International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

Anti- Forensics: The Tampering of Media

Nour Mohammad[1], Hasan Fayyad-Kazan[2], Mohamad Saab[3]
[1, 3] Department of Forensic Science and Molecular Diagnostics, Faculty of Sciences
Lebanese University
[2] Department of Fundamental Sciences, Faculty of Dental Medicine, Lebanese University
[1] E-mail: nourmohammad9896@gmail.com [2] hafayyad@gmail.com [3] mhmdyoussef79@gmail.com

Abstract: In the context of forensic investigations, the traditional understanding of evidence is changing where nowadays most prosecutors, lawyers and judges heavily rely on multimedia signs. This modern shift has allowed the law enforcement to better reconstruct the crime scenes or reveal the truth of any critical event.
In this paper we shed the light on the role of video, audio and photos as forensic evidences presenting the possibility of their tampering by various easy-to-use, available anti-forensics softwares. We proved that along with the forensic analysis, digital processing, enhancement and authentication via forgery detection algorithms to testify the integrity of the content and the respective source of each, differentiating between an original and altered evidence is now feasible. These operations assist the court to attain higher degree of intelligibility of the multimedia data handled and assert the information retrieved from each that support the success of the investigation process.

Keywords: *Anti-forensics, Multimedia evidence analysis, Tampering Software, Authentication Techniques*

1- Introduction

In an era of digital technology and multimedia development, there is no wonder that video, audio and photos serve as significant evidences in the forensic investigations.

These types of evidences allow the court to gain valuable information and clues convincing enough to accuse or exonerate the suspect.

But how much is multimedia a creditable forensic evidence to rely on?

In fact nowadays, with the advent of editing software tools, not only cybercriminals but also non-experts can tamper captured photos or alter the content (audio/video) of any scene at ease.

"Seeing is no longer believing." This potential danger of false evidence imposes providing the authenticity of video and audio before they are produced as evidence in the court of law. Such operations like thorough video analysis, photo forgery and audio tampering detection lead to fruitful and authentic prosecution results.

Figure 1 Multimedia Evidences [31]

2 - General Background

In a world devoid of forensic science, criminals, thieves, assaulters and drug traffickers would be roaming scot-free. Criminal, and even civil investigations, are incomplete without forensic science which deals with the examination and analysis of various types of evidences in order to establish facts admissible to the court of law.

Of all the disciplines that deal with forensic science, digital forensics has the potential to be one of the most collaborative ones since it touches almost every aspect of our life nowadays [5]. The fact that nearly every area of the current time is supported by electronic devices, like smart phones, tablets and digital cameras..., strongly contributes to the steadily increasing importance of digital evidence in crime investigation. One significant element of this kind of evidence is multimedia content, which just like physical evidence, must be followed to reveal the truth behind every serious event.

Since modern life is unthinkable without multimedia and electronic data, the legal system widely recognizes the pivotal role of video, audio and pictures in the investigations and conviction of the court. Upon realizing this substantiality, recent studies show that up to 80% of the cases are forensically interpreted with the support of digital evidences including multimedia as investigative tools[8]. Hence instead of restricting the process by conventional tools and relying only on blood spatters and DNA swabs, that undoubtedly play a vital role in the forensic investigation, multimedia evidence contributes to much of the overall incident scene analysis in ways that may not appear obvious at first.

Eventually there is nothing more cogent to the court and the justice system in their forensic deductions than hearing an audio sent by an intimidator or looking at a burglar face in a video surveillance footage for example. However when analysis is commonly associated with multimedia techniques as forensic evidences, the main focus is on the identification of the authenticity of their content and the information elicited from due to the high possibility of tampering which might lead to injustice in the results.

I. Video

1- Video as Forensic Evidence

Since a few years, a smart-phone camera has become a common property and the spread of video surveillance cameras has widely increased due to the recognition of their role in preserving public and private security. Because of the availability of the recording equipment, an exponential progression of the use of videos as investigative tools is seen nowadays.

A video is a visual multimedia source forming a moving picture to which an audio component corresponds after combining a series of images [3]. Starting from this definition, there is nothing more persuasive to the court in making its verdict based on an evidence that allows watching the whole scene under investigation, hearing all the voices and visualizing all the evidences .

In many cases the only witness to a crime could be a video surveillance camera. This will serve as a key in identifying and finding a criminal or assaulter's face or soft biometrics like height, weight..etc.

Corroboration of witness or suspect statement could also be done with the aid of video evidence recorded by a security camera [16]. Instantly, it can reveal the direction of travel of the perpetrator into or away from the crime scene that helps in the process of the traces' collection and examination. Add to this the common trend of capturing every incident or event through our smart phones that play a potent role in verifying the identity of the suspect appearing through. Many of the violence acts, abuse, terrorism, physical threats, crimes committed in public areas are recorded via our electronic devices and digital cameras, spread on social media and act as a robust evidence in the prosecution.

Was the theft alone or in a multi-person-assisted robbery? What was the model of the car through which the burglar flee? Did the perpetrator look sane when he committed the murder or psychologically unstable? Many more questions could be answered depending on a video record which emphasize on the power of video evidence in analyzing an event aiding investigation and initializing the judgment. Despite its significance, nowadays any type of video could be exposed to tampering due to the easy-to-use and available forgery techniques which makes relying upon it unlawful if the authentication of each evidence is not tested previously to its analysis.

Figure 2 CCTV footage [32]

Eventually it is worthy to mention that there are several types of recorders used to create digital video evidences . Some of these are :

- CCTV / DVR : closed-cicuit TV digital video recorder
- CCTV / NVR : closed-circuit TV network video recorder
- MDVR : mobile digital video recorder
- Body camera
- Concealed camera
- Tazer camera
- Police dash-cam

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

Figure 3 DashCam[33]

Figure 4 Video Evidence captured by a smartphone [34]

2- Video Enhancement and Analysis

According to the circumstance , the type of recordings retrieved is unique in each case as thus its analysis and enhancement is unique as well . Though some recordings appear to be unclear and useless, the collection of every footage is a must for a forensic enhancement technique could clarify unnoticeable details in the video before its processsing [16] . Following the collection of the evidence , the model of the recording device , details about the recording system and the current time/date and that of the recorder's display must be noted by the investigator .

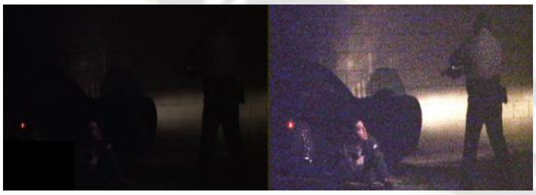


Figure 5 The power of video enhancement [35]

2.1- Basic methods of video enhancement

The technology of today's video recording has evolved from analog , cassete tape recordings , to digital where information is recorded using data blocks of 0s ans 1s [16] . Whether a video evidence is analog or digital , the forensic expert early step after evidence collection must be the creation of a working copy of the video before processing it . This assures the availability of the unaltered form of the original evidence for further comparison with the processed copy.

The handling of a video forensic evidence should be carefully done where the content of the recorded data should never be changed but rather only enhanced. The employment of the video enhancement techniques is important to obtain promising results from the video analysis [16] . Such techniques include :

- <u>Video Stabilization :</u> produce smooth video playback by decreasing the amount of the movement in a video
- <u>Sharpening :</u> clarify the edges of the pictures in the video making them clearer and more distinct
- <u>Masking :</u> protect witness or suspect by covering areas in the video if the record is to be published
- <u>Interlacing :</u> combine two television fields for producing a full frame of a video when working in analog system
- <u>Demultiplexing :</u> isolate each camera when multiple video signals are combined into a single signal in CCTV

2.2- Amped FIVE Software for Video enhancement

AMPED
SOFTWARE

In the context of video enhancement , it is very essential to shed the light on one of the most potent video enhancement softwares Apmed FIVE . Along with other powerful softwares like Blackstone , this latter is on which most law enforcement surveillance and security applications , militiary operations , forensic labs and civil litigations mostly depend on due to its convenience , accuracy , simplicity and its capability of producing complete and rigorous outcomes [25] .

In a fast , precise and simple way , Amped FIVE provides a complete solution to the video processing and analysis . The main key element in Amped FIVE design is to maintain the integrity of the original evidence since any manipulated or doctored evidence will be absolutely excluded by the prosecutors , judges and courts .

The concept of Amped FIVE is based on filtering in which every filter takes the video generated by the previous one and the result will pass to their output filter after processing . By this strategy if any value was modified on a previous filter , this will be reflected as a modification of the

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

final result [2]. This filtering concept is very fast and precise to guarantee high effectiveness of this software .

The features and advantages supplied by Amped FIVE are paramount through the video evidence processing and analysis .

Some of these options include :

1- Motion blur correction

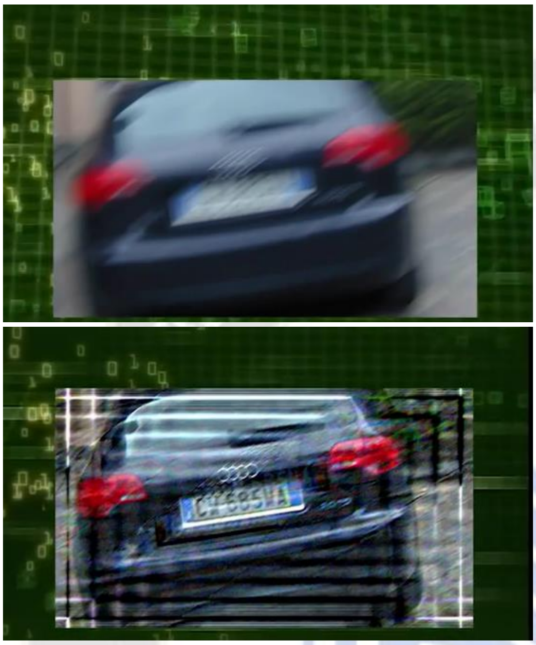


Figure 6 Vehicle number before and after debluring[36]

2- Background correction

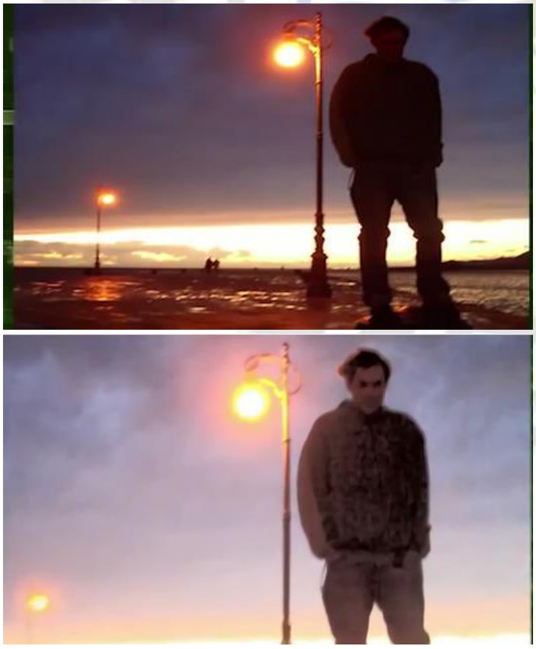


Figure 7 Background view before and after enhancement [37]

3- Optical Debluring

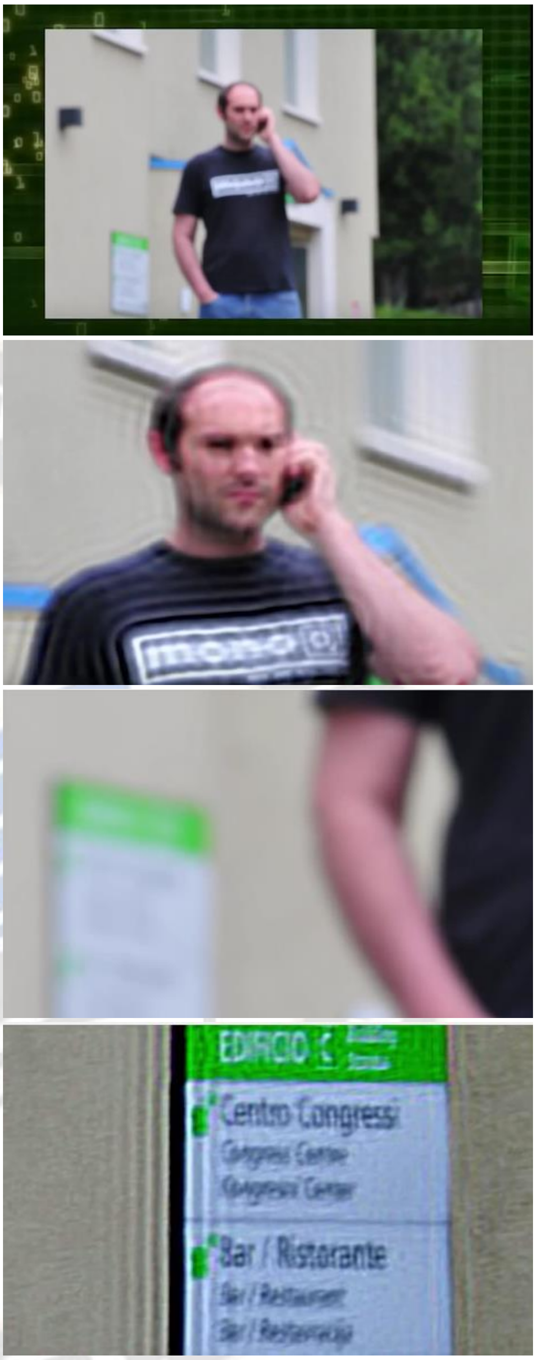


Figure 8 blurred facial and words video frame before and after clarification [38]

4- Poor wheather enhancement

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

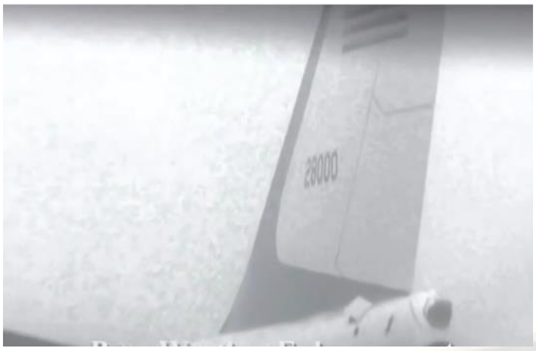


Figure 9 Airplane number before and after clarification [(39)]

5- Average framing

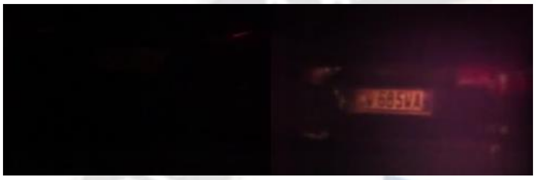


Figure 10 Vehicle number appearance after enhancement [(40)]

6- 3D Measurement

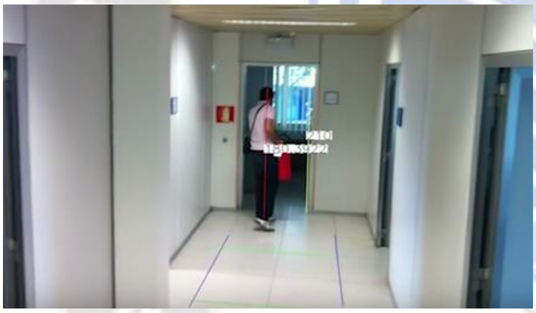


Figure 11 3D measurements of suspect's body height [(41)]

7- Local stabilization

Figure 12 Local stabilization of fast moving motorcycle [(42)]

8- Latent fingerprints enhancement

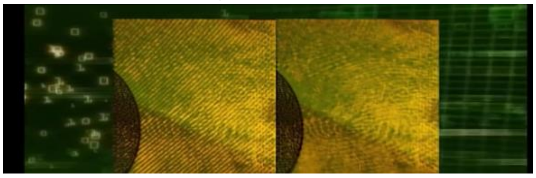


Figure 13 Latent fingerprints before and after enhancement [(42)]

Because Amped FIVE is able to support any video format , reduces time and effort due to its fast processing , generates automatic and accurate reports and has high performance in targeting any type of data from latent fingerprints , crime scene digital videos to CCTV recordings [(2)] , it has become the world's top revolutionary solution for video enhancement and analysis .

3- Video Tampering

The contents of digital videos and recordings serve as valuable evidences and provide crucial information that form the basis of several consequential decisions in the fields of forensic investigations. Since the initialization of the use of video evidence in the courts, its content had been considered infallible. However, the huge proliferation of the inexpensive and portable video-capture devices like digital cameras and cell phones that most people carry nowadays along with the wide spread of variety of low-cost video editing tools has led to the realization that this is no longer the case. A potential danger is produced by this combination as today anyone has the ability to modify the content of a certain video at ease according to his or her wish. From here the necessity of video authentication was enlarged in order to assure the credibility of the evidence to rely on [(8)].

Before going into details concerning video authentication in the next section, let's shed the light on video tampering and its types.

What is video tampering?

Video tampering is the process of furtive manipulation of the content of a video [(3)] .This easy task is done for the purpose of changing the real meaning conveyed by the imagery in the video by concealing or altering an object or event in the video content. In general the several types of video forgeries are categorized into two: Inter-frame forgery and Intra-frame forgery.

3.1- Inter-frame Forgery : Tampering that modify the frames' sequence in a video [(13)] ; This sequence can be altered by four different ways that are :

a. Frame Insertion : adding new frames to the targeted video from different videos
b. Frame Deletion : removing frames from the targeted video
c. Frame Duplication : copying a sequence of frames and pasting it at another location within the same video
d. Frame Shuffling : changing the order of events by changing the order of frames
e. Temporal Splicing : generating a new video by interpolating frames of two or more videos [(3)]

DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

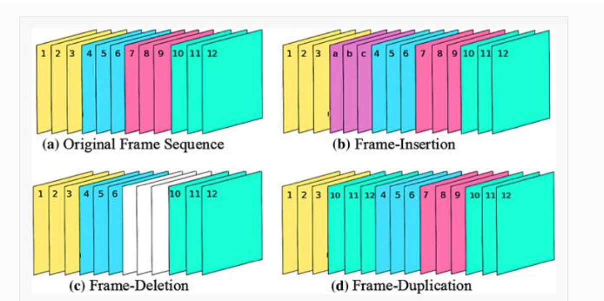

(a) Original Frame Sequence
(b) Frame-Insertion
(c) Frame-Deletion
(d) Frame-Duplication

Figure 14 Types of Inter-frame forgery [42]

3.2 Intra-frame Forgery: Tampering that modify the actual contents of individual frames of the video

a. Copy/paste or Copy/move Forgery : adding or removing a person or object to or from a scene represented in the video frames

It is called partial manipulation since only a small part of the frame is modified and the rest of the frame regions remains unaltered [3].

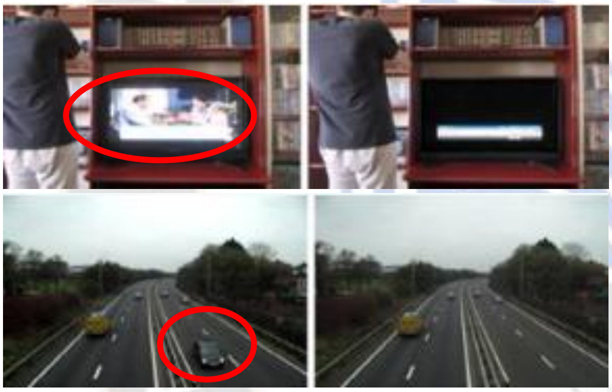


Figure 15 Deletion of video frame objects [42]

While adding an object to the scene could be simple, removing an object from the video frame does not sound so. How will the region left behind the removed part from the scene be covered so that the frame appears as a complete untouched one?

This is solved by *Impainting Technique*. This technique helps restoring the missing part and tainted region left after object deletion in the most visually plausible manner [9].

One important type within the copy/paste forgery is *the Green Screening or Blue Screen Compositing* [3]**.** This allows changing the background in the targeted video and merging any other view or scene behind the foreground objects.

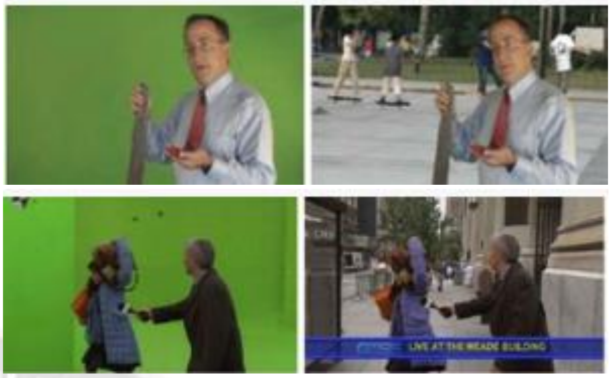


Figure 16 Background Alterations [42]

b. Upscale Crop Forgery: cropping specific frames of a video which allow the elimination of evidence present in a crime scene for example. To fill the gap created, enlargement of the affected frames is followed to maintain resolution consistency of the whole video.

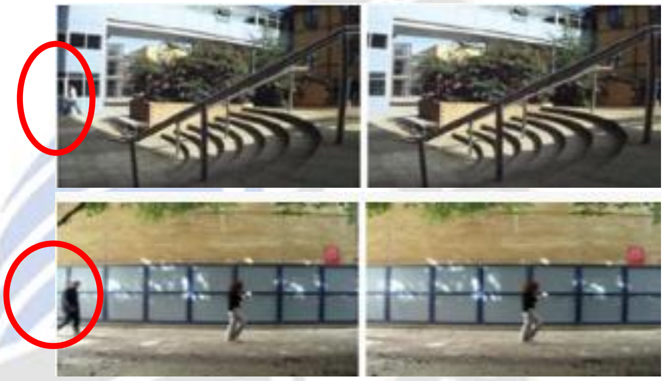


Figure 17 Cropping objects from video frames [42]

These are all examples of how malicious video tampering is and how the created plausible video forgeries could be inconspicuous to a human eye.

3.3- Video Reenactment: Face2Face System

Tampering a video content by cropping a frame to hide a suspect, changing the background to alter time and location or removing an object to conceal evidence could sound familiar to a lot of people somehow. Many of the video-editing softwares like Adobe Premier, Photoshop, Light works and Cinelerra lead to results that most people expect and find simple[9]. But what about manipulating a video in real time to alter the facial expressions and the saying of a target person?! This idea was not considered believable at first.

The existence of new kinds of face tracking softwares has taken the days when we could trust what we see in a video to an official end .The up growth of video reenactment or face tracking algorithms like that of Face2Face led to astonishing outcomes. This latter tends to animate facial and

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

vocal expressions of the target actor in a video by a source actor synthesizing a photo-realistic manipulated output [29].

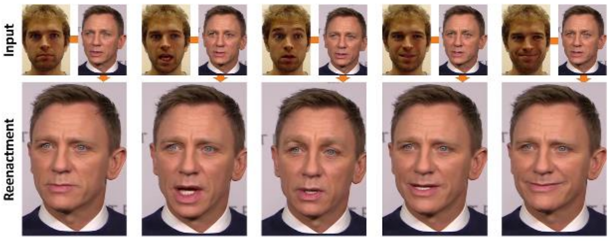


Figure 18 Video Reenactment Input and Output [42]

Face2face can be applied to any video type or format for example a Youtube video [29]. After selecting the targeted person speaking in a video, one should use a standard webcam to capture video of someone (the source actor) whose facial expressions to be transferred to the targeted individual. An efficient and fast reenactment will be carried out by processing both videos by Face2Face system [28] .

The reenactment output video is rendered in the most believable manner so that no one could ever think that there might be a possibility of manipulation in the video watched.

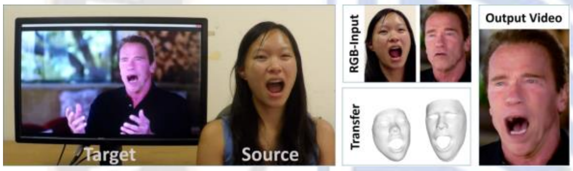


Figure 19 Face2Face Technique [42]

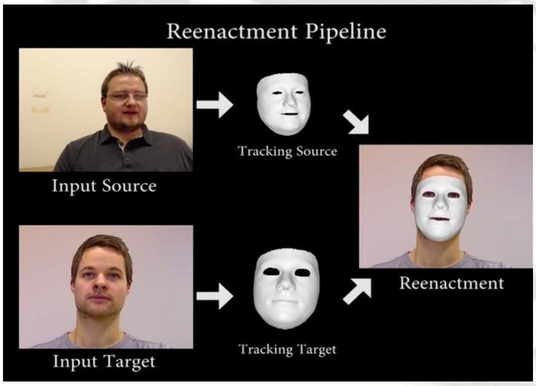


Figure 20 Face2Face Process [43]

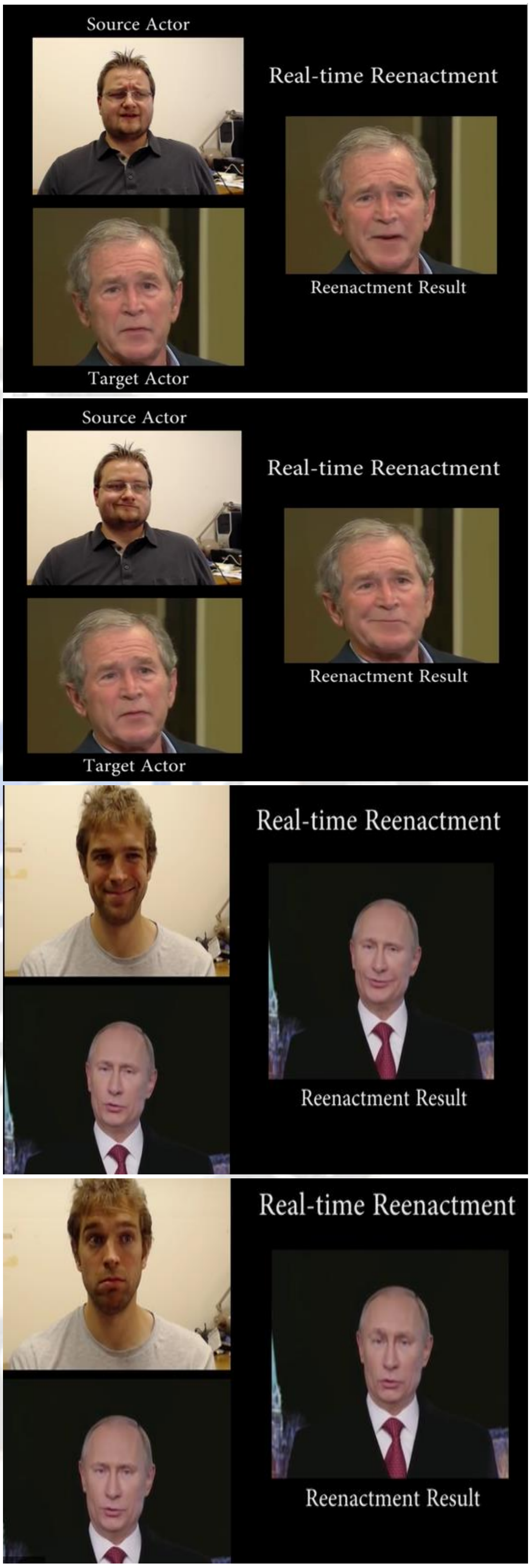


Figure 21 Examples of using Face2Face system [44]

While some people find it funny, the idea has a scary and illegal side. Imagine that someone can synthesize a whole video of you making you say words you didn't and transferring the source actor's facial expressions such as lips movements and eyebrows raises to your face. You, the video subject, will turn into the actor's puppet via a flawless face masking system **[28]**. This concept is dangerous and malicious if taken deeply into consideration. When such a perfectly manipulated video act as an evidence, it can mislead many investigations and judgments, convict many innocent ones and proliferate bias and injustice.

4- Video Authentication

A video evidence is expected to provide a truthful depiction of any event under investigation. For this reason interpreting any video evidence and relying on its content in the courts, video authentication is a must. The evaluation of the authenticity and integrity of the video has become attainable since the development of video tampering detection techniques that aim at finding traces left after any forgery creation. These techniques are classified into active and passive **[26]**.

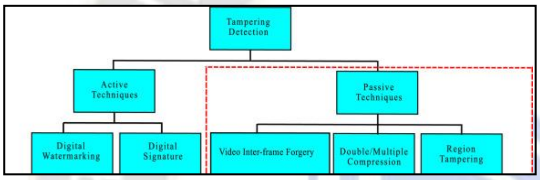


Figure 22 Types of Video Tampering Detection Methods [45]

4.1- Active Tampering Detection Technique

Active techniques are based on watermarking and digital signature**[9]**. Watermarking represents embedding content-based specific codes or digital producer identification labels unique for each multimedia file to verify integrity **[25]**. Digital signatures represent the digital identity that can also be used to sign a file in which any modification in the content will change this signature as well **[26]**. These methods provide key information to detect any video manipulation. However some video capturing devices lack the ability of embedding a watermark or digital signature into the video recording. In these cases active techniques will fail to expose tampering traces **[25]**.Video authentication in such situations leans on passive detection techniques .

4.2- Passive Tampering Detection Technique

Passive techniques or what called blind tampering detection techniques are independent of watermarks and digital signatures **[26]** . They check the authenticity of the video by detecting the footprints left by the video editing operations in the video content. Such footprints help in predicting noise , frame intensity values , motion residues , abnormalities in optical flow and many other complex calculations that these algorithms rely on to detect tampering **[26]** . No further details concerning these calculations will be discussed since these contain complicated information only comprehended by IT experts. It is good to mention that if a perpetrator is aware of these fingerprints and uses anti-forensic tools to hide or reduce them, this process itself will create another footprint to be detected.

In fact passive techniques are classified into three:

1- Detection of double compression:

This type is based on the idea that the compressed video must be decompressed before tampering it. After modifying the content the forged video will be restored in compressed format. Hence the resultant altered has undergone double compression which leaves footprints as artifacts that can be detected by blind tamper detection techniques **[26]** .

2- Region tampering detection:

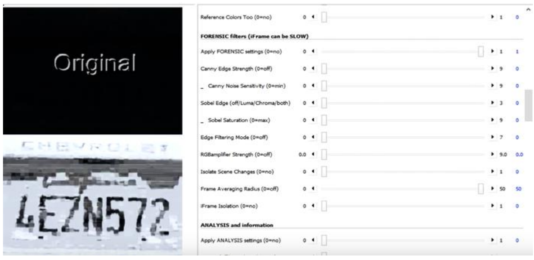
This type is applicable in case of copy/ paste and region/frame duplication tampering. It is based on algorithms that identify the exact location of tampering in the video **[26]**.

3- Video inter-frame forgery detection:

This type is used for detecting inter-frame tampering like deletion, insertion and duplication. It consists of many algorithms that are specific for each kind. One of them is MCEA (Motion Compensated Edge Artifacts) technique that detect frame deletion tampering by producing digital spikes in the locations where frames were deleted (tampered) **[25]**.

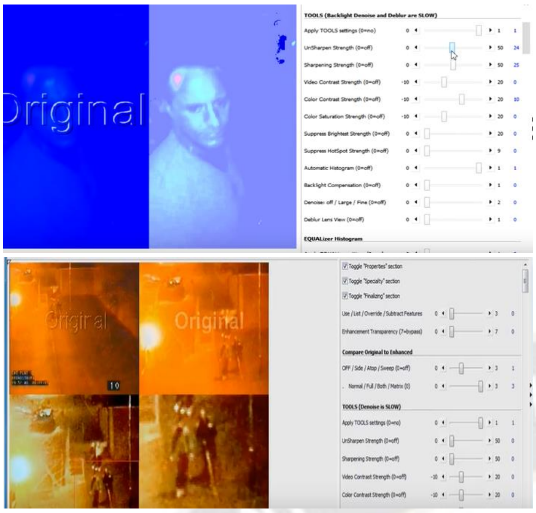
4.3- VideoCleaner for Video Enhancement and Authentication

VideoCleaner is a powerful video enhancement and tampering detection software that uncover the truth in a world of distorted realities **[30]** . It is one of the most efficient video authentication softwares upon which law enforcement rely on worldwide. VideoCleaner facilitates the analysis and enhancement of the video evidence prior of checking its integrity and authenticity. This is done through its effective features such as increasing details clarity, removing electrical noise, correcting the viewing perspective, repairing recordings, improving the brightness of poorly lit scenes and many others that make every small detail in the video content obvious **[30]**.



```
Reference Colors Too (0=no)              0   1   0
FORENSIC filters (iFrame can be SLOW)
Apply FORENSIC settings (0=no)           0   1   1
Canny Edge Strength (0=off)              0   9   0
_ Canny Noise Sensitivity (0=min)        0   9   0
Sobel Edge (off/Luma/Chroma/both)        0   3   0
_ Sobel Saturation (0=max)               0   9   0
Edge Filtering Mode (0=off)              0   7   0
RGBamplifier Strength (0=off)          0.0 9.0 0.0
Isolate Scene Changes (0=no)             0   1   0
Frame Averaging Radius (0=off)           0  50  50
iFrame Isolation (0=no)                  0   1   0
ANALYSIS and information
Apply ANALYSIS settings (0=no)           0   1   0
```

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*



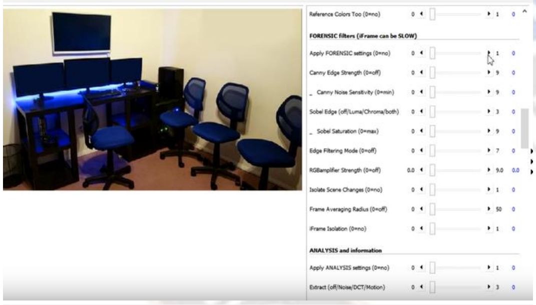
TOOLS (Backlight Denoise and Deblur are SLOW)			
Apply TOOLS settings (0=no)	0	1	1
UnSharpen Strength (0=off)	0	50	24
Sharpening Strength (0=off)	0	50	25
Video Contrast Strength (0=off)	-10	20	0
Color Contrast Strength (0=off)	-10	20	10
Color Saturation Strength (0=off)	-10	20	0
Suppress Brightest Strength (0=off)	0	20	0
Suppress HotSpot Strength (0=off)	0	9	0
Automatic Histogram (0=off)	0	1	1
Backlight Compensation (0=off)	0	1	0
Denoise: off / Large / Fine (0=off)	0	2	0
Deblur Lens View (0=off)	0	1	0
EQUALizer Histogram			

☑ Toggle "Properties" section
☑ Toggle "Specialty" section
☑ Toggle "Finalizing" section

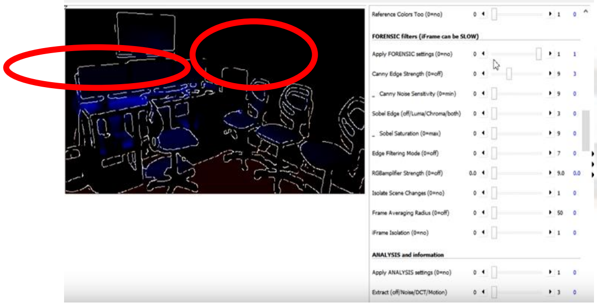
Use / List / Override / Subtract Features	0	3	0
Enhancement Transparency (7=bypass)	0	7	0
Compare Original to Enhanced			
OFF / Side / Atop / Sweep (0=off)	0	3	1
. Normal / Full / Both / Matrix (0)	0	3	3
TOOLS (Denoise is SLOW)			
Apply TOOLS settings (0=no)	0	1	1
UnSharpen Strength (0=off)	0	50	0
Sharpening Strength (0=off)	0	50	0
Video Contrast Strength (0=off)	-10	20	0
Color Contrast Strength (0=off)	-10	20	0

Figure 23 VideoCleaner Outcomes [(46)]

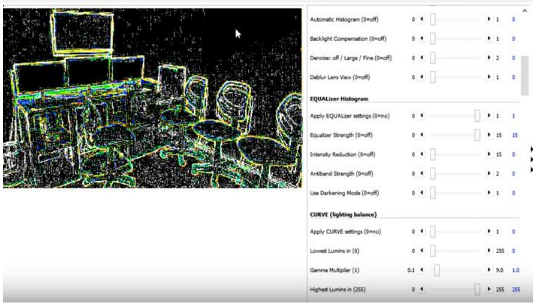
Beside the potent features of VideoCleaner to enhance the analysis by uncovering any hidden details in the content of the video , its recent version has a new 'Forensic Section' that can detect tampering in the video evidence . For example in the figures below , VideoCleaner processsed the frame captured in a video to detect any presence of tampering . As shown in the last pictures , the forensic tools of VideoCleaner has detected the presence of tampering in the specified locations due to pixels difference with respect to the original untouched regions in the relative frame [(30)] .



Reference Colors Too (0=no)	0	1	0
FORENSIC filters (iFrame can be SLOW)			
Apply FORENSIC settings (0=no)	0	1	0
Canny Edge Strength (0=off)	0	9	0
_ Canny Noise Sensitivity (0=min)	0	9	0
Sobel Edge (off/Luma/Chroma/both)	0	3	0
_ Sobel Saturation (0=max)	0	9	0
Edge Filtering Mode (0=off)	0	7	0
RGBamplifier Strength (0=off)	0.0	9.0	0.0
Isolate Scene Changes (0=no)	0	1	0
Frame Averaging Radius (0=off)	0	50	0
iFrame Isolation (0=no)	0	1	0
ANALYSIS and information			
Apply ANALYSIS settings (0=no)	0	1	0
Extract (off/Noise/DCT/Motion)	0	3	0



Reference Colors Too (0=no)	0	1	0
FORENSIC filters (iFrame can be SLOW)			
Apply FORENSIC settings (0=no)	0	1	1
Canny Edge Strength (0=off)	0	9	3
_ Canny Noise Sensitivity (0=min)	0	9	0
Sobel Edge (off/Luma/Chroma/both)	0	3	0
_ Sobel Saturation (0=max)	0	9	0
Edge Filtering Mode (0=off)	0	7	0
RGBamplifier Strength (0=off)	0.0	9.0	0.0
Isolate Scene Changes (0=no)	0	1	0
Frame Averaging Radius (0=off)	0	50	0
iFrame Isolation (0=no)	0	1	0
ANALYSIS and information			
Apply ANALYSIS settings (0=no)	0	1	0
Extract (off/Noise/DCT/Motion)	0	3	0



Automatic Histogram (0=off)	0	1	0
Backlight Compensation (0=off)	0	1	0
Denoise: off / Large / Fine (0=off)	0	2	0
Deblur Lens View (0=off)	0	1	0
EQUALizer Histogram			
Apply EQUALizer settings (0=no)	0	1	1
Equalizer Strength (0=off)	0	15	15
Intensity Reduction (0=off)	0	15	0
Antiband Strength (0=off)	0	2	0
Use Darkening Mode (0=off)	0	1	0
CURVE (lighting balance)			
Apply CURVE settings (0=no)	0	1	0
Lowest Lumins in (0)	0	255	0
Gamma Multiplier (1)	0.1	9.0	1.0
Highest Lumins in (255)	0	255	255

Figure 24 Spotting video tampering traces via VideoCleaner Algorithm [(47)]

Today VideoCleaner, along with several others tools for video enhancement and authentication, delivers a clear and credible video evidence to rely on during forensic investigations. Many research studies are looking forwards to provide more vigorous and precise tools to optimize and check the authenticity of the video evidences.

Eventually there is a growing prominence of using videos in the forensic investigations for their paramount role in assisting the courts to make their judgments. This importance of the video evidence compels checking its authenticity and makes it an imperative due to the wide range of tampering techniques available nowadays.

III. CCTV / Video Surveillance

One of the most powerful video evidence on which many investigators across the globe use in their investigations of crimes and critical events is the recording of the camera surveillance system . Many countries aoround the world are employing CCTV surveillance camera systems in their public and private spaces for recognizing its importance as a tool to secure their streets , airports , businesses , shopping centers , car parks and houses , capture a crime as it unfolds and prevent crimes from happening by discouraging criminals that they will be spotted .

Video surveillance systems or what is called CCTV (closed ciruit television) is a system that relies on a strategic placement of cameras for the aim of monitoring , watching and recording a particular location , event or person for the purpose of security and governing activity [(8)] .

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

Figure 25 CCTV in a car parking [48]

Figure 26 CCTV in an airport [49]

1- Advantages of CCTV

There a several ways in which CCTV footages act as vauable evidences for court trials , help in police operations through crime investigations and deter crime commission [8]. CCTV roles include :

- *Identification of clues , suspects , witnesses and vehicles linked to the event under investigation*
- *Assisting the police to examine the behavior of the suspects before , during and after a certain incident*
- *Precisely detecting the date and time of a specific crime or event*
- *Monitoring an unoccupied home or business to determine the suspect identity if any robbery took place and discompose the burglar while commitiing the crime which could prevent its occurence*
- *Determining the points of entry and exit utilized in a crime scene*
- *Having the ability to help in saving the life of abducted person by providing vital source of information to track him down*

These facilities and many others provided by a surveillance camera system are what make its footages valuable pieces of evidences for law enforcement , capture crimes and add a layer of security for the lives of private and public sectors .

Figure 27 Spotting criminals via CCTV footages [50]

2- CCTV tampering

The primary objective of employing surveillance cameras to extract information to track and identify individuals and their activities and detect crimes , will be misfired in case the recording is tampered or the camera is hacked and distorted . Concerning this issue, tampering a CCTV recording is the impact of extrinsic or intrinsic factors [25] .

Extrinsic camera tamper attacks are categorized to 3 types [27] , including :

- Defocused camera event : altering the focal length of the camera that leads to blurring of the content of the captured video
- Covered camera event : occluding the camera lens partially or totally by external objects
- Moved camera event : changing the camera viewing angle by external forces [27]

All of the three types will be help the perpetrator by inhibiting his face identification .

On the otherhand, intrinsic manipulation of the video recording is also applied by permenantly deleting the recorded footage or altering and distorting the video content via antiforensisc techniques. Practical experiments (as shown in the table) were done using different iOS devides through file signature and timestamp based antiforensic algorithms and showed that the targeted video can be altered and deleted where no data recovery effort is attainable [13] .

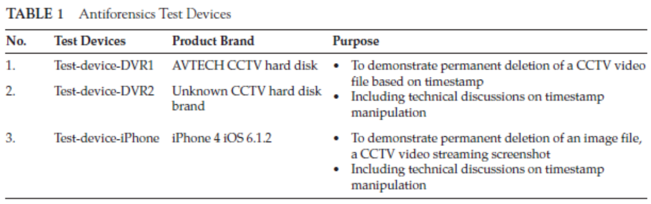


TABLE 1 Antiforensics Test Devices

No.	Test Devices	Product Brand	Purpose
1.	Test-device-DVR1	AVTECH CCTV hard disk	• To demonstrate permanent deletion of a CCTV video file based on timestamp • Including technical discussions on timestamp manipulation
2.	Test-device-DVR2	Unknown CCTV hard disk brand	
3.	Test-device-iPhone	iPhone 4 iOS 6.1.2	• To demonstrate permanent deletion of an image file, a CCTV video streaming screenshot • Including technical discussions on timestamp manipulation

Figure 28 Experiments showing CCTV tampering possibility [51]

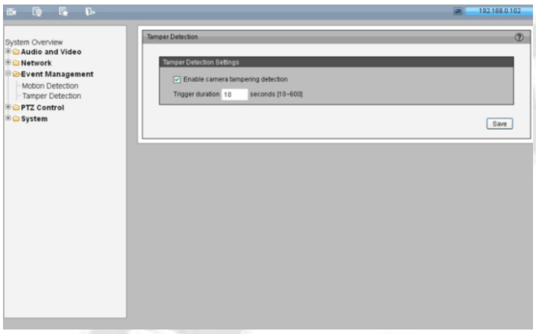
In this way suspects are able to hide their tracks, alter the data/time of a certain event and even permanently remove the whole footage of an incident in order to mislead and foil the investigation.

DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

How to overcome this?

3- CCTV Tampering Prevention and Detection

One solution to reduce the possibility of extrinsic physical tampering in a surveillance camera is activating Tamper Detection setting within the IP camera. This setting will allow sending alerts to the corresponding owner when the camera is tampered with [27]. It is available from several leading IP camera manufacturers including Vivotek, Optica and Axis [25].



Tamper Detection

Tamper Detection Settings

☑ Enable camera tampering detection

Trigger duration 10 seconds [10~600]

Figure 29 Tamper Detection Setting [52]

If anyone is trying to knock the camera down or any other action has been detected to partially or totally block the camera view , Tamper Detection will notify you and the alert will let you know to log into the video management system to see what happened [27]. This option helps detect individuals' malfunctions and peculiar acts and hinders the occurrence of a complete crime by permitting to quickly recall the police officers on the response of the alert sent from the camera distorted in the area.

While this solution, along with many methods for preventing camera hacks like data encryption and firmware updates, seems helpful and simple, it is not always the case. Regarding intrinsic manipulation where the content of video recording is deleted or altered, other more potent techniques are needed. A proposed method for CCTV video content integrity verification is Unified Tamper Detection Algorithm [12]. This algorithm is based on detection of tamper events by measuring the rate of edge pixels disappearance in the current frame compared to the edge pixels in the background frame resulting in a rate termed EDR (edge disappearance rate) [12]. Based on complex operations and further calculations depending on this concept, any deletion or alteration of an object or individual in the video frame will be spotted.

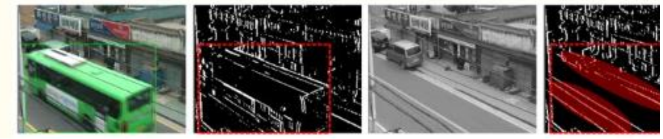


Figure 30 Detecting tampered bus video frame using Unified Tamper Detection Algorithm [53]

In this picture the edge characteristics of the foreground object (the bus) differ from those of the occluded region (where the bus was excluded in the tampered frame) [12]. This will be reflected as an abrupt change in the number of pixels in the current frame which is manipulated. Extraction of the foreground objects could be done with the help of complex algorithms like background-subtraction-based video analytics algorithms [12].

IV. Audio

1- Audio as Forensic Evidence

The important role that video recordings play to assist the forensic investigations does not minify the contribution of audio recordings in the same role. Though an audio lacks the visual part supplied by a video, it can provide the law enforcement and the investigators with significant clues and missing proofs to solve, analyze and judge the case under investigation.

An audio is any sound that can be heard by the human ear within the acoustic range and most commonly exist in the mp3 audio file format [23].

Figure 31 Audio Recording [54]

The impact of audio recording in facilitating the interpretation of large-scale crimes and events exponentially expanded over the past decades. An example of how audio recording can act as an efficient link to complete the puzzle of forensic investigation is the case of Dr. Richard Kimble in the movie The Fugitive [16] . When he was running from the police, he called Chicago Police Department to proclaim his innocence. Though he ended the call before the police could trace it, Dr. Richard was not aware that the sound of the L-train was so loud and can be obviously heard in the phone call. That little detail in the background of the recording which he did not anticipate helped the police to track him and find his location in Chicago by analyzing the audio of the phone call [16]. That is one of the instances in which audio recording renders a valuable evidence in the prosecution of any tough case.

Figure 32 Dr. Richard from The Fugitive movie

In addition to the previous example, an audio recording when rightly collected, enhanced and analyzed can potentially serve a lot of information in many other ways. One of these include identification of particular weapon types. When an audio is recorded in real-time shooting during a crime, fight or war, it can help through weapon signature analysis methods to detect the type used and then establish the order of firing as well [(23)]. Likewise, an audio can specify the make and model of vehicle used in a certain crime or event via vehicle signature analysis of an available audio recorded at the time of occurrence. Moreover an audio is very useful throughout the investigation of air accidents whereby the cause of the crash can be established by the analysis of aircraft engine noise [(23)].

Despite all the above paramount roles of audio evidences, foremost its primary advantage is in speech recognition and talker identification [(8)]. This is done by analyzing phone calls between criminals, voicemails recordings containing threats or planning for a crime, telephone answering machines, police /911 calls and audio files containing immoral content. These audio sources and many others help the investigators to identify the suspects and collect other useful information like their number and location.

Figure 33 Audio Evidence Types [(55)]

Various types of audio recordings can be analyzed to serve as a potential forensic evidence. These include:

- Recordings made on smart phones
- Answering machines' recordings
- Voice mails
- Audio content of videos
- Digital handheld recorders
- Cassette tapes
- 911 police calls
- Courtroom recordings

Regardless in any format an audio evidence is, its authenticity must be established before submitting it to the court to reveal if any tampering method has been applied.

2- Audio Enhancement and Analysis

For an audio recording to bring out specific aspects of an event and facts concerning a particular incident its content must be enhanced prior to any interpretation. This process is important to clarify the audio recording content in order to be intelligible to the investigator, attorney and judges in the court. The techniques of forensic audio enhancement must be applied aiming at reducing the unwanted noise and increasing the desired sounds in order to improve the overall quality of the audio content [(16)]. In this way the enhanced audio will provide an accurate representation of the events.

Similar to the case of video, audio enhancement and analysis is specific to each case and varies with the type of recording device and whether an audio is digital or analog. Despite the uniqueness of each audio recording, there are basic steps that must be followed in the process of audio enhancement and analysis.

Strategy of audio enhancement and analysis:

i. Critical Listening

After creating a duplicate to preserve the original copy of the audio, the early step of audio enhancement and analysis is critical listening whereby each section of the audio is identified [(16)]. The purpose of this step is to detect the depth of enhancement required by each section of the audio content based on the recorded characteristics including signal to noise ratios and frequency ranges [(15)].

For example an audio recording might contain three different portions that require different processing. The first one represents an audible conversation between two people with traffic jam noise from a distance. In a second section the speech clarity decreases due to significant amount of background noise. The third section contains no background noise but rather the people were talking quietly with low voices. Each of the three sections requires specific type of processing and enhancement that is identified by an expert in critical listening.

ii. Noise Reduction

As the main purpose of audio enhancement is to remove unwanted sounds, this step is substantial. The techniques applied for this process are the most effective in the context of audio enhancement. Usually the two common methods used for this aim are compression and echo cancelation [23].

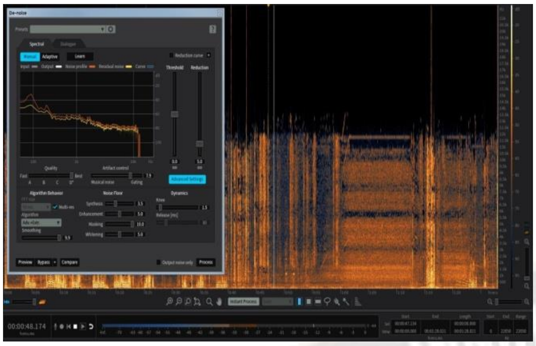
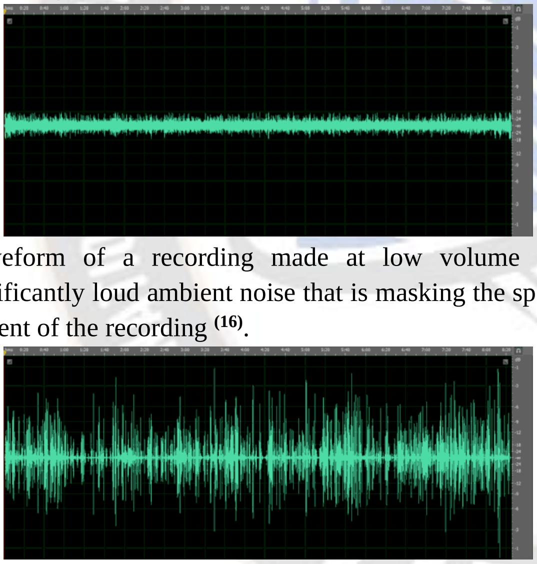


Figure 34 Noise Reduction Step [56]

Compression is applied to boost the faint sounds and reduce the background noise in the audio content [8]. This is done by leveling the signal so that the dynamic range of the material is reduced making soft sounds more apparent [16]. On the other hand echo cancelation is applied for decreasing the reflection of noise and reverberance of space that reduce the clarity of audio content [23]. Hence these techniques ameliorate the intelligibility of the recording and hinder the presence of noise that might become an issue in further processing .



Waveform of a recording made at low volume with significantly loud ambient noise that is masking the speech content of the recording [16].

Figure 35 Audio Recording before and after enhancement step [57]

The same recording after enhancement. The noise is attenuated and the volume of the speech is increased [16].

iii. Frequency Equalization

Now after the audio has become less noisy, frequency equalization is applied for additional help in boosting the desired sounds. Using specific and highly accurate equalizers to cut specific ranges of frequency bands the speech content becomes clearer. Usually the frequency bands containing speech content ranging between 200Hz and 5000Hz are isolated and amplified[15]. Whereas the frequencies corresponding to loud background noises and unwanted overtones will be reduced making them less noticeable. Every specific audio content needs specific number of processors to achieve the desired results [15].

iv. Forensic Transcript

Forensic audio experts demand the formation of forensic transcript in combination with critical listening and frequency analysis in the process of audio enhancement. A forensic transcript is the scientific observation of words under controlled conditions [23] . It is important for verification of spoken dialogue that occur in the recording as the latter is the main wanted sounds to be retrieved. Forensic audio transcription adds certainty to the enhancement and analysis of the audio as it appends a signed scientific document that is sworn by the expert witness as to the words that are spoken ending by:
'Based on the pains and penalties of perjury, I testify that the above forensic transcript is an accurate representation of the dialogue (or events) spoken during the time of this recording so help me' then we sign it.' [8]

As the forensic transcript produced by an expert who is able to conclude to a reasonable degree the unintelligible words that were spoken, it becomes an essential part that must accompany other methods of audio enhancement and analysis.

3- Audio Tampering

"Words fade but voices remain". Yet, the widely spread forgery techniques can turn the rigorous evidence that an audio recording supply to an unreliable one. Currently there are hundreds of softwares that are highly qualified in manipulating any audio recording at ease and in a very short time. In spite of the diverse tampering techniques that can alter the recording in various ways, all of them are based on four methods of falsification [8].

3.1- Basic methods of audio manipulation

- Deletion : stopping the tape to remove wanted words or sounds by over-recording unwanted areas
- Synthesis : using artificial means and specific algorithms to add words or voices to the tape
- Obscuration : masking certain waveform patterns to mix voices or sounds which will be reflected in the recording as sudden stops and starts in inappropriate places
- Transformation : changing the content of the recording by altering the arrangement of words

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

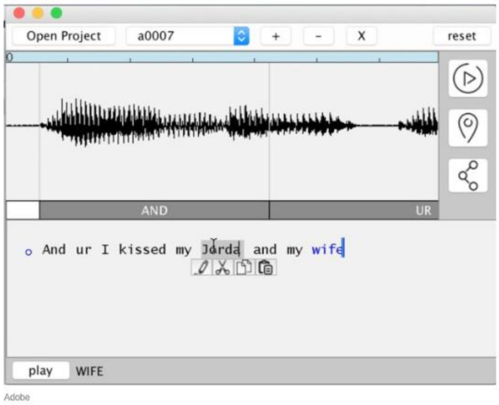
Though the four basic types of tampering have potent capability of manipulating the audio content to nay desired form, they leave detectable magnetic signature in the tape that can be identified through audio inspection by an expert [(23)]. Some of the electromechanical indications - signatures - left by tampering softwares include gaps, fades, transients and equipment sounds [(8)].

- Gaps : represent segments in the recording containing unexplained content's changes like sudden silence , humming or buzzing
- Fades : represent gradual loss of the volume of sounds (when complete inaudibility occurs fades will become gaps)
- Transients : represent abrupt and short sounds like pops and clicks
- Equipment sounds : represent inconsistencies in the audio content caused by the recording equipment itself like whistles or varying pitches

3.2- Voice Morphing and Cloning Softwares

Adobe ProjectVoco

Among all the audio editing and content altering softwares, Adobe ProjectVoco is one of the most interesting to shed the light on. As the well-known Photoshop applications tweak digital images, ProjectVoco affects the audio in the same way. The codenamed software ProjectVoco is designed to be one of the most potent audio editing applications. Beyond the familiar features of standard speech editing and noise cancelation that ProjectVoco provides, what makes it a subject of attention is yet so unique. The standout feature of ProjectVoco is the capability to generate new words in the recording using the speaker's recorded voice [(14)]. This means that it is able to add words to the audio file that were not originally found before. In fact the software targets at least 20 minutes of the desired recorded speech [(14)] . By understanding the makeup of a person's voice, ProjectVoco is able to replicate it generating sound-alike voice saying words that were not said in the original speech. The insertion of newly spoken words is activated by simply typing the desired words and the algorithms of ProjectVoco does the rest of the process resulting in a modified content of the audio recording via inserting unsaid words into the voiceover .



And ur I kissed my Jorda and my wife

Figure 36 Adobe ProjectVoco Algorithm [(58)]

ProjectVoco, Wavenet which is another software for generating realistic human-like voices [(15)] and other similar softwares appear to be very beneficial for audio engineers when working on clips, TV shows, dialogues and news where people may desire to add or change a word or phrase in their speech. Though there are several ethical sorts of applications facilitated by employing ProjectVoco, its unlawful dark side is really worrisome. Imagine if someone records an audio by your own voice saying words that you have never said. The idea itself is so creepy. What if the audio contains a speech mentioning people names that you have not ever known? What if the audio manipulates the time you said that you were planning to go to a certain event? What if the audio contains indecent and abusive verbalism expressed by your voice? What if any of these and other manipulated forms of speech by ProjectVoco are submitted and considered a genuine evidence in the court! Since ProjectVoco has the potential to falsify entire sentences using a person's voice in a near-perfect replication of the talker's , awareness must be raised to general publicity and law enforcements regarding the doctored audio clips that could be generated by such malicious technique .

Lyrebird

The outcomes generated by audio editing softwares like ProjectVoco are really impressive but nothing compared to these of Lyrebird. Lyrebird is a voice cloning software unveiled by artificial intelligence [(14)]. It consists of a set of algorithms that are able to create incredibly human-like synthesized voices by listening to a very short segment of the person's recorded audio. Unlike ProjectVoco that requires at least 20 minutes of the sample audio to alter the voice content, Lyrebird needs a very small segment of the recording cutting this requirement down to just one minute [(14)]. This means that using only one minute of sample audio, Lyrebird is able to create any voice which is a process that was seen impossible a few years ago [(5)]. To add more truthfulness to the voice output created, Lyrebird algorithms are able to infuse emotions with the speech it creates as making the target person's voice sound sympathetic, cheery, angry or stressed out .

Lyrebird
Speaker 1
SOUNDCLOUD
Share
0:02
▶ 51.4K
Lyrebird - Speaker 1 ▶ 51.4K
Lyrebird - Speaker 2 ▶ 45.2K
Lyrebird - Speaker 3 ▶ 40K
Lyrebird - Speaker 4 ▶ 35.7K
Lyrebird - Speaker 5 ▶ 34.2K

Figure 37 Lyrebird Software [59]

Similar to ProjectVoco, Lyrebird also has an advantageous role when employed in the right places. With the help of this advanced software, it is now feasible to read audio books with famous voices and synthesize speeches for people with disabilities or for animation movies [14]. These and many other uses are identified for this powerful tool that can create thousands of sentences in less than seconds after the voiceprint is already detected. Besides, there are other troubling uses of Lyrebird as well. Since the results generated are indistinguishable from human speech, it is possible now to produce a whole audio content, not just a word, by someone's voice who has not spoken what is said in the recording. Through this synthetic voice generator one can steal the identity of anyone and record an audio by his/her voice stating incidents that did not happen, confessing fake truths or replying to questions that he/she has not even answered. These dangerous consequences are very misleading especially when such recordings are used as forensic evidences in the courts. The veracity of audio recordings is brought to question due to the perfectly voice synthesizing software Lyrebird with hardly detectable tampered outcomes. This problem is solved by releasing this technology publicly so that it becomes available to anyone and everyone is aware of its results as they are aware now of the manipulated photos by Photoshop. By this way the forensic investigations should go deeper when analyzing an audio recording subjoining it with other evidences to testify its reliability and originality [5].

4- Audio Authentication

The verification of audio recording originality and integrity is a necessity to neglect the possibility of tampering and make its content reliable in the legal field. Because manipulation of the recording has become an easy task, evaluating the authenticity of the audio is done before it is considered a valuable evidence furnishing credible facts. Several methods are developed to check if any malicious or accidental tampering has been applied to the audio under investigation.

4.1- Basic methods of audio authentication:

i. Electronic Measurement

The main concept of electronic measurement is to check the frequency ranges of the voices in the audio [16]. If any sudden shift in the available frequency to a smaller or larger one occurs, this will be a sign that certain alteration was done. In a similar way any sudden unexplained changes in the background noise or the sudden appearance of a new source of noise are also signs of manipulation[23]. The tools used for measuring this parameter are spectrograms, level meters and frequency analysis panels that are helpful is observing minute changes.

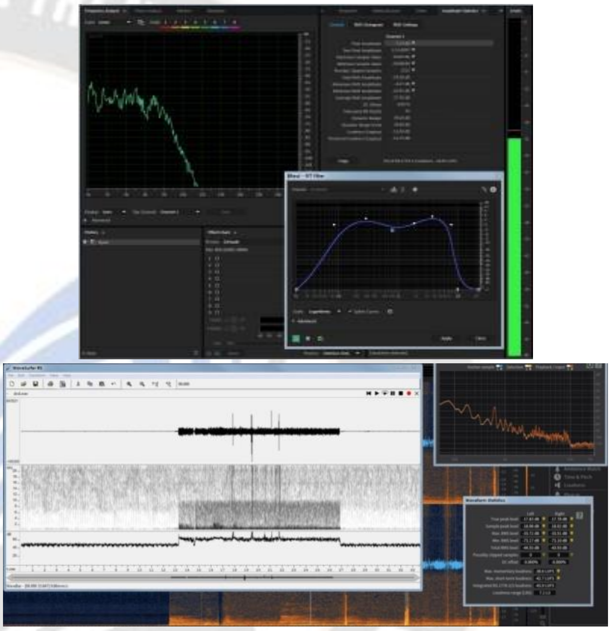


Figure 38 Electronic Measurement Step [60]

ii. Visual Inspection

Visual inspection goes hand in hand with electronic measurement whereby analysis of frequency information and physical wave property are done. The interpretation of the waveform is a critical step in audio authentication. Since waveforms are smooth and continuous, any sudden break in the recording waveforms indicate that a certain edit has been done [23]. Another example of how waveforms' characteristics sign for an alteration is the case when a waveform is inverted. Waveforms sudden breaks , inversions and other similar signs of edits are visualized in a full frequency spectrum shown by the spectrogram[15] .

iii. Analyzing Metadata in Digital Audio Evidence

This method is exclusively applied on digital audio recordings but not for analog ones like standard audio cassette [16]. When an audio is digitally recorded, an extra information can be interpreted while performing audio authentication. Information about how the recording is made and the type of equipment used to create the audio are

DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

revealed in what so called metadata of the digital audio recording **[23]**. Any alteration in the audio content leaves specific footprints in the recording hexadecimal information indicating that the audio was loaded into a software program for audio editing **[15]** .When analyzing metadata of a certain audio an exemplar - a recording made in the same kind of recorder and in close environment of the original - must be established to check any inconsistencies in the data signing for tampering **[8]**.

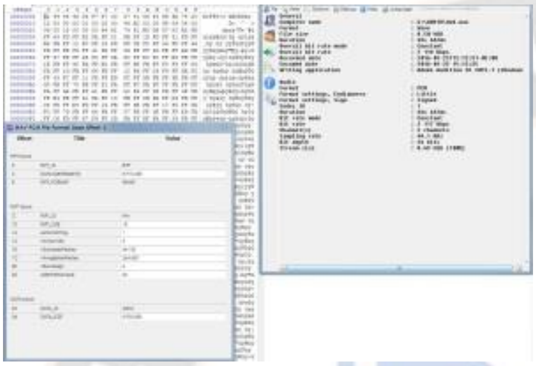


Figure 39 Metadata Analysis [61]

4.2- ACUSTEK for Audio Authenticity

ACUSTEK

Acu-expert has released its powerful software, ACUSTEK, for audio tampering detection and authenticity analysis. It is made of a set of instruments that are developed to expose the traces left by audio manipulating techniques**[1]** . What make it really beneficial are its various useful characteristics such as producing repeatable results, being fast and easy to use, supporting all audio formats, and having scientific fullness since all signals authenticity approaches are covered. ACUSTEK has solved the issue of authenticity analysis and so that it becomes accredited by many forensic audio labs and investigation centers on the world**[1]**. Some of the diverse features of ACUSTEK include:

- Revealing traces of editing via audio software functions and compression types representing results in levelograms **[1]**

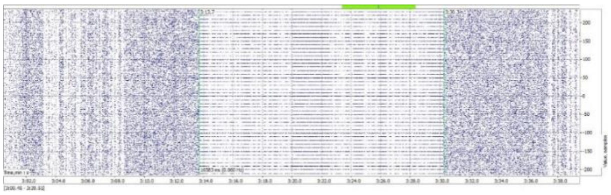
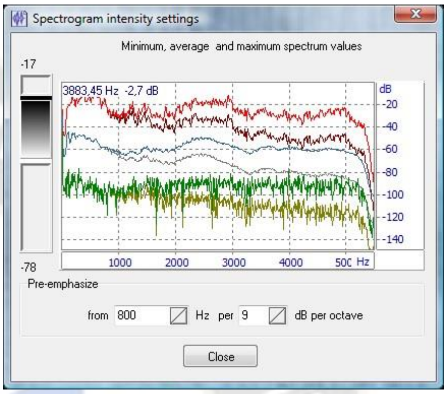


Figure 40 A levelogram[62]



Spectrogram intensity settings

Minimum, average and maximum spectrum values

3883,45 Hz -2,7 dB

Pre-emphasize

from 800 Hz per 9 dB per octave

Close

Figure 41 A view normalizer [63]

- Revealing traces left by unexplained start/stop modes that sign for intentional or accidental alterations
- Revealing matching signal fragments repeated several times to fraud the audio evidence
- Identifying the speaker's identity through voice biometrics and unique vocal elements of the speaker's voice after significantly improving the quality of the speech
- Analyzing audio compression type to detect any mismatch between the audio recording and the recording device via a samples order specification **[1]**

○

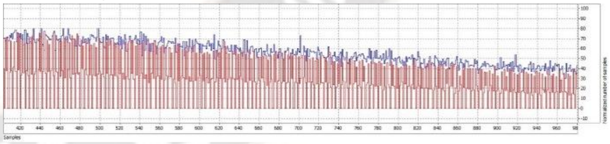


Figure 42 A samples order [63]

Further specifications are valid in ACUSTEK to help reveal any basic audio forgery. Though ACUSTEK does not provide a definitive answer when dealing with cases of tampering like audio cloning as previously discussed, it helps in the following processing once the audio recording is considered doubtful. Regarding other common tampering methods, ACUSTEK is the fundamental solution for unmasking any audio manipulation. Forensic audio experts and researchers are looking forward to develop more advanced technological procedures to depend on for testing the authenticity and reliability of any audio recording.

V. Photo

I. Photo as Forensic Evidence

“Which we drink in at our ears does not piercingly enter as that which the mind does conceive by sight.” Even for a well-trained brain, it is not easy to get a precise conception of any object, location or event via verbal description only. Here comes the role of digital images that offer great assistance for the forensic investigations and the presentation of the cases. There is no doubt that some cases do not rely on photographic support in the first place to be solved, whereas in other cases a photo might be the sole primary evidence [11]. It can now be said that photography has established an important branch in the law evidence. Since a photo is nothing but a frame taken from a video footage , it plays the same vital roles as those of a video evidence like corroboration of a witness or suspect statement and verifying criminals' identities . This essential function of the digital images when served as a forensic evidence admissible to the court does not abolish the importance of proving its authenticity [6].

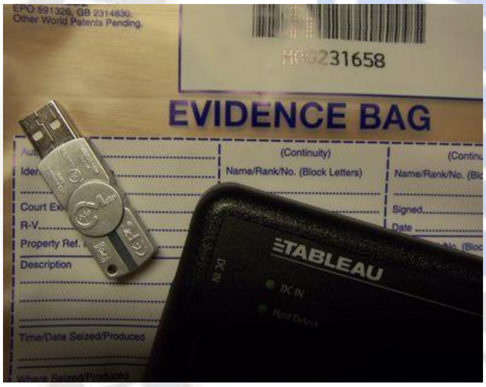


Figure 43 Photo Evidence [63]

As easy as the video is doctored and forged like previously shown in the first section, a photo can be manipulated and modified in various forms where no clue of tampering can ever be detected by a human eye [4] .Hence a potent evidence like a digital image to be reliable and play its role when submitted to the court, it must be first properly identified. Its integrity must be tested and its accuracy and credibility must be shown by diverse techniques specialized for photo authentication [10]. Because all the processes that are applied to a video are similar to these used for a digital image starting from enhancement and analysis to tampering methods and authentication softwares , in this section no further details will be elaborated and repeated concerning each of them .

II. Photo Tampering

Image Steganography

It is notable in the present time how easily an image can be manipulated by cropping, cloning, concealing objects and many other options provided by the wide range of the advanced tampering techniques that were previously depicted in details [4] . However none of these can be compared to how powerful it is to hide whatever data you want under the veil of a single digital image. This is the potency that image steganography offers.

Steganography is the art of hiding the fact that communication is taking place by hiding the information in other information [17]. It has all started from the Greek Histories where a Greek nobleman named Histaeus needed to secretly communicate with his son- in- law living in Greece [24]. For this aim he shaved the head of one of his most trusted slaves and tattooed the text message onto the slave’s scalp so that when the slave’s hair grew back, he was dispatched with the hidden message [24] . For that reason steganography is a word of Greek origin where “stegano” means “cover” and “graphia” means “writing” [17].

Figure 44 Image Steganography [64]

The hidden information can be texts, images, audio or video files carried in many different file formats where the digital images are the most commonly used. Then among the four types of steganography: Text, Image, Audio and Video Steganography, that which is done via an image is the most popular [24].

The basic principle of steganography is significant for the privacy of users, national secretive data transmission and even encrypted communication between criminals whereby an invisible secret message is embedded in another file and only proper decryption methods can detect the presence of this hidden data [17]. Such process of exposing steganography is known as steganalysis that is applied via several tools such as Amped Authenticate which was mentioned in previous sections [24].

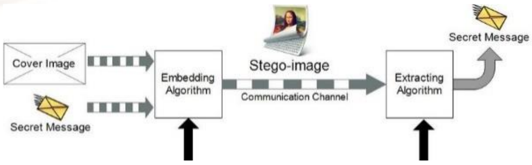


Figure 45 Image Steganography Process [65]

In the context of forensic investigations and lawful prosecutions, steganography is considered a controversial subject whereby it facilitates the movements and connection between criminals enabling them to secretly communicate during an illegal procedure, hatch an escape plan or prepare for a future crime for example.

The techniques of Image Steganography are classified into two categories:

1- Image Domain Techniques
2- Transform Domain Techniques (17)

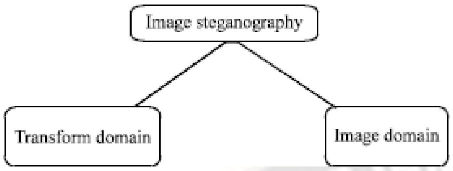


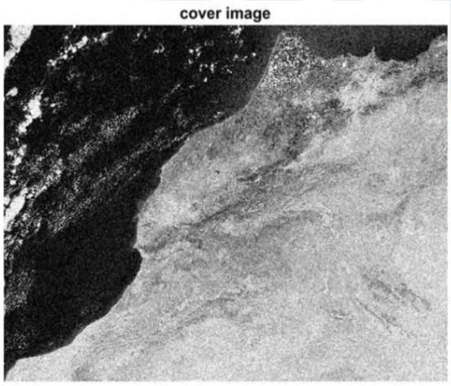
Figure 46 Types of Image Steganography (66)

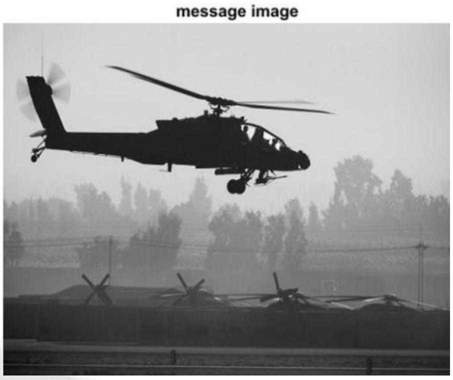
Image domain techniques also known as spatial domain techniques employ bit-wise methods that embed the secret messages in the intensity of pixels directly which make them referred as simple systems (24) . This type of techniques is only applicable for specific image formats hence they are typically image format dependent.

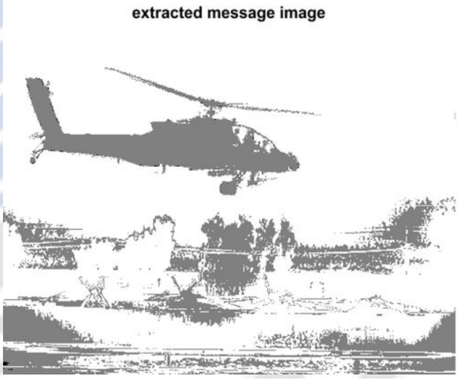
Transform domain techniques also known as frequency domain techniques whereby images are first transformed before embedding the message into its content (17) . This is done with the help of manipulation algorithms and image transforms involved in the process of such techniques. The transformation step that precede hiding the message in the image makes these techniques more robust than spatial domain ones for the message will be hidden in more significant areas of the cover image. In contrast to image domain techniques, transform domain ones are image format independent (17).

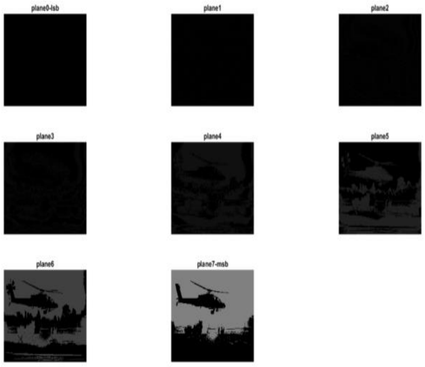
One of the most commonly used steganographic methods is the Least Significant Bit LBS substitution. It is one of the spatial domain techniques with pretty impressing outcomes. The principle of this method is based on the idea that each image can be split into individual bit-planes each consisting of different levels of information where secret messages can be simply embedded (24). The below applications done via this method clearly illustrates its strategy.

Example1:









International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

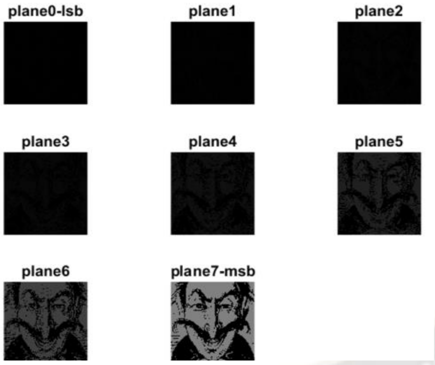


Figure 47 Image Steganography Examples [67]

LBS is one of many others of the steganographic methods employed for hiding information [24]. These methods vary with respect to their function depending on various factors that play a role in evaluating each technique's performance. Some of these factors include invisibility by human eye, robustness against statistical attacks, supporting different image formats [17]... etc.

No steganographic technique encompasses all the strength points together to form an ideal method but no matter how many weaknesses, it has no steganalysis is possible without proper complex software for detecting and retrieving the hidden message specifically for each case [10].

VI. Experimental Part

In this part several experiments were done to demonstrate how the advanced softwares and tools like the ones previously described aid in the forensic investigations through enhancement, analysis and authentication. The following cases consist of photos/video frames that were figuratively submitted as evidences and processed by various softwares like Amped 5, Amped Authenticate, Griffeye Analyze and Camera Ballistics to uncover the truth and assist the prosecution.

1- Experiment 1: Experiment using Amped 5 and Amped Authenticate

Consider that the law enforcement agency was informed about a bank robbery incident by a gang of four thieves. After they broke into the bank and collected an amount of money from the bank officers under stress and fear, they prepared to escape after hearing the police alarms from a distance. Three of them succeeded to reach their car and fled while the last one was a bit late and was left behind. Although the four of them were wearing face masks during the crime, the fourth thief uncovered his face when he reached the street outside the bank. He hid in a very dim light location for a few minutes waiting the police cars following his partners' car to get far away. Then he decided to leave his place and ride a public bus anticipating that no one has figured him as one of the burglars. The police cars were distracted and failed at catching the criminals. As a result the four of them succeeded to flee.

This case could not be solved without the following digital evidences that were analyzed and submitted to convince the court and expose the identity of each of them.

One of the evidences was a video frame taken from a CCTV footage of one of the street cameras near the bank. Despite that CCTV cameras of the bank failed to identify the thieves due to their face masks and that the fourth burglar thought that his face cannot be recognized or captured in poor light conditions, the result achieved after analyzing the frame was astonishing. Via Amped 5 video enhancement software previously described in details, the dark unclear frame captured by the outside CCTV cameras was enhanced and detected the facial identity of the hidden burglar. The digital forensic expert utilized this tool due to its powerful options and promising outcomes.

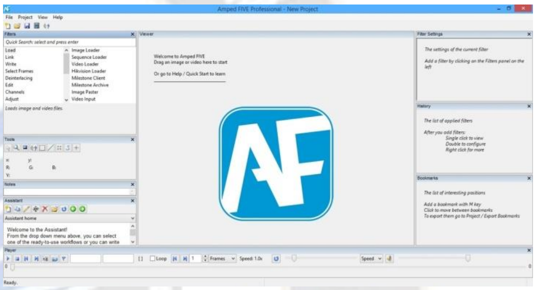


Figure 48 Amped 5 User Interface [68]

part I Steps done using Amped 5 Software

1. Load the evidence picture
   Using the features box:
2. Click on Adjust then modify the Exposure value
3. Click on Presentation then choose Compare Original in order to compare the photo before and after the enhancement

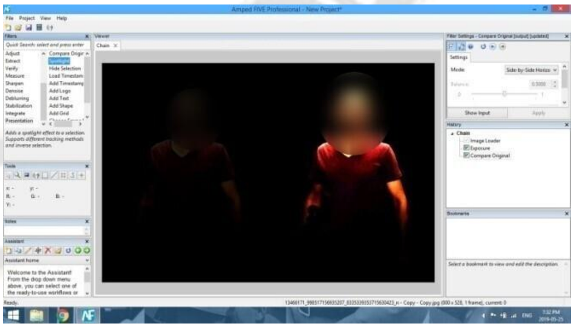


Figure 49 Evidence picture before and after correcting the light exposure

The second piece of evidence was an image of the vehicle number of the bus that the criminal rode, taken by a camera of the agent's mobile phone. The police was aware that the criminal was hiding and asked one of their secret agents to stay and track him in order to gather more information about the other gang members. Unfortunately he could not follow the bus till the end but he was able to take a photo of the bus number which appeared to be blurred since the bus was moving fast. However it brought a great advantage in tracking him after enhancing it by a digital forensic expert using Amped 5 software.

part II Steps done using Amped 5 Software

1. Load the evidence picture
   Using the features box:
2. Click on Deblurring then choose Optical Deblurring
3. Modify the degree of deblurring until the image is clarified
4. Click on Presentation then choose Compare Original in order to compare the photo before and after deblurring

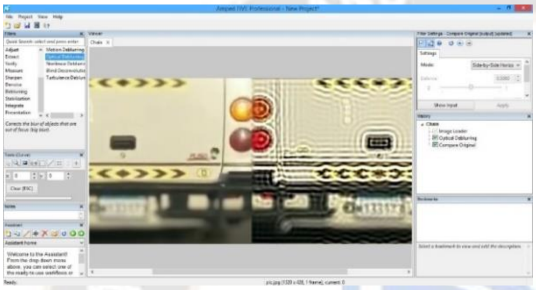


Figure 50 Evidence picture before and after deblurring

A third digital image as well served as a significant evidence. The vehicle number of the car through which the three criminals firstly fled was captured by a witness who was in a car beside the passing car. The photo was taken from an angle in which the vehicle number at first was impossible to be identified and the image looked useless. That was before processing the image by Amped 5 to change the perspective and show the number of the car clearly.

part III Steps done using Amped 5 Software

1. Load the evidence picture

   Using the features box:
2. Click on Edit then choose Correct Perspective
3. Put the curser and select the part of the photo containing the car's number
4. Click on Presentation then choose Compare Original in order to compare the photo before and after editing the perspective

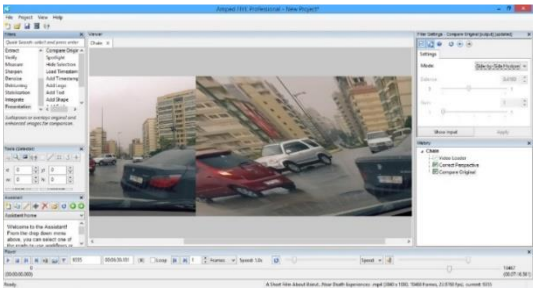


Figure 51 Evidence picture before and after correcting the perspective

When the fourth burglar was heading to the bus his mobile phone fell down and was left behind. The investigators precisely examined all the messages, calls and media files in his phone but could not find an evidence that help in solving the case. One of the pictures examined as unfruitful was an image containing food content sent to the criminal's phone via WhatsApp from an unknown number in a suspicious time. It was first seen as a useless photo but since the digital forensic expert was aware of steganography he decided to analyze it more deeply. After processing the photo, it was revealed that a text message was hidden through it which was planned by the gang as a way of secret communication in case they faced any issue during or after the crime. The text message detected after uncovering its content helped the forensic investigators, along with the other evidences, to track the criminal as it was an escape plan sent by one of the criminals that was still free.

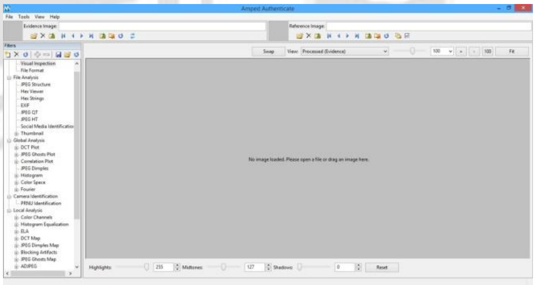


Figure 52 Amped Authenticate User Interface

part IV Steps done using Amped Authenticate Software

1. Load the evidence picture
2. Click on Hex Viewer
3. Scroll down in order to figure out the concealed text message

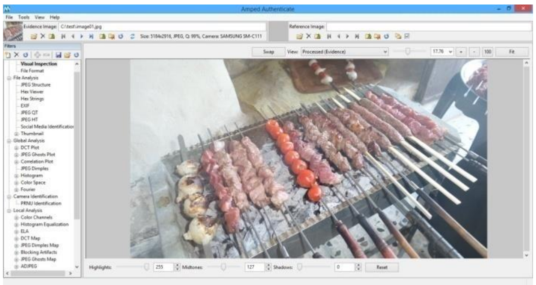


Figure 53 WhatsApp evidence image sent to the criminal's phone

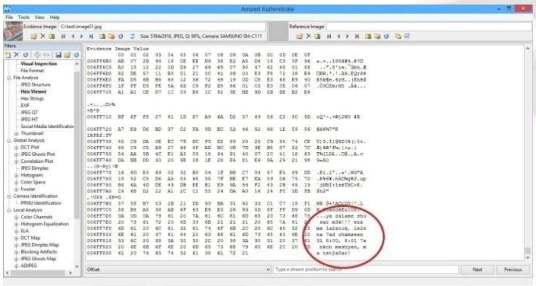


Figure 54 Text message detected after processing the image

2- Experiment 2: Experiment using Griffeye Analyze

Griffeye Analyze is an innovative software used by law enforcement agencies and national security in order to analyze multimedia evidences. This versatile tool helps in detecting critical clues, identifies relationships between suspects and crimes and connects criminals to old crimes via referring to a huge database.

The four core components of Griffeye Analyze Software include:

i. Analyze DI : represents a revolutionary approach to a large amount of multimedia data

ii. Analyze CS Operations : works collaboratively on cases while connected to a shared database which allow the results to be achieved more quickly

iii. Analyze CS Enterprise : collects and manages data across organizational borders allowing access to all relevant materials ever collected

iv. Analyze Forensic Market : provides modules through digital markets allowing users to access tools and means for add-ons

The platform of Griffeye Analyze works with any partner application like facial recognition ones to review individuals' history and analyze relations with other suspects and crimes which exponentially reduced the time consumed during the investigations. With the help of this advanced software, more cases are now being solved since critical clues are no longer missed but rather correctly identified and connected.

After the suspect was detained by the police they wanted to examine if he was linked to other previous crimes. They also needed to look if he was connected to other people that could or could not be suspects but either ways still help in solving the case .For this purpose the digital forensic expert aimed at processing the criminal's face image via Griffeye Analyze Software.

Steps done using Griffeye Analyze Software

1. Load the criminal's image to be analyzed along with the database
2. Right click on the criminal's image
3. Click on the Search button then choose Similar Faces

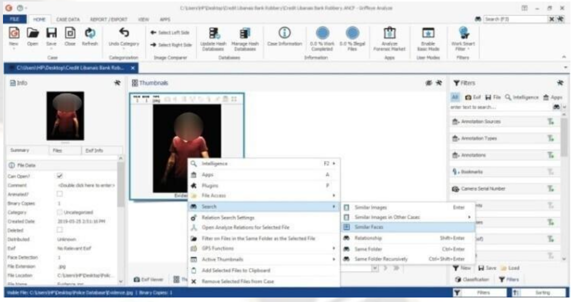


Figure 55 Suspect's image uploaded to Griffeye Analyze

4. Examine the results that show the criminal's related images

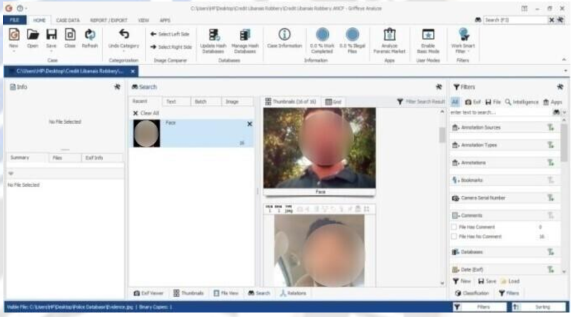


Figure 56 Relevant pictures of the suspect after processing his image via Griffeye Analyze

3- Experiment 3: Experiment Using Camera Ballistics

Camera Ballistics is an advanced software that utilize unique advanced algorithms in order to detect the camera source through which a certain picture was captured. This helps to identify if an image is taken by a suspect's device or not. The principle of this technological tool is based on metadata, the information that describe any digital item’s content. It also uses mathematical processes in order to analyze the physics of each camera sensor. Since metadata is specific for each multimedia file, this software generates a sensor fingerprint unique for each device by using this type of information. Camera Ballistics is an essential software for the forensic investigators for it can differentiate between devices even from the same make and model to tell if there is a match between the evidence picture and the sensor fingerprint.

DOI: https://doi.org/10.17762/ijritcc.v8i10.5447
***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

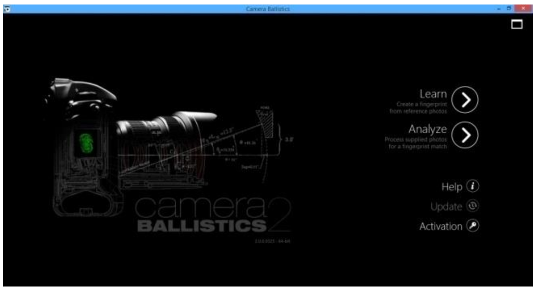

Camera Ballistics
Learn
Create a fingerprint from reference photos
Analyze
Process supplied photos for a fingerprint match
Help
Update
Activation
camera
BALLISTICS
2

Figure 57 Camera Ballistics Interface

After gathering the proper information that led the police to identify the location in which the gang used to plan for the crimes, they break into the place for collecting more evidences. Among these was a USB device that contains a picture of a bank that was attacked one year ago but the case was closed for lacking enough evidences to solve it. The investigator aimed at analyzing the source through which the photo was captured. For this purpose he used the phone that was dropped by one of the criminals to detect if it matches with the photo source.

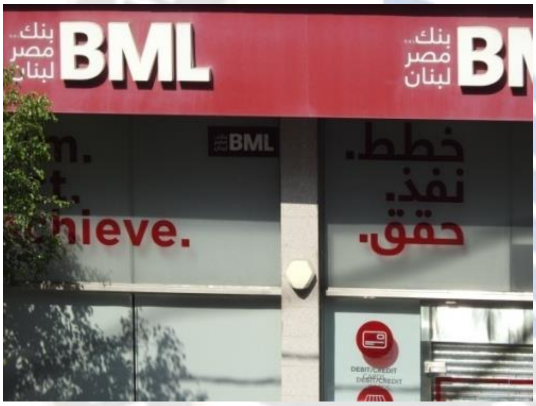
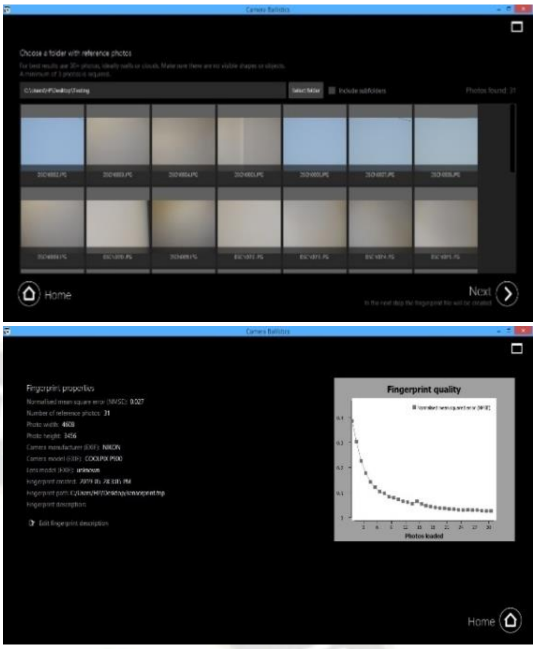


Figure 58 Photo of the bank attacked one year ago

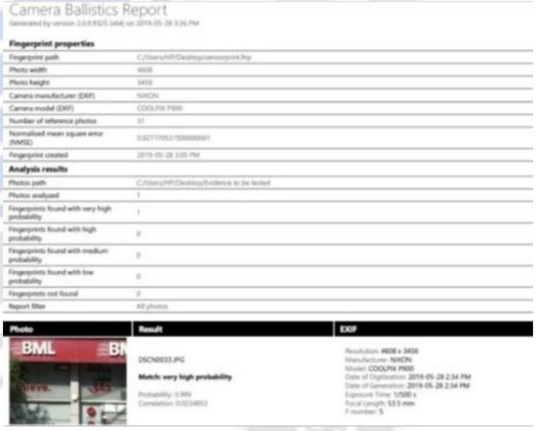
<u>Steps done using Camera Ballistics Software</u>

1. Click on Learn then load 30 images captured from the suspect's device (it its preferred to load photos of the sky or walls for quick processing)
2. Click on Next then save the generated sensor fingerprint of the device
3. Click on Home then choose Analyze
4. Load the evidence pictures
5. Click on Next then Report Automatically
6. Save the report
7. Access the report and read the results to detect if there is a matching probability as the case testified below


Choose a folder with reference photos
For best results use 30+ photos, ideally walls or clouds. Make sure there are no visible shapes or objects.
A minimum of 3 photos is required.

Fingerprint properties
Normalised mean square error (NMSE): 0.027
Number of reference photos: 31
Photo width: 4608
Photo height: 3456
Camera manufacturer (EXIF): NIKON
Camera model (EXIF): COOLPIX P900
Lens model (EXIF): unknown
Fingerprint path: C:/Users/HP/Desktop/sensorprint.fsp
Fingerprint description:

Figure 59 Camera Ballistics experimental steps


Camera Ballistics Report
Generated by version 2.0.0.9325 (x64) on 2019-05-28 3:36 PM

Fingerprint properties	
Fingerprint path	C:/Users/HP/Desktop/sensorprint.fsp
Photo width	4608
Photo height	3456
Camera manufacturer (EXIF)	NIKON
Camera model (EXIF)	COOLPIX P900
Number of reference photos	31
Normalised mean square error (NMSE)	0.0271705315000001
Fingerprint created	2019-05-28 3:05 PM
Analysis results	
Photos path	C:/Users/HP/Desktop/Evidence to be tested
Photos analyzed	1
Fingerprints found with very high probability	1
Fingerprints found with high probability	0
Fingerprints found with medium probability	0
Fingerprints found with low probability	0
Fingerprints not found	0
Report filter	All photos

Photo	Result	EXIF
	DSCN0033.JPG **Match: very high probability** Probability: 0.999 Correlation: 0.0234853	Resolution: 4608 x 3456 Manufacturer: NIKON Model: COOLPIX P900 Date of Digitization: 2019-05-28 2:34 PM Date of Generation: 2019-05-28 2:34 PM Exposure Time: 1/500 s Focal Length: 53.5 mm F-number: 5

Figure 60 Report: results of analysis

After analyzing the report it appeared that the camera model Nikon P900 through which the photo was taken is the same as that of the criminal's camera. Along with the suspect confession later on, it was confirmed that the same gang is also accused for the bank robbery that happened last year. Hence the two cases were solved and closed.

4- Experiment 4: Experiment Using Amped Authenticate for Deletion Detection

In addition to the other evidences that were examined in the location in which they used to plan their crimes, one of the investigators found a firearm under the bed. They dragged the firearm on a white background to preserve all the traces, took the appropriate photos and transferred it to the laboratory for further analysis.

However one day later the firearm disappeared from the laboratory and the pictures were altered in a way that no firearm appears in them. The investigator was shocked,

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

questioned the second investigator that was with him and decided to detect the manipulation in the captured photos.

Steps done using Amped Authenticate

1. Load the evidence picture

   Using the features box:
2. Choose *histogram equalization* then *intensity-false-x: 0, y: 0, w: 0, h: 0
3. Click on View Box then choose Unprocessed Vs Processed to compare the picture before and after tampering detection

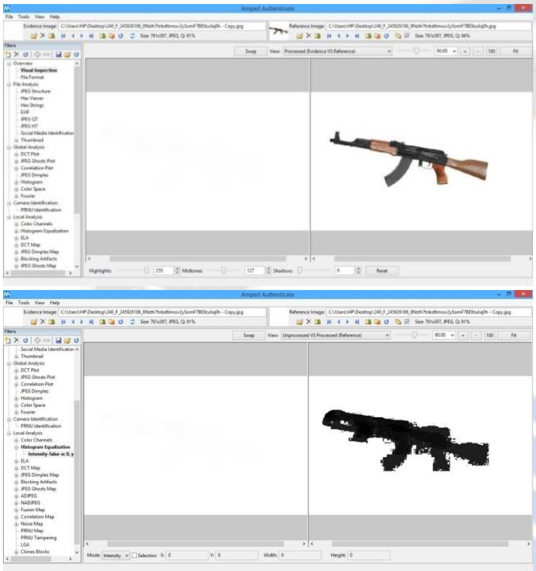


Figure 61 Evidence picture before and after erasing the evidence

In the first part the figure shows the photo of the weapon before being tampered while the second one shows the traces of deletion after processing the white forged photo. Hence he detected that the captured photos were tampered and someone intended to erase the evidence from the pictures. After several questioning and investigation, the second investigator appeared to be an inside man that aimed at reducing the severity of their judgment and was accused along with the criminals as well.

Consequently the suspects were tracked, their location was identified, their identities were unveiled and the case was closed. The experiments of processing each of the images showed how potent these softwares are for enhancing and analyzing the photos that were seen non-sense and unavailing. It was also indicated how a correctly enhanced and analyzed digital evidence such as videos and photos support the common traditional evidences and play a vital role in the forensic investigations .

VII. Conclusion

The past decade has previously seen unimagined advances in the field of digital forensics due to the wide proliferation of multimedia and its trending tools. By the time being investigators' work limits are no longer restricted by the traditional physical evidences they used to only rely on. The potent role that multimedia tools like video, audio and photos play as forensic evidences drove the court for approving their admissibility and emphasizing on their significance in convincing them to make their decisions and judgments.

Although video, audio and photos are paramount evidences that assist the investigators, any unnoticeable incident of tampering will definitely mislead the whole investigation. The possibility of manipulating any multimedia file has increased with the evolution of technological softwares and algorithms specialized for tampering and alteration .The latest advances of tampering is the creation of a whole video sequence of a human face making speech from a handful of photographs by the researchers of Samsung AI Center . On the other hand various advanced softwares are developed to check the authenticity of any multimedia evidence and ensure its integrity and originality. As shown in the previous experiments, different techniques nowadays assist the job of a digital forensic expert in doing so. The technology that delivered such enhancement and authentication tools and made the multimedia evidences credible enough to rely on has made a big favor for the forensic investigators for interpreting any critical event or crime incident .

Acknowledgment

A special appreciation and thankfulness to every person who assisted me throughout witting this dissertation to cherish my goal and attain this successful outcome.

Firstly I would like to express my gratitude to my supervisor Dr. Hassan Kazan for his guidance, motivation and encouragement. Furthermore a special mention to Mohammed Saab, a forensic science graduate, for his support and insightful comments.

Last but not least, a profound sense of grace to my precious family whose love and support are always with me in whatever I pursue to provide me with an unending inspiration.

References

1. Acustek - Technical Surveillance, Technical Countermeasures and Forensic Solutions - Acustek-Technical Surveillance, Technical Countermeasures TSCM, Forensic Audio Solutions. (2019, June 13). Retrieved June 13, 2019, from https://www.acustek.com/en/
2. Amped Software | Forensic Image and Video Processing. (2019, June 20). Retrieved June 20, 2019, from https://ampedsoftware.com/
3. Ariffin, A., Choo, K.-K. R., & Yunos, Z. (2017). Forensic Readiness. In *Contemporary Digital Forensic Investigations*

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

of Cloud and Mobile Applications (pp. 147–162). https://doi.org/10.1016/B978-0-12-805303-4.00010-1

4. Binson, V. A., Thomas, N. M., Thoams, S., Augustine, A., & Sivakumar, K. S. (2016). An advance to cloning detection in digital forensics investigations. *2016 International Conference on Emerging Technological Trends (ICETT)*, 1–5. https://doi.org/10.1109/ICETT.2016.7873743
5. Böhme, R., Freiling, F. C., Gloe, T., & Kirchner, M. (2009). Multimedia Forensics Is Not Computer Forensics. In Z. J. M. H. Geradts, K. Y. Franke, & C. J. Veenman (Eds.), *Computational Forensics* (Vol. 5718, pp. 90–103). https://doi.org/10.1007/978-3-642-03521-0_9
6. Farid, H. (2008, June). *Digital Image Forensics*.
7. Gloe, T., Fischer, A., & Kirchner, M. (2014). Forensic analysis of video file formats. *Digital Investigation, 11,* S68–S76. https://doi.org/10.1016/j.diin.2014.03.009
8. Ho, A. T. S., & Li, S. (Eds.). (2015). *Handbook of Digital Forensics of Multimedia Data and Devices: Ho/Handbook of Digital Forensics of Multimedia Data and Devices*. https://doi.org/10.1002/9781118705773
9. Johnston, P., & Elyan, E. (2019). A review of digital video tampering: From simple editing to full synthesis. *Digital Investigation, 29,* 67–81. https://doi.org/10.1016/j.diin.2019.03.006
10. Joseph, R. M. (2015). *An Improved Anti-Forensics method for JPEG Image Enhancement undetectability & Improved Image quality*. *4*(7), 6.
11. Kuznetsov, A., Severyukhin, Y., & Afonin, O. (2008, February 26). *Detecting Altered Images.pdf*.
12. Lee, G., Lee, M., & Lim, J. (2015). Unified Camera Tamper Detection Based on Edge and Object Information. *Sensors, 15*(5), 10315–10331. https://doi.org/10.3390/s150510315
13. Li, Q., Wang, R., & Xu, D. (2018). An Inter-Frame Forgery Detection Algorithm for Surveillance Video. *Information, 9*(12), 301. https://doi.org/10.3390/info9120301
14. Lyrebird claims it can recreate any voice using just one minute of sample audio - The Verge. (2019, June 13). Retrieved June 13, 2019, from https://www.theverge.com/2017/4/24/15406882/ai-voice-synthesis-copy-human-speech-lyrebird
15. Maher, R. (2009). Audio forensic examination. *IEEE Signal Processing Magazine, 26*(2), 84–94. https://doi.org/10.1109/MSP.2008.931080
16. Mellinger, P. (2011, February 18). *A simplified guide to forensic video and audio analysis.*
17. Morkel, T., Eloff, J. H. P., & Olivier, M. S. (n.d.). *AN OVERVIEW OF IMAGE STEGANOGRAPHY*. 12.
18. Nampoothiri, V. P., & Sugitha, N. (2016). Digital image forgery — A threaten to digital forensics. *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT),* 1–6. https://doi.org/10.1109/ICCPCT.2016.7530370
19. [Cryptographic and Information Security Approaches for Images and Videos]. (n.d.). *International Journal of Advanced Research in Computer Science*.
20. Peterson, G. (2006). Forensic Analysis of Digital Image Tampering. In M. Pollitt & S. Shenoi (Eds.), *Advances in Digital Forensics* (Vol. 194, pp. 259–270). https://doi.org/10.1007/0-387-31163-7_21
21. Putra Justicia, A., & The Society of Digital Information and Wireless Communication. (2018). Analysis of Forensic Video in Storage Data Using Tampering Method. *International Journal of Cyber-Security and Digital Forensics*, *7*(3), 328–335. https://doi.org/10.17781/P002471
22. Rajalakshmi, C. (2017). STUDY OF IMAGE TAMPERING AND REVIEW OF TAMPERING DETECTION TECHNIQUES. *International Journal of Advanced Research in Computer Science*, 5.
23. Renza, D., & Lemus, C. (n.d.). *Audio Authenticity and Tampering Detection based on Information Hiding and Collatz p-bit Code*. 11.
24. Savitha Bhallamudi. (2015). *Image Steganography*. https://doi.org/10.13140/rg.2.2.21323.18727
25. Singh, R. D., & Aggarwal, N. (2018). Video content authentication techniques: A comprehensive survey. *Multimedia Systems, 24*(2), 211–240. https://doi.org/10.1007/s00530-017-0538-9
26. Sitara, K., & Mehtre, B. M. (2016). Digital video tampering detection: An overview of passive techniques. *Digital Investigation, 18,* 8–22. https://doi.org/10.1016/j.diin.2016.06.003
27. Tamper Detection on IP Surveillance Cameras | VideoSurveillance.com. (2019, June 20). Retrieved June 20, 2019, from https://www.videosurveillance.com/tech/tamper-detection.asp
28. Thies, J., Zollhöfer, M., Nießner, M., Valgaerts, L., Stamminger, M., & Theobalt, C. (2015). Real-time expression transfer for facial reenactment. *ACM Transactions on Graphics, 34*(6), 1–14. https://doi.org/10.1145/2816795.2818056
29. Thies, J., Zollhöfer, M., Stamminger, M., Theobalt, C., & Nießner, M. (n.d.). *Face2Face: Real-time Face Capture and Reenactment of RGB Videos*. 9.
30. VideoCleaner FREE forensic video enhancement software - Finalizing. (2019, June 12). Retrieved June 12, 2019, from http://videocleaner.com/about.html
31. https://forensicdetectives.in/forensic-science-technology/
32. https://www.safesitesecuritysolutions.co.uk/knowledge-base/effective-cctv-crime-deterrent
33. http://www.dashcamerazone.com/best-dash-cam-records-speed
34. https://www.khaleejtimes.com/legalview/you-can-be-punished-for-recording-video-without-consent---
35. https://www.videosurveillance.com/schools.asp
36. https://www.airwhizz.com/index.php/2018/07/16/indian-airports-lack-cctv-cameras/
37. https://www.worldbuild365.com/blog/how-cctv-cameras-can-help-to-prevent-a-crime-or-theft-gBIQYX
38. https://doi.org/10.3390/s150510315
39. http://www.dlink.cc/d-link-camera-2/what-is-tamper-detection-and-how-do-i-enable-the-d-link-camera.html
40. https://doi.org/10.3390/s150510315
41. https://ncavf.com/what-we-do/forensic-video-enhancement/
42. https://ampedsoftware.com/
43. https://doi.org/10.1007/s00530-017-0538-9

***Article Received**: 28 August 2020 **Revised**: 20 September 2020 **Accepted**: 08 October 2020 **Publication**: 31 October 2020*

44. https://doi.org/10.1007/s00530-017-0538-9
45. https://doi.org/10.1007/s00530-017-0538-9
46. https://doi.org/10.1007/s00530-017-0538-9
47. https://doi.org/10.1145/2816795.2818056
48. https://www.lgdv.tf.fau.de/publicationen/face2face-real-time-face-capture-and-reenactment-of-rgb-videos/
49. https://doi.org/10.1145/2816795.2818056
50. https://www.cinema5d.com/face2face-real-time-face-capture-and-reenactment-of-videos/
51. https://www.sciencedirect.com/science/article/pii/S1742287616300718
52. http://videocleaner.com/about.html
53. https://www.youtube.com/watch?v=WBz3TJeuKdQ
54. https://showmore.com/record-audio-on-macbook-pro.html
55. https://www.empireonline.com/movies/fugitive/review/
56. https://www.ontariosystems.com/resources/may-i-leave-a-voicemail-message/
57. http://www.audioforensicexpert.com/forensic-audio-enhancement/
58. http://www.forensicsciencesimplified.org/av/
59. https://www.theverge.com/2016/11/3/13514088/adobe-photoshop-audio-project-voco
60. https://www.theverge.com/2017/4/24/15406882/ai-voice-synthesis-copy-human-speech-lyrebird
61. http://www.audioforensicexpert.com/
62. http://www.audioforensicexpert.com/
63. https://www.researchgate.net/figure/Histograms-of-feature-F-for-the-test-audio-corpus-The-DFT-based-phase-estimation-method_fig5_224142452
64. https://acustek.com/en/forensic-solutions/forensic-products/authenticity-analysis.html
65. https://www.thebalancecareers.com/discover-careers-in-forensic-science-974532
66. https://www.researchgate.net/figure/2-An-overview-of-the-proposed-steganography-system_fig12_279748503
67. https://www.researchgate.net/figure/2-An-overview-of-the-proposed-steganography-system_fig12_279748503
68. https://scialert.net/fulltextmobile/?doi=jas.2010.2094.2100
69. https://doi.org/10.13140/rg.2.2.21323.18727