IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010
ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

Watermarking of Digital Video Stream for Source Authentication

Kesavan Gopal[1], Dr. M. Madhavi Latha[2]

[1] Team Leader, Infotech Enterprises Limited
Bangalore, Karnataka, India

[2] Professor, Department of ECE, JNT University,
Hyderabad, Andhra Pradesh, India

Abstract

In this paper, a novel idea of embedding a watermark pattern in BT.656 raw digital video stream is proposed and implemented in Field Programmable Gate Array (*FPGA)* hardware for real time authentication. Earlier many watermarking algorithms are proposed for video authentication both in compressed as well as in uncompressed domain. A watermark is introduced in the stream either at source, channel or at the receiver. Most of methods targets embedding the watermark in the compressed domain before being transmitted over the channel or at the play back, very few techniques concentrates on the raw video data at the source. In this proposed work, we embed the watermark pattern at the very beginning stage of digital video production i.e., at BT.656 video interface. A 64-bit length device DNA or user defined payload is embedded as an invisible watermark. Optionally visible logo is used as a visible watermark. Embedding of watermark bits is done in Discrete Wavelet Transform (DWT) domain for its robustness against various attacks. Only the luminance component of the BT.656 video stream is watermarked. An experimental result shows that the proposed method is operating in real time while maintaining the good perceptual visual quality measured in terms of PSNR.

Keywords: *Real-Time Authentication, BT.656, FPGA, Watermarking, Digital Video Streams. Discrete Wavelet Transform*

1. Introduction

A streaming video system is one in which a source encodes video content and transmits it over data network (wired or wireless) where one or more recipients can access, decodes and displays the video in real time. With the growing demand for the use of digital video streaming in many applications like real-time video conferencing, Video on Demand (VoD) etc., there is an absolute need of authenticating the video streams in order to meet counterfeiting. The parties involved in such applications are in a position to determine and verify the genuineness and originality of streams by embedding and extracting extra information (payload) called watermark to and from the video stream. Watermark embedding in a video can be either frame based or stream based including AVI, MPEG-2 and MPEG-4 / H.264 [*12*] [*13*] [*14*] [*15*] video frames/streams. In frame based embedding the watermark bits are introduced in the video by means of complete frame or tiles of the frame. In stream based watermark embedding technique, only the lines of the video frame are embedded. The method proposed in [*1*] by Frank Hartung *et al.,* uses uncompressed (raw) spatial domain video watermarking. Hartung uses spreading of watermark bits and is modulated with pseudo-noise signal to generate the watermark signal which in turn is used for embedding into the original video frame. It utilizes the blind watermark extraction method by means of correlation receiver consists of one dimensional and two dimensional low pass and high pass filtering. While that of method proposed in [*12*] by Abhinav Gupta *et al.,* uses compressed domain video watermarking. It describes the embedding of watermark bits directly into the bit stream generated out of Advanced Simple Profile (ASP) of MPEG-4 standard. Watermark is added to the luminance plane of the video leaving the chrominance planes and hence the method withstands synchronization attacks. The main draw back of frame/tile based authentication schemes are compute intense in terms of number of MAC (Multiplication and Accumulation) operations and is less efficient for real time video content delivery. Particularly the computation is very high, when the process of watermark embedding and extraction uses two dimensional discrete wavelet transforms (2D-DWT). A lot of work has been proposed and carried out in authenticating the digital video stream in the compressed domain [*2*] [*4*] [*5*] [*6*] [*7*] [*12*] like H.264/MPEG-4 earlier. Post compressed watermarking methods need to be tested for their robustness against video transcoding.

In multicast application scenario like VoD, a video server sends out a networked high quality visual program to its users is shown in fig 1. In this case, authenticating all the outgoing video streams with user specific information exhaust the video server. Note that the same video content

Is watermarked at the source (server side) with their recipient specific information for video finger printing and traitor tracing [8]. Each recipient will receive the embedded video stream having their own information as a watermark. Multimedia fingerprinting and traitor tracing and respective attacks are presented in [3]. By considering the insecure nature of the channel or network, there is highly possible that the video stream under goes counterfeiting or malicious attacks. In such case, it is difficult for the receiver to determine the genuineness and originality of the content with out any authentication mechanism between the parties involved in exchanging the streams. Streaming research for authentication has been motivated in finding ways to overcome the limitations. Watermarking in real time will solve the source authentication issues. The parties involved in real time stream exchange, checks the authenticity of the data received, by extracting the watermark bits embedded in the stream. This watermark can be introduced into the video stream at source, channel or at the receiver side. In our work, we propose a simple video streaming authentication system using watermarking at the source principle rather than at video delivery or at channel. The proposed system is suitable both for unicast and multicasting application. Unique Device DNA (Identification number of the video encoder chip) or user defined payload of 64-bit length is used as a watermark. A line based watermark embedding technique in which, a single line is embedded with the entire payload. If the payload of the watermark is less, then the same watermark pattern is repeated for the complete line of the video frame.

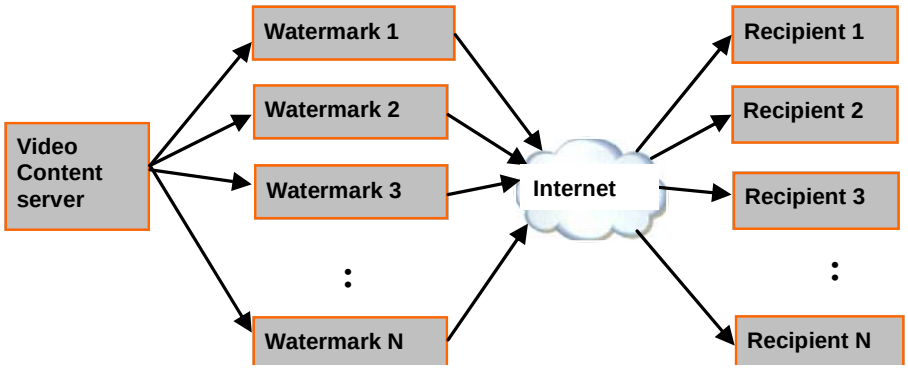

Fig. 1 Multicast Video Streaming over internet

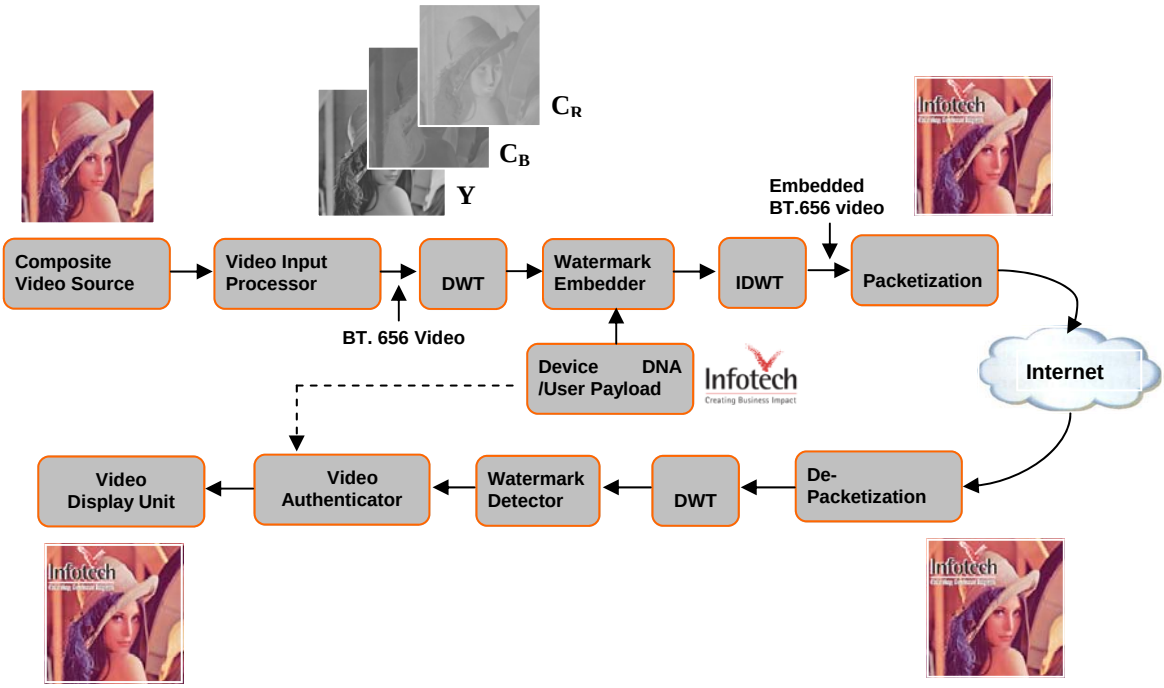

Fig. 2 Video Authentication Systems

The paper is organized as follows: Section 2.0 explains the proposed real time authentication system. Details of BT.656 video format, discrete wavelet transform, watermark embedding, watermark extraction, inverse discrete wavelet transform, and video authentication is also explained in the sub-sections of 2.0. Section 3.0 gives the implementation and experiment results. Conclusion is presented in section 4.0 followed by appendix and references.

2. Real Time Authentication System

The proposed video authentication system is shown in fig. 2. It consists of both watermark embedder as well as extractor. Similar types of embedder and extractor exists at both sides of the transmitter and the receiver for mutual authentication.

The watermark embedding section consists of composite video camera which produces analog composite video burst signal (CVBS). This CVBS signal is converted into ITU-R BT.656 compatible digital video stream by video input processor (or alternatively called video encoder). The BT.656 video format so produced may be either an 8-bit or 10-bit parallel data. For further computations and discussions only processing of 8-bit parallel data is considered and is directly extendable to 10-bit parallel data. At the server side, the 8-bit parallel data output of the video input processor is subjected to 1D-discrete wavelet transform [*10*] to produce the frequency domain coefficients. More details of the discrete wavelet transform and its computation are explained in [*10*] [*11*]. The discrete wavelet transform coefficients are modified according to the device DNA or user defined payload. The modified/embedded frequency domain coefficients are applied to inverse discrete wavelet transform module where the coefficients are converted back to spatial domain pixels. The embedded BT.656 video stream is packetized in order to transmit over the internet. At the client side, the authentication system de-packetizes the received data from the network, extracts the embedded BT.656 and other useful parameters. The embedded BT.656 video stream is again subject to the discrete wavelet transform and tries to extract the device DNA or user defined payload embedded into it for verification. The video authenticator module authenticates the received video stream by comparing and verifying the extracted watermark with the a priori known device DNA or user payload along with the visible logo. If the video authenticator acknowledges that the stream is genuine and not falsified/forged, then it allows the video stream content for the further units and finally reaches the video display unit of the receiver. More details of the individual modules are explained in the following sub sections.

2.1 BT.656 Format

The ITU-R standard BT.656 [*9*] defines the parallel and serial interfaces for transmitting 4:2:2 YC_BC_R digital video between equipment in studio and pro-video applications. The standard supports two active video resolutions of either 720 x 480 (525 line / 60 Hz NTSC video systems) or 720 x 576 (625 line / 50 Hz PAL video systems). To represent the digital video signal the BT.656 interface uses either 8 or 10 bit parallel data of multiplexed YC_BC_R component with fixed 27 MHz Line Locked Clock (LLC). Instead of the conventional video timing signals say H_{SYNC}, V_{SYNC}, and BLANK pulses, BT.656 uses unique timing reference codes embedded within the video stream. This reduces the number of wires required for a BT.656 video interface. Every single line of the digital video frame consists of EAV code for blanking video, SAV code for active video portions. The combination of Start of Active Video (SAV) and End of Active Video (EAV) codes which is always prefixed with (FF_h 00_h 00_h), defines the blanking and sync pulse duration. Ancillary digital information (such as audio, closed captioning, and teletext) may also be transmitted during the blanking intervals. This eliminates the need for a separate audio interface and additional control signals.

$$C_{B1}\ Y_1\ C_{R1}\ Y_2\ C_{B2}\ Y_3\ C_{R2}\ \ldots\ldots..\ C_{B360}\ Y_{719}\ C_{R360}\ Y_{720}$$
(a)

$$Y_1\ Y_2\ Y_3\ Y_4 \quad Y_5\ Y_6\ Y_7\ Y_8\ \ldots\ldots\ldots \quad Y_{717}\ Y_{718}\ Y_{719}\ Y_{720}$$
(b)

Fig.3 (a) BT.656-4 (4:2:2) Video Stream Format (b) Luminance Component Grouping

The multiplexed 4:2:2 YC_BC_R 8-bit parallel data is shown in fig. 3(a). The terms in fig. 3(a) C_B and C_R refers to the chrominance difference components, and the term Y refers to the luminance component. The format for both 525-lines 60Hz and 625-line 50Hz video systems are referenced in [9] [*16*]. After each SAV code the stream of active video data always begins with a C_B sample. Each line of active video is sampled at 13.5 MHz, generating 720 active samples of 24-bit (raw) 4:4:4 YC_BC_R data. This is converted to 16-bit 4:2:2 YC_BC_R data, resulting in 720 active samples of Y per line, and 360 active samples each of C_B and C_R per line. The Y data and the C_BC_R data are multiplexed, and the 13.5MHz sample clock rate is increased by two times to 27 MHz. YC_BC_R and ancillary data may not use reserved 8-bit values of 00_h and FF_h since those values are used for timing reference information, i.e., the bits of 8-bit video format all set to ones and zeros are reserved for identification purpose as per standard. Only 254 of the possible 256 8-bit words may be used to express video signal value. Normally the

luminance (Y) component has its value range from 16 to 235. In our proposed authentication method, we separate the luminance component of the BT.656, and grouped into four samples to be used by the DWT module as shown in fig. 3(b). Both the chrominance components say C_B and C_R are completely bypassed from the further processing. Since modifying the chrominance signal C_B, C_R will affect the perceptual visual quality (color artifacts) of the video. There is high correlation between the successive samples of the luminance components to make the proposed techniques much possible to embed the data. BT.656 video format for both NTSC and PAL video standards are presented in Appendix.

2.2 Discrete Wavelet Transform

The luminance component of the BT.656 video stream is extracted and grouped as per fig. 3(b) is transformed into frequency domain coefficients using Daub Galle 5/3 integer wavelet transform [*11*]. The main advantage of using this reversible transformation is that, it transforms all spatial integer luminance pixels into integer wavelet coefficients and again converted back to spatial luminance pixels with out any loss. Hence the embedding loss due to floating point truncation and rounding is eliminated here, and is widely used in lossless JPEG2000 image compression standard. The *low pass* and *high pass* filter coefficients both for analysis and synthesis filters are shown in Table 1.

Table 1: 5/3 Wavelet Analysis and Synthesis Filter Coefficients

	Analysis Filter Coefficients		***Synthesis Filter Coefficients***	
	Low Pass Filter	High Pass Filter	Low Pass Filter	High Pass Filter
0	6/8	1	1	6/8
±1	2/8	- 1/2	1/2	-2/8
±2	- 1/8			-1/8

For computing the DWT based on conventional convolution, consists of performing a series of dot products between the two filter masks and the extended 1D input signal. An area and time efficient lifting based architecture for computing DWT is presented in [*11*]. Lifting-based filtering consists of a sequence of very simple filtering operations for which alternately odd sample values of the signal are updated with a weighted sum of even sample values, and even sample values are updated with a weighted sum of odd sample values. The lifting based analysis filter which is used to convert the spatial luminance pixels into frequency domain coefficients are given in expressions (1) & (2). Similarly lifting based synthesis filter which is used to convert the frequency domain coefficients back into spatial luminance pixels are given in expressions (3) & (4) respectively.

$$y(2n+1) = x_{ext}(2n+1) - \lfloor (x_{ext}(2n) + x_{ext}(2n+1))/2 \rfloor \quad (1)$$

$$y(2n) = x_{ext}(2n) + \lfloor (y(2n-1) + y(2n+1)+2)/4 \rfloor \quad (2)$$

$$x(2n) = y_{ext}(2n) - \lfloor y_{ext}(2n-1) + y_{ext}(2n+1)+2 \rfloor \quad (3)$$

$$x(2n+1) = y_{ext}(2n+1) + \lfloor (x(2n) + x(2n+2))/2 \rfloor \quad (4)$$

Where $\lfloor a \rfloor$ is the integer part not exceeding a. As shown in fig. 3(b) a group of luminance samples Y_1 Y_2 Y_3 Y_4 are transformed into L_1 H_1 L_2 H_2 regions using one dimensional discrete wavelet transform, Where $L_i \in \{1,2\}$ denotes the low pass filtered coefficients and $H_i \in \{1,2\}$ denotes the high pass filtered coefficients. A set of two bits are embeddable in the LSB of the high frequency coefficients H_i for each group of four luminance samples. A total of 360-bits are embeddable in a single line video stream of BT.656 of either NTSC or PAL frame. However the device DNA or user payload is only of 64-bits, the watermark bit pattern is repeated after every successful embedding of 128-luminance pixels. The same embedding pattern is continued for all the lines of the video frame.

2.3 Watermark Embedding

In this section, embedding of watermark bits into the high frequency DWT coefficients is discussed. We define $w = w_1\ w_2\ w_3 \ldots\ldots\ w_k$, $k = 64$, are the watermark bits to be embedded into a single line of BT.656 video stream. Every two bits of w_k (say $w_1\ w_2$) are embedded into $H_i \in \{1,2\}$ as per the following expression (5).

$$\hat{H}_i = \begin{cases} H_i + 1 & \text{if } w_k = 1 \\ H_i & \text{if } w_k = 0 \end{cases} \quad (5)$$

Where $\hat{H}_i$ is the embedded high frequency wavelet coefficient of $H_i \in \{1,2\}$ for a group of four luminance (Y) samples. After watermark embedding, the DWT coefficients are given by L_1 $\hat{H}_1$ L_2 $\hat{H}_2$. Note that no low frequency coefficients are used for watermark embedding due to its impact on perceptual visual quality of the video. For visual authentication, a visible logo is added to the BT.656 video stream in the appropriate location of the frame as shown in the fig. 2.

2.3 Inverse Discrete Wavelet Transform

The watermark embedded coefficients L_1 $\hat{H}_1$ L_2 $\hat{H}_2$ are transformed back to a group of four embedded luminance pixels using the expressions given in (3) & (4). Embedded BT.656 frame is reconstructed by combining the embedded luminance component (say $\hat{Y}_1$, $\hat{Y}_2$, $\hat{Y}_3$, $\hat{Y}_4$) and

chrominance component C_B, C_R which are direct output of video encoder. The steps mentioned in sections 2.1, 2.2, 2.3 and 2.4 are repeated for all other luminance component of the video frame. Both packetization and de-packetization for transmission and reception of packets are beyond the scope of this paper.

2.4 Watermark Extraction

In order to verify the authenticity of the received video stream, a watermark extraction procedure is carried out at the receiving end of the communication. After de-packetization, the embedded BT.656 is grouped into samples of four luminance components and applied to one dimensional DWT computation similar to that of watermark embedding. High frequency coefficients are analyzed for the presence of the watermark and formed the watermark bits *k*. If there is no losses in the channel the *k* bits and w_k bits are equal, then 100% of the embedded bits are extracted. A blind watermark extraction is used in which the extraction does not require the un-embedded original video frame.

2.5 Video Authentication

This video authenticator module has full knowledge of the device DNA or user payload of the sender (source authentication), which is used for watermark embedding. Comparing the extracted bit sequence *k* bits with embedded bit w_k sequence to determine the video stream has been attacked or not. The percent match between *k* and w_k also determines the lossy nature of the channel. Higher the percent match means the un-attacked stream and lower it may lead to attacked stream.

3. Experimental Results

The proposed video stream authentication method has been implemented using Infotech general purpose FPGA board. The screen shot of the board is shown in Fig. 4. The core part of the board is the Xilinx Virtex-5 LX50-T FPGA with supporting programming devices and operating at 200 MHz master clock frequency from the crystal with 5V DC external power supply. The board supports various industry standard peripherals like CAN, UART, USB, Ethernet, Audio ports line in, Line out, Mic-in, Compact Flash Drive, Composite video-in, S-video-in and VGA out. This proprietary board's video section is designed using Philips video input processor (SAA7113H), Texas Instruments THS8200 video DAC. The Composite Video Burst Signal (CVBS) produced by the analog video camera (SONY CMOS model C5813-62A1 true color camera) is applied to the composite video-in port (RCA) of the board.

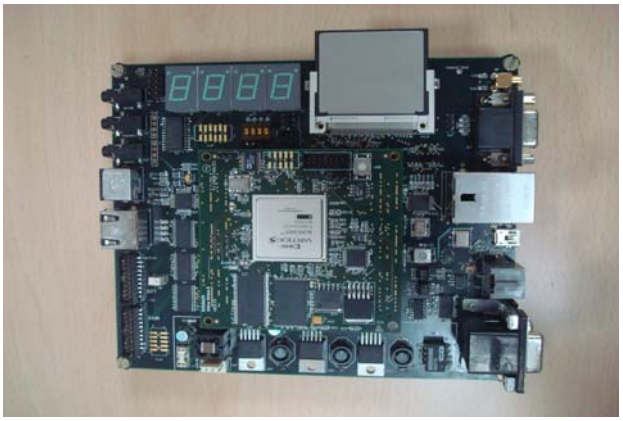

Fig. 4 Infotech general purpose FPGA board

This raw analog input signal is converted into BT. 656 video format by the Philips video input processor. The video encoder registers are configured through the Inter-integrated circuit (I^2C) from the FPGA either to produce the NTSC or PAL streams through eight output data lines. All the parallel 8-bit data is supplied to the FPGA for video decoding to create the H_{SYNC}, V_{SYNC} and blanking pulses. A video decoding logic running in the FPGA extracts the luminance and the chrominance components by identifying the EAV and SAV timing reference codes. The screen shot of the ModelSim simulation of BT.656 video decoding is shown in fig. 5.

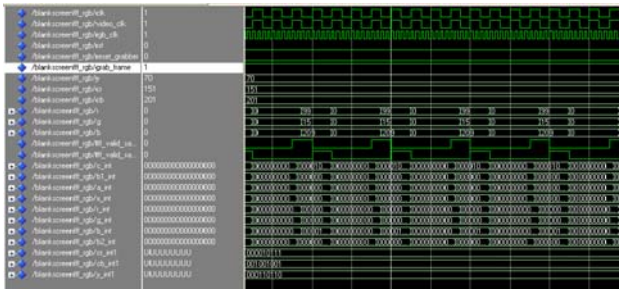

Fig. 5 BT.656 Video Decoding Simulation

User payload of 64-bits is stored in block RAM of the FPGA. The VHDL coding of various sub modules like device configuration using I^2C, discrete wavelet transform, watermark embedder, inverse discrete wavelet transform, watermark Extractor and video authentication is simulated using ModelSim Altera edition 6.3c and implemented using Xilinx ISE 9.1i targeting Virtex-5 LX50-T speed grade -1 FPGA. The RTL Schematic of the BT.656 to RGB conversion for video display is shown in fig. 6. The watermark embedded BT.656 bit stream resulting out of the FPGA is routed to General Purpose Input Output (GPIO) pins which is observed and monitored using the Logic Analyzer (LA) for silicon functionality verification.

Thus the synthesis result shows that the design is able to run at 171.556MHz.

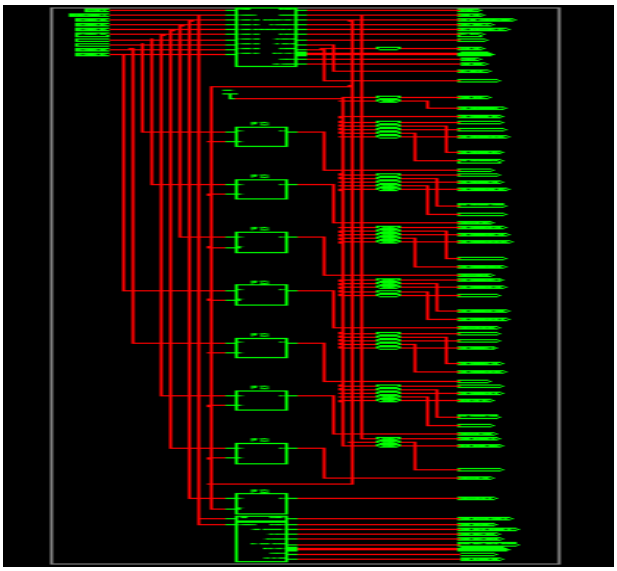

Fig. 6 RTL Schematic 8-bit BT.656 to RGB conversion for video Display

Embedding capacity of the proposed method is very high as comparable to the other raw video frame embedding methods. For example in this method a standard full D1-PAL frame can accommodate 202 Kbits of watermark and full D1-NTSC frame can accommodate 168 Kbits of watermark resulting in a 4.931Mb/s watermark embedding rate. The rate might be slightly lower if all the coefficients are not embedded due to overflow and under flow conditions. There are no exact literatures available on BT.656 video watermarking for direct comparison of results. However we use [*12*] digital video stream with 4:2:2 formats in order to compare the results. The proposed method has higher watermark embedding capacity as compared to [*12*]. The results presented in [*12*] have only 1Kbits to 3Kbits per frame resulting in a 900kb/s.

A Peak Signal to Noise Ratio (PSNR) is used as a metric for measuring the distortion in a signal; however they do not represent the image quality as perceived. Thus the PSNR measurement between the raw video frame and the watermarked video frame shows that the proposed method maintains the perceptual visual quality of the watermarked frame as close to the original. Only the computational methods identify the presence of a watermark in a frame. A software implementation of the proposed method for the QCIF video Foreman and its watermarked video is shown in the fig. 7(a) & 7(b) respectively. The PSNR of unwatermarked and watermarked image is 40.1dB and 42.3dB for a single 64-bit watermark pattern. The amount of distortion or degradation to the raw frame due to watermark embedding is judged easily by subjective visual evaluation. The visual evaluation of fig. 7(b) also shows that there are no visual artifacts except the sharpened watermarked video.

(a) (b)

Fig.7 (a) Foreman QCIF video (b) Watermarked QCIF video

4. Conclusion

In this paper, an innovative technique of watermarking the real time BT.656 video stream is proposed and implemented using infotech general purpose FPGA board. The perceptual visual quality and the payload are highly comparable to that of previously proposed video stream authentication schemes. The method discussed in this paper is semi fragile in nature and with stands unintentional attacks like few packet drop or losses in the network. Using constrained embedding both over flow and under flow of luminance components is well taken care off. Since we are using line based approach of watermark embedding, it thwarts the attacker to analyze the successive frame to find and remove the watermark in the video. This watermarking based authentication provides a solution for fingerprinting and copy right protection and real time authentication. Any illegal distribution of the video is also traced out by extracting the watermark. Further to this work, in future, if the video encoder ASIC chip has a support for device identification information like device DNA, or directly accessing the user payload for embedding into the BT.656 format video. The method adopted above will lead to single chip solution for video stream authentication problems. Also the extensibility of the authentication mechanism towards the USB based video streams needs to be tested.

Appendix

In this annexure, the BT.656 digital video interface format for PAL video standard (format for NTSC video standard is mentioned in the parenthesis) is shown below. The interlaced scanning pattern consisting of both odd (field 1) and even (filed 2) fields are presented. Note that the EAV codes, Blanking video, SAV code, Active Video are in the range of 0 to 255 to transmit the video signal.

Field 1 - First Vertical Blanking (Top) - Repeat for 22 (19) lines															
EAV Code				**Blanking Video**				**SAV Code**				**Active Video**			
255	0	0	182	128	16	128	16	255	0	0	171	128	16	128	16
Repeat 1 (1) time				Repeat 70 (67) times				Repeat 1 (1) time				Repeat 360 (360) times			

Field 1 - Active Video - Repeat for 288 (240) lines															
EAV Code				**Blanking Video**				**SAV Code**				**Active Video**			
255	0	0	157	128	16	128	16	255	0	0	128	240	41	110	41
Repeat 1 (1) time				Repeat 70 (67) times				Repeat 1 (1) time				Repeat 360 (360) times			

Field 1 - Second Vertical Blanking (Bottom) - Repeat for 2 (3) lines															
EAV Code				**Blanking Video**				**SAV Code**				**Active Video**			
255	0	0	182	128	16	128	16	255	0	0	171	128	16	128	16
Repeat 1 (1) time				Repeat 70 (67) times				Repeat 1 (1) time				Repeat 360 (360) times			

Field 2 - First Vertical Blanking (Top) - Repeat for 23 (20) lines															
EAV Code				**Blanking Video**				**SAV Code**				**Active Video**			
255	0	0	241	128	16	128	16	255	0	0	236	128	16	128	16
Repeat 1 (1) time				Repeat 70 (67) times				Repeat 1 (1) time				Repeat 360 (360) times			

Field 2 - Active Video - Repeat for 288 (240) lines															
EAV Code				**Blanking Video**				**SAV Code**				**Active Video**			
255	0	0	218	128	16	128	16	255	0	0	199	240	41	110	41
Repeat 1 (1) time				Repeat 70 (67) times				Repeat 1 (1) time				Repeat 360 (360) times			

Field 2 - Second Vertical Blanking (Bottom) - Repeat for 2 (3) lines															
EAV Code				**Blanking Video**				**SAV Code**				**Active Video**			
255	0	0	241	128	16	128	16	255	0	0	236	128	16	128	16
Repeat 1 (1) time				Repeat 70 (67) times				Repeat 1 (1) time				Repeat 360 (360) times			

Acknowledgments

The author would like to thank **Mr. Jagan Mohan Venneti**, Vice President, Hitech Vertical, Infotech Enterprises Limited, India for his excellent appreciation, motivation and support to carry out this work.

References

[1] Frank Hartung and Bernd Girod, “Watermarking of Uncompressed and compressed Video”, Elsevier Journal Col. 66 No 3, May 1998 PP 283-301.

[2] Uwe Wessely, Stefan Eichner and Dirk Albrecht, "Watermarking of Analog and Compressed Video", Published in Virtual Goods Conference 2003, http://VirtualGoods.tuilmenau.de/2003/videowatermarking.pdf Accessed on 05/01/2010

[3] K. J. Ray Liu, Wade Trappe, Z. Jane Wang, Min Wu, and Hong Zhao, "Multimedia Fingerprinting Forensics for Traitor Tracing" , ISBN 977-5945- 18-6, EURASIP Book Series on Signal Processing and Communications, Volume 4. Hindawi Publishing Corporation.

[4] Shigeyuki Sakazawa, Yasuhiro Takishima, and Yasuyuki Nakajima, “H.264 Native Video Watermarking Method”, ISSN 0-7803-9390-2 IEEE ISCAS 2006.

[5] Maneli Noorkami,Russell M. Mersereau, “A Framework for Robust Watermarking of H.264-Encoded Video With Controllable Detection Performance” ISSN 1556-6013, IEEE Transactions on information forensics and security, Vol 2, No. 1, March 2007.

[6] Shinfeng D. Lin, Chih-Yao Chuang, and Hsiang-Cheng Meng,"A Video Watermarking in H.264/AVC Encoder",proceedings on Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing IEEE 2009.

[7] Razib Iqbal, Shervin Shirmohammadi, and Jiying Zhao, "Compressed domain authentication of live video”, ISSN 4244-1236, ICSPC 2007 IEEE International Conference on Signal Processing and Communications,November 2007.

[8] W. Sabrina Lin, Steven K. Tjoa, H. Vicky Zhao, and K. J. Ray Liu, "Digital Image Source Coder Forensics Via Intrinsic

Fingerprints", IEEE Tranctions on information forensics and security,Vol. 4, No. 3, September 2009.

[9] BT.656 ITU-R recommendation, http://www.itu.int/rec/R-REC-BT/e accessed on 15/03/2010.

[10] Robi Polikar, A Tutorial on Discrete Wavelet Transform, html accessed on 05/03/2010
http://users.rowan.edu/~polikar/WAVELETS/WTpart1.html
http://users.rowan.edu/~polikar/WAVELETS/WTpart2.html
http://users.rowan.edu/~polikar/WAVELETS/WTpart3.html
http://users.rowan.edu/~polikar/WAVELETS/WTpart4.html

[11] Charilaos Christopoulos, Athanassios Skodras, Touradj Ebrahimi, "The JPEG2000 still image coding system: An Overview", IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp. 1103- 1127, November 2000.

[12] Abhinav Gupta,Phalguni Gupta, "Watermarking of MPEG-4 Videos", Springer-Verlag Berlin Heidelberg 2004.

[13] Shintaro Ueda, Shin-ichiro kaneko, Nobutaka kawaguchi, Hiroshi shigeno and ken-ichi okada, "A real time stream authentication scheme for video streams", IPSJ digital courier, Vol.2, Feb 2006,

[14] Eugene T. Lin and Christine I. Podilchuk and Ton Kalker and Edward J. Delp, "Streaming video and rate scalable compression: what are the challenges for watermarking", CERIAS Tech Report 2004-83.

[15] Stefano Chessa, Roberto Di Pietro, Erina Ferro, Gaetano Giunta, Gabriele Oligeri, "Mobile application Security for Video Streaming Authentication and Data Integrity Combining Digital Signature and Watermarking Techniques", ISSN 1550-2252, IEEE Transactions 2007.

[16] http://www.spacewire.co.uk/video_standard.html accessed on 15/03/2010

Kesavan Gopal recieved his Diploma & B.E. Degree in Electronics and Communication Engineering from state board of technical education & university of madras respectively during 1994 and 1997. He received his M.Tech Degree in Digital Electronics and Advanced Communication Engineering from Manipal University, India, during 2003. Presently he is about to complete his Ph D from JNT University, Hyderabad, India. He worked as a lecturer during 1997 to 2001 and Research Engineer during 2002-2004, Deputy Manager during 2005-2007 and presently he is associated Infotech Enterprises Limited. He published more than four international conference and journal papers on video watermarking implementation on FPGA. His research interests include Digital Video Watermarking Technologies, Data Security & Compression; FPGA based System Design and Digital Signal Processing.

Dr. M. Madhavi Latha received B.E. Degree in Electronics and Communication Engineering from Nagarjuna University, Guntur, India in 1986, M.Tech Degree in Digital Systems and Computer Electronics from JNT University, Hyderabad, India in 1998 and Ph.D from JNT University, Hyderabad, India in 2002. She is currently working as a professor in Electronics and Communication Engineering Department of JNT University, Hyderabad. She has published more than 15 research papers in international journal and conferences. Her research areas include signal and image processing, Wavelets and low power VLSI design.