

Authenticate audio video-crypto invisible watermarking approach for enhancing hidden information security and robustness

Mahesh Gangarde*

Department of Electronics Engineering,
Bharati Vidyapeeth Deemed University College of Engineering,
Pune, 411043, India
Email: mgangarde@gmail.com
*Corresponding author

Shruti Oza

Department of Electronics and Telecommunication Engineering,
Bharati Vidyapeeth Deemed University College of Engineering,
Pune, 411043, India
Email: skoza@bvuocep.edu.pune

Janardhan Chitode

Department of Electronics Engineering,
Bharati Vidyapeeth Deemed University College of Engineering,
Pune-411043, India
Email: j.chitode@gmail.com

Abstract: For any type of watermarking techniques imperceptibility, robustness, embedding capacity, security of hidden watermark data and good visual recovery of both cover, as well as watermark secret data, are the major issues. To solve these issues the selected frames of video and the secret data is divided into the equal number of parts and every part is mapped using adaptive pixel location mapping (APLM) algorithm to get watermarked video, hence the embedding capacity and security of hidden watermark data are increased. Furthermore, the proposed system also calculates the key security parameters like peak signal to noise ratio (PSNR), mean square error (MSE), histogram, structural similarity index module (SSIM) and cross-correlation factor (CCF) before watermarking, after watermarking and after recovering the secret data from watermarked video which are found to be identical, hence the proposed system is more insusceptible to any type of attack as compared to existing watermarking approaches.

Keywords: audio video watermarking; APLM; perceptibility; robustness; watermark information security.

Reference to this paper should be made as follows: Gangarde, M., Oza, S. and Chitode, J. (2020) 'Authenticate audio video-crypto invisible watermarking approach for enhancing hidden information security and robustness', *Int. J. Electronic Security and Digital Forensics*, Vol. 12, No. 1, pp.16–42.

Biographical notes: Mahesh Gangarde is pursuing PhD in Electronics Engineering from the Bharati Vidyapeeth University College of Engineering, Pune. He received his BE in Electronics from the Shri Tuljabhavani College of Engineering, Tuljapur in 2002 and ME in VLSI from the Bharati Vidyapeeth University College of Engineering, Pune in 2009. His research area is image/video processing and security.

Shruti Oza is presently working as a Professor and Head in Department of Electronics and Telecommunication at the College of Engineering Bharati Vidyapeeth Deemed University, Pune, India. Earlier she was a Head and Associate Professor at the EC Department, Kalol Institute of Technology and Research Centre, Kalol, 382721, North Gujrat, India. She received her BE in EC from the DDIT, Nadiad, India. She completed her MTech and PhD from the Institute of Technology, Nirma University, Ahemdabad, Gujrat, India. She has published and presented more than 60 research papers in various international/national journals/conferences. Her area of interests is analogue/mixed mode VLSI design and image processing.

Janardhan Chitode is currently working as a Professor in the Bharati Vidyapeeth Deemed University College of Engineering, Pune, India. He completed his BE in Industrial Electronics Engineering from the Bharati Vidyapeeth Deemed University, Pune, India in 1991. He received his ME from the College of Engineering (COEP), Pune at University of Pune, India in 1995. He completed his PhD from the Bharati Vidyapeeth Deemed University, India in 2009. His area of interest is signal processing, speech synthesis, image processing, digital communication, etc. He is actively participating as a member of different professional research societies, like IEEE, ISTE, etc.

1 Introduction

Watermarking is the process of concealing the secret information into digital data like image, video and audio. The main use of watermarking is for copyright protection, security of secret data and authentication. The watermarking technique is classified into visible and invisible watermarking. Invisible watermarking is called as steganography, which is used for information security. As today's digital media techniques are changing rapidly day by day, hence to maintain the security of hidden watermarked data and digital video are the major concern. All the multimedia tools like YouTube, Facebook, WhatsApp, Twitter, etc. uses videos for sharing the confidential, secret information over the digitally transmitted internet protocol. Due to this, different countries and their cultures came together for creating a good society. Implementation of digital multimedia reduces the barrier in society, but great many critical challenges in protecting digitally distributed and duplicated data like messages, text, audio and images. Hence, it is always better to provide information security for all multimedia tools during transmission. Due to this requirement of digital multimedia, video watermarking can provide the perfect solution for these issues. Subhedar et al. in 2015 gave the survey of existing data hiding and its key issues. It also elaborates the fundamental concepts, evolution measures and data security of current data hiding techniques in different domain which provides the present research trends and direction to improve data security of existing methods. It also elaborates major limitations of all existing techniques in terms of embedding capacity

(EC), robustness, perceptibility and tampering of hidden data during transmission for time domain frequency domain, spatial domain type of data hiding approach (Subhedar and Mankar, 2014). In 2017, Sowmya et al. have proposed a literature study on video authentication using watermarking and digital signature where video authentication and tampering detection technique due to intentional changes which are visible or invisible in video are discussed. It also suggested video watermarking weakness and its robustness (Sowmya and Chennamma, 2017). Giri and Bashir (2017) have suggested the potential solution for multimedia authentication tool for digital data such as images, audio and video. The technique of concealing some watermark secret information in the cover data, such as audio, video, text, images or a combination of these is used to establish the ownership rights is called as watermarking. Digital watermarking technique can be used to encourage the content providers to secure their digital information during and after transmission process. Comparative analysis of spatial and transform domain explained in terms of robustness, visual quality, cost, time and EC. The spatial domain technique is less robust, incompetent in dealing with different attacks, provide high perceptual quality, limited EC and it is mostly used in applications where authentication is required. In the last the respective author concludes that the digital watermarking is an evolving field of research in computer science and technology besides many other fields which includes signal processing, information security, cryptology and communication. The diverse nature of this field with respect to multimedia has made research in more exciting and challenging. Digital watermarking is still evolving and is open problem for future researcher (Giri and Bashir, 2017). Sadek et al. gave the literature survey of existing video data hiding techniques in different domains and suggested the advantages and disadvantages since last five years. For ideal and perfect video data hiding approach, it should provide large EC, high imperceptibility, robustness and tamper resistance, but unfortunately no such algorithm does exist in reality. All the reviewed methods have its own advantage and disadvantage in term of hiding capacity and security depending on its application. So it is always better to design appropriate video data embedding algorithm for the given application. Hence we have motivated to develop audio, video watermarking technique which will increase EC, security of hidden data, robustness and perceptibility (Sadek et al., 2014; Bhattacharya et al., 2006). In 2016, Shridhar et al. have proposed an enhanced technique in digital video watermarking with multiple watermarks using wavelet transform for protecting the multimedia data in which secret watermark information is embedded into a host such that secret watermark information is not visible. In this technique luminance band of the selected frames was taken and it is grouped to alternative pixel shares and flip those images. The experimental results show that video quality is good with high PSNR and lowest MSE and there is a scope to improve this algorithm for real time applications (Sridhar and Arun, 2016). Ahuja et al. have focused on a video watermarking scheme using a MPEG-2 coding style which used for the application of copyright protection and it applied various attacks on watermarked video and measured parameters like robustness, perceptibility, EC along with one more issue 'elapsed time', a serious concern in video watermarking. For testing the performance of a video watermarking algorithm and also suggested to apply more video processing attacks like frame insertion, frame deletion, frame averaging and compression attacks (Ahuja and Bedi, 2015). Su et al. have introduced the new blind watermark algorithm which embedded the binary watermark image into the blue component of an RGB image in the spatial domain to resolve the problem of protecting copyright. For embedding the secret watermark, the generation principle and distribution features of direct current (DC)

coefficients are used to direct modify the pixel values in the spatial domain and then four different sub-watermarks are embedded in the different areas of the host image. When the sub-watermark is extracted with blind manner according to DC coefficients of watermarked image and the key-based quantisation steps, and then the statistical rules and the method of “first to select, second to combine” are proposed to form the final watermark. Hence, the proposed algorithm is executed in the spatial domain rather than in discrete coefficient transform (DCT) domain, which shows the quick performance of the spatial domain and high robustness feature of DCT domain. The LSB method proposed in doing the changing of LSB values in a binary word of all possible pixel values. This brings a significant amount of quality degradation which provides poor parameter results. The experimental results show that the existing watermarking algorithm can obtain the better invisibility and stronger robustness of common attacks like JPEG compression, cropping and adding noise, comparison results also shows that the existing approach is better for different types of statistical attacks but with an average value of PSNR = 49.95dB which provide less security and imperceptibility. It is also observed that the existing algorithm has the low EC of 0.0013bpp. In the last the respective author concludes that the existing algorithm can be applied to colour image as original watermark to improve the EC (Su and Chen, 2018).

The detailed steps of secret watermark embedding are given as follows,

Step 1 Obtain a sub-image of the blue component.

In order to improve the robustness of watermarking, the 512×512 blue component of the original host image I is divided into 16 sub-images I_s ($1 \leq s \leq 16$) with size 128×128 pixels based on the security key key1

Step 2 Obtain embedding block.

Each sub-image is divided into 256 non-overlapped embedding blocks with 8×8 pixels. Thus the whole host image can be divided into 4,096 non-overlapped embedding blocks.

Step 3 The DC coefficient of embedding block is further calculated according to equations (1), (2) and (3)

$$DC = C(0, 0) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \quad (1)$$

Step 4 Generate quantisation table $QA(k)$ and $QB(k)$ according to user quantisation step Δ based on secret key2.

$$QA(k) = \min(DC_{i,j}) + (2k - 4) \times \Delta \quad (2)$$

$$QB(k) = \min(DC_{i,j}) + (2k - 5) \times \Delta \quad (3)$$

Step 5 Modified DC coefficient $DC'_{i,j}$ are calculated as per equations (4) and (5).

$$\text{IF } W(i, j) = 1 \text{ then } DC'_{i,j} = QA(k) \quad (4)$$

$$\text{IF } W(i, j) = 0 \text{ then } DC'_{i,j} = QB(k) \quad (5)$$

Step 6 Modified quantity $\Delta M_{i,j}$ of each pixel is given by

$$\Delta M_{i,j} = DC'_{i,j} - DC_{i,j}$$

Step 7 Each input binary (black and white) watermark is embedded into each embedding block. The one input watermark is watermark into one separate block (Su and Chen, 2018).

1.1 Main contribution

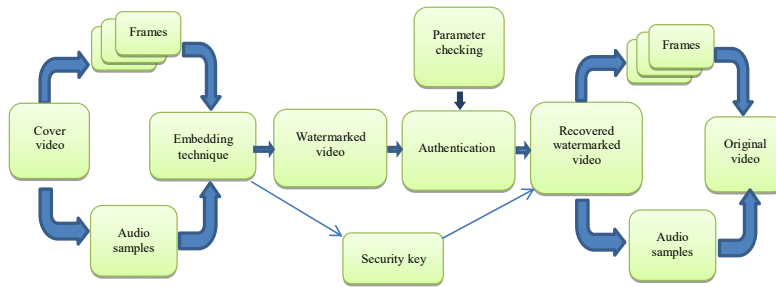
In the proposed method a novel, innovative audio, video-crypto invisible watermarking approach using adaptive pixel location mapping (APLM) technique is proposed to authenticate, increased the EC, imperceptibility, robustness, privacy and security of watermark secret data. The suggested APLM technique is based on mapping the smallest change of pixel values of selected frames of video and secret hidden data. In this technique, the secret watermark data are broken into smaller equal parts and every part is mapped using APLM algorithm to obtain watermarked video. As the video contains a large number of pixel values to embed secret watermark information, EC and the imperceptibility of the secret data is increased. During the extraction process, the proposed technique authenticates the watermarked video by obtaining the key security parameters like peak signal to noise ratio (PSNR), mean square error (MSE), histogram, cross correlation factor (CCF) and bit error rate (BER), before embedding and after recovering from the watermarked video. The suggested technique also checked the authentication process by applying different types of video processing attacks on watermarked video during transmission and recovered the secret hidden data as image or audio and cover video with good visual quality. Hence the proposed algorithm is better than any existing video watermark schemes.

2 Proposed security model for audio video watermarking

The input to the proposed security model is any type of video format and it is split into a number of frames and considered the sequential frames of video to conceal the watermark secret information as image and audio. Before concealing the secret watermark data as image and audio, it is divided it into the number of small parts and every small part is concealed using APLM algorithm into selected frames of the video. To embed audio as a secret data, audio is converted into a number of samples and every sample is converted into pixel values. Every pixel values of audio is embedded into selected frames of video using APLM algorithm. The stereo sound like .mp3 and .wave have double sample values in the range of -1 to $+1$ while the mono sound has single sample value in the range of 0 to 65,335 which gives 16 bit integer values of audio. Once the concealed process has been done, the watermarked video is obtained which is sent from transmitter to receiver. The pixel value of watermark image is searched in the selected frames and takes the location of that frame as a security key structure which is used to reconstruct the watermark image from watermarked video. The incoming watermark video is authenticating by cross checking the key security parameters with different types of attack. The propose work calculates the key security parameters like

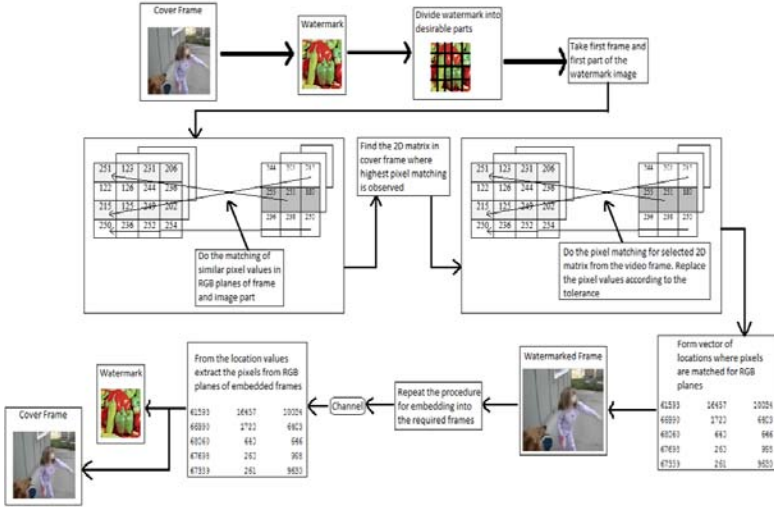
SSIM, BER, CCF and Histogram before embedding and after embedding the secret data into video. The authenticate block will crosscheck all these key security parameters and its values. If all the key security parameters values are found to be correct, then the watermarked video is transferred to receiver end otherwise, it will stop in authenticate block. The proposed approach is sending key security parameter values, secret data along with secret key which is known to both the parties. In the receiver end the watermark video is converted into audio and frames to obtain original secret data. The secret key as shown in Figure 1

Figure 1 Block diagram of proposed video watermarking security model (see online version for colours)



2.1 APLM technique for audio video-crypto invisible watermarking

In this process video is converted into a number of frames as an image. The secret data are divided into predefined number of physical parts and each frame as an image is provided as input to the embedding block in a sequential order for embedding of each part into the selected frames of the video. For concealing the watermark secret image and audio, match the pixel values of RGB planes of selected frames of video with pixel values of RGB planes of watermark secret data. The proposed algorithm search the 2D matrix in the original video frame where maximum pixel value matched with pixel values of watermark data and replace the pixel values according to the difference between two pixel values of selected frames of video and watermark data. Record the locations of pixel values of watermarked frame where pixel values of secret image are matched for RGB planes. Obtained the watermark frame and repeat the same steps for embedding the secret image into required frames of video. Re-conceal the watermark image from the location of pixel values for watermarked frame of video using the record locations of respective pixel values. The key security parameters like PSNR, MSE, SSIM, CCF, BER and histogram are calculated for frames of original video and watermarked video to improve robustness, perceptibility and security of secret hidden watermark data. The image parts, thus obtained from each frame are ordered in a matrix to get single image as shown in Figure 2.

Figure 2 Functional block diagram of proposed APLM algorithm (see online version for colours)

2.2 Embedding and extracting process of secret watermark data

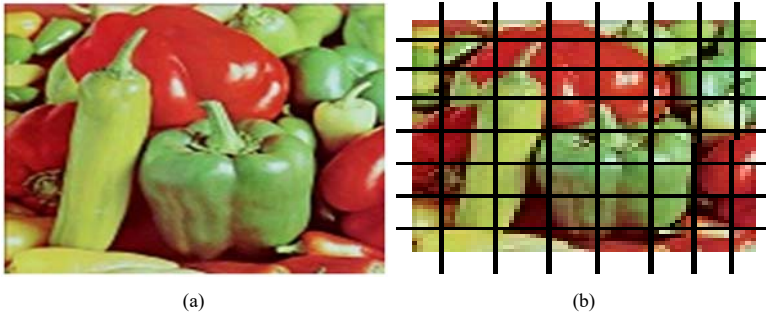
Algorithmic steps: embedding procedure

- i Obtain the colour image as secret watermark data (.png, .jpg, .bmp, 256×256 , 128×128 , 64×64 , 32×32 R.G.B.).
- ii Obtain different video formats (.avi, .flv, .mp4, .wmv).
- iii Divide the secret watermark image into n equal parts.
- iv Embed the first part into randomly obtained frames of video and so on using APLM algorithm.
- v Convert the pixel value matrices of secret watermark image part and video frame in R, G, B planes.
- vi Obtain 2D pixel matrix of watermarked frames of video into a 1D column vector.
- vii Convert the audio into number of sample values.
- viii Obtain the sample values into binary or decimal form.
- ix Repeat the steps iii to vi.

Algorithmic steps: extraction

- i Obtain the watermarked video.
- ii Obtain 1D pixel matrix of watermarked frames of video into a 2D column vector.
- iii Calculate the location of pixel values of watermarked frame of video.
- iv Obtain the location of R, G, B planes of a watermarked frame of video.
- v Reconstruct the secret watermark image and audio from R, G, B planes of a watermarked frame of video.

Figure 3 (a) Watermark image (b) Watermark subdivision (see online version for colours)



Example

- 1 Consider the fruit image of 64×64 and convert it in RGB form as shown in Figure 3(a).
- 2 Select the .avi video of frames 1,059 with a frame size of 360×470 .
- 3 Divide the watermark image into 64 equal parts (eight rows and eight columns). Thus we need 64 frames, i.e., 1st part is watermarked in the 1st frame. Take pixel value matrices of watermark image as a part and video frame of R, G, B planes as shown in Figure 3(b).
- 4 Convert each 2D pixel matrix of the watermark image block into 1D column vector as indicated in the matrix (X).

173	177	133	98
174	143	103	101
166	78	42	101
159	61	59	131

→

173	174	166	159	177	143	78	61	-	-	-	-
-----	-----	-----	-----	-----	-----	----	----	---	---	---	---

Original matrix (X)

- 5 Let us take 1D pixel array of R plane of the 1st part and 1st frame. The upper array (image array) is a part of the secret watermark image with its pixel values while the lower array (frame array) is portion of the selected cover frame of video with pixel locations shown below the values of pixels.

173	174	166	159	177	143	78	61	133	103
-----	-----	-----	-----	-----	-----	----	----	-----	-----

(a) Image array

143	54	173	158	85	162	125	103	173	10
-----	----	-----	-----	----	-----	-----	-----	-----	----

(1) (2) (3) (4) (5) (6) (7) (8) (9) (10)

(b) Frame array

- 6 Generate location array, if the pixel value of the input watermark block is matched, then take that location otherwise take the nearest location for that pixel value as shown in array (c).

3	3	6	4	3	1	5	2	7	8
---	---	---	---	---	---	---	---	---	---

(c) Location array

The pixel values 173, 174 and 177 from image array matches with a nearest pixel value of frame array that is 173 which is located at position (3), similarly 166 assigned to pixel value of 162 at a position (6), 159 assigned to 158 at position (4), 143 to 143 pixel values of image array at position (1), 78 to 85 at position (5), 61 to 54 at location (2), 133 to 125 at location (7), 103 to 103 at position (8) and generated key structure.

- 7 The key structure is used to find the mode value. Select the maximum occurrence of a particular location value as a mode. Here 3 are occurring for maximum number of times in location array. Therefore mode value = 3. Thus take 3rd pixel value of cover video and convert it in 1D array and 2D matrix coordinates of that pixel value in cover video frame as pixel matrix, i.e., (3, 1) row = 1, column = 3. The detail procedure of key structure is explain in step 8 to 12.
- 8 Obtain 64 × 64 the block of size of cover video frame in which (3, 1) pixel values lies.
- 9 Convert 64 * 64 block in to 1D column vector as shown in step 4.
- 10 Divide the column vector into two groups (group A(n * n) and group B(64 * 64) – (n * n)) where the n = size of small part, i.e., for 64 × 64 image, small part will be of size 8 × 8 as shown in the matrix (c). Thus the image array length is n² = 64. Thus 1st column of 64 × 64 block is in group A and rest part is in group B. For 128x128 image first two columns are in group A. In 1D array it can be visualised as shown in following matrix (Y).

A	A	A	A	B	B	B	B	B	B
---	---	---	---	---	---	---	---	---	---

Matrix (Y)

Length of group A = n² = 64 hence group B starts from location n² + 1 as per the matrix (Y) and repeat step 6 for group B.

173	174	166	159	177	143	78	61	133	103
-----	-----	-----	-----	-----	-----	----	----	-----	-----

(d) Image array

143	54	173	158	85	162	125	103	173	10
(65)	(66)	(67)	(68)	(69)	(70)	(71)	(72)	(73)	(74)

(e) Group B: selected frame array

Find the location values where pixel matching appears.

- a If a pixel is matched note the location
- b If a pixel location is already present in location array for previous pixel values find out the difference between present pixel value and previous pixel value. If this difference is less than 3 then take location from group B.

In this technique secret key is used to embed secret watermark data as image and audio as per equations (6) and (7).

$$P = f(x, y) - f'(x', y') > 9 \tag{6}$$

$$P = D > 9 \tag{7}$$

where $D = f(x, y) - f'(x', y')$, P is EC of the watermarked frame of video and $f(x, y)$ is the original pixel values of the video frame and $f'(x', y')$ is the pixel value of selected frames of watermarked video.

- c. If the difference is greater than 3 then take locations from group A sequentially. Here for 173, 174, 177 we got same location 3 in group B. But $f(x, y) - f'(x', y') = |177 - 173| > 3$, thus for 177 take location from group A as per location array (f) and generated key structure-1 as shown in array (g).

67	67	70	68	1	65	69	66	71	72
----	----	----	----	---	----	----	----	----	----

(f) Location array: groups A and B

$n^2 + 3$	$n^2 + 3$	$n^2 + 6$	$n^2 + 4$	1	$n^2 + 1$	$n^2 + 5$	$n^2 + 2$	$n^2 + 7$	$n^2 + 8$
-----------	-----------	-----------	-----------	---	-----------	-----------	-----------	-----------	-----------

(g) Key structure 1

- 11 Change pixel values of the video frame block

Block (location) = image part (I) for with pixel value.

143	61	174	159	78	166	133	103	173	10
-----	----	-----	-----	----	-----	-----	-----	-----	----

(h) Embedded frame block

- 12 Convert the locations found in step 10 with respect to that particular frame to come in accordance with rest of the frame and copy this 64×64 embedded frame block into respective video frame, hence the modified location-based key structure-2 as shown in array (i) is used to reconstruct the secret watermark from watermarked video.

$3 + n^2$ + m	$3 + n^2$ + m	$6 + n^2$ + m	$4 + n^2$ + m	1 + m	$1 + n^2$ + m	$5 + n^2$ + m	$2 + n^2$ + m	$7 + n^2$ + m	$8 + n^2$ + m
------------------	------------------	------------------	------------------	-------	------------------	------------------	------------------	------------------	------------------

(i) Key structure 2

where m is the number of pixels before 64×64 block in a 1D array.

- 13 Repeat all the above steps for watermark image block of all three planes (R, G, B) for embedding the secret watermark data.

Extraction

- 1 Take the watermarked video. Convert the pixel matrices into 1D arrays as shown.
- 2 Access the file with location values of each frame. This file contains the locations of R, G, B plane of each frame obtained from embedding algorithm.

143	61	174	159	78	166	133	103	173	10
-----	----	-----	-----	----	-----	-----	-----	-----	----

(j) Embedded frame block

- 3 By using key structure-2, extract image pixels from the watermarked frame array as shown in array (k).

174	174	166	159	145	143	78	61	103	173
-----	-----	-----	-----	-----	-----	----	----	-----	-----

(k) Extracted watermark image array

This 1D array is converted into 2D matrix. Combine all 64 parts (8x8) to form complete extracted image (64x64).

173	174	166	159	177	143	78	61	-	-	-	-
-----	-----	-----	-----	-----	-----	----	----	---	---	---	---

(l) Original watermark image array

3 Key security parameters and its importance

3.1 Structural similarity index module and cross correlation factor

Structural similarity index and cross correlation factor are used to find the similarity between original video and watermark video which found to be similar to each other. Hence the proposed technique is more secured (Chimanna and Khot, 2013; Shojanazeri et al., 2013; Gangarde and Chitode, 2017). In the proposed algorithm the maximum value of PSNR is 57.21 dB, SSIM is 0.99, CCF is 1 without any type of attack and minimum value of PSNR is 57.01 dB, SSIM is 0.99, CCF is 1 with different types of attack, hence the proposed technique maintain SSIM and CCF values almost same, which indicate the proposed technique is more robust than any other existing technique. SSIM and CCF values are obtained as per in equations (8) and (9)

$$SSIM = \frac{(2\beta_x\beta_y + a_1)(2K_{xy} + a_2)}{(\beta_x^2 + \beta_y^2 + a_1)(K_x^2 + K_y^2 + a_2)} \quad (8)$$

where β_x and β_y are the average of x and y respectively, K_{xy} is the covariance of x and y , a_1 and a_2 are two variables to stabilise the division with weak denominator

$$CCF = \frac{1}{n} \sum_{x,y} \frac{(f(x,y) - \bar{f})(t(x,y) - \bar{t})}{m_f m_t} \quad (9)$$

where n is the number of pixels, $t(x,y)$ and $f(x,y)$ is the standard deviation of f . It measures immunity of watermark against to remove or degrade it. Maximum normalised correlation indicates better robustness (Jiang et al., 2015).

3.2 PSNR and MSE

PSNR is most commonly used to measure the quality of reconstruction of original cover video and watermark secret data. Its typical range is 35 dB to 70 dB. A higher the value of PSNR generally indicates that the reconstruction is of better quality, which can be calculated using equation (10) (Jiang et al., 2015; Moon and Raut, 2015).

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (10)$$

where MAX is the maximum pixel value of the image.

Table 1 Security measures for .avi, .flv, .mp4 video formats and .png, .bmp image formats (see online version for colours)









Video format	Secret data	Attacks	Quality/security metric	Watermark image			Video		
				Original vs. extracted	Original vs. attacked	Extracted vs. attacked	Original vs. attacked	Original vs. concealed	Concealed vs. attacked
.avi 360 × 470		Frame cropping	PSNR(dB)	57.21	57.01	56.12	56.35	54.18	54.00
			SSIM	0.98	0.99	0.99	0.99	0.99	0.99
		Swapping	PSNR(dB)	55.04	54.18	54.06	55.21	53.14	53.00
			SSIM	0.97	0.99	1	0.99	0.99	0.99
.flv 360 × 480		Frame replacement	PSNR(dB)	55.01	54.54	53.51	54.21	52.95	53.01
			SSIM	1	0.97	0.97	0.99	1	0.99
		Reverse rotate	PSNR(dB)	0.98	0.99	0.99	1.00	1.00	1.00
			SSIM	54.32	54.10	52.28	56.21	53.41	54.41
.avi 360 × 470		Poisson	PSNR(dB)	0.98	0.97	0.97	0.99	0.99	0.99
			SSIM	1	0.99	1	1.00	0.99	0.99
		Gaussian	PSNR(dB)	53.20	51.99	52.02	55.13	54.88	54.09
			SSIM	0.99	0.99	0.99	0.99	0.94	0.94
.mp4 320 × 460		Salt and pepper	PSNR(dB)	0.99	0.99	1.00	1.00	1.00	1.00
			SSIM	56.28	55.30	55.19	57.21	55.99	54.00
		Histogram	PSNR(dB)	0.97	0.99	0.99	0.99	0.99	0.99
			SSIM	0.95	0.99	0.99	1.00	1.00	1.00
.avi 680 × 460		Frame cropping	PSNR(dB)	54.06	53.13	52.20	56.21	55.68	54.89
			SSIM	0.96	0.99	0.99	0.99	1	0.99
		Salt and pepper	PSNR(dB)	1	0.99	0.99	1.00	1.00	1.00
			SSIM	53.47	52.02	51.79	54.21	52.95	53.95
.flv 680 × 640		Frame cropping	PSNR(dB)	0.91	0.93	0.93	0.99	0.97	0.97
			SSIM	0.98	0.98	0.98	1.00	0.99	0.99
		Salt and pepper	PSNR(dB)	53.45	52.40	51.99	53.26	52.89	52.02
			SSIM	1	0.99	0.99	0.99	0.99	0.99
.mp4 320 × 460		Poisson	PSNR(dB)	52.90	51.96	52.02	51.69	50.92	51.62
			SSIM	0.99	0.99	0.99	1.00	0.99	0.99
		Gaussian	PSNR(dB)	0.92	0.99	1	1.00	1.00	1.00
			SSIM	52.81	50.33	51.01	50.99	50.12	51.099
.avi 360 × 470		Salt and pepper	PSNR(dB)	0.98	0.97	0.97	0.99	0.99	0.99
			SSIM	1	0.99	0.99	1.00	1	0.99
		Gaussian	PSNR(dB)	53.52	52.22	49.69	52.30	51.22	50.89
			SSIM	1	0.99	0.99	1.00	1.00	1.00

Table 2 Comparison results between different methods without any attack

Image	PSNR			SSIM			CCF		
	Proposed method	Method of Su and Chen (2018)	Method of Das et al. (2014)	Proposed method	Method of Su and Chen (2018)	Method of Das et al. (2014)	Proposed method	Method of Chen (2018)	Method of Su and Das et al. (2014)
Pepper	57.21	50.08	41.01	0.99	0.98	0.97	1.0000	1.00	1.00
Lena	56.71	49.98	41.78	0.99	0.98	0.97	1.0000	1.00	1.00
Baboon	56.36	49.89	40.24	0.99	0.99	0.98	1.0000	1.0	1.00
Avion	56.28	49.86	40.79	0.98	0.98	0.98	1.0000	1.00	1.00

MSE (Shojanazeri et al., 2013) is the sum over all squared value differences divided by image size, determined by equation (11).

$$MSE = \frac{1}{MN} \sum_{mn} (P(m, n) - Q(m, n))^2 \quad (11)$$

where $P(m, n)$ and $Q(m, n)$ represents two images and M and N represents the total number of pixels of secret frame of video and secret watermark data.

3.3 EC and embedding rate analysis

It is one of the important security parameter in any type of watermarking technique. The number of pixel values of cover data is used to watermark the secret data (Cox et al., 2008; Moon and Raut, 2015). In this paper, capacity of the watermark secret image is calculated by embedding rate (ER). The ER is described in bit per pixel (bpp). Suppose the cover frame size is $360 \times 470 \times 8 = 1,353,600$ bits and watermark secret image used for embedding with size 256×256 , which is subdivided into four equal parts, hence EC is $64 \times 64 \times 8 = 32,768$ bits for a given frame size. The convert video frame size is 360×470 , so total available bits are $360 \times 470 \times 8 = 1,353,600$ bits minus used bits, i.e., 32,768 hence unused bits are 1,320,832 bits and calculated ER is $(32,768) / (1,353,600) = 0.0242$ bpp. which is higher than method of Su and Chen 2018 (ER = 0.0013 bpp) and Das et al. (2014) (ER = 0.0156 bpp). It shows that the ER and EC is higher than existing watermarking algorithm due to watermark image subdivision before embedding it into selected frame of video. The EC obtained as per equation (12).

$$EC = \frac{\text{Embedding watermark size}}{\text{Host image size}} \quad (12)$$

4 Simulation results and its analysis

The proposed technique is verified through the number of simulation results on a standard data base of video like .avi, .flv, .mp4 with more than thousand frames of size 720×640 , 640×420 , 512×512 , 620×480 , etc. Different types of secret watermark images like .bmp, jpeg, .tiff of size 256×256 , 128×128 , 64×64 and 32×32 with good resolution. The obtain simulation result is verified by personal computer Intel Core (TM) i5 processor, CPU at 2.5GHz, 8GB RAM, Windows 7, MATLAB 2014(R2014a, 64 bits). As before embedding the secret watermark data is converted into the number of equal parts and every part is embedded into randomly obtained frames of video, EC, ER, Security of hidden secret data is increased. To evaluate the result, the proposed approach considers .avi video format of size 360×470 with frame number of 1,140. The secret watermark image as a fruit (.png 64×64) with a good quality of resolution as a secret data. The proposed technique obtains the key security measurement parameter of value PSNR = 57.21 dB of original video, PSNR = 57.01 dB of watermarked video and 57.12dB of extracting video with an ER = 2.42 bpp, and EC = 32768 bits, SSIM = 1, CCF = 1, MSE = 0.04, BER = 0.3 by applying different attack. With many attacks on

watermark video the key security parameters does not deviate their obtained values which indicate the proposed technique can tolerate any type of manipulation during transmission of watermark video as indicate in Table 1. Table 2 shows the comparison between Su and Chen (2018), Das et al. (2014) and the suggested APLM algorithm in terms of PSNR, CCF and SSIM. As we have divided the secret watermark image into predefined number of physical parts and embed each part into selected frames of the video. Hence it is not easy to recognise the embedded watermark from watermarked video.

4.1 Imperceptibility through CCF and SSIM

The imperceptibility of proposed algorithm has observed with different images as secret watermark information and it indicates that PSNR of proposed is 57.21 dB, which is higher than existing watermarking methods. It applied different video processing attacks to check the performance of proposed video watermarking methods in terms of CCF and SSIM. The proposed method (APLM) has CCF = 1 which shows that the suggested method is more robust and secured than any other existing video watermarking algorithms as shown in Table 3.

Table 3 Comparison results between different methods with attacks

<i>Different attacks</i>	<i>Cross correlation factor (CCF)</i>			
	<i>Proposed method (APLM)</i>		<i>Method of Su and Chen (2018)</i>	<i>Method of Das et al. (2014)</i>
	<i>CCF</i>	<i>SSIM</i>	<i>NC</i>	<i>NC</i>
Salt and pepper	1.00	0.99	1.00	0.80
Gaussian	1.00	0.98	1.00	0.96
Frame replacement	1.00	1.00	0.99	0.98
Frame reverse rotate	0.99	0.99	0.78	0.69
Frame cropping	1.00	0.98	---	---
Frame swapping	0.99	0.99	---	---
Histogram equalisation	1.00	1.00	---	---
Poisson	1.00	1.00	---	---

4.2 Robustness through EC and ER

The proposed approach verifies the existing algorithms on image watermarking which has a less EC, ER and security of secret watermark data. Su and Chen (2018) applied spatial domain watermarking technique for RGB image as a secret date where secret data are split into four equal parts using DC coefficient pixel values of cover image having the value of PSNR = 49.95 dB which provide less security and low EC of 0.0013 bpp. The Su et al. applied spatial domain watermark technique to embed secret watermark image size 32×32 with an ER of 0.0013 bpp having total processing time of value 5.99 s while

Das et al. (2014) applied DCT domain watermark technique with secret watermark size 64×63 having ER 0.0154 bpp with total average time of 6.94 s. In the suggested approach pixel domain APLM algorithm technique is proposed for different secret watermark sizes of 32×32 , 64×64 , 128×128 , 256×256 having embedding rate 0.0313, 0.125 bpp and embedding capacity of value 768, 3072 bits respectively with average processing time 5.1 s and standard deviation of 0.457. But the proposed technique is applicable for video watermarking where the secret data is divided into n equal parts and every part is embedded into randomly obtained frames of video using APLM technique. Hence the value of ER = 0.0242 bpp and EC = 32768 bits is enhanced as shown in Table 4. With dimensions of 64×64 , 32×32 , etc. The image has more natural colours to test the system with most of the possible colour components as shown in Figure 4(a). Embedded the secret data into video frames by obtaining the difference of pixels of the cover frame of video and secret watermark data as per equations (6) and (7) for different values of P. When P = 1, PSNR = 56.41 dB for secret Lena image of size 128×128 , CCF = 1 and SSIM = 1, while for audio secret data (.mp3), the value of PSNR = 53.87 dB, CCF = 1 and SSIM = 1, hence we have recovered good quality of cover video as well as secret data. But as the value of P is increase, the key security (Kumar et al., 2015) parameters PSNR, CCF and SSIM start to decrease. When P = 9, the PSNR = 29.12 dB for image and PSNR = 30.01 dB for audio with CCF = 0.81 and SSIM = 0.77. It indicates that when P = 9, we can not recovered cover video and secret data, hence P = 9 is the threshold value of the proposed system as shown in Table 5. Figure 13 gives the comparison of PSNR values for different images with two existing watermark technique and proposed technique. It is observed that the presented approach has better PSNR as compared to two existing techniques. Figure 14 indicate the comparison of NC values of the proposed technique with two existing watermarking techniques while Figure 15 comparison of SSIM values of proposed technique with two existing watermarking techniques. It is found that the proposed approach has significant values of CCF and SSIM as compared to two existing techniques. The following video named as Go_Bwaaah_3_SECOND_VIDEO_.Avi is taken to analyse the system. It has a total of 973 frames and the embedding work is done on first 64 frames of the video. The video frames have a dimension of 360x470 as shown in Figure 4(b), Figure 4 (c)–(e) indicates watermarked video, attacked video frame and original and recovered audio spectrogram.

Table 4 Functionality comparison with different techniques

Embedding techniques	Domain	Secret watermark image size	ER (ER) (bpp)	EC (EC) (bits)	Total time	
					Average value	Standard variation
Proposed technique (APLM)	Pixel domain	32×32	0.0313	768	5.1022	0.0957
		64×64	0.125	3072		
Su and Chen (2018) technique	Spatial domain	32×32	0.0013	---	5.9972	0.0871
Das et al. (2014)	DCT domain	64×63	0.0154	---	6.9478	0.0507

Figure 4 (a) Original video frame (b) Watermark image (c) Watermarked video frame (d) Attacked video frame (e) Original and recovered audio spectrogram (see online version for colours)



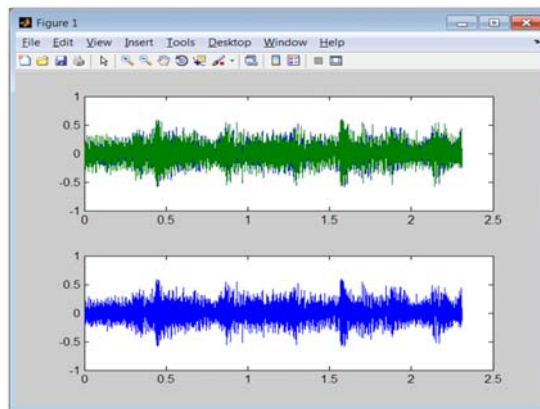
(a)

(b)



(c)

(d)



(e)

Table 5 Result obtained for PSNR, CCF, SSIM for different values of P

<i>Video</i>	<i>P</i>	<i>Image</i>	<i>PSNR(dB)</i>	<i>Audio</i>	<i>PSNR(dB)</i>	<i>CCF</i>	<i>SSIM</i>
.avi 620 × 480 of 970 frames	1	Lena 128	56.41	.mp3	53.87	1	1
	2	× 128	54.17	78,943 samples	50.03	0.99	0.99
	3		50.89		47.68	0.97	0.98
	4		44.36		44.23	0.96	0.97
	5		42.87		42.39	0.93	0.92
	6		39.02		38.03	0.91	0.89
	7		36.18		35.86	0.89	0.87
	8		33.56		33.29	0.85	0.83
	9		29.12		30.01	0.81	0.77

5 System performance through different types of attacks on watermarked video

5.1 Frame cropping

The frame cropping attack is carried out by cropping the desired frame of the watermarked video. This cropping is customisable i.e. the part of the frame to be cropped from each side can be decided. Cropping deletes most of the pixels from all three planes (R, G, B) of the affected frame (Arab and Hashim, 2016; Dadi et al., 2013). To analyse the proposed method the first frame of the video embedded with watermark is cropped and a video is formed with such a cropped frame as shown in Figures 5(a)–(c).

5.2 Frame swapping

To check the robustness of the proposed technique against the order of frames in a video this attack is taken into consideration (Jiang et al., 2015; Ahuja and Bedi, 2017). To verify frame swapping attack the 27th and 40th frames of the watermarked video are swapped with one another. This will lead to the placing of wrong images in the final extracted image. But as the images are small they do not affect the quality of the final image to much extent as shown in Figures 6 (a)–(c).

5.3 Frame replacement

This image has been modified to fit to the dimensions and the resolution of the video and is then replaced with the 90th frame of the video. Thus, the image part is now extracted from this image placed in the video (Arab and Hashim, 2016; Ahuja and Bedi, 2017). The effect of this extraction will entirely depend on the similarity of the image with the rest of the frames and also on the size of the part to be extracted as displayed in Figure 7 (a)–(c).

Figure 5 Watermark images and attacked video with frame cropping attack, (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)



(a)

(b)



(c)

Figure 6 Watermark images and attacked video with frame swapping attack, (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)



(a)

(b)

Figure 6 Watermark images and attacked video with frame swapping attack, (a) original frame (b) attacked frame (c) recovered watermark (continued) (see online version for colours)



(c)

Figure 7 Watermark images and attacked video with frame replacement attack, (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)



(a)



(b)



(c)

5.4 *Frame reverse rotate*

This attack rotates the selected frame clockwise with a specified degree of angle and again reverse rotates with specified angle (Arab and Hashim, 2016; Narkhedamilly et al., 2015). This process affects the pixel values of the frame in all the three planes, i.e., R, G, B. The prominent effect is that of misplacing of the pixel values which eventually will affect the formation of an image during extraction as shown in Figures 8(a)–8(c).

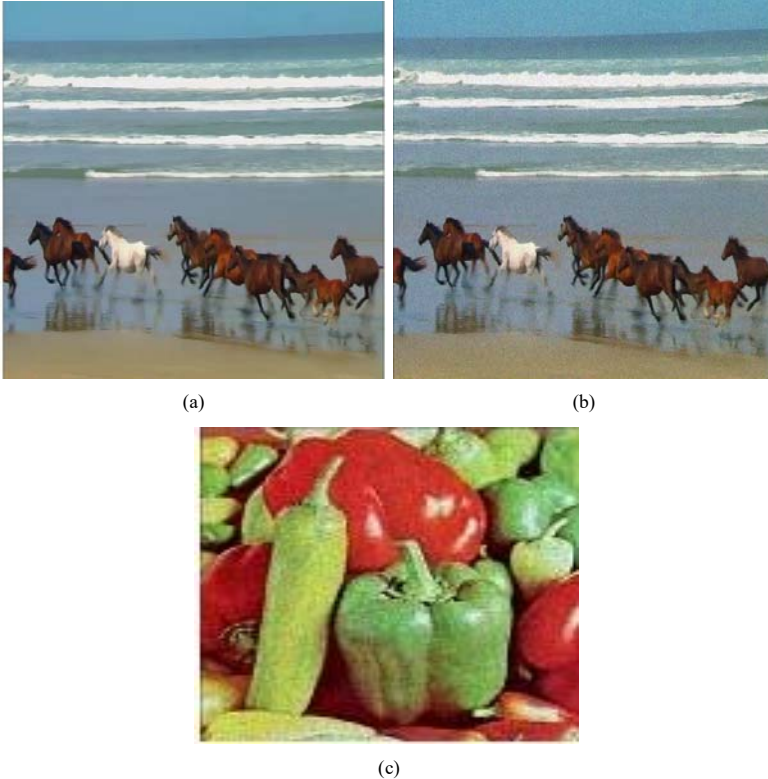
Figure 8 Watermark images and attacked video with frame rotation attack, (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)



5.5 *Poisson attack*

In Poisson type attack, some noise is added into pixel values of a watermark frame of video. This attack is added as a noise on a finite number of frames and extracted watermark image after attack (Arab and Hashim, 2016) as shown in Figures 9(a)–9(c).

Figure 9 Watermark images and attacked video with Poisson attack, (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)



5.6 Gaussian attack

The attack is applied only on selected frames of the watermarked video (Arab and Hashim, 2016; Moon and Raut, 2015; Kumar et al., 2015). It is applied as a process of adding noise to the frames and the intensity of the noise can be varied by changing the mean and the variance of the noise and watermark extracted which shown in Figures 10(a)–10(c) by applying Gaussain attack, the key security parameter does not change or deviate its obtained value.

5.7 Salt and pepper attack

An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions. As the above two attacks this attack too is applied to the selected frames of the video embedded with watermark (Su and Chen, 2018; Gangarde

and Chitode, 2017; Moon and Raut, 2015). The intensity of the attack can be controlled by the parameter called as noise density. The more the density more is the effect visible in the frames as shown in Figures 11(a)–11(c).

5.8 Histogram equalisation

In the proposed method histogram equalisation is obtained for selected frame of cover video, watermarked frame of video and recovered secret watermark image which is found to be identical to each other, hence the proposed technique provided more resistance against histogram equalisation attack (Moon and Raut, 2015) as shown in Figures 12(a)–12(c).

Figure 10 Watermark images and attacked video with Gaussian attack, (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)

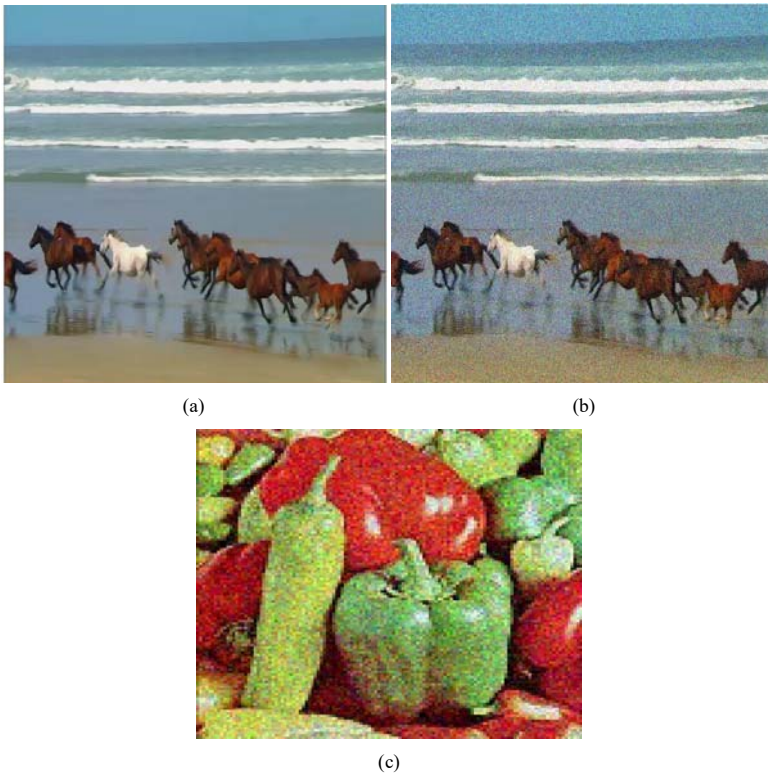


Figure 11 Watermark images and attacked video with salt and pepper attack (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)

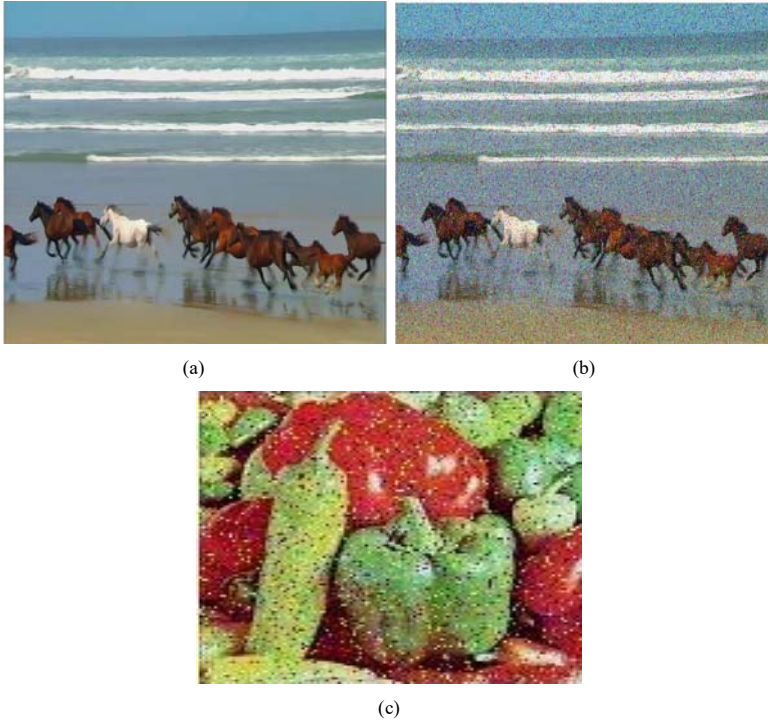


Figure 12 Watermark images and attacked video with histogram equalisation attack (a) original frame (b) attacked frame (c) recovered watermark (see online version for colours)



Figure 12 Watermark images and attacked video with histogram equalisation attack (a) original frame (b) attacked frame (c) recovered watermark (continued) (see online version for colours)



(c)

Figure 13 Comparison of PSNR values of proposed technique with two existing watermarking techniques (see online version for colours)

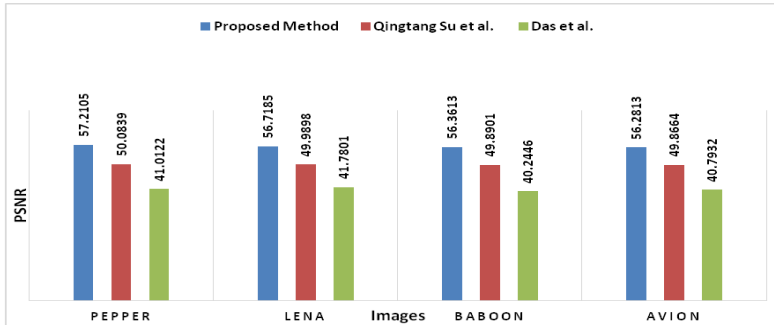


Figure 14 Comparison of CCF values of proposed technique with two existing watermarking techniques (see online version for colours)

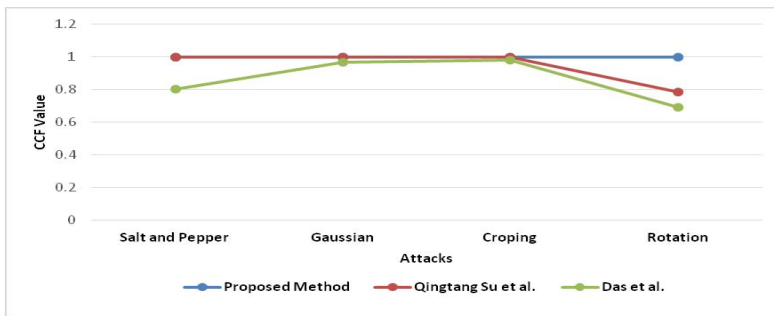
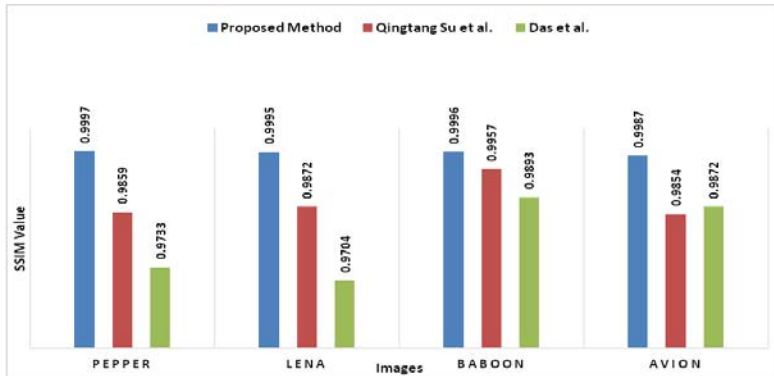


Figure 15 Comparison of SSIM values of proposed technique with two existing watermarking techniques (see online version for colours)



6 Conclusions

This paper proposes authenticate audio, video-crypto invisible watermarking approach for enhancing hidden information security and robustness using APLM approach. We achieve high level information security and a degree of imperceptibility of hidden watermark data, cover video and watermarked video. The cross correlation factor and structural similarity index module have factor value is equal to 1. Hence the proposed system recovered cover video, secret data and recovered video without any loss of information. With experimental results shows that PSNR, MSE, CCF, SSIM are in proper proportion. Robustness of the proposed technique is increased due to a number of attacks have applied on watermarked video during transmission. In future any suitable algorithm and different secret data formats can be implemented for the same approach.

References

- Ahuja, R. and Bedi, S.S. (2015) 'Copyright protection using blind video watermarking algorithm based on MPEG-2 structure', *International Conference on Computing, Communication & Automation*, Noida, IEEE, pp.1048–1053.
- Ahuja, R. and Bedi, S.S. (2017) 'Video watermarking scheme based on candidates i-frames for copyright protection', *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 5, No. 2, pp.391–400.
- Arab, F. and Hashim, A. (2016) 'A robust video watermarking technique for the tamper detection of surveillance systems', *Springer Journal on Multimedia Tools Application*, Vol. 75, No. 18, pp.10855–10885.
- Bhattacharya, S., Chattopadhyay, T. and Pal, A. (2006) 'A survey on different video watermarking techniques', *International Symposium on Consumer Electronics*, IEEE.

- Chimanna, M.A. and Khot, S. (2013) 'Robustness of video watermarking against various attacks using wavelet transform techniques and principle component analysis', *International Conference on Information Communication and Embedded Systems, ICICES*, IEEE, pp.613–618.
- Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J. and Kalker, T. (2008) 'Digital watermarking and steganography', *Morgan Kaufmann Series in Multimedia Information and Systems*, 2nd ed., Elsevier, Burlington, MA01803, USA.
- Dadi, H.S., Sarva, N.K., Lakshmi Sunitha G. and Harish, V.S.V. (2013) 'Robust video watermarking algorithm using discrete wavelet transform', *International Journal of Emerging Technology and Advanced Engineering, IJETAE*, Vol. 3, No. 5, pp.360–366.
- Das, C., Panigrahi, S., Sharma, V.K. and Mahapatra, K.K. (2014) 'A novel blind robust image watermarking in DCT domain using inter block coefficient correlation', *International Journal of Electronics and Communications, IJEC*, Vol. 68, No. 3, pp.244–253.
- Gangarde, M.A. and Chitode, J.S. (2017) 'Application of crypto-video watermarking technique to improve robustness and imperceptibility of secret data', *Fourth International Conference on Image Information Processing (ICIIP)*, IEEE, pp.579–584.
- Giri, K.J. and Bashir, R. (2017) 'Digital watermarking: a potential solution for multimedia authentication', *Intelligent Techniques in Signal Processing for Multimedia Security*, Vol. 660, pp.93–112, Springer.
- Jiang, D.Y., Li, D. and Kim, J.W. (2015) 'Spread spectrum zero video watermarking scheme based on dual transform domains and log polar transformation', *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 10, No.4, pp.367–378.
- Kumar, R., Shaw, D.K. and Alam, M.J. (2015) 'Experimental studies of LSB watermarking with different noise', *Eleventh international Multi-Conference on Information Processing*, Vol. 54, pp.612–620, Elsevier.
- Moon, S.K. and Raut, R.D. (2015) 'Efficient performance analysis of data hiding technique for enhancement of information security, robustness and perceptibility', *International Journal of Electronic Security and Digital Forensics*, Vol. 7, No. 4, pp.305–329, Inderscience.
- Narkhedamilly, L., Evani, V.P. and Samayamantula, S.K. (2015) 'Discrete multiwavelet-based video watermarking scheme using SURF', *Electronics and Telecommunication Research Institute Journal, ETRI*, Vol. 37, No. 3, pp.595–605.
- Sadek, M.M., Khalifa, A.S. and Mostafa, M.G.M. (2014) 'Video steganography: a comprehensive review', *Multimedia Tools Application, Springer Science Journal*, Vol. 17, No. 74, pp.1–32.
- Shojanazeri, H., Adnan, W.A.W. and Ahmad, S.M.S. (2013) 'Video watermarking techniques for copy right protection and content authentication', *International Journal of Computer Inforamtion System and Industrial Management Applications*, Vol. 5, No. 1, pp.652–660.
- Sowmya, K.N. and Chennamma, H.R. (2017) 'Video authentication using digital signature – a study', *First International Conference on Computational Intelligence and Informatics*, Vol. 507, pp.53–64, Springer.
- Sridhar, B. and Arun, C. (2016) 'An enhanced approach in video watermarking with multiple watermarks using wavelets', *Journal of Communications Technology and Electronics*, Vol. 61, No. 2, pp.165–175.
- Su, Q. and Chen, B. (2018) 'Robust color image watermarking technique in the spatial domain', *Soft Computing – A Fusion of Foundation, Methodology and Applications*, Vol. 22, No. 1, pp.91–106, Springer.
- Subhedar, M. and Mankar, V.H. (2014) 'Current status and key issues in image steganography: a survey', *Elsevier Science Review Journal*, Vol. 13, No. 14, pp.95–113.