

VIDEO FORENSIC FOR VIDEO TAMPER DETECTION

*Bandu B. Meshram¹ Manish Kumar Singh²

¹Professor & Chairman, Jeman Educational Society, Navi, Mumbai, Maharashtra,(India)

²Head Of Law Department , NIMS, School of Law. NIMS University Rajasthan, Jaipur,(India)

Abstract—With the wide-spread availability of sophisticated and low-cost digital video cameras camcorders and CCTV and mobile cameras, and the prevalence of multimedia like text, image, audio, video sharing websites and social media digital videos are playing a more important role in our daily life. Sophisticated digital video editing software is making it easier to tamper with videos. The alterability of video or fake video undermines our common sense assumptions about its accuracy and reliability as a representation of reality. As digital video editing techniques become more and more sophisticated, it is ever more necessary to develop tools for detecting video forgery. Advanced video manipulation technology greatly enriches our visual experience. However, as these techniques become increasingly available to the general public, malicious tampering with video recordings is emerging as a serious challenge. The literature survey is made on image, audio, videoediting and forensic tools. Videosare distorted by removing, replicating or inserting a group of frames by using sophisticated video editing software's. Frame tampering is one of the common video forgery operations, which can change the video content and confuse the viewers by removing or inserting some special frames in the video streams. For video temper detection two methods are proposed namely video forensic method 1 detects the forgery based on the residual noise in the video, while second method 2detect video tampering based on the spatio-temporal domain based on footprints left while tampering with a video sequence. Lastly the IP trace back to know the location of the fake video sender is discussed.

Keywords —Video tampering, residual noise, Spato-temporal region, Video Tampering Detection, Video Forensics

I. INTRODUCTION

Digital video refers to the sequence of moving images that can be compressed by reducing both spatial and temporal redundancy. A digital video is basically a sequence of still pictures or frames shot at a sufficiently high rate. With the wide-spread availability of sophisticated and low-cost digital video cameras and the prevalence of video sharing websites such as YouTube, digital videos are playing a more important role in our daily life. There are wide range of applications, such as video surveillance, video broadcast, DVDs, video conferencing, video-on-demand applications and advertisement monitoring where authenticity and integrity of the video data is very crucial. Due to availability of sophisticated video editing software; it has become easier to tamper digital videos & making them unreliable. On the other hand, in many cases the meaning of a video can be distorted by removing, replicating or inserting a group of frames Therefore, video forensics domain became very important & it evolving day by day. In the recent years, video Forensics has emerged to face this problem; experts have proposed a wide set of solutions to reconstruct the video content. These strategies rely on the fact that nonreversible operations applied to a signal leave some traces that can be identified and classified in order to reconstruct the possible alterations that have been operated on the original source. Basically video tampering or manipulation classified into spatial tampering, temporal tampering or combination of them, spatio-temporal tampering. Spatial tampering or intra-frame forgeries, where the attacker alters the content of single frames by adding or removing objects. Spatial tampering refers to changing the image frame, such as cropping and replacement, content adding and removal. Temporal tampering or inter-frame forgeries, where group of frames are entirely deleted, inserted or even replicated. Temporal tampering is the changes made in the time domain, such as adding extra frames, reordering the sequence of frames, dropping, and replacing frames. The usage of videos in varied applications like entertainment industry, video surveillance, legal and law enforcement, social networking, video tutorials, advertising, etc. mark its unmatched role in today's life. However its repercussion depends on the circumstance and the area where it is used. Different areas affected by Video Forgery are: Defamation: Video forgery in society and politics, sexual harassment, social media, theft, bribe has an evident impact as it used to defame a personality or conceal actuality. Video Surveillance: Videos would be easily altered copying, duplicating or removing certain objects or frames within the video sequence. Also it would be

possible to insert into the video, certain objects, events or people present at different locations and cameras at different time. In this case, it is difficult to ensure that the video used as evidence, is the original one actually recorded by the surveillance camera. The forger may forge the video to hide an unsuitable event or object or may plan to embed erroneous evidences and proofs. Policemen should be largely trained to calculate the ‘hash value’ of FIRs that they are to register through video-recording. ie video recording of the statements of victims and witnesses.

The paper is organized as follows: Section II contains literature survey. Section III presents the proposed model for video forgery and video forensic analysis and discussed some of the way to know the IP address of the fake video sender. Lastly section IV presents results and conclusion.

II. LITERATURE SURVEY

The section describes various multimedia editing and forensic tools.

2.1 RELATED WORK

A large volume of video data generated on digital media lead to considerable research in the field of video forensics. In order to address multimedia tempering issue, the multimedia forensic community has proposed many forgery detection algorithms, targeting different kinds of media [1]. More specifically, if we consider visual content, many forensic solutions were proposed for still-images [2], [3], whereas just a few methods address videos [4]. In order to address this issue, the multimedia forensic community has proposed many forgery detection algorithms, targeting different kinds of media [1]. More specifically, if we consider visual content, many forensic solutions were proposed for still-images [2], [3], whereas just a few methods address videos [4]. The authors [5] detect the number of compression steps applied to a video as evidence of video editing. In case double compression has been applied, [6], [7] show how to detect the first used codec in the compression chain. In [8] and [9] methods to detect if a video sequence was re-captured from a monitor are presented. The authors [10] propose a method to detect if a video sequence was temporally interpolated. All these methods provide useful information to determine if a sequence was modified, either maliciously or not. However, they do not provide any information on the forgery location. In [11] video splicing (used to remove an object from a scene) is detected analyzing noise characteristics. In [12], the authors analyze two kinds of attacks: i) spatial copy-move (obtained duplicating an object within the same scene) is detected matching Histogram of Oriented Gradients (HOG); ii) temporal copy-move (obtained copying an object from a frame to another one) is detected exploiting MPEG-2 GOP structure. In [13], the authors analyze the case of splicing attacks, that is, copying a portion of a video sequence into another. The detector exploits the differences of noise characteristics between the original and the spliced sequence, thus being very sensitive to compression. In the recent surveys the authors [14] discussed the domain of video forensics. In [15] the authors presented a survey on the existing video forensics tools by checking common features in the latest software and their strengths and weaknesses. Similarly, a recent survey [16] discussed the video forensics tool’s information with their product information. In another survey [17], the author discussed the active and passive approach to detect video forgery with the semantics of digital data and the authenticity of digital evidence. The authors [18] discussed different techniques for the detection of video forgery using inter-frame and intra-frame video forgery. However, no survey discussed all the detection techniques and approaches in video forensics and different product details together in one survey. In [21], the authors discussed to know the IP Address of the fake video sender on whatsapp. The main purpose of video tampering detection is to identify videos that have been tampered especially [23,24,25] those that can be useful in judicial cases. From time to time many research works has been taken place to find the tampered location [26,27,28 29]. Various methods such as active and passive methods can be used but passive approach [30] have proven to be more effective than the active methods as they do not interfere with the video in any way. These techniques are used to find many tampering types like double compression, frame duplication [31], frame deletion [32,33], and multiple compression [34].

2. LITERATURE SURVEY

A comprehensive survey on digital video forensics and video temper detection techniques : Taxonomy, challenges, and future directions are discussed in [14]. However various new multimedia editing and forensic tools are discussed here with site source.

2.1 Image Editing Tools

Image Forgery can be done by many tools. Although there are some tools available but some of them can be called as expert tools for doing forgery on images. They are listed in *Table 1*

Table 1 Image Editing Tools

Image Editing Tools	Purpose	Site Source
Adobe Photoshop	Creating and editing images	http://www.photoshop.com/products/photoshop

GIMP	Image editing and plugin development	http://www.gimp.org/
Picasa	Image editing and viewing	http://picasa.google.com/

2.2 Image Forensic Tools

The image forensic tools can perform various functions to perform forgery detection, metadata extraction etc. Those tools are enlisted in Table 2.

Table 2 Image Forensic Tools

Image Forensic Tools	Purpose	Site Source
Ghiro	Metadata extraction, GPS localization and Error Level Analysis	http://www.getghiro.org/
OpenStego	Signature watermarking, extraction and comparison	http://www.openstego.info/
JPEG Snoop	JPEG Header values extraction, JPEG compression signature analysis and camera signature extraction and storage	http://www.impulseadventure.com/photo/jpeg-snoop.html
Amped Authenticate	Visual inspection, DCT plot, correlation plot, jpeg ghosts, histogram etc.	http://ampedsoftware.com/authenticate

2.3 Audio Editing Tools

Studied audio editing tools are as shown in Table 3

Table 3 Audio Editing Tools

Audio Editing Tools	Purpose	Site Source
Audacity	Audio editor and recorder	http://audacity.sourceforge.net/download/
Traverso	Small scale recording session and editing	http://sourceforge.net/projects/traverso/odaw.mirror/files/latest/download
Wavesurfer	Audio editor widely used for studies of acoustic phonetics	http://sourceforge.net/projects/wavesurfer/files/latest/download

2.4 Audio Forensic Tools

Audio forensic tools provides various methods which can be used to find out whether video is original or forged as shown in Table 4.

Table 4 Audio Forensic Tools

Audio Forensic Tools	Purpose	Site Source
IKAR lab	Advanced Speech Signal Analysis	http://speechpro.com/product/forensic_analyses/ikarlab
EdiTracker	Assessments regarding audio authenticity	http://speechpro-usa.com/product/forensic_analysis/editracker
Audio Forensics by Fraunhofer IDMT	Edit/Manipulation detection and Technical quality assessment	http://www.idmt.fraunhofer.de/en/Service_Offersings/products_and_technologies/a_d/audioforensics.html
MediaInfo	Metadata tool	http://mediaarea.net/en/MediaInfo/Download
HxD- Hexeditor	Hex editor	http://mh-nexus.de/en/downloads.php?product=HxD
Be.HexEditor	Metadata editor for binary files	http://hexbox.sourceforge.net/

2.5 Video Editing Tools

Table 5 shows video editing tools, its purpose and website link.

Table 5 Video Editing Tools

Video Editing Tools	Purpose	Website Link
Adobe Premier Pro	Video Editing And Video Conversion	http://www.adobe.com/in/products/premiere.html
Windows Movie Maker	Video Editing and Video Creation	http://windows.microsoft.com/en-in/windows-live/movie-maker
Lightworks	Non-linear Video Editing	http://www.lwks.com/index.php?option=com_lwks&view=download&Itemid=206
Corel VideoStudio Pro X7	Video Editing and Video Creation	http://www.videostudio.com/en/products/videostudio/ultimate/#tab=1

2.6 Comparison of Video Editing Tools

Table 6 Comparison of Video Editing Tools

Features	Adobe Premier Pro	Windows Movie Maker	Lightworks	Corel Video Studio
Auto Save	Yes	No	No	Yes
Timeline editing	Yes	Yes	No	Yes
FOSS	No	Yes but not open source	Yes	No
Video Enhancement Capabilities	Yes	Yes but limited	No	Yes
4K support	Yes	No	No	Yes
Plugins Support	No	No	Yes	No
Video Stabilization	Yes	Yes	No	Yes
DVD Burning	Yes	No	No	Yes
Direct camcorder capture	Yes	Yes	Yes	No
Audio Effects	Yes	No	No	No
Skill level required	Professional	Consumer	Prosumer	Prosumer

2.7 Video Forgery Detection Tools.

Table 7 Video Forensic Tools

Video Forensic Tools	Purpose	Website Link
Forevid	Video Forgery Detection	http://www.forevid.org/
VirtualDub	Video Capturing/Processing, Forensics	http://www.virtualdub.org/
Amped Five	Video Enhancement, Surveillance, Forensics	http://ampedsoftware.com/

2.7 Comparison of Video Forgery Detection Tools

Table 8 Video Forgery Detection Tools

Features	Amped Five	VirtualDub	Forevid
FOSS	No	Yes	Yes
Platform	Windows	Windows, Linux	Windows
Plugins support	No	Yes	No
Hash Comparison	Yes	No	Yes
Hex editor	Yes	Yes	No
De-Interlace Feature	Yes	Yes	Yes but limited
Object Tracking	Yes	No	Yes
Denoising Feature	Yes	Yes	Yes

2.2 VIDEO TEMPERING

This section presents the types of video tempering

2.3.1 Types of Video Tampering

Videos can be an important evidence in related judicial cases . Active Forgery Detection includes techniques like Digital Watermarking and Digital Signatures which are helpful to authentic Content Ownership and Copyright Violations. .In passive approach, the basic assumption made is that Videos have some inherent properties or features which are consistent in original videos. When a video is forged these patterns are altered. Passive approaches extract these features from a video and analyses them for different forgery detection purposes. Passive can also be classified into detection of double and multiple compression and region tempering and inter frame forgery detection [35]. Classification of Video tampering detection methods [36] are of two types: i) Active ii) Passive. Active video tampering techniques are a) digital signatures b) water marks c) hash Values. Passive video tampering techniques are –a) Spatial (Copy-Move, Upscale Crop, Splicing) b) Temporal(Frame insertion, frame deletion, frame duplication, frame suffling) and c)Spatio-temporal detection techniques are [36](Statistical based, compression based, texture based, noise based).In Videos Forgeries can be performed by tampering different domains associated with the video sequence. Using the regional property of the video, Video Forgeries include the following types of tampering domains:

Video Forgeries include the following types of tampering domains:

- a) **Spatial Tampering:** This type of tampering is performed on visual contents of the frame along the x- y axis of the video. Spatially Tampering can be performed by manipulating the pixel bits in a frame or the adjacent ones in the video sequence. Thus Spatially Tampering can be performed at Pixel level, Block Level or Shot/Scene Level. The operations that can be included in this type of tampering are crop and replace, morphing, addition and deletion of object.
- b) **Temporal Tampering:** This type of tampering is performed on the concatenated chain of frames in the video. Temporal Tampering works in progression across the time frame. It primarily affects the time sequence of visual data recorded by the device. The operations that can be included in this type of tampering are mostly performed at frame level and include addition or deletion of frame and shuffling of frames.
- c) **Spatio-Temporal Tampering:** This type of tampering is a combination of both the above types of tampering. This tampering involves manipulating both the visual information along with the time sequences. SaptioTemporal Tampering tampers the concatenated sequence of frames along with the visual contents available in the frames of the video.

2.3.2 Digital Video Forgery Techniques [37, 38]

- a) **Video interpolation or In-painting:** is the process of reconstructing lost or deteriorated parts of images and videos. In the digital era, video interpolation refers to the application of sophisticated algorithms to replace small lost or corrupted parts or remove small defects or mainly small regions of the image or video data.
- b) **Frame and region duplication :** is the process of copying certain amount of frame from video and duplicating it. Region duplication is the process of copying any part or region from one frame and pasting it in another frame.

- c) **Digital Tampering: Video** manipulation is a process performed by a digital artist using video-editing software to transform a digital video into a desired video.
- d) **Frame Deletion:** is the process of selecting a frame or group of frames from a digital video and deleting it. For example if the crime scene footage contains the part where the victim uses gun to shoot the hostages then removing that few frames can alter the whole purpose of video and it can never be used as the proof against the victim.
- e) **Integrity and authenticity Violation:** is the type of forgery where the integrity & authenticity of a media is violated by changing the size or shape of it. Digital video is made up of a group of pictures or frames so changing any frame creates the change in video, and it's integrity get violated.

III. PROPOSED FRAMEWORK FOR VIDEO FORENSICS

Proposed framework for Video Temper detection presents integration of two technique namely MPEG Compression and correlation of noise residue and Video Temper detection technique using spatio-temporal region.

3.1 Proposed Video Forgery Process

Video Forgery is a technique of generating tempered, altered or fake videos using video editing software's. In the last few years, the Web has steadily moved towards more democratic forms of information-sharing. Indeed, many websites allow users to upload and share multimedia objects, including audio, images, and video sequences. This has determined an incredible growth of user generated content easily accessible online by anyone. However, the possibility of sharing self-produced media has not been followed by the development of methods to automatically verify the authenticity of the uploaded material. For this reason, while browsing multimedia content available on the Web, it is very common to run into forged and maliciously modified objects. Indeed, social media, newscasts and newspapers are sometimes tricked and make use of forged pictures or videos as if they were authentic Proposed Video Forgery Process Model is shown in figure 1

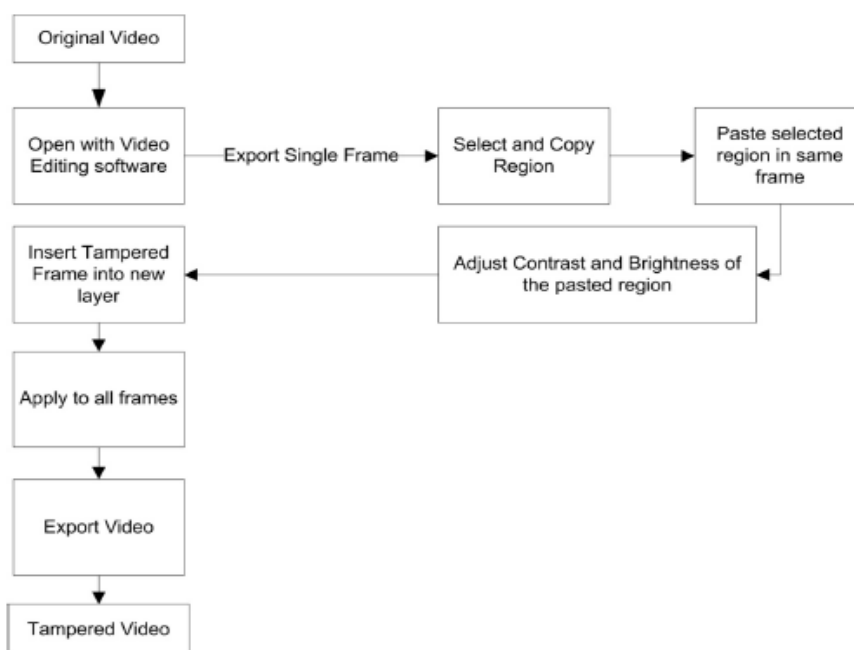


Figure 1 Proposed Video Forgery Process Model

3.2 Proposed Video Forensic Process Model

The proposed video forensic process model is shown in figure 2

- a) **Acquisition of Video :** This subroutine provides the procedure to acquire the video from the device. User will input the video which he/she needs to examine. This module will contain the procedures like importing video from any given location, putting it into work field, etc.
- b) Video forensic package consists of technique selection and video processing subroutine.
 - Technology Selection:** Once the video is acquired it will call to the technology selection subroutine from video forensic which will provide the opportunity for user to select the technique that digital forensic investigator want to apply on video.
- c) Video processing is achieved by using two techniques namely
 - i) Video Temper detection technique using MPEG Compression and correlation of noise residue(section 3.2.1)

- ii) Video Temper detection technique using spatio-temporal region.(3.2.2),
- iii) Every technique can be implemented and their output can be compared (Figure 1 and figure 2 Techniques).
- d)Hash Generation and Comparison of two multimedia or video files.(Figure 5)
- e) Output generation subroutine: The output should be generated to know whether the video is fake video or original video and from which IP the fake video is forwarded.

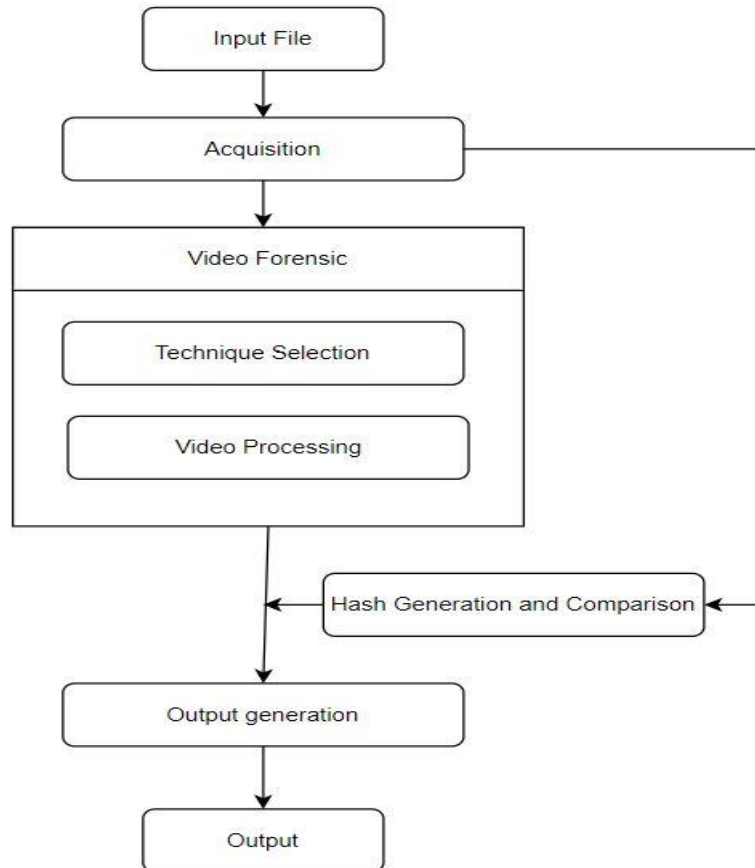


Figure 2.Video Forensic Process Model.

The integrity and authenticity of two multimedia files like text audio, image or video copied from electronic devices, storage media, and electronic files can be checked using cryptographic hash algorithms like MD 5 , SHA 256, RIPEMD-160 ,Whirlpool" . We have used md5 for this implementation as shown in figure 3.

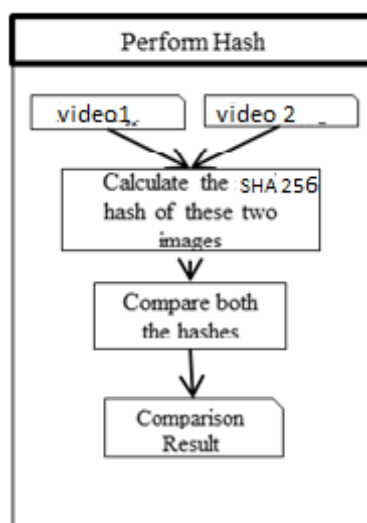


Figure 3 Perform Hash

Algorithm 1 Perform Hash ():
 Purpose :This algorithm takes two files as input and compares them by calculating their md5 hash and generates their comparison result.
Variables used in procedures are as follows:
 File1: first multimedia file
 File2: second multimedia file
 Hash1: SHA 256 hash of first file
 Hash2: SHA 256 hash of second file
Functions used in procedure are as follows:
 Read(): read the video file from user
 Md5sum(): calculate the md5 hash of given file
 Disp(): display the given result

Input: Provide the two multimedia files
Output: Result showing SHA 256 hash and comparison of two multimedia files
Procedure: Perform Hash ()

Begin

1. file1=read(file1);
2. file2=read(file2);
3. hash1= SHA 256 sum(file1);
4. hash2= SHA 256 sum(file2);
5. if [hash1 == hash2]

then

disp(Both hashes are equal so both files are equal);

else

disp(Both hashes aren't equal so both files are not equal);

end

End.

3.3 Technique Selection

3.2.1 . Video Temper detection technique using MPEG Compression and correlation of noise residue

Video forensic process framework consists of 5 sub-systems as shown in figure4.

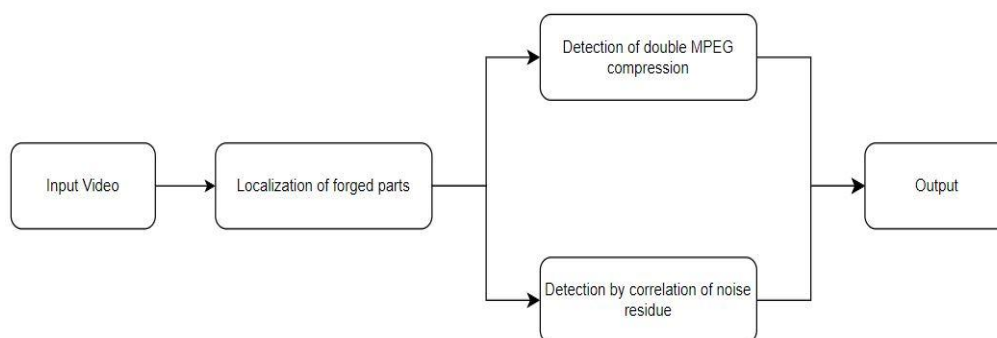


Figure 4 Video Temper detection Model using MPEG Compression and correlation of noise residue

- a) **Localization of forged parts:**In this subroutine, User can provide part from video or a full video for the examining the video. The forensic investigator or examiner selects the part from video which is edited or forged.
- b) **Video ForgeryDetection using Double MPEG Compression:** This technique checks weather video is compressed more than once by checking the original frame rate. Double compression will import disturbance into Discrete Cosine Transform (DCT) coefficients, reflecting in the violation of the parametric logarithmic law for first digit distribution of quantized Alternating Current (AC) coefficients. A 12-D feature can be extracted from each group of pictures (GOP). The serial Support Vector Machine (SVM) architecture is used to estimate original bit rate scale in doubly compressed video is used.
- c) **Video ForgeryDetection by Correlation of Noise Residue:** This module uses De-noising filter to remove the noise from frame of the video and then it creates the image with residue of noise by subtracting the

original image with de-noised image. Then it calculates the correlation between the neighboring blocks and finally applies Bayesian classifier for crating the threshold.

- d) **Collection of results:** This module will contain the video forgery detection results obtained by the two techniques.. This will also contain extra stuffs like edited video or any other information. This result will get interpreted and finally it will call the output generation algorithmsto generate the forensic report.

3.2.2 Proposed Algorithm Design For VideoTammer Detection

The Detection using correlation of noise residue is the algorithm used for tamper detection of video without having original video. The process is as shown in figure 5

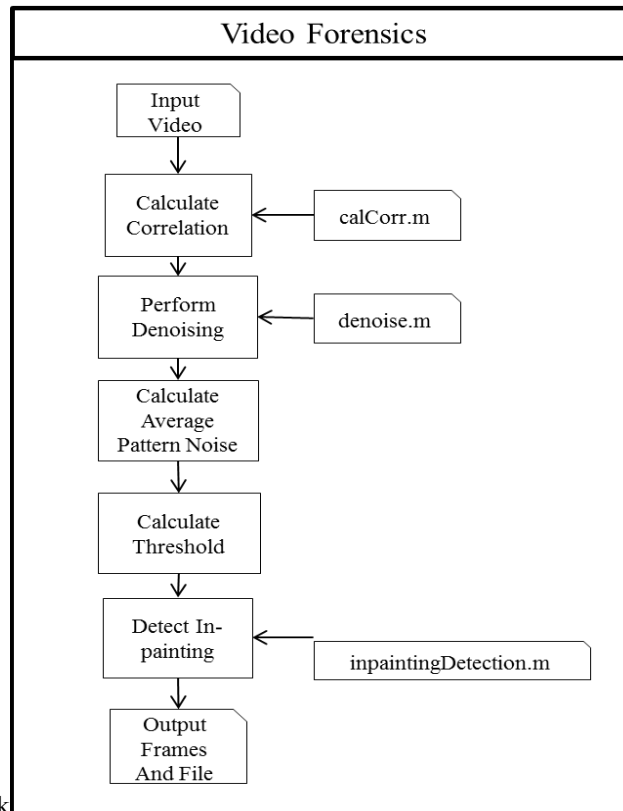


Figure 5 Video Forensic Model for identification of tampered video

Algorithm 2. Design for Video Forensics Algorithm

Threshold Value Calculation :The technique that we are using needs the strong signal processing library.thr1 is the threshold value calculated from the histogram h1 and h2

$$thr1 = 0.5 * ((\max(h1) + \max(h2)))$$

False Alarm Rate and Detection Rate :FalseAlarmRate and DetectionRateare calculate (1) n threshold. It uses the following steps for the implementation.

For this procedure the test based data used is the video frames which are tampered

Variables used

h1 & h2: histograms of original and tempered video

thr1: threshold value calculated from the histogram

path1: path of in-painted frames

type: type of the frame i.e. JPEG, PNG,BMP, etc.

bksize: size of the blocks in the frame

GDpath: path of the frames showing ground truth

Methods used

hist_plot(h1): plots the histogram

display(h1): shows the histogram

Video interpolation :Inpainting Detection(path1, GDpath, type, bksize, thr1): detects the in-painting and provides the statistical results based on the histogram

calCorr: calculates the correlation by denoising the each frame of video and then calculating the noise residue

max(h1): provides the maximum value of histogram

(Video interpolation :**Inpainting Detection**(path1, GDpath, type, bksize, thr1): detects the in-painting and provides the statistical results based on the histogram
 calCorr: calculates the correlation by denoising the each frame of video and then calculating the noise residue
 max(h1): provides the maximum value of histogram

```

Main Program // Design for Video Forensics Algorithms
Input: Path of in-painted video
Output: falseAlarmRate, DetectionRate and histograms showing the correlation between neighbouring blocks
Procedure:
function Main()
1.   begin
2.   read video
3.   calCorr // calculate the correlation value between the blocks of frames
4.   hist_plot(h1), //plot the histogram
5.   hist_plot(h2);
6.   display(h1)// show the histogram
7.   display(h2)
8.   thr1= 0.5*(max(h1)+max(h2))
9.   InpaintingDetection(path1, GDpath, type, bksize, thr1)//to find out Video interpolation
10.  end
    
```

i) Correlation calculation

Here we calculate the noise relation between blocks to get the pattern noise. De-noising[21] is done on the frame & then it is subtracted from the original frame to get the noise between original and de-noised frame. Its algorithm is as follows.

```

ii) Correlation calculation( )
Variables used:
avgPN: avgPN is the average pattern noise present in the block. It is stored in the form of matrix.
pct: pct is the start point of the each frame.
colnum: is the color value of that block
noise: noise obtained in each block
a: length of video frames

functions used:
denoised(avgPN): performs the denoising on the frames
print(round): prints frame no. which is under process

Input: path of in-painted frames
Output: pattern noise between the adjacent blocks.
Procedure:
calCorr
1.   begin
2.   read video
3.   pct=0
4.   a=sizeOf(video)
5.   Matrix avgPN[a][a]=0


$$r = \frac{\sum_i \sum_j (n_{i,j}^t - \bar{n}^t)(n_{i,j}^{t-1} - \bar{n}^{t-1})}{\sqrt{\sum_i \sum_j (n_{i,j}^t - \bar{n}^t)^2 \sum_i \sum_j (n_{i,j}^{t-1} - \bar{n}^{t-1})^2}}$$

// r is the average noise for single block

6.   fori=0 to len-1
       for c=1 to colnum
           avgPN=avgPN+r
           pct=pct+1
       end
    
```

```

print(i)
7.   end
8.   avgPN = denoise(avgPN) – avgPN
9.   end
    
```

ii) In-Painting Detection

In this part we use the calculated threshold to find out the in-painting in the video. The false alarm rate provides the value which gives the total error in the video frames & Detection rate provides the percentage of forged frames. Here pos1 is the value calculated from the forged frames.

Detection Rate is calculated by

$$r = \sum_0^{len-1} \frac{detectedImg(pos1)}{len(pos1)}$$

And false alarm rate is calculated by

$$err = \sum_0^{len-1} \frac{detectedImg(pos1)}{len(pos1)}$$

iii) In-Painting Detection()
Variables used:
 path1: Full Path of File Directory
 type: Image type. ex. 'bmp', 'jpg' i.e. extension filename
 bksize: The frame will be partitioned to blocksize*blocksize
 thr1: threshold value used for forensics
 GDpath: The path of frames showing ground truth
 a1: current frame
 g1: gray image of current frame
 dr: detection rate for each frame
 err: error rate for each frame
 GD: detected frame. Value will be one if forged else zero
 DetectionRate: average of total detection rate
 falseAlarmRate: average of total error rate
 read(frame): reads the frame
 write(): write the frame into file or folder

functions used:
 RgbToGray(a1): converts color image to gray
 ImToBw(GD): converts the detected part to white and remaining part to black

Input: path1, GDpath, type, bksize, thr1
Output: DetectionRate and falseAlarmRate

Procedure:
 InpaintingDetection(path1, GDpath, type, bksize, thr1)

```

1.   begin
2.   read path1
    if path1 is present then continue
    else write("path not present")
3.   if len=0 then return
4.   DetectionRate=0
5.   falseAlarmRate=0
6.   for i=1 to len-1
    a1=read(frame)
    g1 = RgbToGray(a1)
    GD = read(GDpath.type);
    GD = ImToBw(GD)
7.   end
8.   if GD==1 then
    
```

```

//calculate dr
detectionRate = detectionRate + dr
9.   if GD==0 then
//calculate err as in equation (18)
falseAlarmRate = falseAlarmRate + err
10.  print(DetectionRate)
11.  print(falseAlarmRate)
12.  end
    
```

3.2 .METHOD2 Video Temper Detection Technique Using Spatio-Temporal Region

Method 2 presents that, the attacker substitutes a part of a video, by either adding or removing something to/from a scene. ie a small spatio-temporal region is replaced. Due to the temporal dimension in video ,the videos attack consists in replacing 3D volumes (in the spatiotemporal domain), rather than 2D regions. Note that the substitution is followed by a local filtering operation (e.g., brightness or contrast adjustment) in order to make the tampering more realistic.

Video Tampering Detection System

The proposed algorithm is able to detect whether a spatiotemporal region of a sequence (i.e., a block of connected pixels in the spatio-temporal domain) was replaced by either a series of fixed images repeated in time, or a portion of the same video taken from a potentially different time interval. The video temper algorithm consists of two subroutines namely

- Module 1: Zero motion residual analysis algorithm
 - Module 2: Phase correlation analysis algorithm
- a) **Zero motion residual analysis algorithms :**The proposed algorithm is able to detect whether a spatiotemporal region of a sequence (i.e., a block of connected pixels in the spatio-temporal domain) was replaced by either a series of fixed images repeated in time, or a portion of the same video taken from a potentially different time interval. In the this case, the algorithm detects the attack by analyzing the footprint left on the residual computed between adjacent frames, and proves to be robust to mild compression.
- b) **Correlation analysis algorithm:** In the second case, the attack is detected exploiting a correlation analysis. However, proposed approach is fully automatic, and the position of tampered frames is not assumed to be known a-priori.

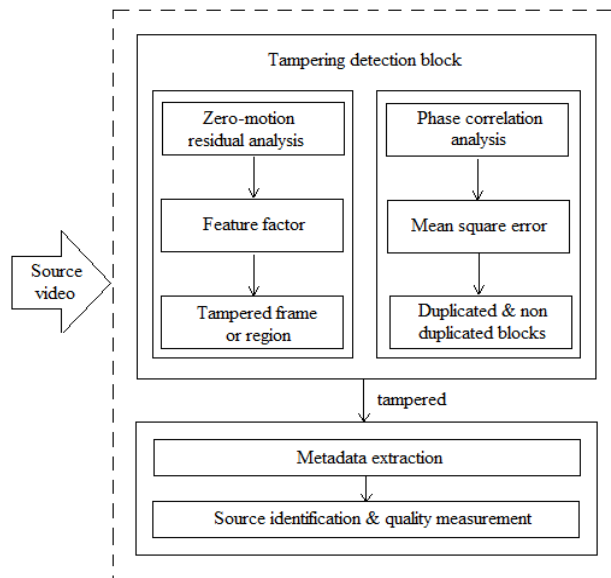


Figure 6. Tampering Detection System

Figure 6 depicts the integrated approach about tampering detection & authentication of digital video. It shows the detection, embedding & video quality measurement procedures .Since there is a high correlation among these duplicated clips, the similarity between two clips is used as a feature to find out those duplicated clips. To

effectively find out duplicated clip, a two-step algorithm scheme is proposed, which is composed of two stages: zero motion residual algorithm and phase correlation analysis algorithm.

Let $X = \{x_{i,j}^t\}$ denote a video sequence, where $i \in [1, I]$, $j \in [1, J]$, and $t \in [1, T]$ are the spatial and temporal coordinates of pixel samples indexed by integer numbers. The attack aims to replace the original set of connected pixels represented by the volume V , with another set of connected pixels \hat{V} of the same size of V , to obtain the forged sequence \hat{X} . In general, the shape of the volume V is arbitrary. For the sake of clarity, consider the simple case in which V is a box-shaped volume of samples. That is,

$$V = \{x_{i,j}^t \mid i \in [i_0, i_1], j \in [j_0, j_1], t \in [t_0, t_1]\}$$

In practice there are two possible choices for selecting the set of pixels \hat{V} , which determine the nature of the attack. The first possibility is to replace the forged region with a series of images, and the second consists in replacing that region with a portion of video. Let us now analyze these two possibilities.

3.2.2.2 Detection of image based attack

Image Based Attack :This method consists in pasting a fixed image over a spatial portion of a frame and repeating it in time. Since the image content does not move in time, this attack is generally applied to static scenes (e.g., when the video comes from a steady camera and has a fixed background). For this reason it is easy to replace V using either an image taken from a frame of the same video (e.g., the background), or another image (e.g., to introduce some text or additional objects). When the image comes from the same video, \hat{V} is populated repeating in time a 2D region of the t -th frame $\{x_{i,j}^t \mid i \in [i_0, i_1], j \in [j_0, j_1], t = t\}$. If the image comes from another source, the concept is the same, but pixels of \hat{V} do not come from X . This attack leaves characteristic footprints on the sequence.

To detect image-based attacks, analyze the zero-motion video residual, obtained by taking the difference between pixels in the same spatial position on consecutive frames. ie the residual is zero where images were spliced. In other words, the aim is to find the largest 3D bounding volume that contains only zero residual values. To achieve this goal, an algorithm based on iterative morphological operations and clustering is created and designed.

(i)The morphological operation that aims to compute a binary 3D map, where 1 indicates that a pixel might have been tampered with. First find residual difference between adjacent frames then find the binary mask of it with $i \in [1, I]$, $j \in [1, J]$, $t \in [1, T - 1]$. The binary mask maps the 0 residual values to 1, and sets everything else to 0. Let $M \in \{0, 1\}^{I \times J \times T-1}$ denote the 3D matrix whose elements are $m_{i,j}^t$.

(ii)Then, apply morphological erosion to M with a 3D Structuring Element (SE) H^{d_i, d_j, d_t} of size $d_i \times d_j \times d_t$, composed by ones, obtaining the final 3D map. where \ominus represents morphological erosion. In this situation, erosion acts as a filter that removes sub-volumes of E containing just a few values equal to 1 (i.e., small regions whose residual is equal to zero), which are more likely to be due to tampering than to compression. Indeed, compression introduces high correlation between frames; therefore the residual may assume zero value even in non-tampered regions. The size of H determines the minimum block of null residual that accept as not due to compression. As a matter of fact, using a large structuring element H would result in deleting all traces of tampering. Conversely, using a small structuring element H would lead to mistaking every small volume with residual equal to 0 for a tampered area. For this reason, start from a large value of H ($16 \times 16 \times 30$ in our experiments), and decrease it iteratively, until a plausible tampering region is detected. according to the criteria indicated as below: In case none of the criteria is met, the iteration is terminated when we reach the smallest acceptable value of H ($4 \times 4 \times 5$ in our experiments). In principle, each value $m_{i,j}^t = 1$ indicates tampering on that pixel position. However, in order to evaluate which pixels actually belong to a tampered area, we associate to each pair of spatial coordinates (i, j) a feature vector $f_{i,j} = [f_{i,j}^1, f_{i,j}^2]$.

The two features are computed as follows:

- $f_{i,j}^1$: this feature is the cardinality of the largest set of adjacent ones in $m_{i,j}^t$ along the temporal direction. It represents the largest number of consecutive frames possibly tampered in the position (i, j) .
- $f_{i,j}^2$: this feature is the t value from which the largest set of adjacent ones starts. It represents the starting frame of the possible tampering of length $f_{i,j}^1$.

By simply analyzing $f_{i,j}^1$ values, find the largest volume of possibly tampered pixels starting from the same frame. More specifically, then search for the pixel positions (i, j) with the highest $f_{i,j}^1$ values, and check if they start from the same time position given by $f_{i,j}^2$. If this volume is bigger than a given threshold (set according to the minimum tampering volume that want to be detected) forensic investigator detect the presence of tampering. The tampering localization map is then built according to the pixels belonging to the detected cluster.

step 1:Zero motion residual analysis algorithm

- 1 Input video
- 2 video into frames create matrix X to denote video sequences
- 3 Find the video residual between adjacent frames

$$r_{i,j}^t = x_{i,j}^t - x_{i,j}^{t+1}$$
- 4 Find the Residual binary mask

```

    if  $r_{i,j}^t = 0$  then  $m_{i,j}^t = 1$  ;
    otherwise  $m_{i,j}^t = 0$ 
    5 Erosion Operation
       $E = \{ e_{i,j}^t \} = \text{erosion}(M(i,j), H^{di,dj,dt})$ 
    6 Feature Factor
       $F_{i,j} = [f_{i,j}^1, f_{i,j}^2]$ 
    7 Tampered frame or region
  
```

3.2 .2.3 Detection Of Video Based Attacks

Video Based Attack :This method consists in replacing a part of the sequence with a portion of video Typically, to better integrate the duplicated region in the new part of the video, a local filtering operation is applied. This attack is typically used for scenes characterized by motion (e.g., to duplicate moving objects, or the background when the camera moves). However, since it is more difficult to realistically integrate two different videos (because of possibly different motion, illumination, etc.), this attack is commonly operated by substituting V with a set of pixels coming from the same video. However, since the forged region ^V comes from the same video sequence X, one can exploit a correlation analysis to find the duplicated region.

The video-based attack does not leave a characteristic footprint such as that left by the image-based attack. For this reason, this kind of attack is not detected by the algorithm described in imaged based attack. However, in practical situations, it is customary to replace a video region with another region from the same sequence (e.g., background copy-move to remove an object or a person). Hence, a new a correlation method aims to find the duplicated content which detect the tampered frames, without assuming a-priori knowledge, thus moving from a semi-supervised to a fully unsupervised method.

The main idea of this step is to detect duplicated content in the 3D domain by cross-correlating small 3D blocks. Indeed, rather than simply correlating frame regions, we correlate spatio-temporal portions of X. In order to reduce the computational complexity, yet achieving high accuracy, we resize the sequence in the spatial domain by a factor of 5, while retaining the full temporal resolution.

To this end, first compute the residual matrix $R = \{r_{i,j}\}$ of the downscaled sequence. Analyzing R rather than X allows us to remove the effect of linear operations (e.g., brightness adjustment) that may have been applied to the duplicated block. Then, we split R into non overlapping 3D blocks B_m^n of size $d_i \times d_j \times dt$, where n is the starting time index of a block, and $m \in [1,M]$ is the block index. We start analyzing all the blocks starting from a given time instant. If none of these blocks is detected to be duplicated (according to the method illustrated below), we analyze the next set of blocks (i.e., we increase the value n).

The detector is based on the phase-correlation between B_m^n and R. Let F is the Fourier transform operator, and * indicates the complex conjugate. This 3D correlation computes the similarity between a selected block B_m^n and the rest of the sequence.. Let us define the maximum correlation value obtained for each time position as $C_{B_m^n}^t$.

Step 2: Phase correlation analysis algorithm

- 1 Input video
- 2 Video into frames create matrix X to denote video sequences
- 3 Find the video residual between adjacent frames

$$r_{i,j}^t = x_{i,j}^t - x_{i,j}^{t+1}$$
- 4 $R_{i,j}^t$ Split into non overlapped blocks B_m^n
- 5 Find the Phase correlation

$$C_{i,j}^t(B_m^n) = F^{-1} \left(\frac{F(B_m^n)F(R)^*}{|F(B_m^n)F(R)^*|} \right)$$
- 6 Find the maximum correlation value

$$C_{B_m^n}^t = \max_{i,j} (|C_{i,j}^t(B_m^n)|)$$
- 7 Confidence value according to max/min ratio

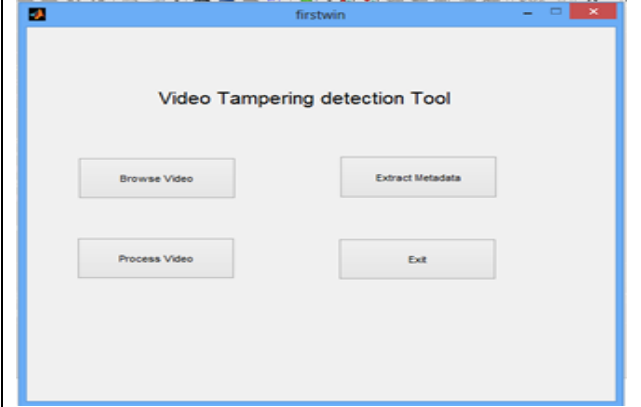
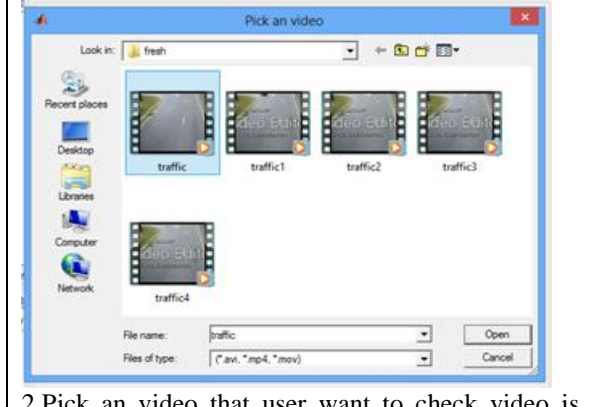
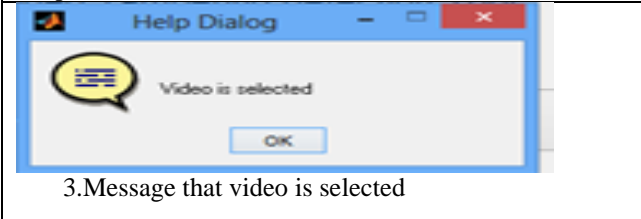
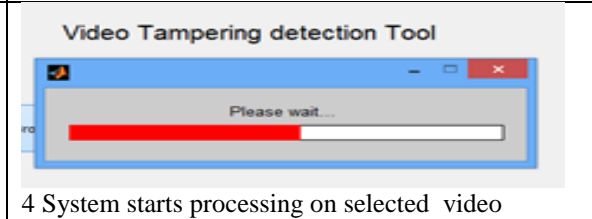
$$PB_m^n = \frac{\max_{i,j} (C_{i,j}^t(B_m^n))}{\frac{1}{(T-1)} \sum_t C_{B_m^n}^t}$$
- 8 Calculated MSE-Find the Duplicated and Non Duplicated blocks

3.3.3 IP address Tracing

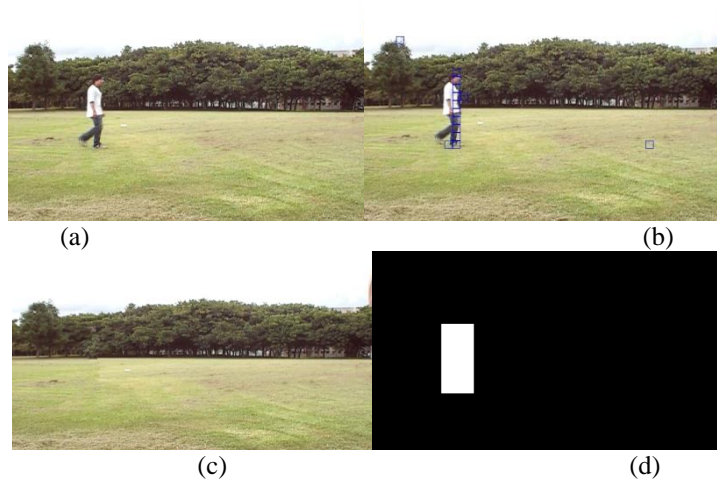
You can use email forensic to trace an Email Sender’s Location through IP address..you can also use dos prompt to execute the commands like tracert, nslookupand “ping host address,” eg“ping www.facebook.com” and then press enter. Social media sites (Facebook, Twitter, Instagram, Snapchat, etc.) do not reveal IP addresses between users, but the site administrators indeed know your IP address. Also, if you click on an ad or link on the site, they will capture your IP address. You can use a website such as IP-Lookup.net or IP-Tracker.org and enter the sender’s IP address to trace their approximate location. Websites such as WhatIsMyIPAddress.com offer help finding IP addresses and uncovering where they’re located.

IV. Results and Conclusion

The screen shots of the package are shown below. The results are also simulated for the given sample video and its temper detection using both the proposed algorithms.

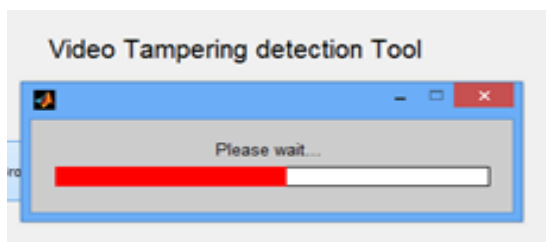
	
<p>1.System ask user to upload video to check video is tampered or not</p>	<p>2.Pick an video that user want to check video is tampered or not</p>
	
<p>3.Message that video is selected</p>	<p>4 System starts processing on selected video</p>

Method 1 Results :In video forensics, as shown in the Screen 1 (a) contains the original frame.(b)shows the detected part which is removed in figure (c). and figure(d) contains the removed part from tampered frame. Screen 2 (a) shows the correlation value distribution in original frame where blue line indicates the forged region which is under the red line which shows non tampered region. Screen 2 (b) shows the correlation value distribution in tampered frame where blue line indicates the forged region which is above the red line which shows non tampered region. Thus proposed system provides forensic technique for audio, image and video files.

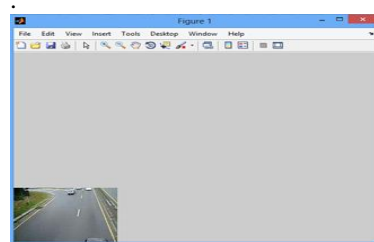


Screen 1. Video forgery detection using co-relation of noise residue; (a)Original Frame (b) Detecte frame (c)Tampered frame and (d)Frame showing removed tampered region

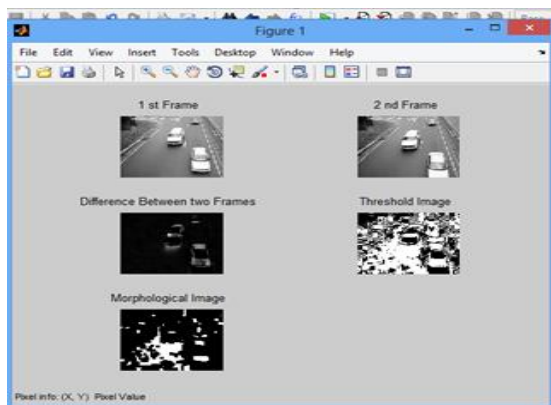
Method 2 System ask user to upload video to check video is tampered or not



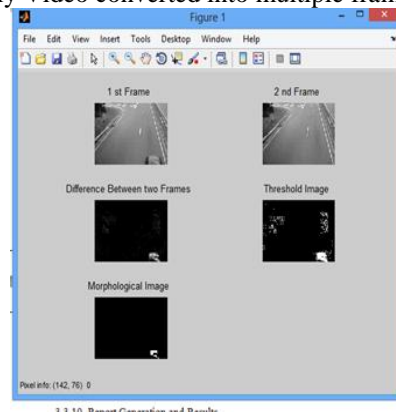
5. System starts processing on selected video



6. Firstly Video converted into multiple frames



7. Frames are compared with each other to calculate residual values & it generate threshold image



8. Apply Morphological filtering



10. Video is tempered

We have used various multimedia editing and forensic tools. The proposed work is also compared with the video forensic tools. With the video editing technology currently available, software solutions allow people to easily forge a video sequence in a way that is realistic. In many cases the meaning of a video can be distorted by simply removing, replicating or inserting a group of frames. For example, such an attack proves to be extremely dangerous in contexts like video surveillance, where eliminating a group of frames can make the video totally useless. Without authentication, a video viewer (or a consumer) cannot verify that the video being viewed is really the original one that was transmitted by a producer. There may be some eavesdroppers who modify the video content intentionally to harm the interests of either or both the producer and the consumer. However we have proposed the algorithms using Video Forgery Detection using Double MPEG Compression and Video Forgery Detection by Correlation of Noise Residue to solve these problems. This also checked the integrity and authenticity of the original video.

The proposed method able to detect happened attack is whether on a spatial region, or a spatio-temporal region of sequences. In the first step, the zero motion residual algorithm detect tampering if video sequence was replaced by image or a series of fixed images. This algorithm is based on the fact that when video tampering happened, it is expected that there exists some footprints left in the processed video. If the spatial-temporal region of sequence was replaced by a portion of video taken from a potentially different time interval, then first step fails so the second step is added into the algorithm. In the second step, the phase correlation analysis algorithm evaluated to detect tampering.

The video-based attack does not leave a characteristic footprint such as that left by the image-based attack. However, in practical situations, it is customary to replace a video region with another region from the same sequence (e.g., background copy-move to remove an object or a person). Hence, the proposed correlation method aims to find the duplicated content. It also detect which are the tampered frames, without assuming a-priori knowledge, thus moving from a semi-supervised to a fully unsupervised method. The main idea of this step is to detect duplicated content in the 3D domain by cross-correlating small 3D blocks. Indeed, rather than simply correlating frame regions, it also correlate spatio-temporal portions of X. In order to reduce the computational complexity, yet achieving high accuracy, we resize the sequence in the spatial domain by a factor of 5, while retaining the full temporal resolution. Mat lab is used for coding the algorithms.

REFERENCES

- [1] S. Chen and H. Leung, "Chaotic watermarking for video authentication in surveillance applications," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 5, pp. 704–709, May 2008.
- [2] B. Zhu, M. Swanson, and A. Tewfik, "When seeing isn't believing [multimedia authentication technologies]," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 40–49, Mar. 2004.
- [3] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, "Image authentication techniques for surveillance applications," *Proc. IEEE*, vol. 89, no. 10, pp. 1403–1418, Oct. 2001.
- [4] P.-C. Su, C.-S. Wu, I.-F. Chen, C.-Y. Wu, and Y.-C. Wu, "A practical design of digital video watermarking in H.264/AVC for content authentication," *Signal Process, Image Commun.*, vol. 26, nos. 8–9, pp. 413–426, Oct. 2011.
- [5] D. Xu, R. Wang, and J. Wang, "A novel watermarking scheme for H.264/AVC video authentication," *Signal Process., Image Commun.*, vol. 26, no. 6, pp. 267–279, 2011.
- [6] J. Fridrich, M. Goljan, and A. C. Baldoza, "New fragile authentication watermark for images," in *Proc. ICIP*, vol. 1. Vancouver, BC, Canada, 2000, pp. 446–449.
- [7] K. Maeno, Q. Sun, S.-F. Chang, and M. Suto, "New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization," *IEEE Trans. Multimedia*, vol. 8, no. 1, pp. 32–45, Feb. 2006.
- [8] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 43–55, Mar. 2006. [9] J. Sang and M. S. Alam, "Fragility and robustness of binary phaseonly filter based fragile/semi-fragile digital image watermarking," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 595–606, Mar. 2008.
- [10] M. Fallahpour, M. Semsarzadeh, S. Shirmohammadi, and J. Zhao, "A realspatio-temporal watermarking scheme for H.264/AVC," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, Minneapolis, MN, USA, May 2013, pp. 872–875.
- [11] K. S. Wong, K. Tanaka, K. Takagi, and Y. Nakajima, "Complete video quality-preserving data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 10, pp. 1499–1512, Oct. 2009.
- [12] R. Iqbal, S. Shirmohammadi, A. E. Saddik, and J. Zhao, "Compressed domain video processing for adaptation, encryption, and authentication," *IEEE Multimedia*, vol. 15, no. 2, pp. 38–50, Apr./Jun. 2008.
- [13] J. Zhao, W. J. Tam, S. Wang, D. Zheng, and F. Speranza, "A digital watermarking and perceptual model based video quality measurement," in *Proc. IEEE Conf. Instrum. Meas. Technol.*, May 2005, pp. 1729–1734.
- [14] Abdul Rehman Javed a, Zunera Jalil a, Wishah Zehra b, Thippa Reddy Gadekallu c, Doug Young Suh d,* , Md. Jalil Piran A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions.
- [15] Shahraki, A.S., Sayyadi, H., AMRI, M.H., Nikmaram, M., 2013. Survey: Video forensic tools. *J. Theor. Appl. Inf. Technol.* 47 (1).
- [16] 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.
- [17] Wahab, A.W.A., Bagiwa, M.A., Idris, M.Y.I., Khan, S., Razak, Z., Ariffin, M.R.K., 2014. Passive video forgery detection techniques: a survey. In: 2014 10th International Conference on Information Assurance and Security. IEEE, Okinawa, Japan, pp. 29–34

- [18] Kaur, H., Jindal, N., 2020a. Deep convolutional neural network for graphics forgery detection in video. *Wirel. Pers. Commun.* 1–19.
- [19]. Kaur, H., Jindal, N., 2020b. Image and video forensics: A critical survey. *Wirel. Pers. Commun.* 112, 1–22.
- [20] Huang, C.C., Zhang, Y., Thing, V.L.L., 2017. Inter-frame video forgery detection based on multi-level subtraction approach for realistic video forensic applications. In: *Proc. 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP)*, Singapore, pp. 20–24
- [21] 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 and Security (NTMS)*. IEEE, pp. 1–7.
- [22] Al-Obaydy, W.N.I., Suandi, S.A., 2020. Open-set single-sample face recognition in video surveillance using fuzzy ARTMAP. *Neural Comput. Appl.* 32 (5), 1405–1412.
- [23]. Bestagini, P., Battaglia, S., Milani, S., Tagliasacchi, M., Tubaro, S., 2013a. Detection of temporal interpolation in video sequences. In: *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*. IEEE, pp. 3033–3037.
- [24]. Bestagini, P., Milani, S., Tagliasacchi, M., Tubaro, S., 2013b. Local tampering detection in video sequences. In: *Multimedia Signal Processing (MMSp), 2013 IEEE 15th International Workshop on*. IEEE, pp. 488–493.
- [25]. Bidokhti, A., Ghaemmaghami, S., March 2015. Detection of regional copy/move forgery in MPEG videos using optical flow. In: *Artificial Intelligence and Signal Processing (AISP), 2015 International Symposium on*. pp. 13–17.
- [26]. Chetty, G., Biswas, M., Singh, R., 2010. Digital video tamper detection based on multimodal fusion of residue features. In: *Network and System Security (NSS), 2010 4th International Conference on*. IEEE, pp. 606–613.
- [27]. Cozzolino, D., Poggi, G., Verdoliva, L., Oct 2014. Copy-move forgery detection based on patchmatch. In: *2014 IEEE International Conference on Image Processing (ICIP)*. pp. 5312–5316.
- [28]. Hsu, C.-C., Hung, T.-Y., Lin, C.-W., Hsu, C.-T., 2008. Video forgery detection using correlation of noise residue. In: *Multimedia Signal Processing, 2008 IEEE 10th Workshop on*. IEEE, pp. 170-174
- [29]. Joshi, V., Jain, S., March 2015. Tampering detection in digital video - a review of temporal fingerprints-based techniques. In: *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*. pp. 1121–1124.
- [30]. Lin, C.-S., Tsay, J.-J., 2014. A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. *Digital Investigation* 11 (2), 120– 140.
- [31]. Lin, G.-S., Chang, J.-F., Chuang, C.-H., 2011. Detecting frame duplication based on spatial and temporal analyses. In: *Computer Science & Education (ICCSE), 2011 6th International Conference on*. IEEE, pp. 1396–1399.
- [32]. Liu, H., Li, S., Bian, S., 2014. Detecting frame deletion in H.264 video. In: *Information Security Practice and Experience*. Springer, pp. 262-270
- [33]. Shanableh T. Detection of frame deletion for digital video forensics. *Digital Investigation* 10 (4), 350–360. , 2013
- [34]. Milani, S., Bestagini, P., Tagliasacchi, M., Tubaro, S., 2012a. Multiple compression detection for video sequences. In: [35] *Multimedia Signal Processing (MMSp), 2012 IEEE 14th International Workshop on*. IEEE, pp. 112–117.
- [35] K. Sitara a, b, B.M. Mehtre, Digital video tampering detection: An overview of passive techniques, *Digital Investigation*, Volume 18, September 2016, Pages 8-22
- [36] Mubbashar Saddique1 , Khurshid Asghar etal Robust Video Content Authentication using Video Binary Pattern and Extreme Learning Machine , (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 8, 2019.
- [37] Vinay Kumar, Abhishek Singh, Vineet Kansal, Manish Gaur 1 A Comprehensive Analysis on Video Forgery Detection Techniques Vinay Kumara , Abhishek Singhb , Vineet kansalc , Manish Guard, *RD International Conference On Innovative Computing and Communication (ICICC-2020)*