ISSN XXXX XXXX © 2016 IJESC

Research Article Volume 6 Issue No. 12

Tampering Detection for Encrypted Compressed Video Watermarking Using Bit Substitution for Copy Right Protection

M. Ramya Devi[1], P.Suneetha[2]
PG Scholar[1], Associate Professor[2]
Department of Electronics and Communication Engineering
Vignan's Institute of Information and Technology, Vizag, India

Abstract:
The project presents that data hiding and logo watermarking in encrypted compressed video bit streams, for privacy information like binary watermark to protect videos during transmission or cloud storage. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. Data hiding and embedding watermark approaches are necessary to perform in these encrypted videos for the purpose of content notation and tampering detection. Here, Data hiding and embedding watermark directly in the encrypted version of H.264/CAVLC video stream is approached, which includes the following three parts, i.e., H.264/CAVLC video encryption, watermark embedding, data embedding, watermark extraction and data extraction. By analyzing the property of H.264 codec, the code words of intra prediction modes, the code words of motion vector differences, and the code words of residual coefficients are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using bits wrapping technique, without knowing the original video content. Arnold transform is used here to scramble/descramble the secret watermark before/after data embedding/extraction. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. The simulated results shows that used methods provides better performance in terms of computation efficiency ,high data security and video quality after decryption. The parameters such as Mean square error, PSNR, correlation and SSIM are evaluated to measure its efficiency.

I. INTRODUCTION:

The identification of objects in an image and this process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures. The clever bit is to interpret collections of these shapes as single objects, e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skilful programming and lots of processing power to approach human performance. Manipulation of data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, and is most familiarly represented by such patterns as those of a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer. Digital information revolution and the thriving progress in network communication are the major driving forces of this change. The perfect reproduction, the ease of editing, and the Internet distribution of digital multimedia data have brought about concerns of copyright infringement, illegal distribution, and unauthorized tampering. Techniques of associating some imperceptible data with multimedia sources via embedding started to come out to alleviate these concerns. Interestingly, while most such techniques embed data imperceptibly to retain the perceptual quality and value of the host multimedia source, many of them were referred as digital watermarking whose traditional counterpart is not necessarily imperceptible.

Cryptography and Steganography

Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden.

Information to be hidden + cover object = stego object.

To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A stego object is one, which looks exactly same as cover object with an hidden information.

II. PROBLEM STATEMENT:

The goals for this Project have been the following. One goal has been to compile an introduction to the subject of steganography and watermarking. There exist a number of studies on various algorithms, but complete treatments on a technical level are not as common. Material from papers, journals, and conference proceedings are used that best describe the various parts. Another goal has been to search for algorithms that can be used to implement for the detection of steganographic and watermarking techniques. A third goal is to evaluate their

performance of with different image quality metrics. These properties were chosen because they have the greatest impact on the detection of steganography algorithms A final goal has been to design and implement the Data and watermarking detector in MATLAB[2].

III. BLOCK DIAGRAM:

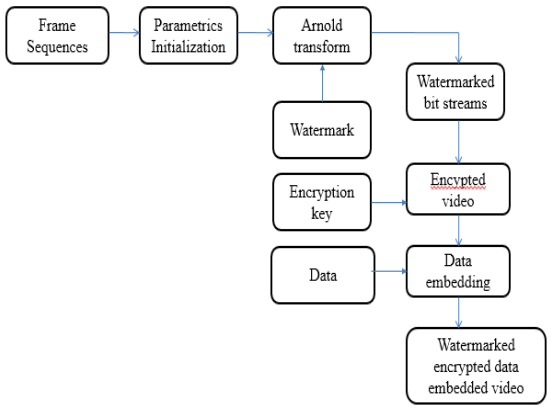

Figure.1. Block Diagram: Video Encryption, Data Hiding and watermarking

Digital Watermarking:-

We would normally like to increase the energy of the watermark (or payload of the watermark) in order to increase its robustness. However, increasing the payload of the watermark degrades the visual quality of the image such that human eye will notice the degradation. A dual reasoning leads us to think that it might be better to increase the payload of the watermark by embedding the watermark bits into places where human eye will not detect the changes to the image. Several watermarking schemes were proposed by researchers that aim to exploit the characteristics of the human visual system. For example, suggests to make the gain factor luminance dependent. This is because of the fact that Human Visual System (HVS) is less sensitive to changes in regions of high luminance. We can exploit this property by increasing the payload (energy) of the watermark in those specific areas.

Logo Image:

Figure.1. logo image

IV. ARNOLD TRANSFORM:

We can create a mask image that consists of those areas that are less sensitive to distortions and modulate the watermark bits using this mask image.By using Arnold transform we can embed the watermark logo. The following equation explains the Arnold transform.

WI(i,j) = I(i,j) + Mask(i,j).k.W(i,j)

W is the watermark pattern (image), k is the gain factor, and Mask is the mask image as mentioned above. In my implementation, I generate the Mask image using an edge detection algorithm. I convert the edge image into a binary image. I amplify the effect of watermark bits by k on pixels where edge image is '1' and keep the effect of the watermark bits minimal on pixels where edge image is '0'. This increases the energy of the watermark along the edges in the image. I use the canny edge detector to extract the edge information out of the image.

Logo Image or QR Image:-

QR codes or Quick Response code is a two-dimensional barcode and has been designed way back in 1994 by the Japanese Company to track the vehicles produced during the automobiles manufacturing. Having a faster scanning response, the QR codes find its way to the public life easily. The code consists of black modules (square dots) arranged in a square grid on a white background, and can be of practically of size which is totally dependent on the designing of the user. The applications popular these days are in Intelligent Advertisement and in the field of Real Estates. Other applications which can be effective with the QR codes are.

- Stamps
- Business Cards
- Banners
- Website Down able

Figure.3. QR Image

VIDEO:-

Frame processing is the first step in the background subtraction algorithm, the purpose of this step is to prepare the modified video frames by removing noise and unwanted object's in the frame in order to increase the amount of information gained from the frame and the sensitivity of the algorithm.The following flow chart explains the step wise implementation of our video encryption.

Flowchart:

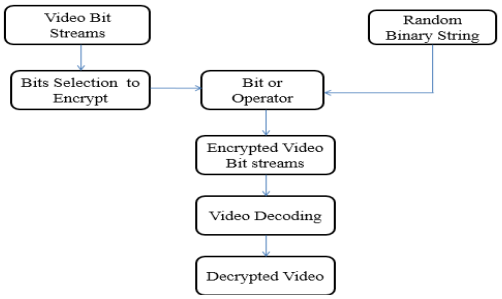

Figure.4. Input videos

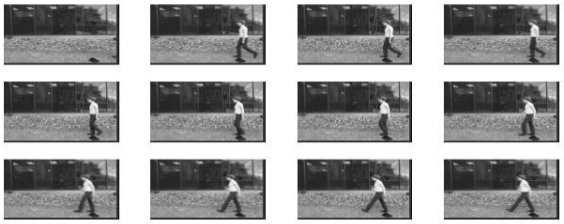

Figure.5. Frame Separations for Input Video

Pre-processing is a process of collecting simple image processing tasks that change the raw input video info a format. This can be processed by subsequent steps. An Input Video **(.avi files)** is converted into still images for processing it and to detect the moving objects. These sequences of images gathered from video files by finding the information about it through **'aviinfo'** command. These frames are converted into images with help of the command **'frame2im'** Create the name to each images and this process will be continued for all the video frames. H.264 divides the sequence of frames into several group of pictures (GOPs). These frames are labeled as I (intra), P (predicted), and B (bidirectionally predicted) frames. At the source part, each frame is divided into non overlapping blocks of uniform size (i.e., 16×16 pixels) called macro blocks, and these macro blocks are handled uniquely depending on their types. Each macro block can be further divided into smaller blocks with 4×4 being the smallest possible block size. These macro blocks are subjected to discrete cosine transform (DCT), quantization, and entropy coding. First, the pixel values in a macro block are used in the DCT and quantization process. The quantized DCT coefficients are further utilized for dequantization and inverse DCT process for prediction and motion estimation purposes. In I-frame, the pixel values in a block are either coded directly by using coefficients in the transformed domain or predicted (i.e., intra-prediction) using neighboring blocks in the same frame to exploit the spatial redundancies within a frame. In P-frame, motion estimation (i.e., inter-prediction) between two frames can be implemented to take advantage of the temporal redundancies. For that, the previously encoded frame, which itself could be a motion compensated frame, is decoded and its prediction errors, if any, are decoded and added to the decoded frame for motion estimation purposes. There are two entropy coding methods are used to encode the quantized transform coefficients, namely, context-adaptive variable length coding (CAVLC) and context-adaptive binary arithmetic coding (CABAC).

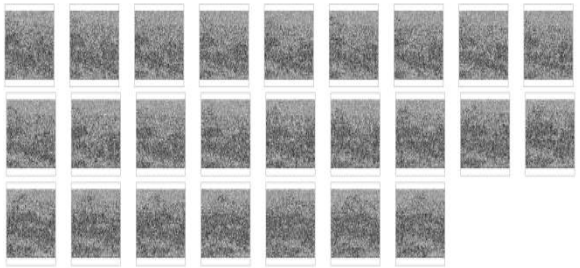

Figure.6. Encrypted Images (Frames)

Data and Logo Embedding:-

Data hiding is a process to conceal secret message bits into another medium like image, audio or video files.Here, the hiding is performed under compressed bit stream of cover image. After obtaining of bit streams, it is allowed to encrypt with random binary string using bitSubstitution operation.Before data hiding, the text message will be encrypted using bit Substitution to make second level security during transmission. The following algorithm depicts the data and logo hiding in selected video.

ALGORITHM:

Step1:Embed the watermark by using Arnold transform in encrypted bit streams

Step3: Select the data to hide and hide the data by using bit substitution method. In bit substitution method we are generating codeword's for given data and hiding them by using bit–xor operation. Bits wrap method is used here to conceal secret text bits under encrypted compressed bit streams. It is performed using logical bitwise operations like 'bitand' and 'bit-xor' operations. After hidden the data, image reconstruction and data extraction will be performed to measure the system performance. Logo is embedding by using Arnold transform. By applying logo bits directly to image may vary the image values. So that Arnold transform get the exact information without losing data in images and logo.

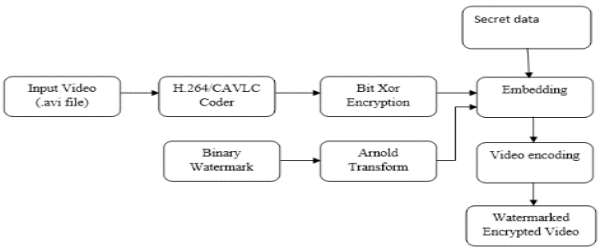

Figure.7. Data and Logo Recovery:-

At this stage, Secret hidden text messages are extracted from encrypted video streams followed by reconstruction of video frames. Hidden text bits are extracted using bitwise logical operators from the specific bit locations and the extraction of desired number of bits will be performed by using logical bitwise operators called 'bit and' and 'bitor'. Finally all extracted message characters are applied to Bit Substitution operation

decrypt the data with symmetric keys.Then the video bit streams are decoded using h.264 decoder to reconstruct the each encode frame and all the frames concatenated to form recovered original video. Logo is recovered by applying Arnold transform in reverse .Video quality will be measured using some parameters such as PSNR, SSIM and Correlation etc.

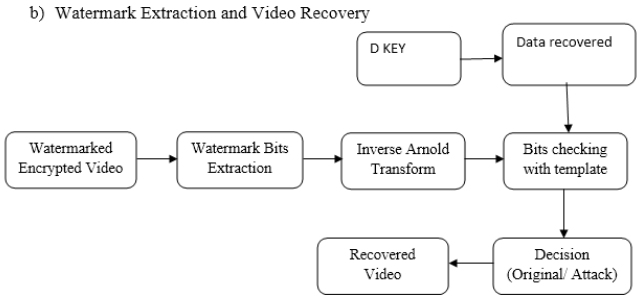

Figure.8. Block Diagram: Data Extraction and Video Decryption

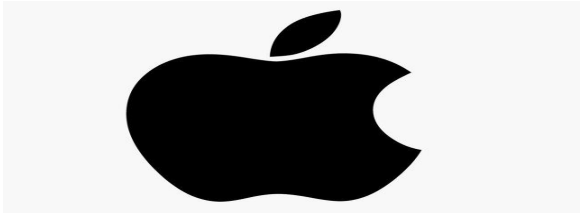

Figure.9. Recovered watermark logo

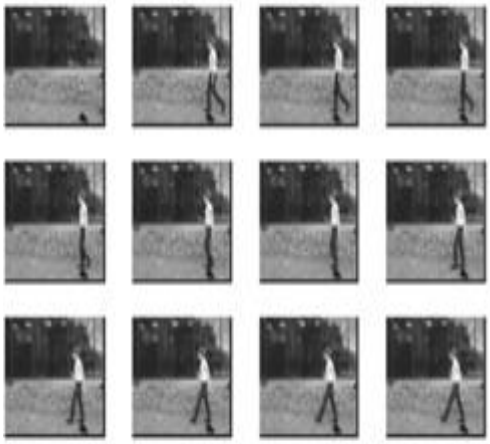

Figure.10. Recovered frames

S.No	Input Videos	Input 1			Input 2			Input 3		
QPValue	No. of frames	5	15	30	5	15	30	5	15	30
QP=16	Raw Input File Size(in Bytes)	126720	380160	760320	126720	380160	760320	126720	380160	760320
	Compressed File Size (in Bytes)	37283	102153	200555	13172	38496	74131	30470	86609	171517
	Compression Ratio	3.3988	3.7215	3.7911	9.6202	9.8753	10.2564	4.1588	4.3894	4.4329
	Maximum Capacity(Kbits/s)	91.9370	91.9370	91.9370	25.6540	25.6540	25.6540	59.8090	59.8090	59.8090

S.No	Input Videos	Input 1			Input 2			Input 3		
QPValue	No. of frames	5	15	30	5	15	30	5	15	30
QP=24	Raw Input File Size(in Bytes)	126720	380160	760320	126720	380160	760320	126720	380160	760320
	Compressed File Size (in Bytes)	21563	55986	108309	5966	17194	32754	15694	43470	85635
	Compression Ratio	5.8766	6.7903	7.0199	21.2399	22.1089	23.2128	8.0743	8.7453	8.8785
	Maximum Capacity(Kbits/s)	60.7740	60.7740	60.7740	14.6540	14.6540	14.6540	34.1620	34.1620	34.1620

S.No	Input Videos	Input 1			Input 2			Input 3		
QPValue	No. of frames	5	15	30	5	15	30	5	15	30
QP=34	Raw Input File Size(in Bytes)	126720	380160	760320	126720	380160	760320	126720	380160	760320
	Compressed File Size (in Bytes)	9090	21360	39440	2866	7413	13630	5076	13182	25712
	Compression Ratio	13.9404	17.7975	19.2775	44.2091	51.2820	55.7818	24.9615	28.8388	29.5699
	Maximum Capacity(Kbits/s)	30.2560	30.2560	30.2560	8.3320	8.3320	8.3320	13.9850	13.9850	13.9850

V. RESULT ANALYSIS:-

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio.

Mean Square Error:-

The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$MSE = \sigma_q^2 = \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance.

Peak Signal to Noise Ratio:-

The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\mathbf{PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)}$$

Table.1. Parameter values for different input videos and QP values

		QP = 16	QP = 24	QP = 34
Input 1	MSE	0.5839	3.1098	20.8667
	PSNR (dB)	50.4672	43.2035	34.9363
	Correlation	0.9998	0.9989	0.9922
	Residual diff	0.0478	0.1089	0.2803
	SSIM	0.9959	0.9815	0.9063
Input 2	MSE	0.2806	1.0174	4.4386
	PSNR (dB)	53.6496	48.0557	41.6584
	Correlation	1.0000	0.9999	0.9995
	Residual diff	0.0332	0.0636	0.1151
	SSIM	0.9939	0.9814	0.9581
Input 3	MSE	0.4912	2.2660	12.3776
	PSNR (dB)	51.2179	44.5782	37.2044
	Correlation	0.9998	0.9988	0.9938
	Residual diff	0.0441	0.0975	0.2194
	SSIM	0.9936	0.9726	0.8821

Figure.11. Bar graph of various parameters for different Qp values

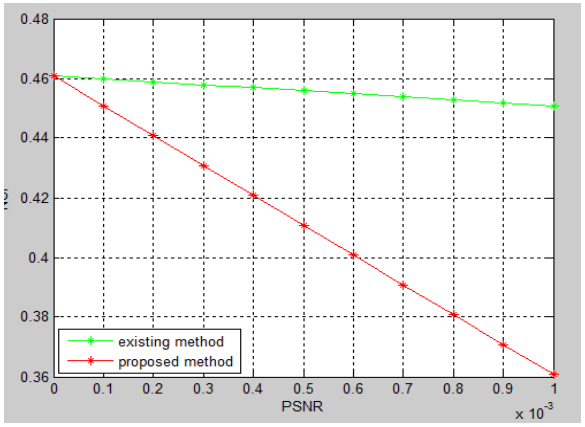

Figure.12. Comparison between PSNR and NSI for existing and proposed methods.

VI. CONCLUSION:

Data hiding and watermarking in encrypted media is a new topic that has started to draw attention because of the privacy-preserving requirements from cloud data management. In this paper, an algorithm to embed additional data in encrypted H.264/AVC bit stream is presented, which consists of video encryption, data embedding, logo watermarking and data, watermark extraction phases. The algorithm can preserve the bit-rate exactly even after encryption and data, watermark embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, since hiding is completed entirely in the encrypted domain, our method can preserve the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides two different practical applications. Another advantage is that it is fully compliant with the H.264/AVC syntax and the embed logo is used for copyright protection. Experimental results have shown that the proposed encryption, data and logo

embedding scheme can preserve file-size, whereas the degradation in video quality caused by hiding is quite small. Further we can implement by combination of cryptography, steganography and watermarking for high resolution videos.

VII. REFERENCES

[1] T. Y. Chung,M.S.Hong, Y.N. Oh, D.H.Shin, andS.H.Park, "Digital watermarking for copyright protection of MPEG2 compressed video," *IEEE Trans. Consum. Electron.*, vol. 44, no. 3, pp. 895–901, 1998.

[2] G. C. Langelaar and R. L. Lagendijk, "Optimal differential energy watermarking of dct encoded images and video," *IEEE Trans. Image Process.*, vol. 10, no. 1, pp. 148–158, Jan. 2001.

[3] B. G. Mobasseri, "Watermarking of MPEG-2 video in compressed domain using VLC mapping," in *Proc. 7th ACMWorkshopMultimedia and Security Int. Multimedia Conf., MM-SEC '05*, New York, NY, USA, Aug. 2005, pp. 91–94.

[4] D. Zou and J. Bloom, "H.264/AVC substitution watermarking: A CAVLC example," in *Proc. SPIE, Media Forensics and Security*, San Jose, CA, USA, Jan. 2009, vol. 7254.

[5] D. Zou and J. Bloom, "H.264 stream replacement watermarking with CABAC encoding," in *Proc. IEEE Int. Conf. Multimedia and Expo, ICME '10*, Singapore, Jul. 2010.

[6] M. Noorkami and R. M. Mersereau, "A framework for robust watermarking of H.264 encoded video with controllable detection performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 14–23, Mar. 2007

[7] M. Noorkami and R. M. Mersereau, "Compressed-domain video watermarking for H.264," in *Proc. IEEE Int. Conf. Image Process., ICIP '05*, Genova, Italy, Sep. 2005, pp. 890–893.

[8] D. Zou and J. A. Bloom, "H.264/AVC stream replacement technique for video watermarking," in *Proc. 2008 IEEE Int. Conf. Acoustics, Speech and Signal Process., ICASSP '08*, Las Vegas, NV, USA, Mar. 2008, pp. 1749–1752.

VIII. AUTHOR PROFILE'S

M.Ramya devi received the B-tech degree from Sai Ganapathi Engineering college. M-tech degree from Vignan's institute of information and technology. The current research interests includes digital image processing, Encryption of video, data hiding, Multimedia information security.

P. Suneetha received the B-tech degree from Tandrapaparayudu Engineering College, M-tech degree from Sri chaithanya engineering college .Associative professor of Vignan's institute of information and technology.