Ensuring Video Integrity Using Watermark - Chaining by SVD and DWT

Aditya Tiwari[1], Ayush Pandey[2]

[1]aditya3.1416[at]gmail.com
[2]ayushpand97[at]gmail.com

Abstract: ***In the era of increasing crime rates and thefts, the video evidences plays an important part in identifying the theft and helps in conviction of the people involved in the foul act. As these video evidences plays an important part the probability of these evidences getting tampered is very high, therefore there is a high need to protect these evidence. Our algorithm implements a robust mechanism through which the tampering in the video evidence can be identified. The video evidence is divided in the number of frames according to the frame rate and the length of the video then the first frame of the video is encrypted by the genesis watermark of the video, then the other frames are encrypted using the previous frames mathematically operated already by the genesis watermark which results in the formation of a blockchain like structure in the video itself. A blockchain is a structure where the previous blocks are connected to the next through encryption and any block missing in between the chain can verify that the blockchain is tampered. The whole video once encrypted shows almost no signs of watermarking or glitches. Now if the video is tampered in a way such that the frames are missing from the video, the verification algorithm can find the exact point of time in the video from which the frames are missing as it breaks the blockchain of frames. The algorithm can verify that the video evidence is tampered. This concept can be used in wide range of categories where video evidences or in general videos are used, for example road accidents CCTV videos, surgical videos for organs where trafficking of human organs can be done etc.***

Keywords: Watermarked block chain, DWT, SVD, Logistic mapping, image processing, video processing, watermark embedding

1. Introduction

The need for evidence legitimacy is very high in the era of rapid growth and development where crime rates on record breaking high. These cases of theft of any kind such as human organ trafficking, cases of theft and burglary are very risky and to have a proper conviction the evidence needs to be protected and verified. Various researchers have proposed the idea of having a video equipment in the operating room, which can be used as an enhancement of the performance and which will eventually make surgical procedure more transparent[1,2]. Some also believe that having video equipment in the hall will ensure that doctors and other medical staff do their job more professionally [3]. In addition, digitized media are easily manipulated by the use of computers. For example, one cracker could selectively crop and integrate part of a digital work into her or his own one, pointing towards the tampering of video in such a way that it can’t be used as evidence. The algorithm implemented provides the verification scheme such that we can verify that the evidence is legitimate or not. The algorithm uses traditional watermark embedding, in which secret information can be hidden inside the photos in such a way that it is invisible to the naked eyes. This technique is also used in one of the sections of our algorithm which in turn protects the legitimacy of video as a whole. Considering the above observation, many researchers have proved that digital watermarking techniques can serve as the solution of the security problem up to some extent. The idea behind the technique of this kind is marking the data as a watermark based on the information of copyright, data block header. This information is embedded signals of various types such as audio or video.

Usually, watermarking Techniques are divided in four fields based on the kind of data which has to be watermarked. In general, (i) text, (ii) image, (iii) video and (iv) audio [4, 5, 6, 7]. Research in terms of image watermarking has already been done to some extent and focus is on Videos due to advancement in content creation. Nowadays more and more of research in being done in the video watermarking domain as a lot of content is being created online and it is necessary to prove the authenticity of the videos, In similar way protection of these video is also necessary against various attacks or tempering which can be proved fatal in many cases.

In case of images, these techniques are categorized based in the domain of embedding. Usually, Frequency [8] and Spatial or transform domain [9, 10]. In spatial domain, [11] the watermarks are embedded in the image directly by changing the image pixels by some operations which is not referred as direct modification can affect the important details which the image contains, that is why in spatial domain watermarking can be done in following two ways (i)visible and (II)invisible. Mostly, invisible watermarking is recommended for content verification [12]. The spatial watermarks are judged based on (i) the embedding power (capacity) of the photograph .this capacity can be increased by embedding the watermark in a way such that pixel of watermark are embedded with the different pixels of the original image based on its color value [13], (ii) the reliability of the concerned image can be enhanced by embedding, focused on the image prediction error pattern and it might be able to match with the properties of HVS[14], (iii) dependability of the entire system can be focused on by encrypting the watermark image on the most important part of the image which is also regarded as ROI (region of interest)[15].

Already implemented algorithms does not provide the robustness required to resist the various attacks on the image in the spatial domain[16],but when compared to transform domain it works faster compensating the robustness. To get over with the disadvantages of the spatial domains new domain called frequency domain was introduced. It is changing the different images to the multiple frequencies using reversible transforms[17] which makes the embedding more robust because of the transformed coefficients. The theory related to the robustness of the following single frame watermarking techniques systems using methods like DFT alone , DWT alone, DCT alone [18], SVD alone [19] and combined techniques such as Radon and DFT [20], SVD and DCT [21], SVD and DWT [22] and DCT, SVD & DE [23]. Many techniques are present in the image processing field for the watermarking but the discrete wavelet transform (DWT) is highly recommended because of the better impact with the human visual system (HVS) and better frequency features.

Watermark techniques are evaluated based on the following criteria such as following (i) robustness, (ii) imperceptibility and (iii) capability of encryption. A watermark is regarded as imperceptible if the original image when compared with the watermarked image are indistinguishable. Robustness is defined by the capacity of the image to fight against the distortion of the various kinds of attacks. The capacity is defined by the number of embedded images on the image using various watermarking techniques. To achieve the goal of embedding more number of watermarks, most of the watermarking techniques suffer due to the more amount of additional information, which also increases the complexity of the technique. Video watermarking can be differentiated from the image watermarking by the following parameters: to achieve the imperceptibility in a video is very hard compared to images because of the fact that the temporal variations have to be considered because of the three dimensional properties of the video. Third problems is that as the video contains may frames and collection of all of them forms the video, the watermarks have to be embedded In all of them are each frame is important and is unique cause it contains different information from all the other frames, so many watermarks have to be chosen and have to be embedded which can make the whole process more lengthy and compute exhaustive [24, 25]. The method is proposed for the averaging difficulty by Su in [24] which states that there can be different watermark embedding in motionless frames. Therefore, the video can have two types of watermarks. Various other research have been done in aspect of the videos for example Niu and Sun et al.[26] embedded a decomposed a watermark and embedded it in decomposed vide on its decomposition level.

To address the above mentioned issues our algorithm implements a combination of robust techniques which includes video segmentation, which then is processed by the watermark embedding. Watermark embedding uses logistic scrambling of the genesis watermark, which then is further mathematically inserted into one of the regions of the initial frame obtained by the application of discrete wavelet transform technique, after which singular valued decomposition is also applied to the low-low region of the image. The further technique involves generating a new watermark with the help previously encrypted frames by the scrambling and DWT and SVD procedures again mathematically operated with genesis watermark. This gives to rise in formation of blockchain like structure within the video itself, which is very complicated as the dependency of the next frame is on the previous frame and this criteria is applied throughout the video, which makes the video ready anytime legitimacy check.

2. Preliminaries

Singular Value Decomposition

Singular Value Decomposition (SVD) is commonly used in linear algebra. This mathematical tool can be used in many applications, such as signal or image processing, including digital watermarking. In watermarking techniques where SVD is used, the technique usually works on the host image, which on being processed is divided into many small blocks which are then further applied into SVD to obtain the singular value, which is also used to embed watermark information. Many advantages are there in this type of technique which are (i) the coefficient size of SVD is fixed, and these values can be used to replicate the basic algebraic features the host image. (ii) Another advantage of this is that it these singular values don’t change much when slight changes are made in the image for example embedding of the watermark in the host image. Following is the formula of the decomposition:

$$I = U \cdot \ S \cdot \ VT$$

where I is the matrix of $m\times n$ corresponding to a image, U is the matrix of $m\times m$, V is the matrix of $n\times n$, S is the diagonal matrix with the sane size of I , and T is the matrix transformation coefficient.

Discrete wavelet transform

For multi-scale and spatial-frequency decomposition of the image Discrete Wavelet Transform (DWT) can be used. In this technique the host image on which DWT is applied is decomposed into four type of sub-bands Low-Low (LL), High-Low (HL), Low-High (LH) and High-High (HH). The LL region obtained from this process, this component has a low resolution, this gives approximate information of an image. The other three components which are obtained represent the comparatively more detailed version of the image. It is not necessary to embed the watermark or the other information in only one of the bands out of four, the watermark encryption can be done in more than one sab-bands but this might result in more complexity and distortion of the image. In the field of image compression and enhancement this technique is widely used for HVS. This wavelet transform has the characteristics of multi-resolution; therefore the hierarchical display can be the applicable application of continuous image transmission. To make complexity less for the computation, the watermark is embedded hierarchically by applying the DWT technique. This technique which is based on DWT also provides better robustness against various attacks while compared with watermarking in spatial domain. There are various filters like Haar, Bioorthogonal, Coiflets amd Daubechies can also be applied when required quite easily. Continuous splitting of the multidimensional signals is done into high and low frequencies multiple times until the image is completely decomposed. The reconstruction of the image can be done by applying the inverse wavelet transform (IDWT), the image can be restored from DWT coefficients.

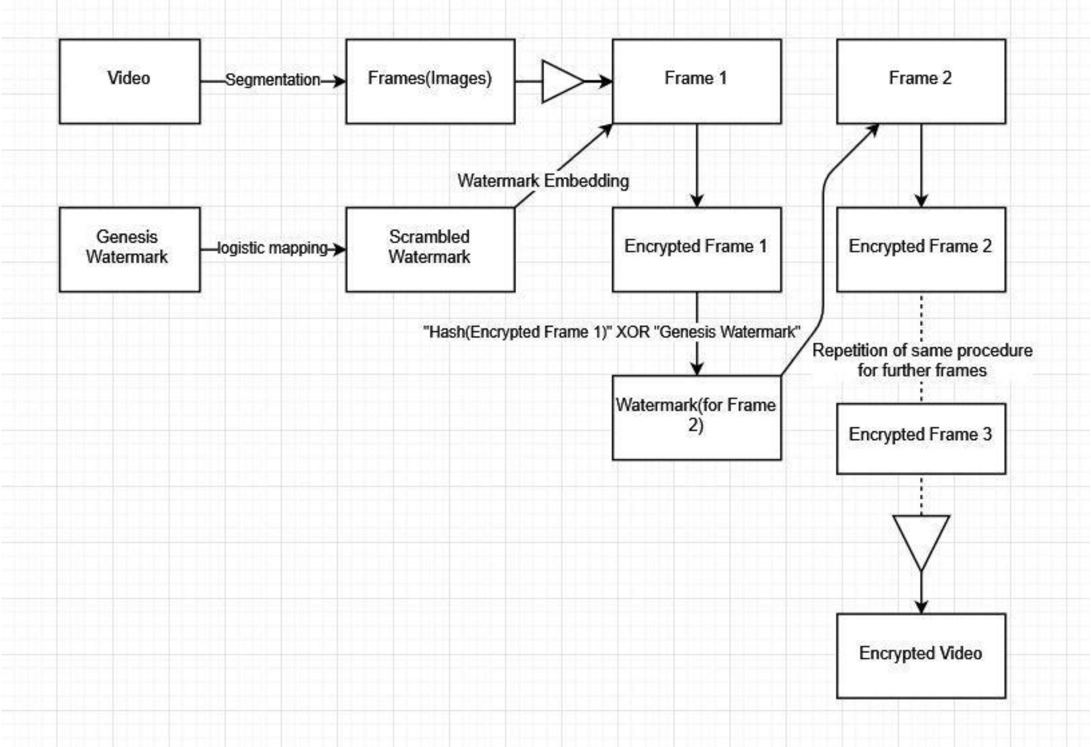
Logistic mapping –

Logistic mapping is a kind of a polynomial, one-dimensional chaotic mapping 0, it is widely used in Multimedia security, Digital-communication security and other fields. The formula for the logistic mapping is initially developed from a demographic model which featured a simple form but a very significant regularity. It is defined as: X (k 1) u X (k)[1 X (k)] , k 0, 1, ...,n, X (k) (1, 1), u (0, 4) (1). In this formula, X (k) is the mapping variable while u is the system parameter. When the given two conditions are met, the function of logistic mapping works in a mixed state, i.e. in a disorderly and unpredictable way. 0 X (0) 1, 3.5699456 u 4. The basic idea behind the formula is that when we iterate a given initial value n times, n values are produced, X (1), X (2), ...,X (n), which is a one-dimensional chaotic sequence. When we encrypt an image of m n to obtain a one-dimensional sequence, it must be iterated m n times. The sequence is then normalized to get a new sequence in range of (0, 255). Later, the new sequence is converted into a two-dimensional matrix, which is in fact the encrypted image matrix. The secret key used here is [X (0), u]. We can achieve a higher level of security when encrypting an image with a logistic mapping scheme for the sequences generated by this encryption function with features of a periodic, irrelevant and non-convergent. Moreover, the function is very sensitive to the initial values, i.e. even if the initial conditions are too close, the iteration results won’t be the same, and the number of the uncorrelated chaotic sequences is quite large. So, it is difficult for an attacker to deduce the exact initial conditions of the chaotic system from a finite length sequence.

3. Methodology

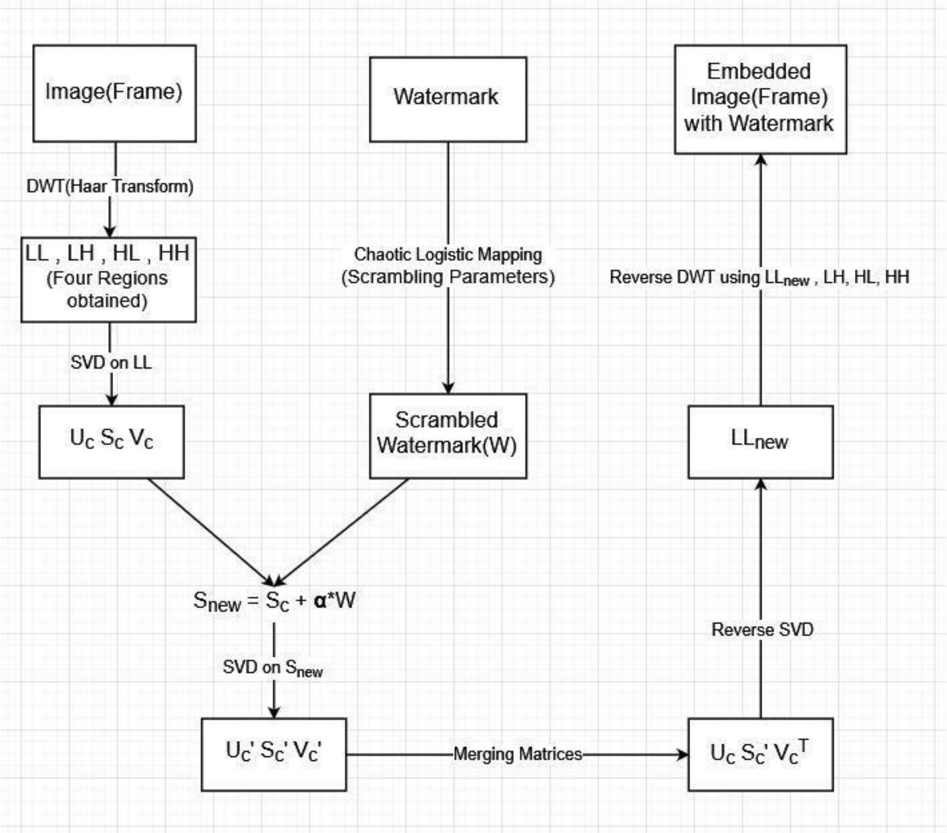
The whole process involves the two parts, video encryption and decryption. Along with video encryption some other information is also sent which is required for the decryption of the video such as logistic parameters etc.

Video Encryption – The Proposed Algorithm



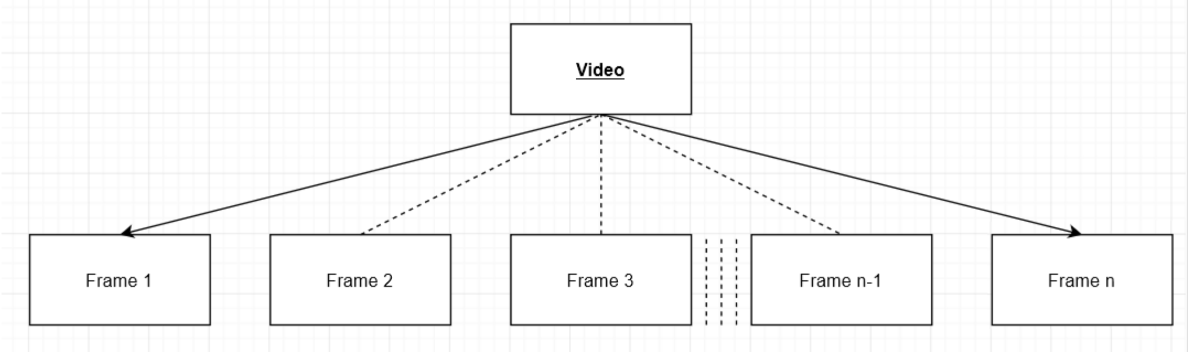
In this section we propose a new algorithm for encrypting the video in such a way that water can be embedded inside the video in each and every frame with the help of genesis watermark. The algorithm in such a way that it doesn’t have a major visible effect on the video itself when observing from the naked eye. The algorithm uses various techniques for water mark encryption which includes the watermark embedding as well**.

Watermark Embedding


Image(Frame)
DWT(Haar Transform)
LL , LH , HL , HH (Four Regions obtained)
SVD on LL
Uc Sc Vc
Watermark
Chaotic Logistic Mapping (Scrambling Parameters)
Scrambled Watermark(W)
Snew = Sc + α*W
SVD on Snew
Uc' Sc' Vc'
Merging Matrices
Uc Sc' VcT
Reverse SVD
LLnew
Reverse DWT using LLnew , LH, HL, HH
Embedded Image(Frame) with Watermark

The above mentioned algorithm is used for watermark embedding which uses various techniques like singular valued decomposition and discrete wavelet transform, the detailed explanation of the above algorithm and techniques are explained in the following section.

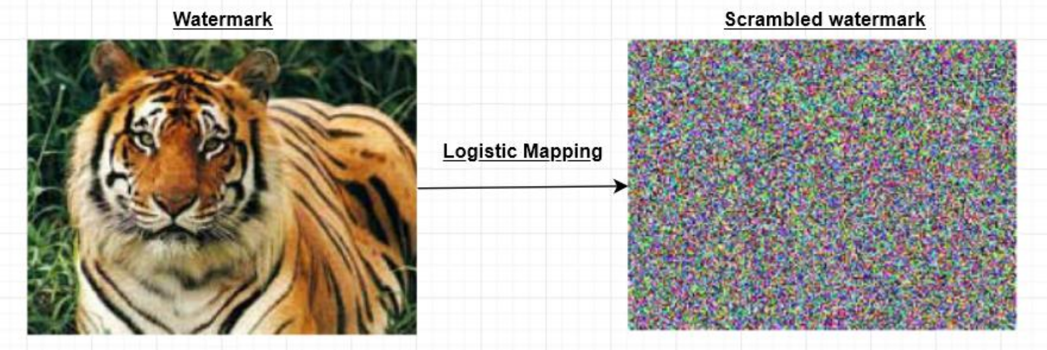
Step 1 – Video Segmentation

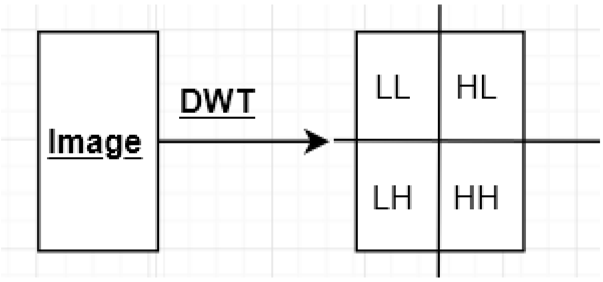


First of all the as the video is encrypted in a manner that the next frame is connected to the previous one, we have to take out the frames from the video. The video can be segmented according to its frame per second (fps) rate. Outcome of this process gives us the frames which are stored then processed in the further steps.

Step 2

Genesis Watermark is taken which is to be used initially and is selected by the user. After this watermark is decided, it is undergone through the logistic mapping method i.e.





Step 3

The four regions obtained in the previous process have specific properties but for the encryption process the LL region of the image is used as it had lower resolution and manipulation of its bit have the minimum impact on the original image. The lower impact is considered here as finally all the encrypted frames are merged and the video is formed again.

Singular Value Decomposition (SVD) is applied

$$LL = U_c . S_c . V_c$$

Step 4

The matrix "S" is obtained which is singular with positive values, this is further processed and information about the watermark is embedded by the following mathematical equation.

$$S_{new} = S_c + \alpha * W$$

Hence by the above equation we obtain the new matrix S_{new} which is then undergone through the SVD process again and we observe the following

$$S_{new} = U_c' S_c' V_c'$$

We obtain a new matrix S_c' which is used in rebuilding the image again which eventually forms the whole video again after merging all the frames back together.

Further we take U_c, S_c' and V_c and get the product to obtain the new LL_{new} region of the encrypted image by applying Reverse SVD.

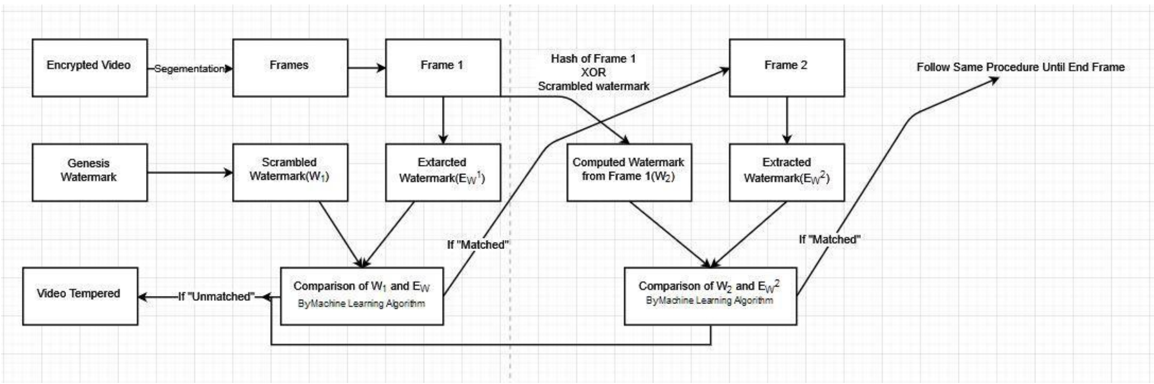
Now Reverse DWT is used on LL_{new} and LH, HL and HL regions of the original image which results in the formation of the encrypted image which cannot be distinguished my HVS and which is very similar to the original image.4

Step 5

The next step is to apply the XOR operation between the encrypted image of the previous frame with the genesis watermark, the watermark for the next frame is obtained by this procedure. Once the watermark is obtained then the same process from step 2 is repeated until the last frame.

The whole process once completed results in the encrypted frames which are then merged back to make the whole video again hence completing the video encryption procedure.

Video Verification -


Encrypted Video
Segementation
Frames
Frame 1
Hash of Frame 1
XOR
Scrambled watermark
Frame 2
Follow Same Procedure Until End Frame
Genesis Watermark
Scrambled Watermark(W_1)
Extarcted Watermark(E_W^1)
Computed Watermark from Frame 1(W_2)
Extracted Watermark(E_W^2)
If "Matched"
If "Matched"
Video Tempered
If "Unmatched"
Comparison of W_1 and E_W
ByMachine Learning Algorithm
Comparison of W_2 and E_W^2
ByMachine Learning Algorithm

The above algorithm is used to check if the video used is tampered or not, the algorithm works similarly in the initial phase until video segmentation and scrambling of genesis watermark, from the starting frame of the video the watermark is extracted by reverse applying the procedure used in watermark embedding. This extracted watermark is then compared to the watermark made from genesis watermark, if this match then algorithm moves forward to the next frame computing the next extracted watermark and then computing the watermark which should be embedded then comparing them again. If at any point of time the watermark extracted and ideal (which should be embedded originally) does not match the algorithm comes to a conclusion that video is tampered.

4. Results and Discussion

A series of experiments were conducted on various raw videos, one of those experiments includes the following –

Video Encryption

1. Video split into frames (original video consists of more than 120 frames in total of 7 seconds)

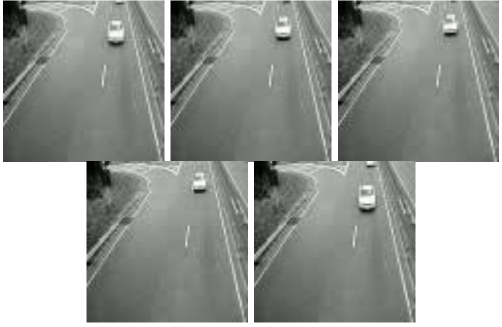
Genesis watermark – Scrambled watermark

2. Watermarks which are to be embedded

3. Watermark embedded frames

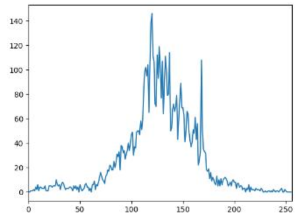
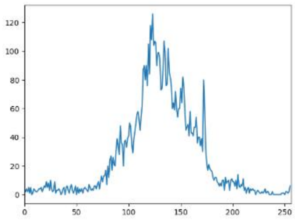
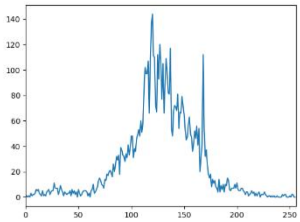
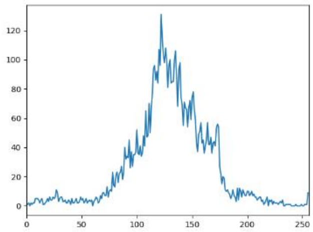
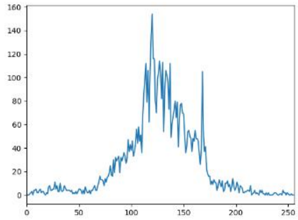
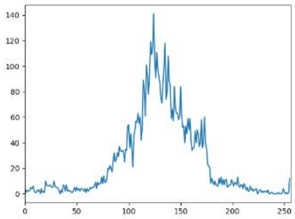
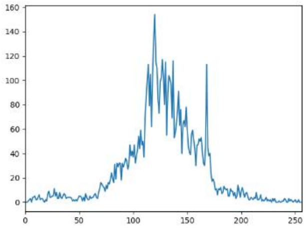
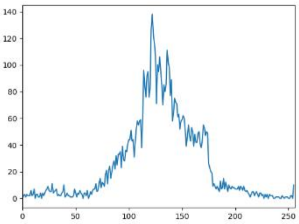
Video Verification

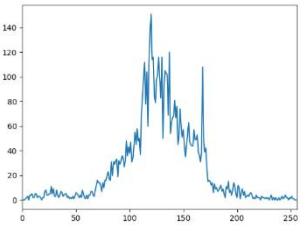
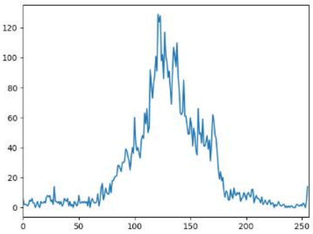
4. Extracted frames from encrypted video



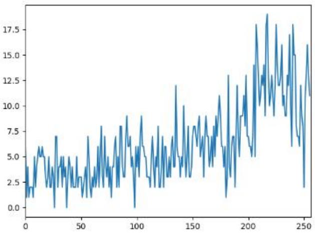
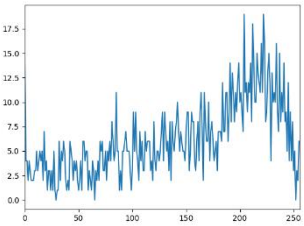
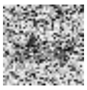
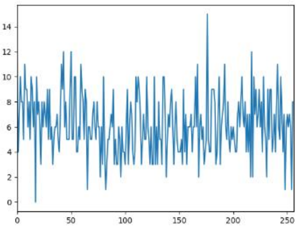
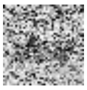
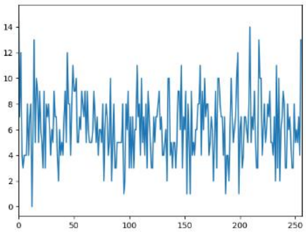
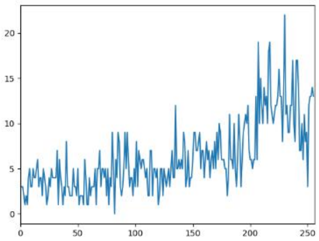
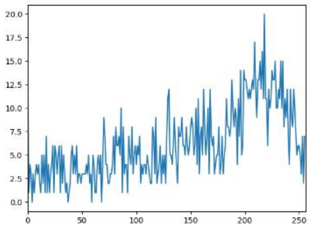
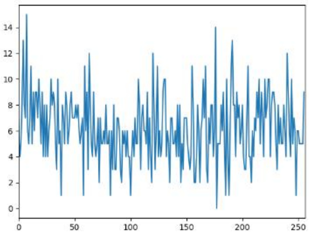
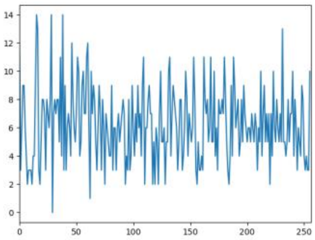
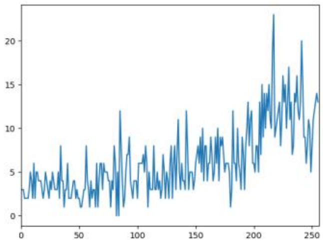
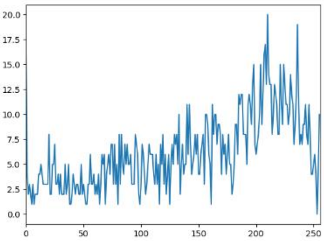
5. Extracted watermarks from encrypted video

Histogram Comparison 1

Frames of original video	Histogram of original frames	Frame of encrypted video	Histogram of encrypted frames
			
			
			
			

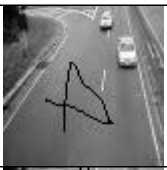
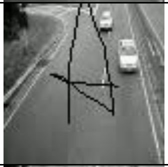
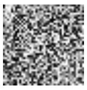
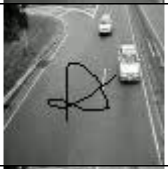
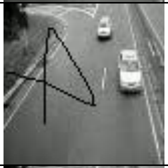
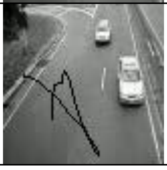
Histogram and structural similarity comparison 2

Encrypted watermark	Histogram of encrypted watermark	Extracted watermark	Histogram of extracted watermark	Structural similarity (ssim)
				0.979584
				0.981053
				0.982984
				0.980216
				0.974501

From the above table we can observe that the structural similarity between the unaltered video is always more than 0.971 units which gives us the criteria that the legitimate video frames always have the structural similarity of >0.971.

Now for example of altered/tampered video we make some alteration in the video itself by using altering software which gives us the following result which is showed in terms of following table

Comparison of encrypted video, embedded watermark, altered video and extracted watermark

Encrypted frame	Embedded watermark	Altered frame	Extracted watermark	Structural similarity comparison (embedded vs extracted watermark)
				0.940110
				0.932580
				0.948703
				0.948531
				0.927807

References

[1] Joo S, Xu T, Makary MA Video transparency: a powerful tool for patient safety and quality improvement. BMJ Qual Saf 2016;doi:10.1136/bmjqs-2015-005058. doi:10.1136/bmjqs-2015-005058

[2] Makary M, Xu T, Pawlik TM Can video recording revolutionise medical quality? BMJ 2016;351:h5169.

[3] Chris, “Using video surveillance as evidence in court,” SECURITYBROS, 2014

[4] Huang J, Shi YQ (2001) Embedding gray level images. Proc. IEEE Int. Symp. Circuits and Systems, vol. 5,Sydney, Australia, pp 239–242

[5] Langelaar GC, Setyawan I, Lagendijk RL (2000).Watermarking digital image and video data. A state-of-theartoverview. IEEE Signal Proc Mag 17:20–46.

[6] Rajendra Acharya U, Acharya D, Subbanna Bhat P, Niranjan U (2001) Compact storage of medical images with patient information. IEEE Trans Inf Technol Biomed 5:320–323

[7] Nikolaidis A, Pitas I (2003) Asymptotically optimal detection for additive watermarking in the DCT and DWT domains. IEEE Trans Image Process 12 (5):563–571.

[8] Briassouli A, Strintzis MG (2004) Optimal watermark detection under quantization in the transform domain. IEEE Trans Circ Syst Video Technol 14 (12):1308–1319.

[9] Mukherjee DP (2004) Spatial domain digital watermarking of multimedia objects for buyer authentication. IEEE Trans Multimed 6:1–15.

[10] Cox IJ,Miller ML, Bloom JA, Fridrich J, Kalker T (2008) Digital watermarking and steganography, 2nd edn. Morgan Kaufmann Publisher, San Francisco

[11] Phadikar A, Maity SP, Rahaman H (2009) Region Specific Spatial Domain Image Watermarking Scheme. IEEE International Advance Computing Conference (IACC 2009), pp 888–893.

[12] Memon N (2001) Analysis of LSB based image steganography technique. IEEE Proc ICIP 3:1019–1022

[13] Hao P, Shi Q (2000) Comparitive Study of color transforms for image coding and derivation integer reversible color transform. IEEE, pp 224–227.

[14] Hong I, Kim I, Hem S (2001) A blind watermarking technique using wavelet transforms. IEEE Proc ISIE 3:1946–1950

[15] Su Q, Niu Y, Zou H, Liu X (2013) A blind dual color images watermarking based on singular value decomposition. Appl Math Comput J 219:8455–8466.

[16] Liu Y, Zhao J (2010) A new video watermarking algorithm based on 1D DFT and Radon Transform. Signal Process 90:626–639.

[17] Wu X, Sun W (2013) Robust copyright protection scheme for digital images using overlapping DCT and SVD. Appl Soft Comput 13:1170–1182.

[18] Gaurav Bhatnagar, Balasubramanian Raman (2009) A new robust reference watermarking scheme based on DWT-SVD. Comp Stand Inter 31:1002–1013

[19] Ali M, Ahn CW, Pant M (2014) A robust image watermarking technique using SVD and differential evolution in DCT domain. Optik 125:428–434

[20] Wolfgang RB, Podilchuk CI, Delp EJ (1999) Perceptual watermarks for digital images and video. IEEE Proc 87 (7):1108–1126

[21] Doerr G, Dugelay J (2003) A guide tour of video watermarking. Signal Proc Image Commun 18 (4):263–282

[22] Checcacci N, Barni M, Bartolini F, Basagni S (2000) Robust video watermarking for wireless multimedia communication. IEEE Proc WCNC 3:1530–1535

[23] Doerr G, Dugelay J (2003) A guide tour of video watermarking. Signal Proc Image Commun 18 (4):263–282

[24] Checcacci N, Barni M, Bartolini F, Basagni S (2000) Robust video watermarking for wireless multimedia communication. IEEE Proc WCNC 3:1530–1535

[25] Dong J., Li J. (2016) A Robust Zero-Watermarking Algorithm for Encrypted Medical Images in the DWT-DFT Encrypted Domain. In: Chen YW., Tanaka S., Howlett R., Jain L. (eds) Innovation in Medicine and Healthcare 2016. InMed 2016. Smart Innovation, Systems and Technologies, vol 60. Springer, Cham

[26] Serdean C, Ambroze M, Tomlinson M, Wade G (2002) Combating geometrical attacks in a DWT based blind video watermarking system. In: Proc. Eurasip-IEEE VIPPromCom. p 263–6

[27] C.-S. Lu, J.-R. Chen, H.-Y. M. Liao, and K.-C. Fan, “Real-time MPEG2 video watermarking in the VLC domain,” in Proceedings of the 16th International Conference on Pattern Recognition Proceeding, vol. 2, pp. 552–555, 2002

[28] Guangxi, Chen &amp; Ze, Chen &amp; Daoshun, Wang &amp; Shundong, Li &amp; Yong, Huang &amp; Baoying, Zhan. (2019). Combined DTCWT-SVD-Based Video Watermarking Algorithm Using Finite State Machine. 179-183.10.1109/ICACI.2019.8778517.

[29] Delaigle JF, De Vleeschouwer C, Macq B (1998) Watermarking algorithm based on a human visual model.Signal Process 66 (3), pp. 319–335.

[30] Kundur D, Hatzinakos D (1997). A robust digital image watermarking method using wavelet-based fusion.Proc IEEE Int Conf Image Process 1:544–547

[31] Swanson MD, Zhu B, Tewfik AH (1998) Multiresolution scene-based video watermarking using perceptual models. IEEE J Select Areas Commun 16 (4):540–550

[32] Langelaar G, Setyawan I, Lagendijk R (2000) Watermarking digital image and video data. IEEE Signal Process Mag 17:20–43

[33] Liu X, Sun S (2000) A new wavelet based digital watermarking for video. In: Proc. IEEE Digital Signal Processing Workshop