International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 5 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195524

A Review : Video Tampering Attacks and Detection Techniques

Ruksana Habeeb*[1], Dr. L. C. Manikandan[2]

*[1]M Tech Student, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

[2]Professor and Hod, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

ABSTRACT

Technological advancements of various video and image editing tools has reached such a level that the tampering of digital video or image can be performed easily without degrading their quality or leaving any visual evidence. This review paper presents an overview of various types of video forgery and the different types of techniques that are employed for its detection. Passive and active forgery detection techniques are commonly used methods for detecting the tampering in a digital video. Passive and active tampering detection techniques are utilized for detecting the integrity as well as the authenticity of a given video. The aim of this review is to provide some productive information about video tampering attacks for upcoming researchers.

Keywords : Active and Passive Techniques, Copy-Move Forgery, Support Vector Machine, Spatial and Temporal Tampering , Video Forgery Detection, Watermarking, Video Authentication,Digital Signature

I. INTRODUCTION

In this day and age, digital video tampering has been made simple with widely available sophisticated and ready to use editing software's like Adobe Photoshop. As a result of this it is very difficult to distinguish the tampered videos from the authentic ones. The illegitimate or the offensive modification of the video is termed as video tampering or video forgery. The videos and images available at various social networking platforms like YouTube, Facebook etc., are playing a vital role in the scientific development and socio-economic perception. Apart from this videos are used in a variety of applications like legal evidence, video tutorials, advertisements, video surveillance . Eventhough this signify their remarkable role in today's context , there are also some darker sides associated with it[15] .It includes the abuse or circulation of wrong information through videos. This means that the videos that are available in social networking websites like youtube or that are seen in mass media like television may have undergone tampering. Following figure is an example that depicts the tampering in a digital video . Figure 1. represents the object removal attack in the original video frame sequence.

From the Figure 2. it's clear that there was a tree in the actual video frame sequence which is removed as a result of tampering.

Figure 1. Original Video Frame Sequence

Figure 2. Forged Video Frame Sequence.

Even though video tampering is comparatively harder to perform than image tampering [17], it is not rare to find some doctored video editing cases in real life. Moreover, in many instances, the tampered videos have appeared in news or social media. As a result of this various video tampering detection techniques have been developed to cope up with the video tampering problem. Video tampering detection techniques can be classified into two different categories which includes the passive approach and the active approach. The active tampering detection technique is mainly based on the hidden data. This technique [1] requires the pre-embedding of data like digital signature, watermark into the video inorder to validate its origin and authenticity. The passive tampering detection technique does not require any pre-embedded data, instead it make use of the statistical features of digital video inorder to determine its origin and authenticity.

II. FAMOUS VIDEO TAMPERING ATTACKS

Some of the famous manipulations with the digital video is shown in figure 3,4 and 5. These video tampering examples reveals the fact that even the television channel broadcast is not spared from video tampering [17].

A. RNC political propaganda, December 2005

Figure 3. shows the last screen shot of a Republican National Committee(RNC) political video of a U.S. soldier watching television. In this final shot, we read "Our soldiers are watching and our enemies are too". Actually this is a digitally manipulated video. This tampered video was created from another video where the soldier was actually watching the movie named "*How the Grinch Stole Christmas*".

Figure 3. RNC political propaganda, December 2005

B . CBS broadcast, December 2000

Figure 4. depicts the tampered video of the CBS broadcast. When this live video was broadcasted a CBS emblem was inserted inorder to hide the NBC emblem that was displayed on the background [17].

Figure 4. CBS broadcast, December 2000

C. Russian talk show in 2007

Figure 5.depicts the frame from a Russian talk show in the fall of 2007. In that program ,a prominent political analyst named Mikhail G.Delyagin made some tart comments about Russian president Vladimir V.Putin. Later, when the program was broadcasted his remarks were removed and he was also digitally removed from the show. However, the technicians neglected to remove his legs and hands in one shot[17] .

Figure 5. Russian Talk Show ,2007

III. VIDEO TAMPERING ATTACKS

Malicious tampering performed on the video can either alter the contents of the video or affect the temporal dependency between the frames[11]. Based on the frontier of its occurrence the variants of video tampering attacks can be categorized into three major domains: spatial tampering, temporal tampering and spatio-temporal tampering. They can be further divided into their subcategories as shown in Figure 6.

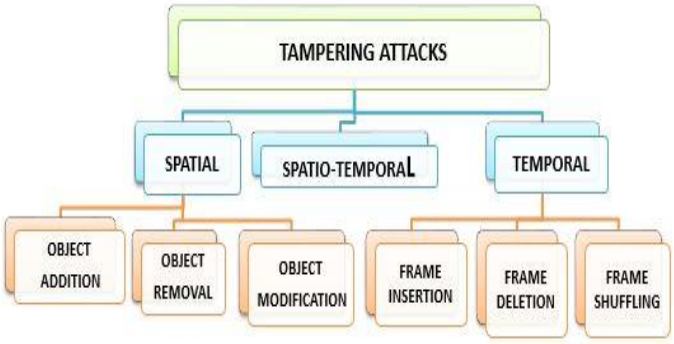
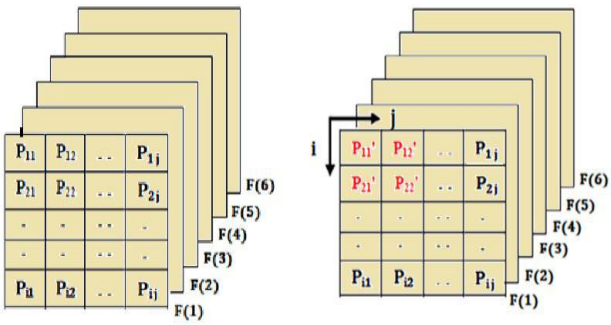


Figure 6. Classification of Video Tampering attacks

A. Spatial Tampering

In spatial or intraframe editing the malicious modifications alter the contents of single frame or several frame. The intraframe tampering is shown in Figure 7. in which the frame F(1) of the original input video V_O is spatially tampered to produce the forged video V_T. Here (i, j) denote the height and width of frames of the input video V_O respectively. Fundamentally the contents of the video frames are treated as objects [4].The objects of the frames can be categorized into two classes: Foreground objects and Background objects. The foreground objects are those which are captured as individual elements, omitting the background, in a frame. The background object is the background part of the frame omitting all of the foreground objects. The different types of spatial tampering attacks include object removal, object addition and object modification [11].



(a)Original Video (V_O) (b) Tampered Video(V_T)

Figure 7. Spatial Tampering

Object Addition

In object addition attack an object of interest is inserted to a single frame or to a set of frames. This attack can be performed with both kinds of objects, background objects and foreground objects. The copy – move forgery or copy-paste forgery is an example for the object addition attack [18]. Using this attack an intruder can insert or delete an object to or from a scene depicted in the video frames. Figure 8.shows an example of copy-move forgery in which an additional tree as a foreground object is copied from the original frame and added to a different location in the same frame.

(a)Original Frame (b)Tampered Frame

Figure 8. Object Addition Attack

Object Removal

In object Removal attack the objects of the frames of video are removed or deleted. This attack can be performed with both background object as well as foreground object [2] .When an object is deleted from a video scene, a technique called inpainting can be utilized to reconstruct the deleted or corrupted regions

in a visually believable manner. Inpainting can be performed in two ways. Either the removed regions are filled in with the help of sample textures [Exemplar-Predicated Texture Synthesis (ETS)] or the most coherent blocks from temporally adjacent frames are utilized to fill in the removed region [Temporal Copy and Paste (TCP)].Upscale-crop is another attack in which the frames of a video are cropped to delete the proof of occurrence of a crime in the outermost parts of video, and then enlarging the damaged frames so as to preserve consistent resolution across the whole video. Figure 9. shows an example of object deletion attack in which a foreground object is deleted from original video frame.

(a)Original Frame (b) Tampered Frame

Figure 9. Object Removal Attack

Object Modification

In Object modification attack, an existing object of the frame can be modified in such a manner that the original identity of that object is lost. The object modification attacks can be performed in many ways in the given video. This attack can be executed with both background and foreground objects. For instance, the size and shape of the object can be changed, the color of the object can be changed and with the help of extra effect the features of the object and its association with other objects can also be changed [22]. These attacks are performed at pixel level. Hence it is very difficult to detect this kind of attack. Figure 10. shows an example of object modification attack where the face of a person has been changed in such a manner that the new face of the person cannot be identified as the same as in original frame.

(a)Original Frame (b) Tampered Frame

Figure 10. Object Modification Attack

B. Temporal Tampering

Temporal or interframe tampering is the type of tampering that is applied to the video frames. This tampering mainly affects the time sequence of visual content, captured by video capturing devices. Common attacks of this type include frame insertion, frame deletion and frame shuffling or frame reordering. Figure 11. represents the original video V_O that consists of six frames [4].

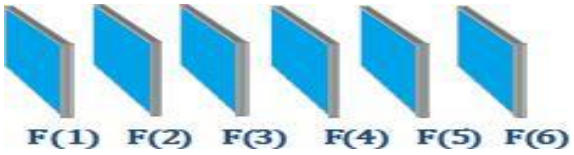


Figure 11. Original Video (V_O)

Frame Insertion

In frame insertion attack, additional frames from another video, which has the same statistical properties, are intentionally inserted at some arbitrary locations in a given video. The prime intention of this attack is to camouflage the original content and provide erroneous information. Frame count get incremented when new frames are inserted into the source video [7]. A typical example of the frame insertion attack is shown in Figure 12. In which two frames F(a) and F(b) are inserted at random location in the original video V_O to produce the tampered video consisting of eight frames.

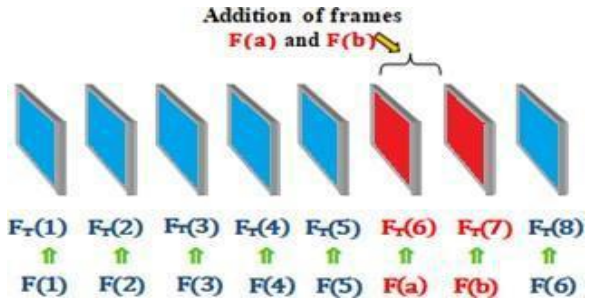


Figure 12. Frame insertion attack

Frame Deletion

In frame deletion attack the frames are deliberately removed. In this kind of attack, frames can be eliminated from different locations or it can be removed from a specific location. Frame count get decremented when frames are removed from the source video [10]. Depending upon the motive it is normally performed on surveillance video where the attacker wants to delete his/her presence in the video. Figure 13. shows a typical example of frame deletion attack in which the frames labeled F(3) and F(4) are removed from original video V_O to generate tampered video consisting of only four frames.

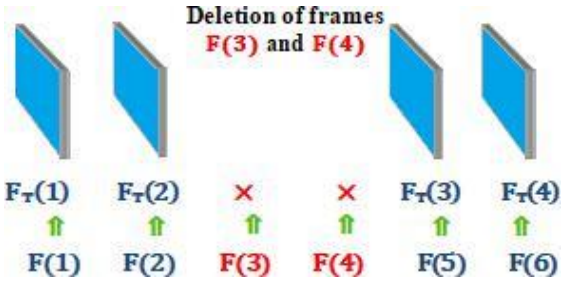


Figure 13. Frame Deletion Attack

Frame Shuffling

In frame shuffling attack, frames of a given video are rearranged or shuffled in such a manner that the actual video frame sequence is intermingled and erroneous information is produced by the video as compared to original video [11]. Frame count remains the same when frames are reordered in the source video. A typical example of frame shuffling attack is shown in Figure 14. Where two frames labeled F(2) and F(5) of the original video V_O are shuffled.

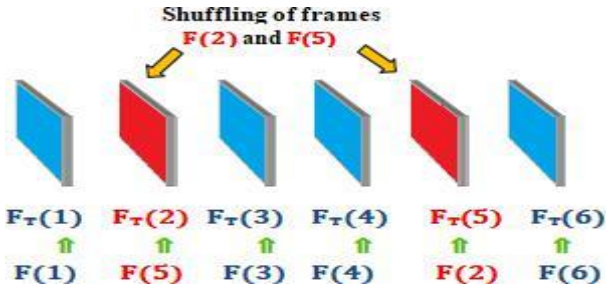
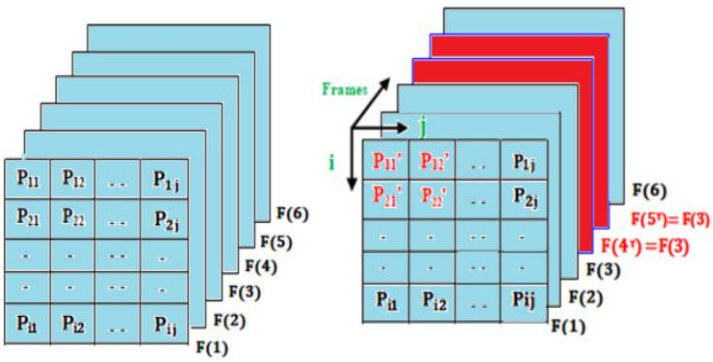


Figure14. Frame Shuffling Attack

C. Spatio - Temporal Tampering

Spatio-temporal tampering attacks are the combination of spatial as well as temporal tampering. The blending of both Inter frame forgery and Intra frame forgery is found here. Numerous tampering techniques found in temporal and spatial domain is also seen here. The authentication system must be robust enough to recognize both kinds of tampering [8]. The diagrammatic representation of spatio-temporal tampering is shown in Figure 15. In it the occurrence of both temporal and spatial tampering can be observed. Here (i, j) denote the height and width of the input video frame sequence. From the Figure 15. it's clear that V_T is the tampered video generated from source video V_O . As a result of the temporal tampering in frame F(4) and F(5) and spatial tampering in frame F(1) of the original source video V_O the spatio-temporally tampered video V_T is generated.



(a)original video(V_O) **(b)Tampered video(V_T)**

Figure15. Spatio-Temporal Tampering

IV. LEVELS OF TAMPERING

In a video the tampering can be performed at different levels which includes the shot level tampering, frame level tampering, block level tampering and pixel level tampering [5].

A. Pixel Level Tampering

The contents of a video are altered at pixel level in pixel level tampering. This is the smallest level at which tampering can be performed[11]. Many normal video processing operations are done at pixel level. Therefore the video authentication system must be robust enough to distinguish between the pixel level tampering and the normal video processing operation. Spatial tampering is normally performed at pixel level.

B. Block Level Tampering

A specified region on the frame of the video is termed as block. The tampering attacks are performed on the blocks in block level tampering. The content of the video frame is considered as blocks on which manipulation is done. In block level tampering the blocks can be morphed, cropped, modified or replaced. Spatial tampering is normally performed at block level.

C. Frame Level Tampering

In frame level tampering the malicious manipulation is applied to the video frames. Frame insertion, frame deletion and frame shuffling are the common tampering attacks that can be performed by the attacker at frame level. Temporal tampering is commonly performed at frame level[4].

D. Shot Level Tampering

In shot level tampering the forgery is performed at the shot level. In this any specific shot of the given video is manipulated. In shot level tampering a shot can be inserted or removed from the video. Shot level tampering can be performed with all kinds of tampering attacks.

V. VIDEO TAMPERING DETECTION TECHNIQUES

In general the video tampering detection techniques can be broadly categorized into two major domains: active video tampering detection techniques and passive video tampering detection techniques

A. Active Tampering Detection Technique

The active technique make use of the pre-embedded concealed data [6,4]like digital signature or watermark in order to verify the authenticity and integrity of a digital video. The different types of active techniques include digital signature, intelligent techniques and watermark as shown in Figure 16. The active approach has following drawbacks:

- During the acquisition phase it requires a specialized hardware like specially equipped cameras for the purpose of insertion of watermark or digital signature into the video.
- Numerous encryption techniques can prevent unauthorized people from accessing and manipulating the digital video content, nevertheless these encryption techniques cannot prevent the owner of digital video from modifying the video before encryption.
- Factors like compression, scaling, noise etc., have an impact on the robustness of Watermarks and digital Signatures

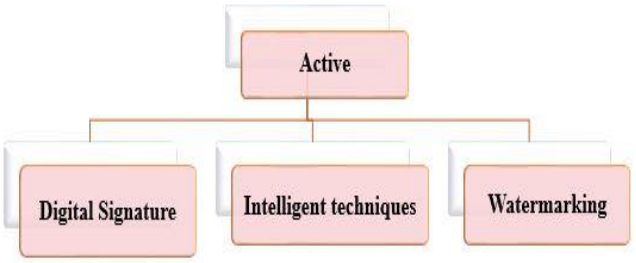


Figure16. Active Tampering Detection Technique

Digital Signature

In 1976 Diffie and Hellman introduced digital signature for the authentication purpose of multimedia data and to verify its integrity. The digital signatures can be saved in two different ways for authentication purposes. Either it can be saved as an independent file or it can be saved in the header field of the compressed source information. It proves to be better because the digital signature remains unaltered even if the pixel values of the images or videos are changed and it provide better results[11,23]. In the digital signature authentication the digital signature cannot be forged because the digital signature of the signer depends on the content of data and on some secret information, which is only known to the signer. The recipient can authenticate a received multimedia data by analyzing whether the contents of data match the information conveyed through the digital signature.

Intelligent Techniques

The intelligent techniques make use of database of video clips for video authentication. The database consists of both tampered as well as authentic videos. The main advantage of intelligent technique over other techniques like digital signature and watermark is that it does not require any watermark embedding procedure or computation and storage of any secret or public key. An intelligent technique for video authentication was proposed by authors in [20], which make use of the intrinsic video information for the authentication purpose. It make use of the Support Vector Machine (SVM) for the categorization of the forged and authentic video clips. This algorithm is executed in two stages:

- The first is the SVM training stage
- The second is the tampering detection and classification stage.

In the training stage the algorithm trains the SVM by utilizing a manually labelled training video database. A trained hyper plane with classified tampered and non-tampered video data is the output of SVM training stage [11].

Watermarking

The process of inserting information into multimedia data is known as digital watermarking. Watermark embedding or watermark insertion are the other terms that are used interchangeably with watermarking. Besides ascertaining the integrity of the digital data and apperceiving the malevolent manipulations, watermarking can be utilized for the authentication of the producer or author of the content [9]. Watermarks can be embedded with the multimedia data, without transmuting the actual meaning of the content of the data. The salutary feature with the watermarks is that, they can be embedded without degrading the quality of multimedia data too much. Since the watermarks are embedded in the content of video data, once the data is modified, these watermarks will also get modified such that the authentication system can be used to validate the integrity of multimedia data. The technique of video watermarking is divided into two segments [19]:

- Embedding or encoding of watermark into input video.
- Extraction or decoding of watermark from the video.

Watermark Embedding

The process of video watermarking or encoding is performed at the source end. In this process watermark is embedded into the input video by using any watermarking algorithm [19]. The entire process is shown in Figure 17. This can be thought of as a function that maps the input video (Vin), Watermark (Vw) and key (k) to the output watermarked video(Vw). The encoding can be depicted mathematically as

$$Vw = E(Vin, W, K) \text{ ----------(1)}$$

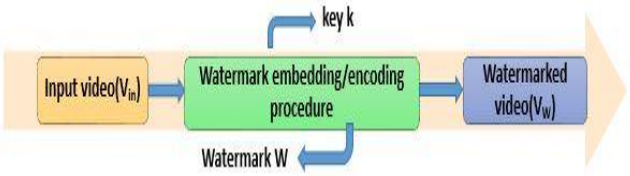


Figure17. Watermark Embedding

Watermark Extraction

The process of decoding or watermark extraction from the watermarked video is the reverse process of embedding algorithm. The entire process is shown in Figure 18. The decoding can be expressed mathematically as

$$Vin = D(Vw, W, K)\text{----------(2)}$$

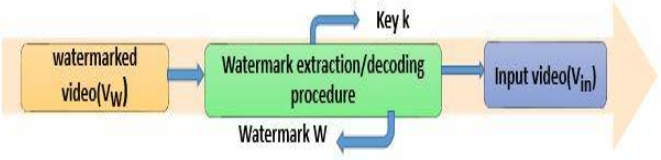


Figure18. Watermark Extraction

B . Passive Video Tampering Detection Techniques

Passive video tampering detection technique is also known as blind video tampering detection technique[24] .These are the techniques that can be used to verify the authenticity of a video without depending on pre- embedded or pre-extracted data [12]. The passive tampering detection can be performed using the methods that are shown in Figure 19. which include camera- based editing detection, detection based on coding artifacts, detection based on inconsistencies in the content, copy–move detection in videos [13]. The passive approach can be used inorder to overcome the inefficiency encountered in the active detection techniques. The advantages of passive approach are as follows:

- Inorder to detect editing history it does not require any pre-embedded information about the video contents, instead it depends only on the available tampered video and its intrinsic features.
- It does not require any specialized hardware to detect editing history.

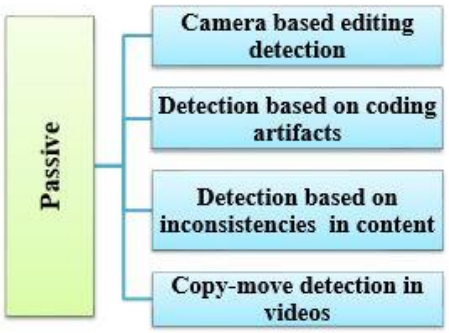


Figure19. Passive Forgery Detection Techniques

Camera based editing detection

In recorded videos a characteristic fingerprint is leaved by camcorders. This fingerprint is not only used for device identification but it can be also used for tampering detection in video. A straight application of the PRNU (Photo Response Non Uniformity) fingerprinting technique to video sequences is suggested by Mondaini et al. [21].Using this technique several types of tampering can be detected. Kobayashi et al. [18] suggested a camera –based approach in which it make use of the noise characteristics of the acquisition device to detect the suspicious regions in video recorded from a static scene.

Detection based on coding artifacts

The performance of the camera based tampering detection technique is greatly affected by the video encoding process. Video coding is performed to embed artifacts in the video that can be used to determine the integrity of the video content by extracting and verifying it. In recent years the video forensic researchers rely on this artifacts to determine the integrity of the video and to locate the tampered regions in the video. Wang and Farid [22] proposed a method that can be used to detect the inter-frame tampering and the intra-frame tampering.This approach is mainly focused on MPEG compressed videos.

Detection based on inconsistencies content

For a given input video it is very difficult to determine whether the geometry ,physical or the lightning properties of a scene are consistent and free of any types of tampering on a frame-by-frame basis. In order to determine the editing history the existing techniques utilize the phenomenon associated with motion. Uptill now two approaches [16] have been suggested to determine this type of tampering: i)An approach based on the artifacts that are left behind as a result of video inpainting, ii) An approach that disclose the inconsistencies in the movement of objects in free-flight.

Copy-move detection in videos

The copy-move forgery attack that can be performed on the video can be classified into two types which includes the intra-frame copy move forgery and inter-frame copy move forgery. Theoretically the intra-frame copy-move forgery of the video is identical to the copy- move tampering performed in images. In intra-frame forgery a portion of the frame is copied and replicated in a different location in that frame [3,6].This is usually done inorder to conceal or duplicate some object of a single frame or several frames. In inter-frame forgery malicious modifications is applied to the sequence of frames and the various types of this attack include frame insertion, frame deletion and frame reordering. Wang and Farid [25] proposed a method that can be used to detect copy-move tampering in video.

VI. Video Tampering Detection Framework

Copy-move forgery is one of the most popular tampering attack in video. Copy-move forgery is a type of tampering in which a portion of the video is copied and replicated to a different location in the same video.The general detection process for video forgery is depicted in Figure 20. The framework comprises of six step process which includes Frame Extraction, Feature Extraction, Block Matching, Post-processing which culminates into final decisive step that gives the result about the tampering detection and its localization [3].

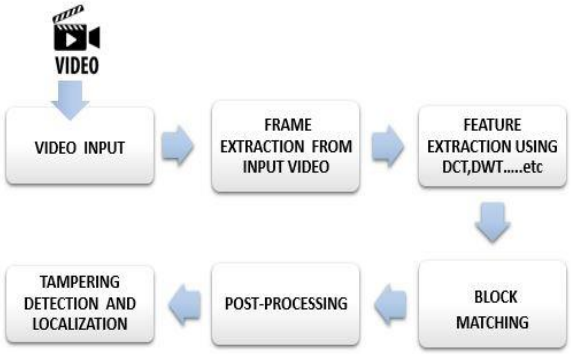


Figure 20. Video Tampering Detection Framework

The first step is to divide the input video and extract frames from it. This is followed by the Feature Extraction step for finding or extracting feature vectors. In this step various feature extraction techniques like DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) etc., is used. In the next step Overlapping Block Matching techniques like K-SVD tree (K-Singular Value Decomposition) and radix sort can be applied. After performing block matching post-processing operations are performed and the final crucial step concludes the type of Video tampering and its location in the frame.

VII. CONCLUSION

In this paper various types of video tampering attacks like spatial tampering, temporal tampering and spatio - temporal tampering , levels of tampering ,video tampering detection techniques like passive and active techniques and video tampering detection framework has been discussed.

VIII. REFERENCES

[1]. Omar Ismael Al-Sanjary , Ahmed Abdullah Ahmed, Hawar Bahzad Ahmad, Musab A. M Ali1, M.N. Mohammed1,Muhammad Irsyad Abdullah1, Zurida Binti Ishak1(2018), “Deleting Object in Video Copy-Move Forgery Detection Based on Optical Flow Concept”, 2018 IEEE Conference on Systems,Process and Control (ICSPC 2018),pp. 14-15.

[2]. RaahatDevenderSingh1 ,Naveen Aggarwal(2018), “Video content authentication techniques: a comprehensive survey”, Multimedia Systems, Springer-Verlag Berlin Heidelberg, pp.211-240

[3]. Omar Ismael Al-Sanjary, Ghazali Sulong (2015),” DETECTION OF VIDEO FORGERY: A REVIEW OF LITERATURE”, Journal of Theoretical and Applied Information Technology ,pp.207-220

[4]. Rohini Sawant, Manoj Sabnis (2018)"A Review of Video Forgery and Its Detection" ,IOSR Journal of Computer Engineering (IOSR-JCE) 20.2: 01-04.

[5]. Mrs. J.D. Gavade,Mrs. S.R. Chougule. (2015),” Review of Techniques of Digital Video Forgery Detection”, Advances in Computer Science and Information Technology (ACSIT), Volume 2 , pp.233-236

[6]. Ainuddin Wahid Abdul Wahab, M. A. (2014),” Passive Video Forgery Detection Techniques: A Survey”, 10th International Conference on Information Assurance and Security. IEEE

[7]. Gironi, A., M. Fontani, Tiziano Bianchi, A. Piva, and M. Barni(2014), "A video forensic technique for detecting frame deletion and insertion", In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6226-6230

[8]. Subramanyam, A. V., and Sabu Emmanuel(2013),"Pixel estimation based video forgery detection.", In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3038-3042

[9]. Gopal Prasad, Atul Kumar Singh, Arun Kumar Mishra(2013),”Digital Video Watermarking Techniques and Comparative Analysis : A Review”, International Journal of Engineering Research &Technology (IJERT), vol. 2, pp. 2041-2046

[10]. Chao, Juan, Xinghao Jiang, and Tanfeng Sun(2013), "A novel video inter-frame forgery model detection scheme based on optical flow consistency", Digital Forensics and Watermaking. Springer Berlin Heidelberg, pp. 267-281.

[11]. Saurabh Upadhyay, Sanjay Kumar Singh(2012),“Video Authentication: Issues and Challenges” , IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012 ISSN (Online):1694-0814

[12]. D. Qiong, Y. Gaobo, Z. Ningbo, (2012). “A MCEA based passive forensics scheme for detecting frame-based video Tampering”, Digital Investigation. Journal of Elsevier pp. 151-17

[13]. S. Milaniet al.,(2012) “An overview on video forensics,” APSIPA Trans. Signal

[14]. Stamm, Matthew C., W. Sabrina Lin, and KJ Ray Liu(2012), "Temporal forensics and anti-forensics for motion compensated video", Information Forensics and Security, IEEE Transactions on 7.4 (2012): 1315-1329

[15]. Chuang Weihong, Su Hui, Wu Min(2011),” Exploiting compression effects forimproved source camera identification using strongly compressed video”, In Proceedings of IEEE Conference on Image Processing (ICIP),1953-1956

[16]. V. Conotter, J. O’Brien, and H. Farid(2011), “Exposing digital forgeries in ballistic motion,” Information Forensics and Security, IEEE Transactions on, vol. PP, no. 99, pp. 1.

[17]. Rocha Anderson, Scheirer Walter, Boult Terrance, Goldenstein Siome(2011),“Vision of the unseen:

current trends and challenges in digital image and video forensics", ACM Computing Surveys 2011;43(4):26-40

[18]. Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato (2010),"Detecting forgery from static-scene video based on inconsistency in noise level functions," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 883-892.

[19]. Jamal Hussein and Aree Mohammed (2009), "Robust Video Watermarking using Multi-Band Wavelet Transform", IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1.

[20]. S. Upadhyay , S.K. Singh, M. Vatsa, and R. Singh(2007), "Video authentication using relative correlation information and SVM", In Computational Intelligence in Multimedia Processing: Recent Advances (Springer Verlag) Edited by A.E. Hassanien, J. Kacprzyk, and A. Abraham, 2007.

[21]. N. Mondaini, R. Caldelli, A. Piva, M. Barni, and V. Cappellini(2007),"Detection of malevolent changes in digital video for forensic applications," in Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX.

[22]. Weihong Wang and Hany Farid (2006), "Exposing digital forgeries in video by detecting double MPEG compression",in MM&Sec.

[23]. W. Diffie and M. E. Hellman, New Directions in cryptography(1976), IEEE Trans. on Information Theory, Vol. 22, No. 6, pp.644-654.

[24]. Vahideh Amanipour, Shahrokh Ghaemmaghami (2018),"Video-Tampering Detection and Content Reconstruction via Self-Embedding", IEEE Transactions on Instrumentation and Measurement (Volume: 67 , Issue: 3 , March 2018) Page(s): 505 - 515

[25]. 25 Weihong Wang and Hany Farid, "Exposing digital forgeries in video by detecting duplication," in MM&Sec,2007.

AUTHOR PROFILE

RUKSANA HABEEB is currently pursuing M Tech in Computer Science and Engineering at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, INDIA. She has received B Tech degree in Computer Science and Engineering from Sree Buddha College of Engineering Pathanamthitta, Kerala, INDIA. Her research area of interest includes the field of multimedia forensics security, Information security, machine learning and biometrics.

Dr. L. C. Manikandan is working as Professor at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, INDIA. He has received Ph.D. degree in Computer and Information Technology from Manonmaniam Sundaranar University, M.Tech Degree in Computer and Information Technology from Manonmaniam Sundaranar University, M.Sc., Degree in Computer Science from Bharathidasan University and B.Sc. Degree in Computer Science from Manonmaniam Sundaranar University. His main research interest includes Video Surveillance, Image Compression & Video Coding in image processing.

Cite this article as :

Ruksana Habeeb, Dr. L. C. Manikandan, "A Review : Video Tampering Attacks and Detection Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 5, pp. 158-168, September-October 2019. Available at doi : https://doi.org/10.32628/CSEIT195524
Journal URL : http://ijsrcseit.com/CSEIT195524