ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 5, March 2018

VIDEO AUTHENTICATION AND DATA HIDING USING DIGITAL WATERMARKING

M.Murugeswari[1], M. Prabhavathi[2], G. Sivakamasundari[3]
[1,2] UG Student, [3]Assistant Professor, [1,2,3] Department of Computer Science and Engineering
[1,2,3] National Engineering College

***Abstract*-This paper has been proposed to ensure the data security as well as the content authentication. The proposed system consists of embedding the image into the video using the private key and the image is extracted from the video using that key. Here the image acts in two ways. In case of authentication purpose, this image acts as a watermark image and in case of data security, this image acts as the data that has to be sent secretly. Hence this system can be used for dual purpose. The frame of the original video is converted from RGB colour space into YCbCr colour space. Then from that colour space the chrominance component Cb is alone partitioned into blocks of pixels which are non-overlapping. The image is also divided into pixels and the pixels of the image are embedded into CB pixel of video and combined to form YCbCr. Then YCbCr is converted into RGB Frame which results in the watermarked frame. In the receiver side, the RGB watermark frame is converted into YCbCr and from that CB is divided into non-overlapping blocks and finally, the image is extracted from that block.**

Keywords* — *Content Authentication, Fragile ***Video Watermarking, Modulation factor***

I.INTRODUCTION

One of the biggest challenges in today's world is the effective data security services and ensuring an end to end security. Due to the rapid growth of cyber-attacks and other crimes the data reliability is not ensured. Further, in digital forensics, the video acts as the main evidence. There is a chance of attempting the changes to the content of the video. Hence video authentication is very important. This authentication method is proposed in this video. Further, this method can also be used to send the messages secretly. Even if the attackers capture the video in between the message will not be displayed. Since it is embedded in the video only the video will be displayed and not the image.

The security service includes various features. They are

Confidentiality:- It ensures that the information transmitted is accessible only by authorised parties. The information transmitted should not be known to third party members

Authentication:- It ensures the message is found correctly with an assurance of identity is true

Integrity:-It ensures that only authorised parties are able to make changes in the information. The changes include writing, deleting or replaying of messages.

Non-Repudiation:- It requires that both the sender and receiver should not deny the transmission of information. Hence to provide the above security features, the digital watermarking scheme is applied. Digital watermarking is the method of embedding data into digital multimedia content. This paper presents a single methodology which can be used for authentication of video and data hiding. Here an image is embedded into a video by watermarking techniques. The data to be hidden can be made in the form of the image thereby the data can be sent safely and in case of authentication purpose of the video, we can use the watermark image thereby the receiver can ensure the correct sender.

II.RELATED WORK

[1] The paper "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis" presented by Sanjana Sinha et.al in the year August 2011.Its emphasis on two techniques. Here the system is based on mainly DWT and PCA. Initially, the video is converted into frames are the frames are decomposed by using DWT technique and then the watermark is embedded into the wavelet coefficients components. Here the video frame is decomposed into

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 5, March 2018

wavelength coefficients. The PCA helps to reduce the correlation so that the watermark bits are dispersed into the coefficients. That It can be implemented on the watermarked video, such as cropping, filtering, colour change, the addition of noise and other geometric attacks. [2] The paper "recent survey on data hiding techniques" presented by Sandeep Singh et.al in the year February 2017. Data hiding is a process of concealing the content from the outside world. Data hiding can be done in digital contents like audio, video, and image etc.., Some data hiding techniques focus on safety concerns and some on robustness. The amount of information which has to hidden is also the important one. The various schemes like Steganography and other cryptography, watermarking were discussed here. The method Steganography is concerned with hiding one form of information into another. Cryptography includes encryption and decryption of information. Watermarking is concerned with embedding the host image with watermark information and the watermarked image is now sent and received by the receiver where it is extracted.[3]The paper "Data hiding technique in the video using a secret key" by Chaitali.D.Raut in the year 2016.Here the data to be kept the secret is embedded in the image. The content holder conceals the original message using a secret key in a medium. In the receiver side he follows the reverse method and by using the key he extracts the data. Here to hide the data LSB method is used. But there is the disadvantage while using LSB. There is a chance of change in the least significant bit of image while using the lsb. Hence the quality of the image can be affected. Hence to overcome the defects, we framed an improved LSB with 1,4,3 bit position technique. In order to hide data, the block size of 4x4 is used here.[4]The paper "A new reversible data hiding algorithm in the encryption domain" by Shuang yi et.al in the year October 2014.It uses the new reversible data hiding algorithm. It combines the data concealing and the encryption process to achieve more security. The main aim of this paper is to fully recover the original content. This technique can be used in the fields where we need to protect both the cover image and the secret data. The various steps are followed here. The first step is to encrypt the image by xor operation. Then the encrypted image is separated into non -overlapping blocks of size a*a. Finally, the secret data is embedded into each block by flipping another advantage is that the image recovering and data extraction can be done individually by using different security keys.[5]The paper "A Fragile Video Watermarking Algorithm for Content Authentication based on Block Mean and Modulation Factor" by A.F.ElGamal et.al in the year October 2013.This paper proposes the fragile watermarking technique to detect the tamper or changes made in the video. It involves the following steps. The frame of the original video is converted from RGB colour space into YCbCr colour space. Then from that colour space the chrominance component Cb is alone partitioned into blocks of pixels which are non-overlapping. The image is also divided into pixels and the pixels of the image are embedded into CB pixel of video and finally, thereby the image is embedded. The experimental result shows that it achieves low computation cost and high rate of detection. It also ensures that the quality of video is not affected [6]. The paper "The Robust Digital Image Watermarking Scheme with the Back Propagation Neural Network in DWT Domain" by Nallagarla Ramamurthy et.al in January 2013.This paper uses novel scheme image watermarking. Here they have used two techniques. They are neural network and backpropagation. Here the the blue pane is embedded with watermark of the colour image using discrete wavelet transform and Back Propagation Neural Network. Here the image is decomposed into various components. The various components are LL, HL, LH, and HH. From the many components, LL is first chosen and decomposed. Here by adjusting the weights, the relationship between coefficients of original wavelet and watermarked wavelet is established. Another feature here is we can extract the watermark image without using original signal

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 5, March 2018

III. PROPOSED METHODOLOGY

In the proposed system, the fragile watermarking algorithm is used. It consists of three phases. Video conversion, Embedding phase and Extraction phase. In video conversion first, the video is converted into frames. In Embedding phase, the video frame is transformed from RGB colour space into as YCbCr. Now, the chrominance component Cb is chosen. Now the Cb component is tilled into B*B non-overlapping blocks of pixels, now the image bits pixels are embedded into the CB pixels. Finally, the embedding is done. The procedures of the extraction phase are performed in a reverse order to the embedding

MODULES:

- Video Conversion
- Embedding Phase
- Extraction Phase

A. Video Conversion

It takes the input video and converts the video into many frames

B. Embedding Phase

In Embedding phase first, the video frame is converted from RGB colour space into YCbCr colour space. Conversion from RGB to YCbCr is done by

Y=(77/256)*R+(150/256)*G +(29/256)*B
Cb=-(44/256)*R–(87/256)*G+(131/256)*B + 128
Cr=(131/256)*R–(110/256)*G–(21/256)*B+128 **(1)**

Next, the chrominance component Cb is chosen for watermarking because the chrominance part can lose much data, without affecting the frame quality. Then the Cb component is tilled into B*B non-overlapping blocks of pixels and each block is watermarked separately. Finally, the watermarked frame is converted back from YCbCr colour space to RGB. Conversion from YCbCr to RGB is done by

R = Y+1.37*(Cr-128)
G =Y–0.69*(Cr-128)–(0.336)*(Cb-128)
B = Y+1.732*(Cb-128) **(2)**

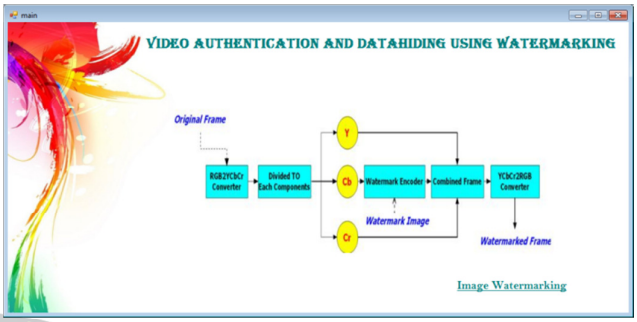

FIG 1: VIDEO AUTHENTICATION

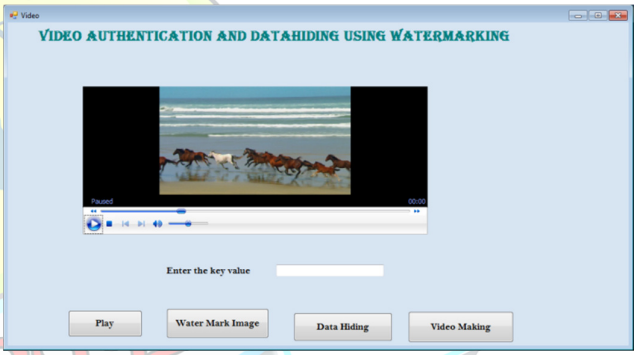

FIG 2: INSERTION OF WATERMARK IMAGE

C. Extraction phase

The procedures of the extraction phase are performed in a reverse order to the embedding**.** The details of the extraction algorithm are listed as follows:

Input: Watermarked colour video.
Output: Binary watermark image.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 5, March 2018

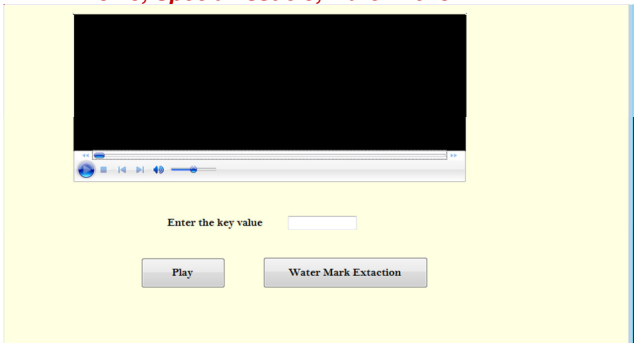

FIG 3: WATERMARK IMAGE EXTRACTION

Steps:

(1) Load the the video which is watermarked.

(2) Divide watermark into distinct watermarked frames.

(3) Convert the frame from RGB colour space into YCbCr format.

(4) Select the chrominance component Cb of each frame to extract the watermark.

(5) Divide Cb into non-overlapping blocks (with the size b*b) according to the number of bits of the original.

(6) Collect the watermarked blocks to get the watermarked frame.

(7) Convert back the watermarked frame from YCbCr colour space to RGB and output the extracted watermark.

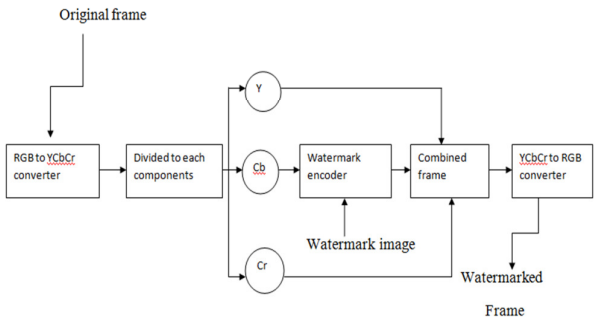

Fig. 1 Overall System Architecture

IV. RESULT

The experimental result shows that this method can be able to detect various defects like the addition of salt and pepper noise, cropping, rotation, filtration, flipping. Hence the proposed algorithm is desirable to provide an indication of how much alteration has occurred and where it is located.

V. CONCLUSION

In this work, we proposed the fragile watermarking algorithm for data hiding and the content authentication. The results show that the proposed algorithm can able to detect and locate the video without any effect on the visual quality of the watermarked video.

REFERENCES

[1] The paper “Digital Video Watermarking using the Discrete Wavelet Transform and Principal Component Analysis” by Sanjana Sinha, Ankul Jagatramka, Dipak K. Kole, Aruna Chakraborty, Swarnali Pramanick, Prajnat Bardhan.

[2] The paper "recent survey on data hiding techniques" by Sandeep Singh, Amit Kumar Singh, S P Ghrera in the year February 2017

[3] The paper "Data hiding technique in video using a secret key" by Chaitali.D.Raut

[4] The paper “A new reversible data hiding algorithm in the encryption domain” by Shuang yi, yicong zhou,chi-man pun

[5] The paper "A Fragile Video Watermarking Algorithm for Content Authentication based on Block Mean and Modulation Factor"

[6] The paper “The Robust Digital Image Watermarking Scheme With Back Propagation Neural Network In DWT Domain” by Nallagarla Ramamurthy and S.Varadharajan