictures of the faces of virtual peoplewith hidden features like identity, expression,posture,&lightingthatdon'taffecteachother. –When doing adversarial learning, you mightwanttouse3Dpriors[58].
Face Shifter	https:///ohlingzhili.com/FaceShifterPage.com High-fidelity face swappingby using&combiningthetargetfeatures.Nospecial Training is need edtouseany fresh face combination[59].
Avatar Me	https://github.com/lattas/AvatarMe.com –Makesa3Dfacefromr&omphotostaken "inthewild."A3Dfacewitha resolutionof4thousandand6thousandcanberebuiltfromasinglelow-quality

Table 3: Detailed introduction to deep fake face applications.

V. FORENSICTOOLSOVERVIEW

Since technology has improved, investigators need methods to filter through multimedia devices' vast amounts of content. Investigators must make sure their equipment works & is correctly set up (Horsman, 2018) to present credible evidence in court. Multimedia forensic investigation tools have been created in the last decade. Teel Tech Canada provides video forensics technologies. To underst& more about an intriguing object, use Corepro to reverse project photographs. Impress filters videos. M&et helps detectives verify video authenticity. All three Teel Tech Canada tools are free after registration. Cognitech offers two video forensic tools. Video Investigator enhances videos for investigations. Photogrammetry "auto measure tools" measure scenes & biometrics. Both tools are paid with no free trials. Amped Software offers two forensic video analysis programs. Amped Five enhances videos, while Amped Authenticate detects fraud. Both Amplify tools require purchase. DiViLine Expert Solutions' Forensics Video-FA program detects motion & extracts data from video. Trials cost money. Video Cleaner also enhances & detects tampering. Free & easy to install. Ocean Systems' investigative software improves forensic video footage. Kinesense software augments & recognizes objects. Trial versions are available for paid programs. Vocord's Video Expert answers questions using facial recognition, video enhancement, verification, & reports.

Forensic investigators can employ many video tools. Investigators can assess their needs, choose a product that fits their dem&s, or use a tool to help them.

VI. CHALLENGES OFVIDEOFORENSICS

Even though the area of video forensics has advanced significantly since a decade ago, some issues still exist. These are some of these:

A. General challenges

While analyzing video media content, some similar problems arise in a variety of situations & epochs. The following is an explanation of these:

- Forensicsidentification
- Preparation advance in future
- Connection& recognition
- New face-recognition and approaches
- Video best quality issues

B. Resource challenges

Video evidence from multiple sources has created a vast data set. Data volume may limit resources (Mohammmed). Due to resource limits, obtaining & assessing forensic evidence takes time (Bhatele). Massive data may dem& additional staff. Video forensics also struggles to find technical analysts (Karie). Due to hardware constraints, huge videos cannot be saved for forensic examination (P&ey).

C. Legal challenges

Forensic video analysis may raise privacy problems. Examine the footage without violating the victim's or organization's privacy (Mohammmed). Maintaining evidence submission & analysis st&ards is another legal challenge for investigators (Caviglione). Forensic investigators face many administrative obstacles (Bhatele). Video forensic tools & techniques are making court data acquisition & evaluation harder (Karie). Ethics can arise when h&ling sensitive data (Karie).

D. Technical challenging

Evidence integrity analysis is hindered by encryption, steganography, different media formats, & analysis (Bhatele). Free encryption software helps the perpetrator hide evidence. Forensic investigators must decode data (Mohammmed). Video forensics investigators face a growing problem as criminals use advanced steganography to hide data (P&ey). New video file formats make investigation difficult as technology advances (Caviglione).

VII. CONCLUSION & FUTURESCOPE

We evaluated many video forensic methodologies, including general, resource, legal, and technical obstacles, as well as DL issues like the theory of DL, constrained datasets, and real-time processing.Moreover, we looked at a number of different video forensic methodologies. We also highlighted the difficulties that may arise for intelligent IoT devices as machine learning & deep learning become more widely used in AI. In addition, an overview of the most effective video forensics tools for investigation & analysis was provided. Because of the high dataset resolution & the increased frame rate, there has been a lot of progress made in the areas of object detection & tracking. It's possible that in the not-too-distant future, camera technology may include object tracking that has specialized features that can move in the direction of the target. Data gathered from Internet of Things devices & social networks can be efficiently categorized as suspicious or routine with the use of lightweight deep learning algorithms.

REFERENCES

[1.] Afchar, D., Nozick, V., Yamagishi, J., Echizen, I., 2018. Mesonet: a compact facial video forgery detection network. In: Proc. 2018 IEEE International Workshop on Information Forensics & Security (WIFS). IEEE, pp.1–7.

[2.] Ahmed, W., Shahzad, F., Javed, A.R., Iqbal, F., Ali, L., 2021. Whatsapp network forensics: Discovering the IP addresses of suspects. In: 2021 11th IFIP International Conference on New Technologies, Mobility & Security (NTMS). IEEE, pp. 1–7.

[3.] Al-Obaydy, W.N.I., Su&i, S.A., 2020. Open-set single-sample face recognition in video surveillance using fuzzy ARTMAP. Neural Comput. Appl. 32(5), 1405–1412.

[4.] Al-Sanjary, O.I., Ahmed, A.A., Ahmad, H.B., Ali, M.A., Mohammed, M., Abdullah, M.I., Ishak, Z.B., 2018a. Deleting object in video copy-move

forgery detection based onoptical flow concept. In: 2018 IEEE Conference on Systems, Process & Control (ICSPC).IEEE,Melaka,Malaysia,pp.33–38.
[5.] Al-Sanjary, O.I., Ahmed, A.A., Jaharadak, A.A.B., Ali, M.A., Zangana, H.M., 2018b.
[6.] Detection clone an object movement using an optical flow approach. In: 2018IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). IEEE,Penang,Malaysia,pp.388–394.
[7.] Al-Sanjary,O.I., Sulong, G., 2015. Detection of video forgery: A review of literature.
[8.] J. Theor. Appl. Inf.Technol.74(2). Alsmirat, M. A., Al-Hussien, R.A., Al-Sarayrah, W.T., Jararweh, Y., Etier, M., 2020. Digital video forensics: a comprehensive survey. Int. J. Adv. Intell. Paradigms 15(4), 437–456.
[9.] Bakas,J., Naskar, R., Bakshi, S., 2021. Detection & localization of inter-frame forgeries in videos based on macro block variation & motion vector analysis. Comput. Electr.Eng.89,106929.
[10.] Basit,A.,Zafar,M.,Liu,X.,Javed,A.R.,Jalil,Z.,Kifayat,K.,2020.Acomprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun.Syst.1–16.
[11.] Bhatele, K.R., Jain, S., Kataria, A., Jain, P., 2020. The fundamentals of digital forensics. In: H & book of Research on Multimedia Cyber Security. IGI Global, pp.165–175.
[12.] http://dx.doi.org/10.1109/tifs.2014.2318433.
[13.] Bhattacharya, S., Kaluri, R., Singh, S., Alazab, M., Tariq, U., et al., 2020. A novel PCA-fire fly based xgboost classification model for intrusion detection in networks using GPU. Electronics 9(2), 219.
[14.] Bidokhti, A., Ghaemmaghami, S., 2015. Detection of regional copy/move forgery in MPEG videos using optical flow. In: 2015 the International Symposium on Artificial Intelligence & Signal Processing (AISP). IEEE, Mashhad, Iran, pp.13–17.
[15.] Bruehs, W.E., Stout, D., 2020. Quantifying & ranking quality for acquired recordings on digital video recorders. J. Forensic Sci.65(4),1155–1168.
[16.] Butt,U.A.,Mehmood,M.,Shah,S.B.H.,Amin,R.,Shaukat,M.W.,Raza,S.M.,Suh,D.Y., Piran, M.,etal., Sep.2020. A review of machine learning algorithms for cloud computing security. Electronics 9(9), 1379.
[17.] Caviglione, L., Wendzel,S.,Mazurczyk,W.,2017. The future of digital forensics: Challenges & the road ahead. IEEE Secur.Priv.15(6),12–17.