Multimed Tools Appl (2014) 73:763–778
DOI 10.1007/s11042-012-1208-8

Robust transcoding resistant watermarking for H.264 standard

Rohit Nair · Vijayaraghavan Varadharajan · Sagar Joglekar · Rajarathnam Nallusamy · Sanjoy Paul

Published online: 24 August 2012

Abstract Content in the digital form can be easily copied and distributed without permission of the owner. As a result, it is of paramount importance to protect content and deter illegal distribution using content protection mechanisms like embedding an imperceptible watermark into the content. Given that consumers want access to content from anywhere using any device, it is necessary to transcode content keeping in mind the limitations of the devices in terms of processing power and network connectivity. However, it is important that the watermark embedded in the content is preserved even after transcoding. The proposed approach embeds in a video, an imperceptible yet robust watermark which is resistant to transcoding. This approach focuses on the H.264 codec because of its widespread use in the industry.

Keywords H.264 · Robust watermark · x264 · ffmpeg · DCT

1 Introduction

With the advent of Internet, content distribution becomes easier and can be done with click of a mouse. This inadvertently has the implications that are usually not seen in non-digital forms of content distribution. It becomes extremely easy for anyone to copy or distribute

This work is carried out when Rohit, Sagar and Sanjoy is at Infosys Ltd.

R. Nair · V. Varadharajan (✉) · S. Joglekar · R. Nallusamy · S. Paul
Infosys Labs, Infosys Ltd, 44, Electronics City, Bangalore 560100, India
e-mail: vijayaraghavan_V01@infosys.com

R. Nair
e-mail: roguehit@gmail.com

S. Joglekar
e-mail: sagarjoglekar@gmail.com

R. Nallusamy
e-mail: rajarathnam_N@infosys.com

S. Paul
e-mail: sanjoy.paul@gmail.com

without permission from the original provider. Torrent and other P2P websites provide a huge cache of movies [http://brainz.org/how-download-watch-free-movies-video-online/], music and e-books. This makes easy to download illegal and pirated versions. So it becomes important for providers to find and plug the source of piracy and hence new digital copyright technologies have become main stream in today's multimedia security. While encryption of multimedia content can provide an excellent frontend to reduce piracy efforts, it nonetheless fails to protect content after it has been decrypted. Such vulnerable content can be watermarked with unique IDs and any subsequent illegal distribution of content can be traced back to its source, thereby thwarting piracy. A good watermark typically has following qualities [4]

1. High robustness—it should be ideally impossible for an attacker to destroy the embedded watermark without eroding the usefulness of the cover object.
2. High capacity—the amount of information that can be embedded should be more.
3. Invisible—an embedded watermark should remain imperceptible, when a user views the watermarked content.

Digital age has also ushered cheap availability of entertainment devices like HDTV, Music players and Laptops. These devices have widely differing capabilities in terms of processing power and screen sizes. Thus, content has to be tailored according to the platform on which they are intended for viewing [8]. This requires transcoding which is a process that converts content from one format to another depending on the capabilities of the said devices. Transcoding is defined as any change or transformation of data container or data representation file format which may include encoding/compression of original data. This transcoding process can adversely affect watermarks that are present in the original content. This work is focussed on tackling the effects of transcoding on videos.

Rest of the paper is organized as follows. Section 2 provides a brief background on the current state of watermarking techniques. Section 3 provides insights on the choice for H.264 format. Watermark insertion, extraction and reconstruction procedures are discussed in section 4. Section 5 extensively shows the obtained results followed by conclusions and future work.

2 Literature review

There are numerous ways in which a watermark can be inserted in a video. Sridevi et al. [9] have proposed a 2-D gray scale watermark pre-processing technique. In their method watermark is compressed by pre-processing before embedded into the MPEG video. This method ensures better visual quality of the video. Coria et al. [2] have proposed a robust video watermarking scheme that generates codeword which keeps control of the distance between code words. This method is robust in particular to video compression. The three main categories in watermarking are—inserting watermark in the uncompressed video, inserting watermark in compressed video and insertion during encoding process itself. A lot of prior work has been done in the first category since it directly involves dealing with raw pixel values which eases the application of signal processing. Uncompressed domain watermarks can be further divided into spatial watermarking [7] or frequency spectrum based watermarking [3, 10]. In Entropy based selective spread spectrum (EBSSS) [10], the authors used the SS technique to insert the watermark in bands of frequencies which have higher entropy content. Cox et al. [3] pioneered the Spread Spectrum (SS) technique for video watermarking where the watermark information is spread over significant frequency bands so that energy in any particular band is too small to detect.

In compressed domain watermarking, modification of the bit-stream which is produced after compression is carried out while preserving its compatibility and syntax with prescribed decoders [1]. In the final type, the watermark is inserted during the encoding process itself [5, 6]. In Tien-Ying Kuo et al. [5], the authors have selected optimal position to insert watermark which provides the best trade-off between visual quality and watermark robustness. The proposed work falls in the third category where insertion of watermark is done in the encoding process itself.

3 H.264 watermarking

Media content is rarely stored in an uncompressed raw format. Typically in uncompressed domain the raw watermarked video is transcoded to compress video using some kind of codec so as to reduce storage space. Most watermarking schemes are robust to such transcoding process but it nonetheless produces undesirable effects which degrades the quality of the inserted watermark. This motivated us to take the approach of inserting watermark during the encoding process itself without degrading the quality of the inserted watermark instead of inserting the watermark in the source video.

H.264 is one of the most popular codecs currently in the market. It is used widely by Video on Demand (VoD) services, streaming websites and other user generated content sites such as YouTube. Facebook currently uses an implementation of H.264 called x264 for its backend video encoding needs [http://x264dev.multimedia.cx/?p=39]. A recent usage statistics revealed by *encoding.com* shows that H.264 accounts for almost 66 % of Web Videos [http://techcrunch.com/2010/05/01/h-264-66-percent-web-video/]. Therefore, an implementation of watermarking technique based on the H.264 video codec is decided. Specifically, the proposed work integrates the watermarking implementation in x264, which is an open-source library and also because it is the best H.264 encoder in the market currently [http://www.compression.ru/video/codec_comparison/h264_2010/]. As for decoding the video, the proposed work uses *ffmpeg* which is another open source library having the capabilities to decode a H.264 bit-stream [http://www.ffmpeg.org].

Figure 1 shows a H.264 encoding cum watermarking process. For more information on H.264 encoding refer [11]. H.264 is a transform coding based compression standard. The input I frames are divided into 16×16 Macroblocks (MB) and transformed using a modified version of Discrete Cosine Transform (DCT) algorithm, popularly known as the H.264 DCT. The algorithm calculates DCT coefficients of a 16×16 MB in subsections of 16 4×4 Sub-blocks. It utilizes only additions, subtractions and right shift operations to arrive at the final value. Once these DCT coefficients are obtained, quantization is applied, where some information is lost. Trellis quantization algorithm is used in the state of the art encoder x264. Trellis quantization finds the most optimal quantization parameter based on the trade-off between bit-rate and Peak Signal to Noise Ratio (PSNR). The sizes of some DCT coefficients are reduced after trellis quantization while sizes of other coefficients are increased to take their place. The De-blocking filter is then applied to reduce and smoothen artefacts that occur because of block nature of encoding. De-blocking filter increases vastly the subjective quality of an image at the cost of increased bit-rate. Finally, entropy coding is applied to obtain the output bit-stream.

The core idea of the proposed transcoding resistant solution is that the DCT coefficients more or less retain their values after transcoding and hence hiding data in these coefficients

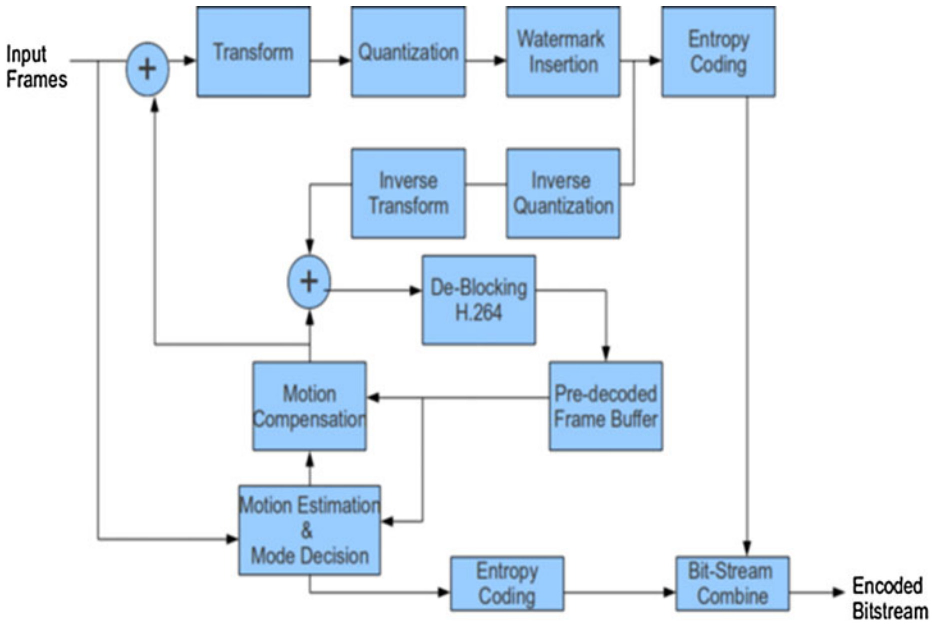


Fig. 1 H.264 encoding cum watermarking process

becomes viable. The proposed work uses a selective insertion technique based on energy of MBs which greatly improves the robustness of watermarks against transcoding. The process of DCT encoding in H.264 is done on macro block level where each macro block can vary from 4×4 to 16×16. The property of DCT based compression is that the compression of DCT coefficients is done on the basis of their strengths. The proposed method implies the same fact which allows us to select macro blocks which are less prone to compression using coefficient pruning and such MBs are preserved during transcoding.

4 Proposed watermarking scheme

4.1 Watermark insertion

Tien-Ying Kuo et al. [5] illustrate that bit positions 5 to 11 of a 4×4 sub-block appearing in the zig-zag scan order provide the best trade-off ratio when considering the quality degradation and robustness of inserted watermark. This paper builds on their work by selectively distributing rows of watermark based on the energy content of MB. H.264 prescribes the use of adaptive selection of MB type depending on the content. There are three fundamental types of MBs which are I_16×16, I_8×8 and I_4×4. The H.264 encoding algorithm selects I_16×16 to encode areas in the frame which are relatively uniform and do not contain much information. Typical examples of such areas are blue sky, parts of anime having uniform colour distribution. I_16×16 type of MB is not used since it has less information holding capacity. I_8×8 and I_4×4 are selected for parts which have greater variance in content. I_4×4 is selected by H.264 to encode areas having highest Chroma/Luma variances, since this mode gives the greatest resolution in terms of quality retention of the original picture. This was found by analyzing the various modes. Another important observation that helped to shape the final algorithm is that I_4×4 MBs are most robust to transcoding since they are used to encode highly perceptual areas. These areas typically consist of edges, corners and regions having high Luma variance. Thus, the proposed algorithm uses only MB of type I_4×4.

The insertion algorithm works by identifying an I-frame and generating a random sequence S of length N equal to number of rows in the watermark. This sequence is treated as a reference for inserting watermark rows into the frames.

$$S = \{s_1, s_2, ..., s_N\},\ where\ N = Number\ of\ watermark\ rows$$

The MB at S_i is then checked for an I_4×4 type. Here i is the index of the watermark row that is being inserted. In case if the MB is not I_4×4 type, then S_i is incremented till the MB at S_i is of type I_4×4. If the MB satisfies the I_4×4 condition, then the energy of residual MB is checked against a threshold. This threshold is empirically arrived upon after extensive testing and for the test video it is set to 30.

The energy E of the MB at S_i is calculated using Eq. 1.

$$E = \sqrt{\frac{\sum_{i=0}^{4}\sum_{j=0}^{4} I(i,j)^2}{4*4}} \tag{1}$$

where E is the energy of the macro block, i,j are indices and I(i,j) describes the value of the (i,j) pixel in the MB. The Energy equation is similar to the root mean squared energy because the individual values of the macro block pixels can go way above or below the threshold, but the RMS gave us a better sense of validity of the MB.

Figure 2 shows Zig-zag scan order as used in the encoding process post quantization. If the energy of MB is greater than the threshold then ith row of watermark is inserted in the 5–11 bit positions of the 16 sub-blocks (each having size 4×4) of the MB as it appears in the zig-zag scan order.

4.1.1 Insertion steps

Figure 3 shows watermark insertion steps.

Step 1- Identify an I-frame and generate a random sequence depending on the size of the watermark which is to be inserted.

Step 2- A sequence S of length N is generated, N=Number of rows in watermark.

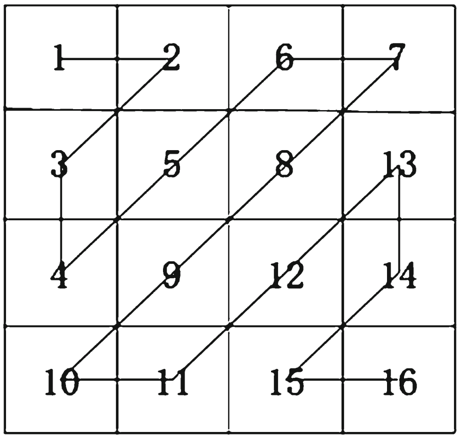


Fig. 2 Zig-Zag scan order for a 4×4 sub-block

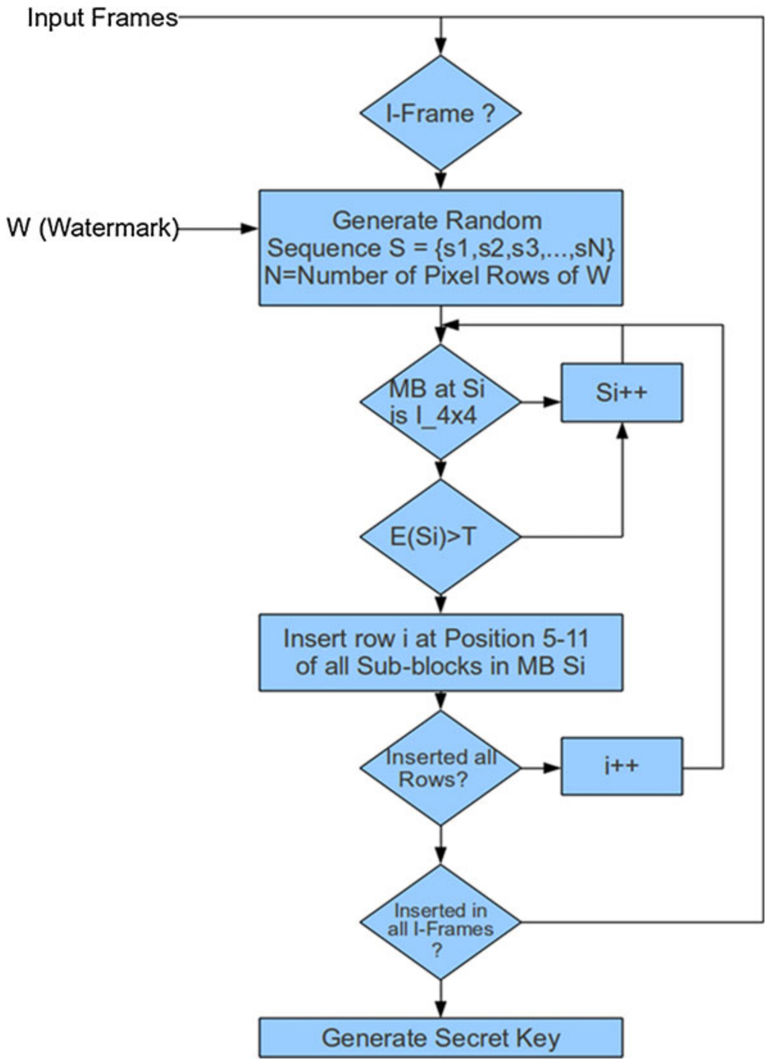


Fig. 3 Flowchart for watermark insertion

Step 3- The MB at S_i is then checked for I_4×4. If it is not I_4×4 then S_i is incremented till MB at S_i is of type I_4×4.
Step 4- Energy of MB is checked against a threshold (T), if its lower then step 3 is repeated to determine the next I_4×4 type.
Step 5- Row *i* of watermark is inserted in the MB at S_i.
Step 6- Repeat 3, 4, 5 till all N rows are inserted.
Step 7- Generate a secret key on the basis of the addresses of MB used.
Step 8- Repeat process for all I-frames in the video.

Repeating the process for all I-frames build a certain redundancy into the system. Moreover since the sequence generated for every I-frame is different, the same watermark is spread differently over different frames. Each inserted watermark thus reacts differently to

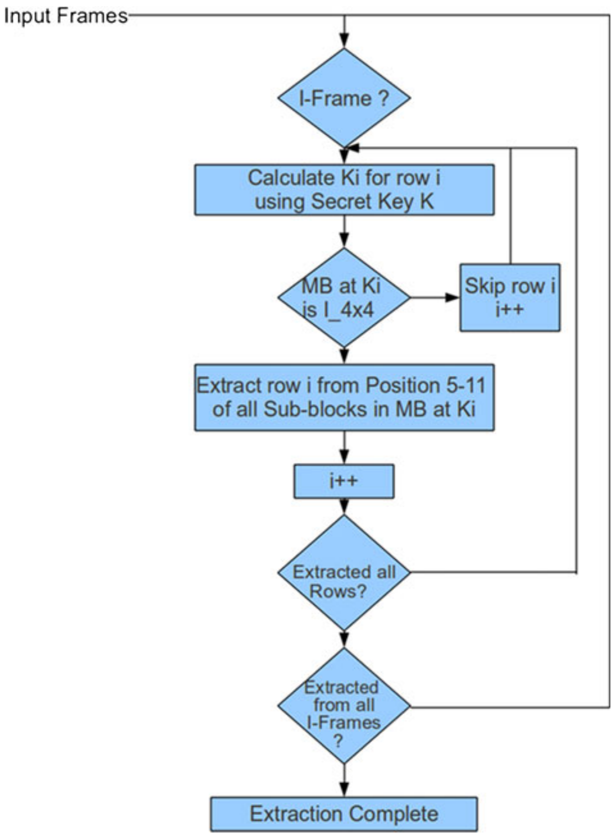


Fig. 4 Flowchart for watermark extraction

the transcoding process and hence allows using the common redundant information to reconstruct the watermark as explained in Section 4.3. The secret key contains address of MB for each row of watermark which is inserted. Without this key it is not possible to extract the watermark, thereby giving added security.

4.2 Watermark extraction

Extraction process requires decoding the video to obtain the DCT coefficients. The ffmpeg [http://www.ffmpeg.org] decoder is modified to identify only I-frames and then calculate the address of MB for each row of the watermark. The secret key K provides the address of each watermark row.

$$K = (k_1, k_2, \ldots.., k_N), k_i \textit{ is the address for the ith watermark row}$$

Using this information each row is sequentially extracted till all rows are recovered. Transcoding process can change the type of MB depending on the parameters set of the H.264 codec. This causes a total loss of information and hence forces the extraction algorithm to skip MB at K_i which is not of type I_4×4. The process is then repeated for every I_Frame. The steps for watermark extraction are shown in Fig. 4.

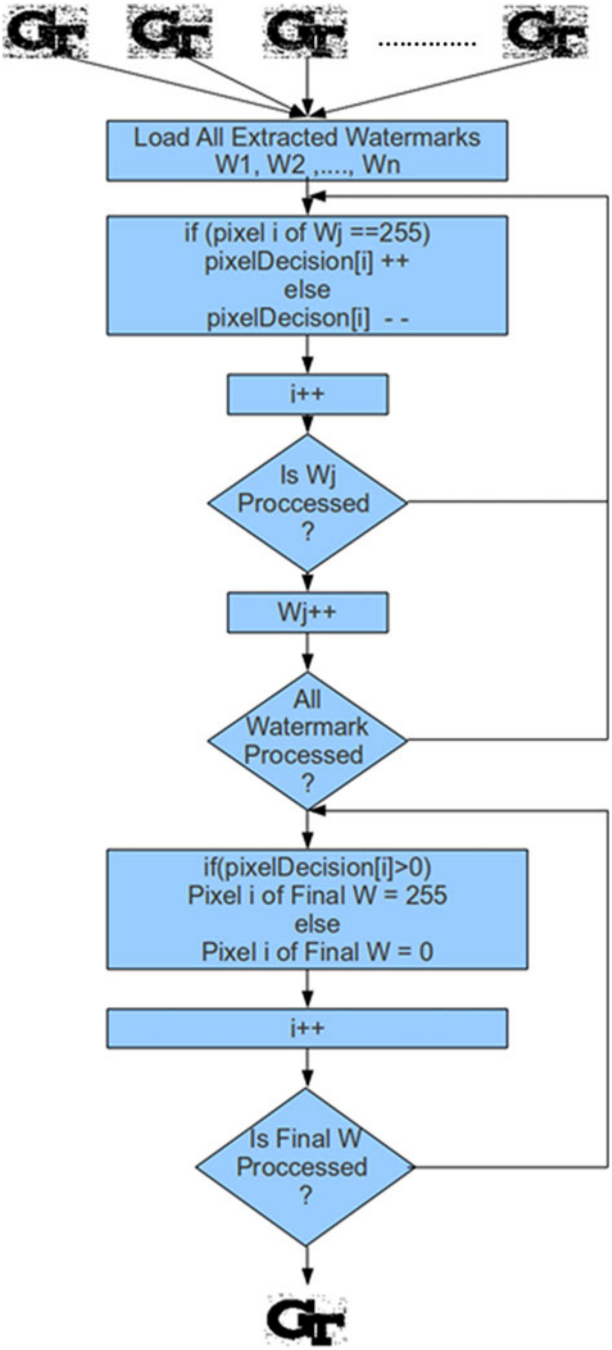
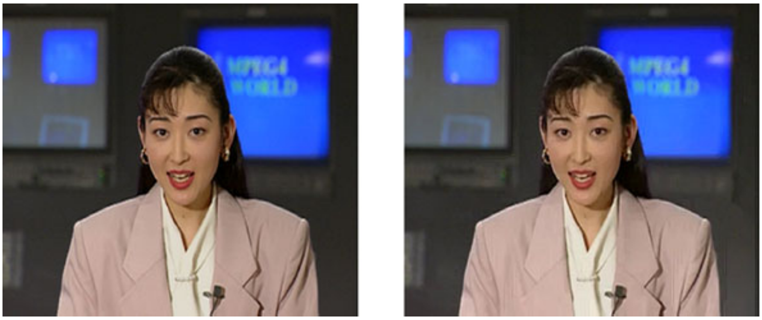


Fig. 5 Flowchart for watermark reconstruction

4.2.1 Extraction steps

Step 1- Identify I-frame while decoding the video.



Original (Pre-Insertion) With Watermark (Post-Insertion)

Fig. 6 Akiyo transparency test

Step 2- Calculate address K_i of row i from the secret key K.
Step 3- Check if MB at K_i is I_4×4; if not skip this row.
Step 4- If MB at K_i is I_4×4, extract the ith row from position 5–11 of all 16 sub-blocks (each of size 4×4) in MB at K_i.
Step 5- Repeat 2, 3, 4 till all rows of the watermark are extracted.
Step 6- Repeat the process for all I- frames in the video.

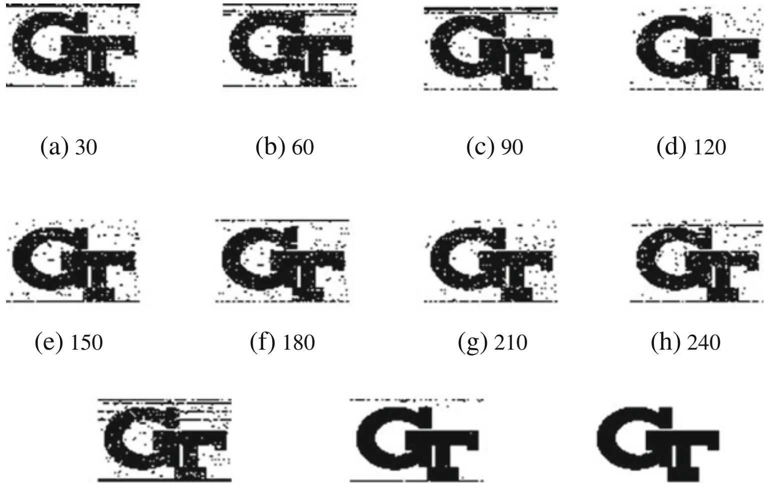
The watermarks extracted from such individual frames are then used for the reconstruction process. This reconstruction process takes advantage of the fact that each watermark has been distributed differently and combining these watermarks give a better version than each of the independent watermarks.

4.3 Watermark reconstruction

All watermarks are loaded and an array variable called pixelDecision[] is used for the reconstruction procedure. The pixelDecision is calculated for every pixel in the watermark and is incremented if that pixel is 255 on greyscale (white) and decremented if pixel is 0 on greyscale (black). This is repeated for all the loaded watermarks. Pixels of final watermark are assigned 255 if pixelDecision for that particular pixel is greater than zero or 0 if it is less than zero. Figure 5 shows watermark reconstruction steps.

Original (Pre-Insertion) With Watermark (Post-Insertion)

Fig. 7 Flower transparency test



(a) 30 (b) 60 (c) 90 (d) 120

(e) 150 (f) 180 (g) 210 (h) 240

(i) 270 (j) Reconstructed (k) Original

Fig. 8 Extracted (**a**–**i**), reconstructed and original watermarks used in Akiyo

4.3.1 Reconstruction steps

Step 1- Load all watermarks.
Step 2- For a pixel of each watermark calculate the pixelDecision variable.
Step 3- Repeat till every pixel of each watermark has been covered.
Step 4- Use the variable to reconstruct the watermark.

5 Results and discussion

The proposed algorithm is tested on Flower and Akiyo videos. These videos are standard test videos available at [http://media.xiph.org/video/derf/]. Original videos are in the raw YV12 format which is encoded to H.264 bit-streams encapsulated in either Matroska or AVI containers. High-profile of x264 has been used for the encoding process. Thereafter, these *.mkv or *.avi videos are transcoded to *.mp4 using MediaCoder software [http://www.mediacoderhq.com/]. MediaCoder is a free and extensive transcoding solution that can handle H.264 videos.

Sequential Insertion
Noise Degradation – 9.23db

Energy Based Insertion
Noise Degradation – 2.34db

Fig. 9 Noise degradation comparison for sequential vs. energy based selective insertion

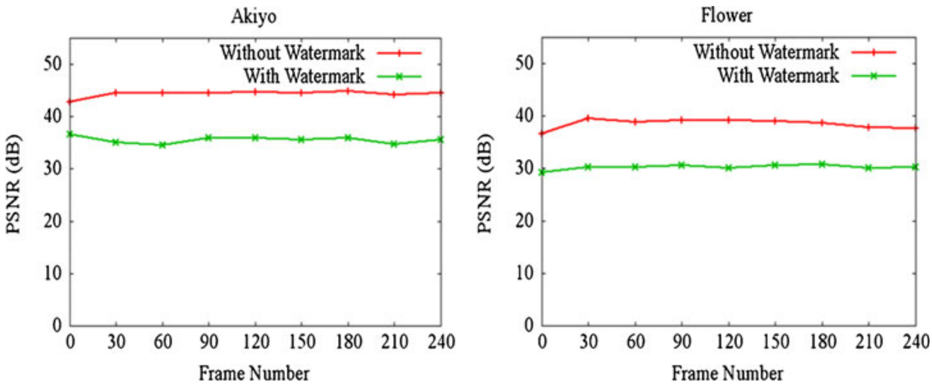


Fig. 10 PSNR comparison for Flower and Akiyo

Figures 6 and 7 shows a particular frame of Akiyo and Flower with and without a watermark. As can be seen the subjective quality of frames even after inserting watermark remains largely intact.

The reconstruction algorithm uses multiple copies of the extracted watermark to arrive upon the final watermark. Figure 8 (a)–(i) show individual watermarks recovered from I-frame numbers 30–270 in the video, Fig. 8 (j) shows the reconstructed watermark and Fig. 8 (k) shows the original inserted watermark. From Fig. 8, it is visually evident that reconstruction process yields a high fidelity image which is quite similar to the original inserted watermark.

Noise degradation of a watermark can be used as a yardstick for quality comparison. To evaluate it numerically, the difference in Root Mean Square (RMS) energies of recovered and original watermarks are calculated. This is because the noise being added is due to false positives or negatives which are added in the form of binary speckle noise. Had the inserted and reconstructed watermarks been same, the difference between the RMS energy values would be zero thereby proving zero noise addition. The addition of binary speckle noise could be measured in a much smoother fashion, if we used difference of RMS energies of the watermarks.

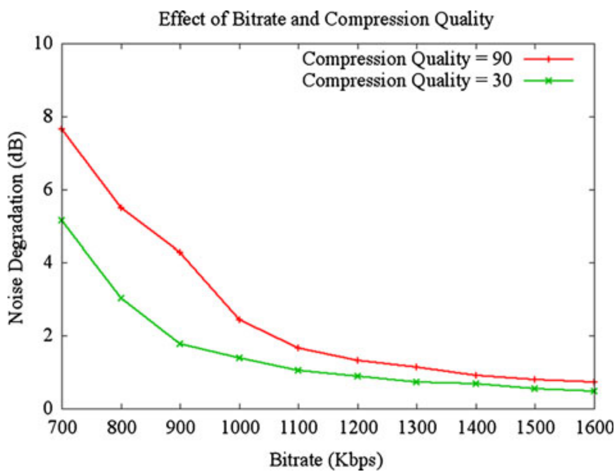


Fig. 11 Effect of bit-rate and compression on watermark quality

This difference is the RMS value of the noise added during transcoding procedure.

$$\text{Noise} = \text{RMS E (Original)} - \text{RMS E (Extracted)}$$

The RMS energy of an image is calculated using Eq. 2.

$$E = \sqrt{\frac{\sum_{i=0}^{m} \sum_{j=0}^{n} I(i,j)^2}{(m^*n)}} \tag{2}$$

where I(x,y) are the individual pixel values in gray scale, *m* and *n* are the dimensions of the watermark.

The sequential insertion method as proposed in [5] is more susceptible to the transcoding attacks, thereby degrading the inserted watermark. Figure 9 shows the reconstructed watermarks for sequential insertion and the proposed energy based insertion method. The same set of encoder settings are used on Flower video to obtain these results. The noise degradation for sequential insertion is 9.23 dB whereas for the proposed energy based insertion the degradation is only 2.34 dB. It can also be seen visually that noise degradation is significantly lower for the proposed energy based insertion approach.

Since the watermark insertion process induces some noise into the frames the PSNR of the frames decrease. Figure 10 shows PSNR comparison with and without watermark for Akiyo and Flower videos. The PSNR is computed using the original frame and the same frame after transcoding. If $I_1(x,y)$ are pixels in the original frame, and $I_2(x,y)$ are pixels in the frame after transcoding, we first find the Mean Squared Error (MSE) using Eq. 3.

$$MSE = \frac{1}{m^*n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I_1(i,j) - I_2(i,j)]^2 \tag{3}$$

Finally the PSNR of each frame was found using Eq. 4.

$$PSNR = 20.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{4}$$

Where MAX_I is the maximum possible pixel value in an image frame.

H.264 codec parameters can make a huge difference on the watermark quality. Higher the bit-rate better is the retrieved quality of watermark. Higher Quality of Compression (qcomp) degrades watermark more severely than lower values of qcomp. Figure 11 shows these effects for Flower video.

6 Conclusions and future work

Effects of transcoding on H.264 videos have been studied and an effective implementation for a watermarking scheme has been proposed. Using selective macroblocks (MB) based on the energy content, the robustness against transcoding of videos can be greatly improved. The proposed work primarily dealt with efficient reconstruction of embedded watermark by inserting it in the I frame. This limits the capacity of the video to carry the watermark information. Further research would deal with exploiting the diversity in the video frame structure to increase the watermarking capacity without compromising the watermark robustness. Since H.264 is a complex codec standard, not all aspects of encoding related effects on watermarks have been fully explored. Features like Rate-Distortion optimizations, Trellis Quantization can be fully leveraged to reduce frame distortions post insertion of watermark. Furthermore, motion vector information can be used to enhance the MB selection procedure so as to increase the PSNR of watermark inserted frames. The proposed current implementation cannot handle resizing leaving a lot of scope for future work.

References

1. Caccia G, Lancini R. Data hiding in MPEG-2 bit stream domain. EUROCON'2001, International Conference on Trends in Communications, 2001 –Vol. 2 pp 363–364. doi:10.1109/EURCON.2001.938138
2. Coria L, Nasiopoulos P, Ward RK (2006) A robust content-dependent algorithm for video watermarking. 6th ACM Workshop on Digital Rights Management, pp 97–101, Alexandria, VA, October 30, 2006
3. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing 6(12):1673–1687
4. Ishtiaq M, Jaffar MA, Khan MA, Jan Z, Mirza AM (2009) Robust and imperceptible watermarking of video streams for low power devices. Communications in Computer and Information Science, Vol. 61, Signal Processing, Image Processing and Pattern Recognition, pp 177–184
5. Kuo T-Y, Lo Y-C. A hybrid scheme of robust and fragile watermarking for H.264/AVC video. IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2010, pp 1–6. doi:10.1109/ISBMSB.2010.5463151
6. Liu Q, Liu H. Robust video watermarking algorithm based on H.264. 4th International Conference on Wireless Communications, Networking and Mobile Computing, (WiCOM '08), 2008, pp. 1–3. doi:10.1109/WiCom.2008.770
7. Nasir I, Weng Y, Jiang J. A new robust watermarking scheme for color image in spatial domain. Proceedings of the 2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, pp 942–947, December 16–18, 2007. doi:10.1109/SITIS.2007.67
8. Paul S, Jain M (2008) Convergence gateway for a multichannel viewing experience. Annual Review of Communications 61:221–230
9. Sridevi T, Krishnaveni B, Vijaya Kumar V, Rama Devi Y (2010) A video watermarking algorithm for MPEG videos. A2CWiC '10 Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India. doi:10.1145/1858378.1858413
10. Vijayaraghavan V, Sagar J, Rajarathnam N, Sanjoy P (2010) Transcoding resistant robust watermarking technique using entropy based selective spread spectrum. International Journal of Multimedia Intelligence and Security 1(4):350–362
11. Wiegand T, Sullivan GJ, Bjontegaard G, Luthra A (2003) Overview of the H.264/AVC video coding standard. IEEE Transactions on Circuits and Systems for Video Technology 13(7):560–576. doi:10.1109/TCSVT.2003.815165

Rohit A Nair is currently working at Qualcomm Inc where he is developing device driver for the memory management unit of Snapdragon series of chipset. He was an Intern at Infosys and completed his Masters at the school of Electrical & Computer Engineering, Georgia Institute of Technology. He received his BE degree from Mumbai University in 2009, majoring in Electronics & Telecommunication.

Vijayaraghavan V is a Senior Research Scientist at Infosys Limited where he is doing research in the field of Security Assessment and Security in Converged Networks. Prior to that, he was an Assistant Professor at a reputed engineering college affiliated under Anna University, Tamil Nadu. He received BE degree in Electronics and Communication Engineering and M.Tech degree in Advanced computing. Also he received Ph.D degree in Information and communication engineering from Anna University in 2008. He is a frequent author in the areas of Information Security and Multicast Communication.

Sagar P. Joglekar is currently with Citrix Online where he is working on design and development of platforms that allow Citrix collaboration products to work on mobile systems. He was a research engineer at Infosys Ltd where he was doing research and development in the field of digital image processing and Computer Vision. Prior to that, he worked as a research assistant and intern with Paragon technologies limited, Nevada, alongside pursuing undergraduate degree in Electronics engineering from the reputed University of Pune. He completed the B.Tech in 2008. He has filed a patent in the field of computer Vision and contributed in various projects in this field.

Rajarathnam Nallusamy is currently a Principal Research Scientist and Head, Convergence Lab at Infosys Labs. His current focus area is Security in Converged Networks. He has 25 years of experience in various domains including Aviation Type Certification, Software Development, System Integration, and about eight years in Information Security. He has been involved in architecting security solutions for many large enterprises and government organization in India, implementation of Information Security Management System, and rollout of PKI based solutions. He received B.Sc. in Physics from Madras University, Madras in 1982, B.Tech. in Aeronautical Engineering from Anna University, Chennai in 1985, M.Tech. in Applied Mechanics from Indian Institute of Technology, Delhi in 1997, and Ph.D. in Applied Mechanics from Indian Institute of Technology, Delhi in 2008.

Sanjoy Paul is a Senior Vice President at Accenture serving as the Country-Director and Head of Accenture Technology Labs India. Dr. Paul has been leading Innovations for Emerging Economy at Accenture Technology Labs and also leading the R&D activities in Software Engineering globally across Accenture. Prior to joining Accenture, Sanjoy was Associate Vice President and General Manager at Infosys Ltd where he led research and innovation in the field of Communications, Media and Entertainment. Earlier, he was also a Research Professor at Rutgers University, Founder of RelevantAd Technologies, Director of Wireless Networking Research at Bell Labs, Lucent Technologies, and CTOs of two start-up companies based in New York. Sanjoy is known for many inventions, including, iSmart Power Strip, an award-winning innovation in the field of Energy Management; Reliable Multicast Transport Protocol, one of the first reliable transport protocols over IP Multicast; and Smart Content Caching, the key concept behind Lucent Technology's Internet Content Distribution and Delivery product line.

He has over twenty five years of technology expertise, specifically in the areas of Mobile Wireless Networking and Applications for various Verticals, such as, Healthcare, Retail, Energy, Transportation etc.; Cloud Computing and Applications for Emerging Economy; Software Engineering Tools and Frameworks;

Future Internet Architecture and Design; and Security Technologies including multi-modal Biometrics. He served as an editor of IEEE/ACM Transactions on Networking, Guest Editor of IEEE Network Special Issue on Multicasting, Steering Committee member of IEEE COMSNETS, General Chair of ICDCN 2011, IMSAA 2010 and COMSWARE 2007; Technical Program Chair of COMSWARE 2006, and as a Technical Program Committee Member of several IEEE and ACM International conferences.

He has authored two books, the first one on Multicasting (Kluwer, 1996), and the most recent one on Digital Video Distribution (Wiley, 2010), published over 100 papers in International Journals and refereed Conference Proceedings, and authored over 100 US patents (32 granted, 70+ pending). He is the co-recipient of 1997 William R. Bennett award from IEEE Communications Society for the best original paper in IEEE/ACM Transactions on Networking and the co-recipient of Infosys Excellence Award for Innovations and Thought Leadership for the invention of iSmart Power Strip. Sanjoy, with his colleague, also received MIT Technology Reviews' Grand Challenges for India 2010 award for innovation in Smart Energy. Sanjoy holds a Bachelor of Technology degree from IIT Kharagpur, an M.S and a Ph.D. degree from the University of Maryland, College Park, and an MBA from the Wharton Business School, University of Pennsylvania. He is a Fellow of IEEE and a Fellow of the IET.