International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.01 (Feb-2024)

http://dx.doi.org/10.12785/ijcds/150163

# Detection Tampering in Digital Video in Frequency Domain using DCT with Halftone

**Wafaa H. Alwan** [1] **and Sabah M. Alturfi** [2]

[1] *College of Computer Science  Information Technology, University of Kerbala, Kerbala, Iraq*
[1]*College of law, University of Kerbala, Kerbala, Iraq*

*Received 07 Agu. 2023, Revised 29 Jan. 2024, Accepted 31 Jan. 2024, Published 05 Feb. 2024*

**Abstract:** In recent years, the rapid technological development and the emergence of mobile devices, cameras, etc., in addition to the availability of video production, editing, and formatting programs, made it easy to edit, manipulate, and fake or tamper video. As they know that pictures or videos give more information than texts; Video is a very important medium for transferring information from one place to another. One of the important types of evidence in road accidents and theft crimes. Moreover, when forensic analysis is essential for any video, the availability of origin video may be rare therefore the forensic experts must establish decisions based on the present video (under surveillance) and decide if this video is fake (tampered) or not fake. There are multiple methods to tamper video, including active and blind passive methods. In this research, we tried to combine the behavior of active methods in the process of embedding the halftone current frame of video in the DCT Coefficients of next frame of the same video with the behavior of passive methods by comparing the information embedded after extracting with the information of the current frame to determine whether there is a fake in the video or not and which frame contains tamper. The experimental results of the submitted method showed a huge level of success in locating frames in which falsification or tampering occurred through copying, deletion or insertion, or even if copy-move regions. Also, in proposed method we attempted to post-processing the fake frames using the information included in the subsequent frame, if it is not faked. Finally, the original video, the embedded halftone video, and the tamper (fake) video after post processing were compared using PSNR and SSIM similarity scales. At last, the accuracy and precision scores of tampered and non tampered frames are computed.

**Keywords:** Video tampering · DCT transform. Halftone algorithm. PSNR- SSIM Similarity measure · Gaussian filter.

## 1. Introduction

Digital video is considered one of the most serious pieces of evidence for solving many cases such as Theft crimes, accident road, judicial forensics and play vital role even in stopping or broadcasting Political, economic and social rumors in social media, therefore authentication of digital video has respected as critical research domain that attaches with the evolution of methods and tools to identify if the digital video has been fake or not.

In addition, the high proliferation and simple utilization of video editing software make the original digital video is easily be forged with various video clips, even if it is by non-professionals. The tampering or faking in the origin video destroyed the authenticity of it. This causes a great perverting for police inspectors. As a result, it guides to termination of justice, and rises considerable damage to others. Tamper detection of digital video considers one of most significant methods to manifest the authentication of digital media and to solve such these issues.

Any digital video application includes three hands: A producer (sender), a receiver, and a third party. The producer creates the video, and the receiver extradites the video from the producer over the third party. The third could be a storage tool (e.g., Memory Flash/CD/DVD) or it could be a noisy channel in a video stream. Video tampering means an operation of bad modification of video content, so as to hide an object, an incident or alter the concept transmitted by the imagery in the video. this alteration of Video content is intentionally making by the attacker on third party. Detection of video tampering has to find the vestiges of alteration in the video content and test the correctness and safety of this content. These methods can be divided into active and passive (blind) methods; the active methods are divided into signature and watermarking techniques, while the passive methods are divided into three kinds of techniques: spatial, temporal, and hybrid of them as explain in Figure1 [1].

As we see in figure 1 the tamper detection methods category into types active and passive methods. The inherently way for adding some specific data in the video through video shooting was the base of active detection method. To do

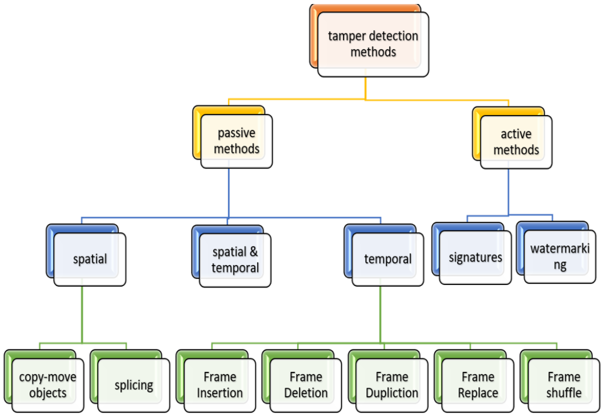


Figure 1. Types of video tampering detection methods

so, it locates whether the video is tampered or not by revealing the safety of the particular data that embedded in the video. The active methods are chiefly interested with the data hiding techniques, like digital signature and digital watermark [2], [3]. Both digital signature, watermarking (Fragile and semi-fragile) required to be embedded when the video has been registered, this making active techniques less use than passive techniques because they dependent on both algorithmic and hardware implementation [4], [5]. Also, due to increase cost and price of these devices which make the study of passive detection techniques more pressing[6].

The base work of passive video tampering detection methods through employing traces left in the frames of the video due to forge and cannot be seen with the bared eye. IN spite of, these methods unlike active methods do not need any previous particular data inserted in videos. But the statistical features are modified during the tampering procedure. The modification in statistics, the conflicts of different features like noise, residues, texture, abnormalities in video, etc., are the key for detecting tamper in passive methods. Moreover, when video is important evidence in a crime and forensic test is needed of this evidence, the passive methods are the best option for forensic experts because most of devices of surveillance have not contain digital signature or watermark. therefore, in this case, the active methods are not workable[7]. There are Variety kinds of passive tamper methods some of them focus on feature extraction and compare with adjacent frames. On the other hand, some of them focus on copy, insert, delete, add, shuffle frames. In this paper,We try to hybrid between active and passive methods to reveal tampering in video. Briefly, all these video tampering passive blind methods are generally grouped to tampering of intra-frame or tampering of inter-frame such as:

### 1) *tampering of Intra-frame:*

In this type of forgery means the veritable contents of specific frames are changed. Examples of these tampers are the followings:

1- Copy-move object means the third party may include or remove an object to / from a frame of video

2- Upscale-crop means cropping a video frame to get rid of evidence of the video tampering, and then spreading the altered frames to retain the same resolution through the entire video.

3- Splicing means copies regions from different source images and pastes them to the goal image. All these methods show in figure2. This figure2 explain clearly how can insert object into video frames/ delete object from video frames and substitute position with pixels from neighboring regions. All the methods of tampering can be done in spatial domain, but the main difference of copy move and splicing. In copy-move the object/s is copied and pasted in frames of the same video and in situation of eliminate the object/s from the video, the region/s is stuffed with the neighboring pixels from the same frame of that video, while in situation of splicing the tampering is carried out with the object/s from different video/s [8].

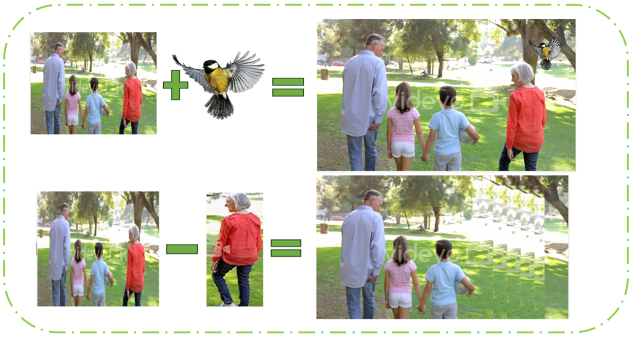
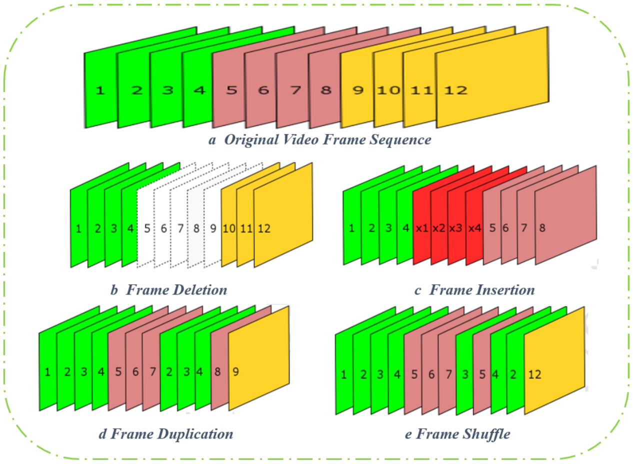


Figure 2. Video Frame Tampering Insert/ Delete object

### 2) *tampering of Inter-frame:*

This type of tampering impact in some way the sequence of frames in a video. Normally, these tampers include eliminating a set of frames or inserting them from/ into a particular video.In addition, Shuffle video frames that only changes the ordering of sequence of video frames consider in temporal techniques. Also, Duplicate a frame is still a kind of this forgery which can be recalled as tampering of inter-frame copy-paste. Figure3 clarifies different types of video forgeries in this category [9]. The active and passive detecting tamper approaches can be performed in temporal and spatial domain. Spatial domain tampering usually removes/ inserts certain objects in the frame [6].

The remainder of this paper is layout as follows; section 2 presents literature survey of recent video tampering detection methods.in section 3 we explain methods of proposed model. Section 4 demonstrates a proposed model in figures with brief explanation. Section 5 explained the of recent video tampering detection methods. Finally, the conclusion of this paper is presented in Section 6.



a Original Video Frame Sequence

b Frame Deletion

c Frame Insertion

d Frame Duplication

e Frame Shuffle

Figure 3. Video Frame Tampering

## 2. Literature Survey

There are variety researches of tamper detection for digital video. Some of these paper deal with active tamper detection methods and other deal with passive tamper detection methods. In this section we show some of these papers of active and passive detection methods: for example; Han Pu, Tianqiang Huang and et al. Proposed a new coarse-to-fine video tampering detection process that merges spatial constraints with stable feature. both the low-motion area and the high-texture area are extracted in the coarse detection stage. Then acquire the regions with wealthy quantitative correlation through merged above two areas that are applied for extracting video optimal similarity features. The luminance gradient component of the optical flow is calculated and counted as comparatively steady feature. Then, the fishy tampered points are discovered by mixing the above two features. The exact tampering points are determined in the fine detection stage. Finally, the similarity of the gradient structure based on the characteristics of the human visual system is used to further decrease the false detections. this suggestion focusses on to defeat video passive forensics methods that just employ the similarity between adjacent frames. Because of bear from high false detection rate for the videos with severe motion [10] . DUJAN B. TAHA and her colleagues in there's manuscript suggest method for detecting active tamper in video, that include a novel low-cost algorithm for detecting video tampering through correlation coefficients between the video frames that are encrypted and embedded into first frame of the video stream. Empirical findings for measuring visual quality and robustness showed the high achievement of the suggested algorithm due to the capability to discover forgery even in easy and low-impact attacks [11].

Trimly to progress the vigorous of passive video tampering detection, Wei Wei, Xunli Fan and et al suggest a content-based video similarity tamper algorithm based on multi-scale normalized mutual information that can perform copy, insertion, and deletion video frame tamper detection. This submitted algorithm involves multi-scale content analysis, single-scale content similarity measure, multi-scale content similarity measure, and tampering positioning. In the 1st step, the Gaussian pyramid transform is used to obtain the scales of the visual content of the video frame; in 2nd step, the similarity of single-scale visual content gauged through locating adjacent normalized mutual information of two frames; in3rd step, the multi-scale normalized mutual information descriptors are building to realize the multi-scale visual content similarity measure of adjacent two frames. ultimate, they employ the local outlier isolated factor detection algorithm to uncover the position of the video tampering. Empirical outcomes of the suggested method clarify not only just reveal the position of video frame tampering that removed, copied, and added successfully, but also can reveal the tampering of various video formats. The accuracy for feature detecting increase on rate 93 and rate of 96 beyond the post processing operations [12].

Hiroki Ueda and et al proposed passive method to reveal the presence or absence of tampering in videos. They demonstrated the effectiveness of the suggested proposed forgery detection method that includes capturing the differences between successive frames, that is rely on the Gaussian pyramid to out high-frequency features , before extracting the high-frequency features of sequential frames to improve the detection accuracy, they tried to Increment dataset through Trimming, then for the feature extraction using HOG descriptor that being robust to the image scale, and machine learning method -SVM- to classify into 2 classes tamper and non tamper frames. Finally, they computed the accuracy for tamper detected proposed method before and after trimming of dataset [13]. G. Sujatha and et al focused on passive tamper methods that manifest more functional in expressions of preserving the originality of the video through using adopted Difference hashing algorithm (D-Hash) to proceed tamper detection. In this paper, the D-Hash algorithm computing the difference between the intensities of the pixels to determine the binary value of each of the frames. then, the decimal value is encrypted and added up to the origin video after converted from binary value that computed by hash algorithm. finally, transmit it to the receiver. The receiver then executes the identical set of tasks and then investigation occurs. If the received hash value identifies with the computed value, then the receiver can infer that there is no tampering otherwise it is tampering [14]. Ye yao, yanqing shi and et al. suggest deep learning-based method to detect object falsification in video. The high-dimension features are automatically extracting from the patches of input image by CNN. Also, the offered method unlike the classical CNN models, it permits video frames push through three preprocessing layers previous to feed into proposed model of CNN. They comprise of a frame absolute difference layer, a max pooling layer and a high-pass filter layer to reduce temporal redundancy between video frames, to decrease computational complexity of image convolution, and to foster the residual signal neglected by video falsification consequently [15].

Also, a modern technique is proposed for recognizing real and forgery digital video by Mubbashar Saddique; Khurshid Asghar and his collegous. The submitted method is constructed according to deep model, that embraces of three kinds of layers: motion residual (MR), convolutional neural network (CNN), and parasitic layers(P). The MR layer shows up the forgery vestiges by collecting of frames. The CNN layers cipher these forgery vestiges. ultimately, (P) layers classify the video into real or forgery [16]; In this paper [17], the researcher suggest a passive blind approach accomplished of two distinct algorithms to uncover frame falsification and region duplication in videos; algorithm I detect copy-moved frame through get the mean features in frame and calculate correlation. As well, algorithm II uncovers them by calculating the error of the similarities between regions of two frames /within affected frame.

While Bandu B and his colleagues in 2023 suggest two techniques to reveal forgery in video: the 1st way is determining the falsification rely on the residual noise in the frames of movie, while 2nd way to disclose video imitation based on the spatial-temporal domain using footprints left while falsifying with a video sequence. Finally, the IP trace back to see the place of the imitation video transmitter is considered[18].

## 3. Methods Of Proposed Model

Before clarifying the proposed model, we explain some methods that are used briefly in this section.

### A. *Discrete Cosine Transform (DCT) method*

Discrete Cosine Transforms (DCT) has been one of the major interesting types of research to enhance the images. The DCT aids disconnect the image into portions (or spectral sub-bands) of varying significance with consideration for visual quality of the image ; i.e., it's great amount of information is saved in very low frequency coefficients of a image and other rest frequencies having quite little information that can be saved by employing very little number of bits (ordinarily, at most 2 or 3 bit) [19], [20]. We take this advantage by applying binary mask on small DCT coefficients to embed halftone information extracted from every frame into next frame circularly; i.e., until embed halftone of last frame into first frame of video.

### B. *Halftone image Algorithm*

A method of convert or print image into black and white image that shows different shades of grey by changing the number of black dots in an area of the image. In sound ward; Halftoning is the printing technology in which each pixel in halftone image is represented by single bit.Hence halftoning gives 87.5 compression ratio" [21]. For obtaining halftone image from continuous image by hiring operator that it is convolved with continuous image, then quantization process is applied on the result of prior step to transform into binary value. The pixel value in each plane of color image was represented in 8-bit while the same pixel in a halftone image was represented in 1-bit, therefore The halftoning procedure affords a compression ratio of 8:1 [21]. From benefit of halftone image, first we resize every frame in video into 1/4 of original size, then applying halftone algorithm on these resized frames to reduce the capacity of saving halftone current frames into DCT coefficients of next frame.

### C. *Quantization Method for embedding*

To embed halftone frame that every pixel in it equal to 1 bit either 0 or 1 based on binary mask that selected the lower frequencies of DCT as show in figure 4 the left image represents DCT coefficients the center image shows binary mask. At last right image is halftone frame. The embedded process is implemented in quantization process based on the equations 1:

$$C^{'} = \begin{cases} S * \frac{C}{S} * \frac{3}{4} * S, & \text{if } halftone_i m = 1 \\ or & \\ S * \frac{C}{S} * \frac{1}{4} * S, & \text{if } halftone_i m = 0 \end{cases} \tag{1}$$

Were C being halftone image value: 0 or 1, S threshold value being selected interval between [4-12] based on the decision of the creator of video if he want to recover tamper frame with high quality; i.e., selecting small value for S enough for deciding which the video frame is tamper or not and trying to recovery tamper video frame with acceptable quality. while selecting large value for S not only detecting which frame is tamper but also try to recovery it with high quality from halftone frame embedded into next frame. Figure4 illustrate these three methods and how to embed halftone value in small value of DCT Coefficient's that detected in white area of binary mask. Then inverse DCT do for all frames after embedding implement. Finally, construct video against tamper or fake and transfer to the receiver. Also, the total number of frame video and S value, height, width of frames embedded into last four byte of the first frame. when the receiver wants to extract embedded halftone frames must implement DCT to video frame then extracted based on the equation2 and value of S

$$halftone_i m = \begin{cases} 1, & \text{if } C^{'} - S * \frac{C}{S} \geq \frac{1}{2} * S \\ or & \\ 0, & \text{if } C^{'} - S * \frac{C}{S} < \frac{1}{2} * S \end{cases} \tag{2}$$

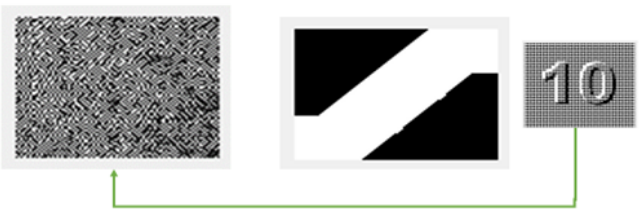


Figure 4. DCT coefficients image, binary mask, halftone image of video clip count

## 4. Proposed Model

In this section we explain the proposed method that include two parts. we assume that the video create by the sender after implements first part as showed in figure5. In the first part of this proposed method used halftone image algorithm for every frame and watermarking this halftone of every frame in DCT coefficients of the next frame for all video. To protect video from forgery, but; when this video attacked by third person so that tampering. We can try to detect forgery video forgery in second part will be started.

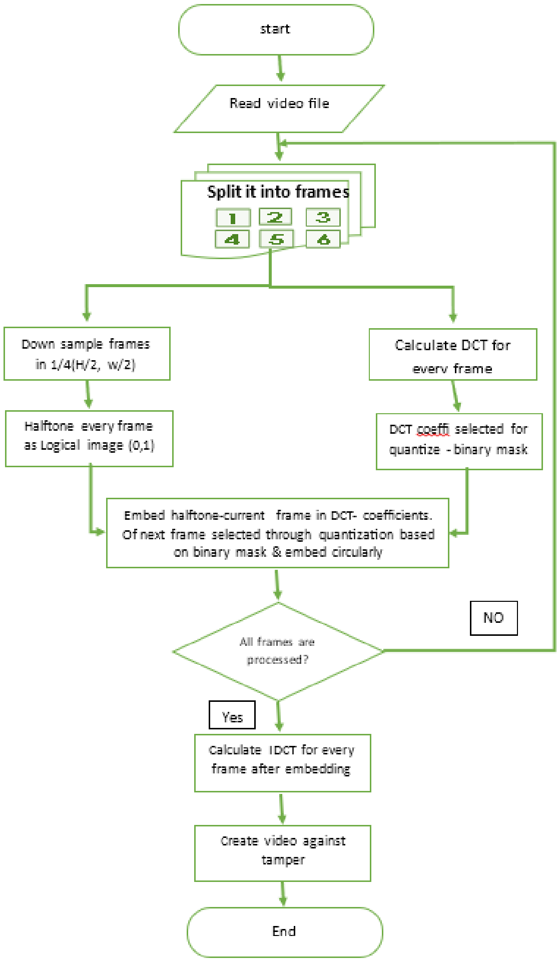

start
Read video file
Split it into frames
1
2
3
4
5
6
Down sample frames in 1/4(H/2, w/2)
Halftone every frame as Logical image (0,1)
Calculate DCT for everv frame
DCT coeffi selected for quantize - binary mask
Embed halftone-current frame in DCT- coefficients. Of next frame selected through quantization based on binary mask & embed circularly
All frames are processed?
NO
Yes
Calculate IDCT for every frame after embedding
Create video against tamper
End

Figure 5. The embedding halftone process

In the 2nd part; we will be able to detected this tampering in video frame based on difference between halftone tampered frame and halftone frame extracted from the next frame, and try to recovery tampers' frame from halftone this frame that extracted from next frame, therefore the receiver divided this 2nd part into three stages as showed in figure6.

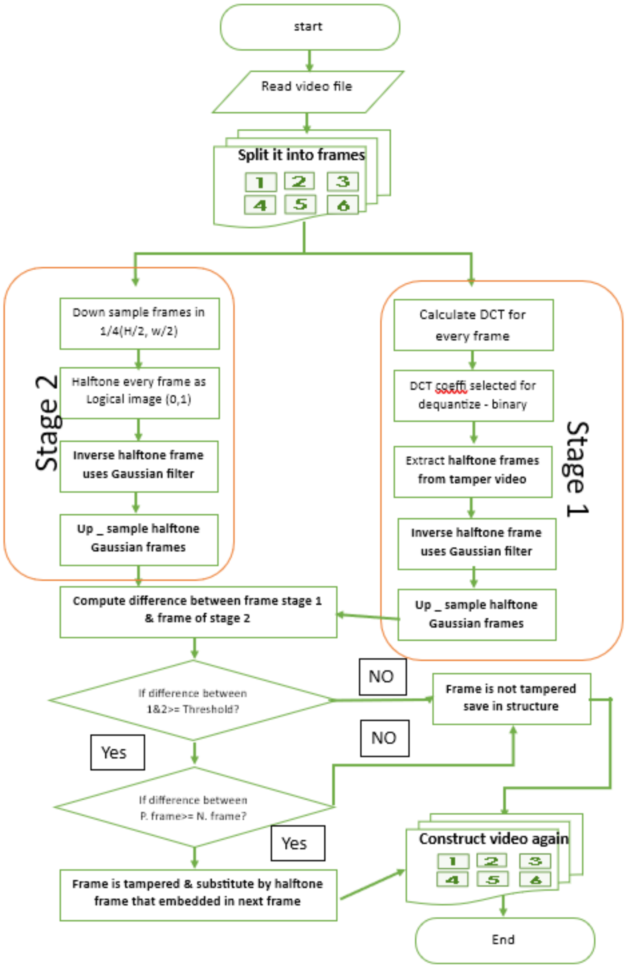

start
Read video file
Split it into frames
1
2
3
4
5
6
Stage 2
Down sample frames in 1/4(H/2, w/2)
Halftone every frame as Logical image (0,1)
Inverse halftone frame uses Gaussian filter
Up _ sample halftone Gaussian frames
Stage 1
Calculate DCT for every frame
DCT coeffi selected for dequantize - binary
Extract halftone frames from tamper video
Inverse halftone frame uses Gaussian filter
Up _ sample halftone Gaussian frames
Compute difference between frame stage 1 & frame of stage 2
If difference between 1&2>= Threshold?
NO
Frame is not tampered save in structure
Yes
NO
If difference between P. frame>= N. frame?
Yes
Frame is tampered & substitute by halftone frame that embedded in next frame
Construct video again
1
2
3
4
5
6
End

Figure 6. The extracting detecting tampering processes

In stage1; extract the embedded watermarking halftone current frame from DCT coefficients of the next frame for all video frames. Then, in stage2: halftone image every frame and compare Inverse halftone current frame with the Inverse halftone frame that extracted from next frame through applied Gaussian filter to detected tampering and recovery based on difference between them through comparing with threshold that specified as 2 in this paper. if mean difference grater that threshold there exist tamper in video, then compute the mean differences between previous and next Inverse halftone frame and Inverse of embedded halftone frame; if the mean difference of previous greater than mean difference of next the receiver decide the current frame is not tamper the next frame is tamper, otherwise the current frame is tamper, therefore by taking the mean differences exactly detect which frame is tamper , then the receiver try to recovery fake frame from halftone's frame that extracted from next frame in third stage based on S value.

## 5. Result

Trimly, to evaluate the effectiveness of the proposed model, the proposed model (experiments) was test on five small videos of format .AVI and .mp4 that have various number of frames with diverse frame size. We know that embedding the halftone of every frame in next frame caused some degradation in visual quality of next frame, therefore we embedding halftone of every frame with select small S value such as 4. Then Perceptual quality and robustness test before forgery video frame using two measures ”peak signal to noise ratio PSNR” and ”similarity SSIM” are measured. Table I shows details of video experimentation: The first col. shows type and number of video that used in experiments,the second and third cols. explain the number and size of frames in each videos. Finally, the PSNR and SSIM -perceptual measures- measure the differences between original video before/after embedded video with halftone, also between embedding halftone video before and after tampering as explain in columns 3,4,5 and 6 respectively.

TABLE I. Explain PSNR SSIM Measures

| Video name. | No. of frame | Frame size | P.M. Original video B&A embeding halftone | | P.M. Embedded halftone video B&A tampering | |
|---|---|---|---|---|---|---|
| | | H*W | PSNR | SSIM | PSNR | SSIM |
| **Count.avi** | **16** | **176*144** | **49.86** | **0.9909** | **45.34** | **0.8823** |
| **Shark.avi** | **69** | **256*256** | **49.68** | **0.9986** | **24.95** | **0.9366** |
| **Rabbit.mp4** | **205** | **240*360** | **50.51** | **0.9960** | **23.55** | **0.9569** |
| **Park.mp4** | **314** | **180*320** | **48.64** | **0.9916** | **24.80** | **0.9751** |
| **Family.mp4** | **313** | **360*640** | **48.12** | **0.9976** | **24.89** | **0.9690** |

### A. Type of tampering methods in the experiments

In this subsection, as we know from the introduction of paper there are different types of tamper methods and techniques, therefore we used some of them on the five video that used in experiments such as insert or delete objects in some frames or in all frames of each video.Some of these types of tampers that are applied on five videos explain below in table II. From the results of inserting or deleting objects in/from all frames of video we noticed the difference between halftone current frame and extracted halftone from next frame is very high therefore the proposed method can easily detect tampering with high accuracy. But, Although the high perceptual quality for PSNR and SSIM values between tampered video and embedded halftone video is high which are shown in table1, the proposed method could not recovery tamper video. On other hand tampering some video frames not only permit to detect tamper video frame but also permit to reconstruct it from halftone’s frame. -

TABLE II. Example of tamper types on five videos

| *Video no.* | *Type of tampered* | *Proposed method* |
|---|---|---|
| Count.avi | Partial tamper 3frames object<br>Insert full frame 2<br>Delete 1 frame | Detect by difference<br>Detect by difference &<br>total no. frame compared |
| Shark.avi | Partial tamper all frames with object size[80 80]<br>Delete 10 frames 100 110 | Detect by difference<br>Detect by difference &<br>by total no. frame compared |
| Rabbit.mp4 | Delete 30 frames 100 129<br>Partial tamper all frames with object size [150 150] | Detect by difference<br>Detect by difference&<br>by total no. frame compared |
| Park.mp4 | Partial tamper all frames with object size [100 100]<br>Insert full frame 5 in different location | Detect by difference<br>& histogram |
| Family.mp4 | Partial<br>tamper all frames with object size[150 150]<br>Insert full frame 5 in different location | Detect by difference<br>& histogram |

After that, tampering some frames of video experiment with different method of tampering such as copy- move whole frame or splicing region; i.e., Insert or delete regions. We take video no. 1 that contain 16 frames and tamper some its frames with different methods such as ( delete /insert /copy objects or insert or delete frames) as shown in the next figures. So, figure 7 is the original video frames that contain sixteen frames, while figure 8 represent the tamper video frames with different type of tampering partially tamper as frames 7,15 or totally tamper as frame 12. Also we can notice the type of tamper from the contrast of histogram of these frame as shown in figure9. we know the successive frames of video scene are same with a few differences between them therefore the histogram of them are approximately identical. This figure showed how the histogram of tamper frame has vary from others in same scene. Also , we can easily detect the forgery through differences/contrast in histograms of frames , e.g variety histogram 0f frame12, as well as we notice very small differentiate in frame 7 and 15 that can be detected through difference between halftone current frame and it’s embedded halftone extracted from next frame, therefore if not all frames of video are tampering, these frames can reconstruct from it’s halftone that embedded in the next frame with acceptable quality as explain in figure10.It shows the substitution of the tamper frames 7,12,15 from it’s halftone that extracted from the next frames 8,13,16 respectively. where figure11 shows this substitution.

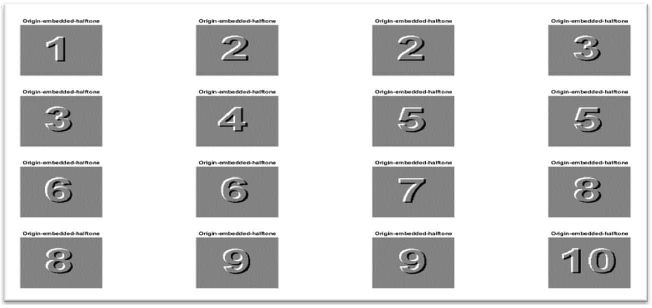


Figure 7. Original Video Frames

### B. Accuracy result of detection tampering

[h!] Unfortunately, in previous section we cannot recover all tamper video because if all the frames of video were tampered caused the halftone also destroyed, but we can detect tampering of video frame either partial or all frames of video are tampered with high accuracy. Therefore, in

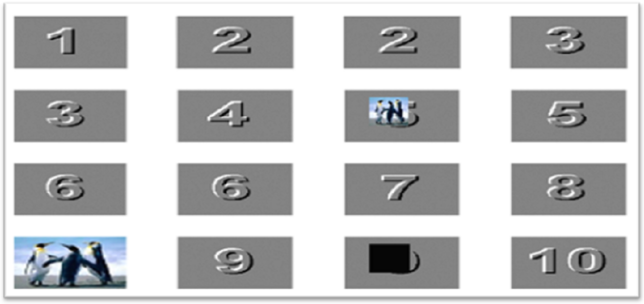


Figure 8. Tamper Video Frames

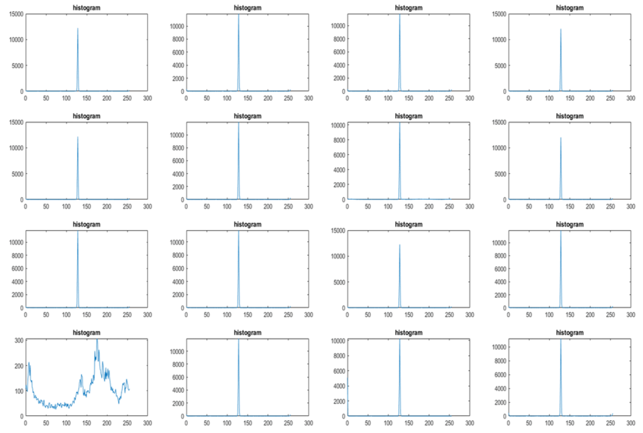


Figure 9. Histograms of Tampered Video

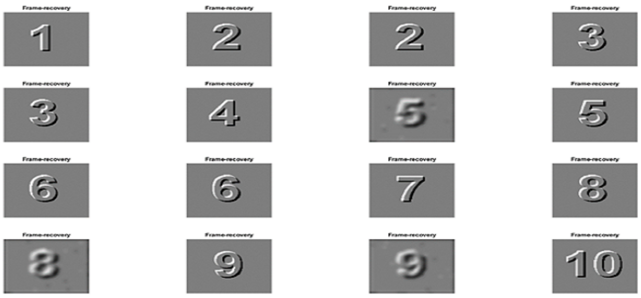


Figure 10. Recovery video frames tamper based on threshold and halftone embedded

this subsection, we compute the accuracy for the result to detect video is tampering or is not as shown in table III through measure the accuracy score - the proportion of true positives and true negatives to total positive and negative frames. and the precision score that measures the rate of positively predicted frames that are actually tamper. TP frame (i.e., tamper frame that true detected) FP frame (i.e., tamper frame that false detected). Precision is affected by the class distribution [22]. Mathematically, compute accuracy score and precision score based on these equations 3,4:

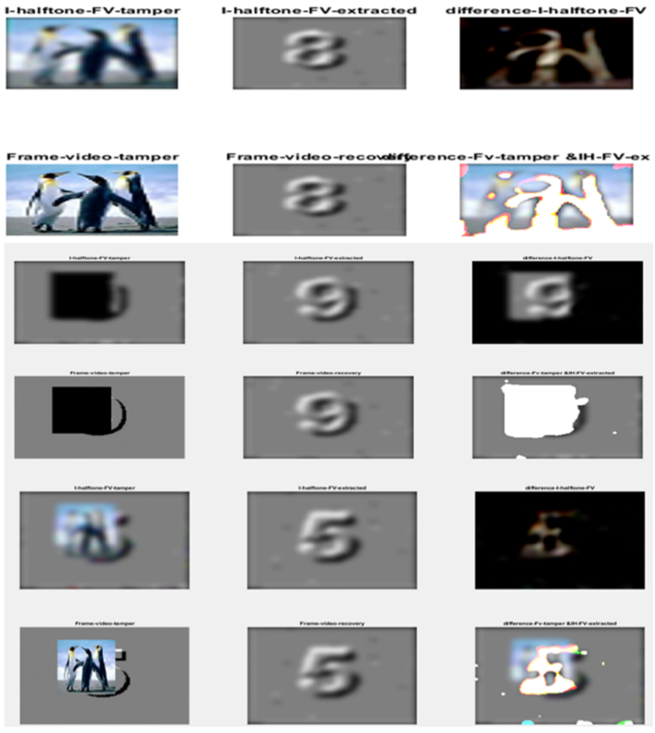


Figure 11. Explain reconstruct frame7,13,15 from substitution halftone embedded in frames 8,14, 16

TABLE III. Accuracy Precision of detect tampering in video

| Video no, | Accuracy score | Precision Score |
|---|---|---|
| Count.avi | 93.75 | 80 |
| Shark.avi | 100 | 100 |
| Rabbit.mp4 | 100 | 100 |
| Park.mp4 | 100 | 100 |
| Family.mp4 | 100 | 100 |

$$AccuracyScore = \frac{TP + TN}{TP + FP + TN + FN} \quad (3)$$

$$PrecisionScore = \frac{TP}{TP + FP} \quad (4)$$

We can conclude from the results of the tests for the five experiment videos that clearly explained in table II if all frames of video are tampered even if tampered with small object then halftone embedded will be destroyed. although the tampered video have good perceptual similarity as shown in column 5 and 6 in table1,but we can simplicity detect if the video is forgery or not forgery . Finally, we tried to match the results of proposed model with paper of literature survey [12], the accuracy and precision ratios of tamper detection of the suggested method is vital efficacious which is shown is Table IV.

TABLE IV. Explain accuracy ratio and precision ratio of suggested method result with other

| Methods | Accuracy ratio | Precision ratio |
|---|---|---|
| **Proposed method** | **93–100** | **80–100** |
| **Paper [12]** | **93.33** | **96.55** |

## 6. Conclusions and Future Work

In this paper a proposed model of embed halftone current frame in DCT coefficients of next frame provide a powerful tool to reveal any type of tampering either passive such as insertion, removing, shuffling, copy -move whole frame / regions of frame through taking the mean difference between frame and it's halftone embedded in next frame or detect active tampering methods if next frame doesn't contain the watermark halftone of previous frame which means tamper detecting in video. Therefore, Experimental results of this hybrid detecting tampering proposed model is feasible and effective. In other word, the halftone of the current frame is embedded in the next frame it makes this proposed identification system has a strength point because it serves as evidence of the presence of tampering. This means; when the video is analyzed by the other party by comparing the halftone of the current frame with its own halftone extracted from the next frame, the presence of any change determines that there is tampering or forgery in the frame and therefore there is tampering in this video. Also, this model provides a chance to reconstruct tamper frame from it's halftone in the next frame if it isn't tamper. In future work our team embed in spatial domain or using another transform such as DWT.

### *A. Abbreviations and Acronyms*

- DCT Discrete cosine transform
- PSNR Peak Signal to Noise Ratio
- SSIM Structural Similarity Index Measure
- DWT Discrete Wavelet Transform
- *BA* Before and After
- P.M Perceptual Measure

### *B. Authors and Affiliations*

1- Wafaa H. Alwan College of Computer Science Information Technology, University of Kerbala, Kerbala, Iraq
2- Sabah M. Alturfi College of law, University of Kerbala, Kerbala, Iraq

## References

[1] K. Sitara and B. M. Mehtre, "Digital video tampering detection: An overview of passive techniques," *Digital Investigation*, vol. 18, pp. 8–22, 2016.

[2] M. Tong, W. Zhang, J.-L. Zhang, and T. Chen, "A video watermarking framework resistant to super strong cropping attacks based on nmf with sparseness constraints on parts of the basis matrix," , vol. 34, no. 8, pp. 1819–1826, 2012.

[3] X. Jun-Yu and S. Yu-Ting, "Smoothing filtering detection for digital image forensics," , vol. 35, no. 10, pp. 2287–2293, 2013.

[4] H. Chen, Z. Chen, X. Zeng, W. Fan, and Z. Xiong, "A novel reversible semi-fragile watermarking algorithm of mpeg-4 video for content authentication," in *2008 Second international symposium on intelligent information technology application*, vol. 3. IEEE, 2008, pp. 37–41.

[5] F. Di Martino and S. Sessa, "Fragile watermarking tamper detection with images compressed by fuzzy transform," *Information Sciences*, vol. 195, pp. 62–90, 2012.

[6] Z. Pan, P. Jin, J. Lei, Y. Zhang, X. Sun, and S. Kwong, "Fast reference frame selection based on content similarity for low complexity hevc encoder," *Journal of Visual Communication and Image Representation*, vol. 40, pp. 516–524, 2016.

[7] N. Akhtar, M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, and Z. Habib, "Digital video tampering detection and localization: review, representations, challenges and algorithm," *Mathematics*, vol. 10, no. 2, p. 168, 2022.

[8] J. Wang, Z. Li, C. Zhang, J. Chen, Z. Wu, L. S. Davis, and Y.-G. Jiang, "Fighting malicious media data: A survey on tampering detection and deepfake detection," *arXiv preprint arXiv:2212.05667*, 2022.

[9] R. D. Singh and N. Aggarwal, "Video content authentication techniques: a comprehensive survey," *Multimedia Systems*, vol. 24, pp. 211–240, 2018.

[10] H. Pu, T. Huang, G. Guo, B. Weng, and L. You, "Video tampering detection algorithm based on spatial constraints and stable feature," in *Advances in Computational Intelligence Systems: Contributions Presented at the 19th UK Workshop on Computational Intelligence, September 4-6, 2019, Portsmouth, UK 19*. Springer, 2020, pp. 541–553.

[11] S. A Hasso and T. Basheer Taha, "A new tamper detection algorithm for video," *Journal of Engineering Science and Technology (JESTEC)*, vol. 15, no. 5, pp. 3375–3387, 2020.

[12] W. Wei, X. Fan, H. Song, and H. Wang, "Video tamper detection based on multi-scale mutual information," *Multimedia Tools and Applications*, vol. 78, pp. 27 109–27 126, 2019.

[13] H. Ueda, H. Kang, and K. Iwamura, "Video tampering detection based on high-frequency features using machine learning," in *Proceedings of the 2020 3rd Artificial Intelligence and Cloud Computing Conference*, 2020, pp. 19–24.

[14] G. Sujatha, D. Hemavathi, K. Sornalakshmi, and S. Sindhu, "Video tampering detection using difference-hashing algorithm," in *Journal of Physics: Conference Series*, vol. 1804, no. 1. IOP Publishing, 2021, p. 012145.

[15] Y. Yao, Y. Shi, S. Weng, and B. Guan, "Deep learning for detection of object-based forgery in advanced video," *Symmetry*, vol. 10, no. 1, p. 3, 2017.

[16] M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, H. A. Aboalsamh,

and Z. Habib, “Classification of authentic and tampered video using motion residual and parasitic layers,” *IEEE Access*, vol. 8, pp. 56 782–56 797, 2020.

[17] G. Singh and K. Singh, “Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation,” *Multimedia Tools and Applications*, vol. 78, pp. 11 527–11 562, 2019.

[18] B. B. Meshram and M. K. Singh, “Video forensic for video tamper detection,” *American Journal of Multidisciplinary Research & Development (AJMRD)*, vol. 5, no. 05, pp. 01–18, 2023.

[19] W. A. Mustafa, H. Yazid, W. Khairunizam, M. A. Jamlos, I. Zunaidi, Z. Razlan, and A. Shahriman, “Image enhancement based on discrete cosine transforms (dct) and discrete wavelet transform (dwt): a review,” in *IOP Conference Series: Materials Science and Engineering*, vol. 557, no. 1. IOP Publishing, 2019, p. 012027.

[20] W. Chen, M. J. Er, and S. Wu, “Illumination compensation and normalization for robust face recognition using discrete cosine transform in logarithm domain,” *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 36, no. 2, pp. 458–466, 2006.

[21] H. Kekre, S. R. Sange, G. S. Sawant, and A. A. Lahoty, “Image compression using halftoning and huffman coding,” in *Technology Systems and Management: First International Conference, ICTSM 2011, Mumbai, India, February 25-27, 2011. Selected Papers*. Springer, 2011, pp. 221–226.

[22] A. Kumar, “Accuracy, precision, recall & f1-score-python examples,” *Data Analytics*, 2020.

**WAFAA HASAN ALWAN** was born in Karbala, Iraq, in 1979. She /received the B.S. degree in computer science from Mustansiriya University, Baghdad, Iraq, in 2001, and the M.S. degree in computer science from Babel University, Babel, Iraq, in 2006. She received the Ph.D. degree in computer engineering with the Ferdowsi University of Mashhad, Iran in 2021. .

**Sabah M. Al-Tarfi** , Current place of work: College of Law - University of Kerbala He was born Karbala – 1985, address: Iraq/ Karbala, he completed his bachelor degree at university of Kerbala, and the master degree from College of Science and Engineering – LaTrobe University – Australia, 2015. Email: SABAH.M@UOKERBALA.EDU.IQ