



AN EFFICIENT VIDEO WATERMARKING SCHEM FOR CONCEALING DATA RECORDS USING LABVIEW

Dr.G.R.Gnana King¹, L.Nithya Devi², E.Pavithra³, T.Sahana⁴,A.Subhashini⁵

^{1,2,3,4,5}Department of ECE, Kathir College of Engineering

Abstract-This paper proposes a watermarking algorithm for hiding the data securely over the public network. A watermark is embedded into YCBCR (Y-Luminance, CB-Chrominance Blue, and CR-Chrominance Red) colour channels of each video frame using Discrete Wavelet Transform with Principle Component Analysis. The process of digital watermarking involves the modification of the original multimedia data to embed a watermark containing a key information such as authentication copyright codes. The embedding method must leaving the original data perceptually unchanged, yet should expose modification which can be detected by using an appropriate extraction algorithm. This method is implemented using LabVIEW.

Keywords: Video Watermarking, Defence Data Records, Principle Component Analysis, DWT.

I. INTRODUCTION

The Digital watermark is a digital signal or pattern inserted into a digital content. The digital content would be a still image, an audio clip, a video clip, a text document or some form of digital data that the creator would like to protect. The watermarking is used to identify who the owner of the digital data and also identify the intended recipient. Basically they all write desired information directly onto image or audio data in such a manner that they are not damaged.

Embedding a watermark should not result in a significant increase or reduction in the original data. The digital watermarking play vital role in data management system to protect the defence data. According to the classification of digital watermark carrier type embedded in the digital products in different types. Digital products including image, video, audio, text corresponding digital and video watermarking[1-2]. DWT protect the copyright of the images [3].The watermark extraction algorithm to extract the watermark information embedded procedure from extraction from the region [4].

In contrast more recent algorithms distributed prediction error by exploiting the correlation between the neighbouring pixels so that less distribution is caused by data hiding[5-8].DWT is very suitable to identify the exact location in host image where a watermark can be embedded effectively[9].Wavelet transform decomposes the image into a set of band limited components which can be reassembled to recover the original image without loss[10].Information hiding technology is also used in defence applications[11].Wavelet transform based watermark is very useful to identify correct locations for hiding the data [12-14].

II. PROPOSED SYSTEM

In the case of invisible watermarks, the locations in which the watermark is embedded are secret, only the authorized persons extract the watermark. This watermark is not viewable by an ordinary eye. It is more secure and robust than visible watermark. In this paper the watermark includes the defence data records. It is used to provide high imperceptibility and robustness against attacks.DWT is used in the embedding process to get the best location for hiding the watermark.

2.1 DATA EMBEDDING PROCESS

Framing

Framing is the process by which the video is segmented into frames, wherein each frame is embedded with watermark. The video is divided into frames ($2n \times 2n$), and then convert RGB frames into YCBCR frames.

Discrete Wavelet Transform

If maps of a function of a continuous variable is expanded in a sequence of number the resulting coefficients are called DWT. Choose luminance(Y) component of each frame apply DWT on it. This result in four multi-resolutions sub-bands(NXN):LL1,HL1,LH1,and HH1.For each band apply DWT again to get 16 sub-bands($N/2 \times N/2$).For each band in the 16 sub-bands, apply one more DWT to get 64 sub-bands each is ($N/4 \times N/4$).

Principle Component Analysis

It is the process by which the exact location for embedding the watermark is found. Where each frame is divided into blocks and then PCA is applied so that finding the exact location becomes an easier process.

Watermark Preparation

The defence data information is inserted into text file. This text file is converted into binary form, according to text file generate a watermark and then convert the binary image into vector of zeros and ones.

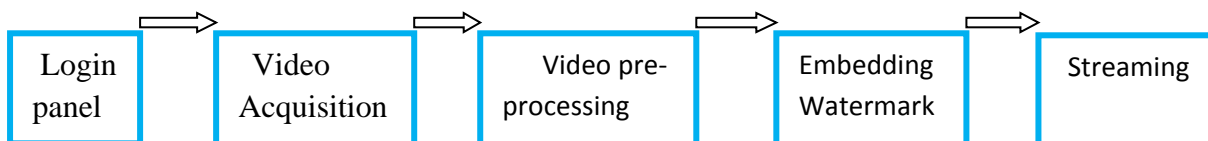
2.2 DATA EXTRACTION PROCESS

Initially convert the watermark video into YCBCR frame. For each .For each Y, CB, CR component apply DWT to decompose the channel into 64 multi resolution sub-bands. The each sub-band is divided into NXN non-overlapping blocks.

The first secret key can get the watermarked blocks.PCA is apply for each block. Using the second secret key to extract the watermark and it is compared with the original watermark by computing the similarity between them. The Two secret keys are used to extract the Watermark.

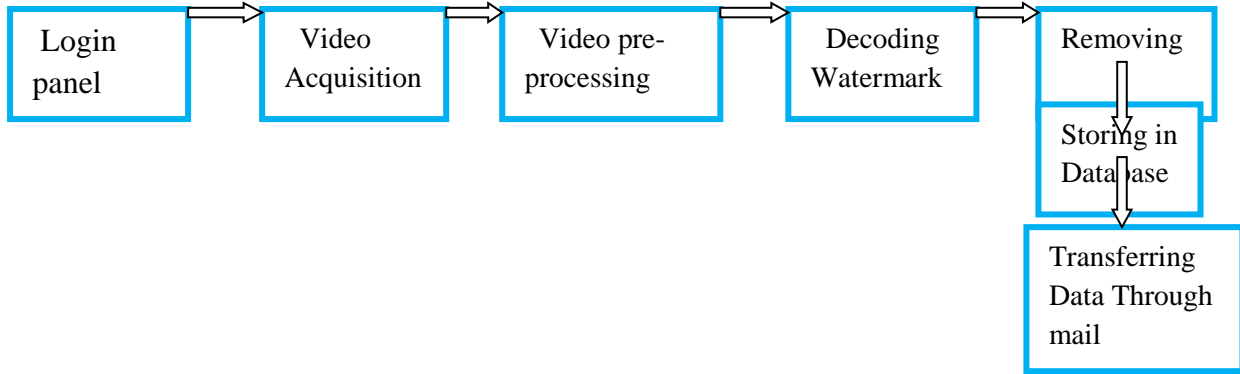
III. ARCHITECTURE

3.1 Flow process of embedding the watermark templates



Login panel is used for security purpose. In login panel we just give a user name and password, and then we access the video which contains the secured defence data. In video acquisition ,we acquire the video and it is send to video preprocessing.In video pre-processing, the FPS (frame per sec) is verified and also verify the video has any blur in it (or) not, then the video is send to embedding watermark. In embedding watermark, the hidden data is embedded into the video. Streaming which requires a source media such as video camera, audio interface to delivered live video.

3.2 Flow process of Removing and transfer the watermark templates



The above process is repeated till video pre-processing. After that, we decoding the video and remove the watermark. The hidden data is retrieve and it is stored in database. The data is transferred through the mail.

The second secret key extracts the watermark by using the given equation,

$$W' = \frac{M'i-Q}{\alpha}$$

The extracted watermark is compared with the original watermark by using the given equation,

$$NC = \frac{\sum_i \sum_j W(i,j).W'(i,j)}{\sum_i \sum_j W(i,j)^2}$$

Where, NC is the normalized correlation. If the NC value is one both watermarks are identical and NC value is zero both watermarks are totally different from each other.

Finally the binary watermark is converted into a text. This text is compared with the original text. Sometimes the error is occurred in text, the error character should be counted. The character error rate is computed by using given formula,

$$CER = \frac{E_{ch}}{T_{ch}}$$

This proposed system is tested using CT video frames. The algorithm is evaluated when varying the watermark size by changing the number of characters in the embedded text. In any watermarking scheme PSNR (Peak Signal to Noise Ratio) is used to measure the visual quality of the watermark system. The MSE (Mean Square Error) is used to compute the error between the original and extract watermark.

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [I(i,j) - I'(i,j)]^2$$

The PSNR is defined as,

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

IV. CODE COMPILATION

The LabVIEW includes a compiler that provides native code for the CPU platform. The graphical code is translated into executable machine code by interpreting the syntax by compilation. The LabVIEW technique is enforced during the editing process and compiled into the executable machine code when requested to run or upon saving.

V. EXPERIMENTAL RESULT

The performance of the proposed algorithm is used to hiding the defence data with high security. It is tested using CT video frames. The size of the frame is 512x512. This algorithm is evaluated when varying the size of the watermark by changing the number of characters in embedded watermark.

The PSNR value of Y, CB and CR channels are varied. The PSNR value of CB and CR channels are higher than the PSNR value of Y channel.

Table 1: Extracting 16x16 watermark from Y channel

Frame No.	PSNR	NC
1	59.1916	0.9853
2	59.1047	0.9853
3	59.0100	0.9632
4	58.6087	0.9706

Table 2: Extracting 16x16 watermark from CB channel

Frame No.	PSNR	NC
1	61.3997	1
2	61.4464	1
3	61.1314	1
4	61.2983	0.9926

Table 3: Extracting 16x16 watermark from CR channel

Frame No.	PSNR	NC
1	60.8848	1
2	60.9737	0.9853
3	61.1682	1
4	61.7171	1

Table 4: Summary Table

Colour Channel	Y	CB	CR
PSNR	59.13	61.15	61.10

A. 16x16 watermark with 36 characters

Colour Channel	Y	CB	CR
PSNR	51.95	54.18	54.16

B. 32x32 watermark with 73 characters

Colour Channel	Y	CB	CR
PSNR	45.00	46.68	46.52

C. 64X64 watermark with 146 characters

In the existing scheme which consists of colour channel like Y, CB, CR and they have the PNSR value of 45, 46.68, and 46.52. But in the proposed scheme the PSNR value we attain is 60. Frame size is same for both the schemes. We received high value PSNR while compared with the existing scheme [Table 1-5].

LabVIEW is the advanced technology while compared to MATLAB, because LabVIEW is fond of graphical icons. This technology which overcomes the existing drawbacks in MATLAB.

The Fig 4.1, shows LabVIEW is used to create the username and password. The purpose of using the user id and password is for secure the concealing data, without knowing the id and the password no one can't access and hence, the data being safe and secured. Labview is used to Capture the image

and retrieve the video and display the concealing message fig 4.2. Then the retrieved video is stored in the database. By using this database we can use the data n no of times.

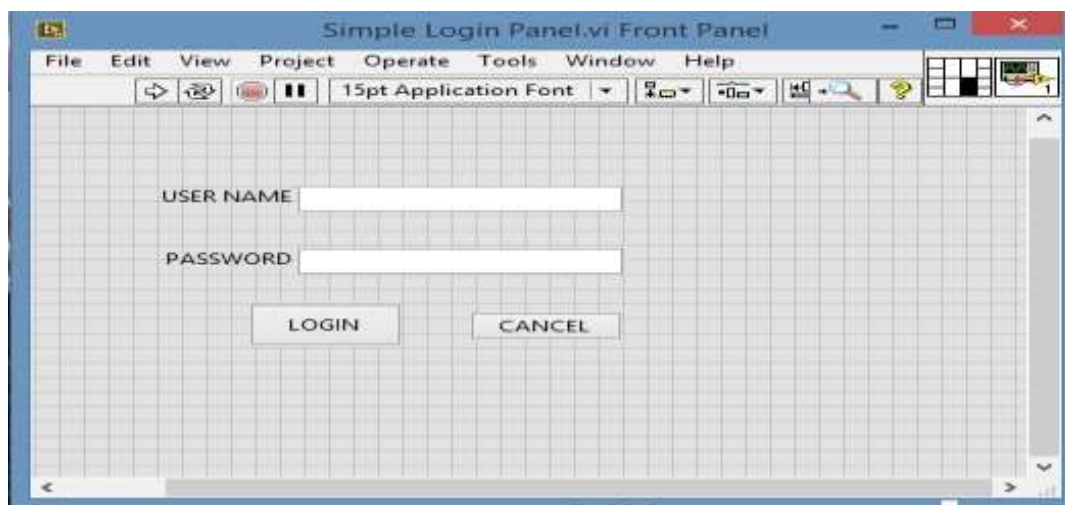


Fig: 4.1 Simple login panel

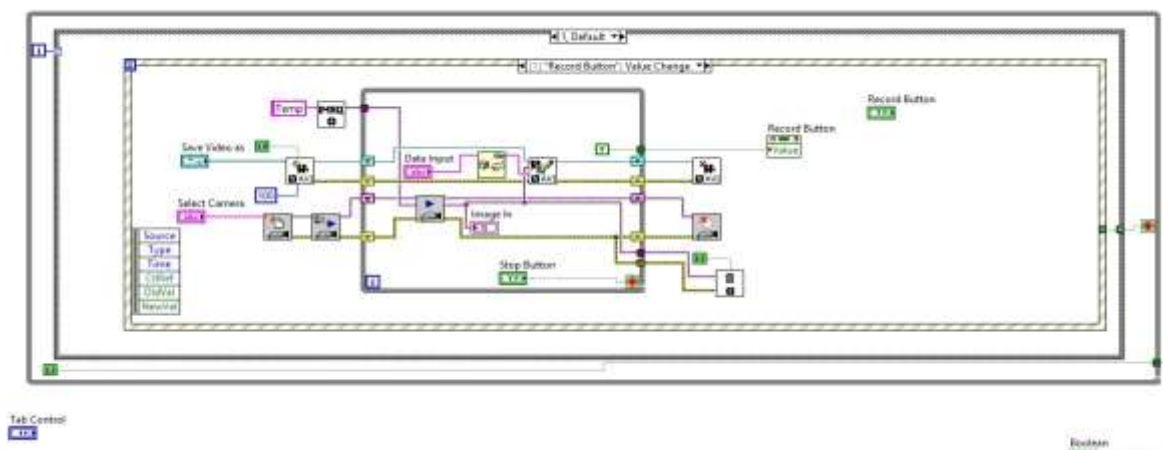


Fig: 4.2 Retrieve the video and display the concealing message

VI. CONCLUSIONS

This paper presented a high capacity watermarking scheme which can be used in defence applications. The algorithm depends on embedding a data records into defence videos. DWT with PCA transform is used in the embedding process. This transform is used to identify the best locations for hiding the watermark. It has a good performance compared with previous schemes. The simulation result shows that the algorithm provides security, invisibility and robustness. Improving the algorithm robustness and applying it to the medical and satellite videos for the better imperceptibility, will be our future work. This concept is used in many applications such as Transaction tracking, Content authentication, Automatic monitoring of copyrighted material on the web.

REFERENCES

1. Li Jian, Pan Qing, Yang Taint, "Colour Based Greyscales-fused Image Enhancement Algorithm for Video Surveillance", Third International Conference on Image and Graphics, pp.47-50, 2004.
2. S.C.Mukhopadhyay, S.DeBChoudhury, T.Allsop, V.Kasturi and G.E.Norris,"Assessment of pelt quality in leather making using a novel non-invasive sensing approach", Journal of biochemical and biophysical methods, Elsevier, JBBM Vol.70, pp.809-815, 2008.
3. Ramesh, S.M and Shanmugan, A."An efficient robust watermarking algorithm for embedding the digital signature into images using DWT".European Journal of Computer Scientific Research, vol.60, no.1, 33-44.2011

4. G.Sen Gupta, S.C.Mukhopahyay, Michael Sutherland and Serge Demidenko,"Wireless Sensors Network of selective activity", IEEE IMTC conference,Warsam,Poland .2007
5. V.Sachnev,H.J.Kim,J.Nam,S.Suresh,and Y.Q.Shi,"Reversible watermarking algorithm using sorting and prediction,"IEEE Trans.Circuits Syst.Video Technol.,vol.19,no.7,pp.989-999,Jul.2009.
6. X.Li, B.Yang, and T.Zeng,"Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,"IEEE Trans.Image.Process., vol.20, no.12, pp., Jan.2011.
7. Z.Zhao, H.Luo,Z-M.Lu,and J-S.Pan,"Reversial data hiding based on multilevel histogram modification and sequential recovery,"Int.J.Electron.Commun.(AEU),vol.65,pp.814-826,2011.
8. H.T.Wu and J.Huang,"Reversible image watermarking on prediction error by efficient histogram modification,"Signal process. vol.92, no.12, pp.3000-3009, DEC.2012.
9. Ali Al-Haj,"DWT-DCT Digital Image Watermarking". Journal of computer science 3(9):740-746, 2007.
10. Transform,"Proc.IEEE international conference on telecommunications, MAY 2007.
11. W.Bingxi and P.Tianyang,"Information Hiding Technology"," National Defence Science Technology"press,pp.64-86,2007.
12. H.Lian,B.N.Hu,R.M. Zhao and Y.L.Hou,"Design of Digital watermarking algorithm based on Wavelet Transform", proceeding of the Ninth international conference on machine learning and cybernetics,IEEE,2010.
13. I.Cox, J.Bloom and M.Miller, digital watermarking principle and practice, Morgan kaufmann publishers, first edition, 2001.
14. X.G.Xia, C.G.Boncellet and G.R.Arce,"Wavelet Transform based watermark for digital images, "optics express, pp.497-511, 1998.