Video Watermarking using Dynamic Frame Selection Technique

Jigar Madia
SAKEC, Chembur,
Mumbai,
Maharashtra, India

Kapil Dave
PVPPCOE, Sion,
Mumbai,
Maharashtra, India

Vivek Sampat
Saraswati College of Engineering
Kharghar
Navi Mumbai,
Maharashtra, India

Parag Toprani
Siddharth College of Engineering,
Hyderabad, Andhra Pradesh, India

ABSTRACT
The rapid development in the field of communication has led to a very widespread dissemination of digital videos leading to their significant production and circulation. The advent of advanced technology has also led to a large scale illegal distribution and piracy of digital videos. To identify the source of piracy and to ensure the ownership and copyrights of the original creator we propose a watermarking technique to authenticate the video.

General Terms
Experimentation, Algorithm

Keywords
Digital Videos, Digital Watermarking, Video Piracy, Data Hiding

1. INTRODUCTION
With the growth of Digital Videos, there has been a rapid increment in copyright and ownership issues along with piracy of videos. Ownership issues arise in case of disputes between two or more parties claiming the video while piracy is illegal distribution of the videos without proper authorization from the owner of the video.

To insure the authenticity of the video we propose a technique to tactically place watermark in multiple frames of video. "Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove"[1]. "Video watermarking is relatively a new technology that has been proposed to solve the problem of illegal manipulation and distribution of digital video"[2].

Watermark can be kept visible on file or it can be hidden in the file as required. Visible watermarks can be a logo or text on frames of videos either in all frames or in just a few selected frames. If it is present in selected frames then it passes off without being noticed, due to high speed of change of frames. Invisible watermarks or Hidden watermarks on other hand are present in the file in such a way that they cannot be sighted but have to be extracted. Watermarks provide security in such a way that the ownership information cannot be removed by anyone without significant loss of quality to the data making it useless. The proposed algorithm uses dynamic frame selection process making it impossible to find a pattern in selection. Dynamic frame selection is a method where frames are selected at runtime based on the key inserted by the user. We furthermore provide a corruption technique to corrupt the videos if information is tried to be extracted with incorrect keys.

The rest of the paper is organised as section II for Proposed Architecture, Section III for Proposed Algorithm, Section IV for Experimental results and concluding with Section V followed by references.

2. REATED WORK
The origins of watermarking go way back in history. Initially used on currency notes and postage stamps to stop the counterfeiting operations, watermarking became a widely used concept to provide watermarks to digital data on documents, files and then extending to reach out multimedia objects like Digital Images and Digital Videos. Now-a-days almost all digital videos are watermarked by their creators due to rapid sharing and viewing of videos over the internet. A few Video Watermarking techniques have been discussed below:

2.1 JAWS [13]
Just Another Watermarking System or JAWS is designed by Philips Research and targeted for embedding watermark for broadcast system. This offers good real time performance and used for DVD applications [4]. In this method, a normally distributed reference pattern is generated with a secret key, which is then used to generate a reference watermark pattern as per following equation.

$$Wr = Pr - shift(Pr, message)$$

Where, Wr = generated watermark pattern

Pr = Normally distributed reference pattern

Message = Message to be embedded

This watermark is then perceptually shaped for each frame so that the watermark remains perceptually invisible. Perceptual shaping is done by taking activity measure of the frame (complex texture has high activity, flat area has low activity) and used for embedding information. An authorized detector can find out the watermark by computing FFT and IFFT to

obtain peaks of the normally distributed reference pattern and watermark pattern. Peaks orientations provide sign information of the embedded bits.

2.2 Spread Spectrum Technique [12]

Spread spectrum technique, as described in [1], is a simple but very effective method for embedding digital watermark for compressed domain video. This method assumes incoming bitstream in H.261/H.263 or MPEG format. In this method, video bit-stream is first parsed
syntactically and data related to header information, motion, texture are separated out in separate buffers. Header information and motion data are kept unchanged and simply added to the output bit-stream without any alteration. DCT data is computed by performing Huffman decoding and inverse quantization. Watermark data, which is to be embedded into the stream, is first suitably converted (encryption may be used) so that it is amenable for addition to the DCT data. Watermark data is then added to the obtained DCT coefficients carefully so that it does not result in increased bit-rate. Usually 10 to 20% of DCT coefficients are altered in this manner. Altered DCT coefficients are then re-quantized and Huffman coded and then added to the bit-streams. The diagram below shows the technique. This method of Watermarking by spreading watermark information into DCT bits may result in degradation in the video signal over a period of time. To avoid this problem, a method known as "Drift Compensation" is applied. In this method, after a certain interval, the difference between
watermark and un-watermarked signal is calculated and a drift compensation signal is generated. Propagation error that occurs due to Watermarking is subtracted from the drift compensation signal. This generic method can be modified by adding advanced tools liked gain control, bit-rate controller, synchronization template for low-bit rate video.

3. PROPOSED ARCHITECTURE

The proposed algorithm is a unique blend of both visible and invisible watermarking techniques aimed at providing secure and efficient watermarks across a video. Fig. 1 gives an overall view of data flow in the proposed algorithm. First and foremost we extract frames from the video to be watermarked. This selection is done based on the key, a 10 digit number, provided by the user. The selection is done by very carefully designed special functions such that watermarking is spread evenly on the whole video and avoiding the clustering or concentration of watermarked frames in one chunk. After extracting the required frames

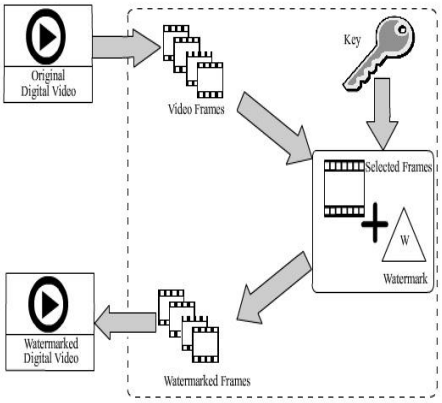

Figure 1: Proposed Architecture

from the video we start applying the watermark on them. Here we use both visible and invisible watermarks explained in detail in next section. After watermarking the frames, we insert them back in the video at their respective places and assemble the video again. We also set up a passkey identifier to give only five trials to the user. If the user inserts more then 5 wrong keys then it is assumed that he is trying to find the watermarked frames by trying random keys or even brute-force. If five wrong entries are made then the video is corrupted leaving no data behind.

4. PROPOSED ALGORITHM

The proposed algorithm is divided into four procedures. We start with accepting the digital video 'V' and a key 'K' where 'K' is 80 bits (Each 8 bits form one digit).We also provide the watermark image to be stamped across and a text file 'T' where 'T' contains the information to hide in the frames.Normally it is seen that the average FPS is 25 which means there are 1500 frames approximately in every one minute of video. We make 1% watermarking in every 1500 frames i.e. 15 frames are watermarked in every 1 min of the video. Additionally we use 10 visible and 5 hidden watermarks for every 1500 frames i.e. 1 visible watermarked frame every 150 frames and 1 hidden watermarked frame every 300 frames.

A. Procedure 1: Find and Extract Frames
Input: Digital Video, Key
Output: Selected Frames

1. Start.
2. Divide the key 'K' into 10 parts where each part is of 8 bits.
3. Using the following 10 functions we prepare offset values from x1...x10 which are

If the passkey is a b c d e f g h i and j respectively then

X1 = ad	X2 = gj
X3 = ce	X4 = fh
X5 = bi	X6 = be
X7 = fi	X8 = (X6+X7)
X9 = (X1+X3)	X10 = (X4+X2)

Here in first 7 functions we just join 2 digits and take its decimal value as offset. While in last three functions we add the values from first 7 functions. Here if any value goes beyond 150 then we use the cyclic150 () method to keep it in the range of 150. The above values are added to every multiple of 150 to get the frame number. These frames are for visible watermarking.

4. Using the following 5 functions we prepare the offset values y1...y5 which are

If the passkey is a b c d e f g h i and j respectively then

Y1 = (e+f) +2(d+g) +3(c+h) +4(b+i) +5(a+j)
Y2 = (e+f) +2(c+h) +3(d+g) +4(a+j) +5(b+i)
Y3 = (e+f) +2(a+j) +3(b+i) +4(c+h) +5(d+g)
Y4 = (Y1+Y2)-Y3
Y5 = (Y1+Y3)-Y2

Here if any value goes beyond 300 we use the cyclic300 () method to keep it in the range of 300. The above values are added to every multiple of 300 to get the frame number. These frames are for invisible watermarking.

5. Stop.

End Procedure 1

B. Procedure 2: Set Visible Watermarks

Input: Offset values X1…X10
Output: Visible Watermarked Frames

1. Start
2. Accept the watermark image.
3. Add the watermark image to every multiple of 150 plus the corresponding offset.
4. Stop

End Procedure 2

C. Procedure 3: Set Hidden Watermarks

Input: Offset values Y1…Y10, Key
Output: Hidden Watermarked Frames

1. Start
2. Accept the text file 'T'.
   Where (T.Size<=100Bytes)
3. Byte[] data=T.toBytes
4. Using the key we select 100 pixels randomly from the frame and replace them with the text file data.
5. If text file is smaller than 100 bytes then put 0 in empty places.
6. Stop

End Procedure 3

D. Procedure 4:Reassemble frames and set corruption bits

Input: Reassembled Frames, Key Checksum
Output: Reassembled Watermarked Video

1. Start
2. Generate a checksum value of all the digits of the passkey.
3. Store the checksum at the pixel position 'i' of frame number 'j' where
   i = (V.Duration*10)
   j = (V.FPS*8)
4. Set the value of pixel (i+1) to 0 and increment every time checksum goes wrong.
5. When (i+1) reaches 5 corrupt the video file.
6. Stop

End Procedure 4

With this we complete our proposed algorithm. After watermarking the video insert the video and passkey to check if the watermarking is done properly. The frame number of frames with visible watermark will be displayed. We can even get the text file hidden in the pixels of many frames.

5. EXPERIMENTAL RESULTS

The main focus of this algorithm is its dynamic and key dependent frame selection technique. We have implemented and experimented it using Java and some third party software's like 'Video to JPEG Convertor' and 'Total Video Convertor'. The experimental results are as below which show original frame and watermarked frame.

Figure 2: Original Image

Figure 3: Watermarked Frame

The results prove that the algorithm is up to the mark for watermarking and the results were as expected. One drawback is the time factor because of the time taken in dividing and reassembling the frames. This drawback can be overcome by using a high configuration Multimedia Station.

6. CONCLUSION

Thus in the proposed algorithm we presented a novel approach for frame selection in watermarking along with a combination that is both effective and secure, providing a very

good watermarking technique. The proposed algorithm is dynamic, provides multiple watermarking and corruption facilities along with small size covert communication facility.
In future this algorithm can be expanded by data mining, decreasing the frame division time and dynamic key verification and authentication technique.

7. ACKNOWLEDGEMENT

The Authors would like to thank the institutes: Shah and Anchor Kutchhi Engineering College, Padmabhushan Vasantdada Patil Pratihans College of Engineering and Saraswati College of Engineering for providing its valuable resources and assistance to the authors in their research work.

8. REFERENCES

[1] Lama Rajab, Tahani Al-Khatib, Ali Al-Haj, "Video Watermarking Algorithms Using the SVD Transfor" European Journal of Scientific Research ISSN 1450-216X Vol.30 No.3 (2009), pp.389-401 © EuroJournals Publishing, Inc. 2009

[2] Martin Zlomek," Video Watermarking", MASTER THESIS, Department of Software and Computer Science Education Supervisor: RNDr. Josef Pelikán

[3] V. Potdar, S. Han, and E. Chang, 2005. "A Survey of Digital Image Watermarking Techniques", in Proceedings of the 2005 IEEE International Conference on Industrial Informatics, pp. 709-716.

[4] Hong-mei Liu, Ji-wu Huang and Zi-mei Xiao: An Adaptive VideoWatermarking Algorithm. International Conference on Multimedia and Expo, 2001

[5] Jun Zhang, Jiegu Li and Ling Zhang: Video Watermark Technique in Motion Vector. Proceedings of the 14th Brazilian Symposium on Computer Graphics and Image Processing, 2001

[6] Langelaar, G., I. Setyawan, and R. Lagendijk, 2000. "Watermarking Digital Image and Video Data: A State-of-Art Overview", IEEE Signal Processing Magazine 17, pp. 20-46.

[7] Ingemar J. Cox, Joe Kilian, Tom Leighton and Talal Shamoon: A Secure, Robust Watermark for Multimedia. Proceedings of the First International Workshop on Information Hiding, 1996.

[8] V. Cappellini, F. Bartolini,R. Caldelli, A. De Rosa, A. Piva and M. Barni: Robust Frame-based Watermarking for Digital Video. Proceedings of the 12th International Workshop on Database and Expert Systems Applications, 2001

[9] B. Zhu, M. D. Swanson and A. H. Tewk: Multiresolution Scene-based Video Watermarking Using Perceptual Models. IEEE Journal on Selected Areas in Communications, 1998.

[10] Stefan Thiemert, Thomas Vogel, Jana Dittmann and Martin Steinebach: A High-Capacity Block Based Video Watermark. Proceedings of the 30th EUROMICRO Conference, 2004.

[11] Raju Halder, Shantanu Pal, and Agostino Cortesi, Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, The Journal of Universal Computer Science, vol 16(21), pp. 3164-3190, 2010.

[12] Frank Hartung and Bernd Girod; University of Erlangen-Nuremberg (Watermarking of compressed and uncompressed video)

[13] Gwenaël Doërr and Jean-Luc Dugelay; Multimedia communication and image group (Video Watermarking – overview and challenges)