Watermarking Using Transformation Domain Technique Using Visual Cryptography

Jyoti V. Prasad1, Padmashree G2, Venugopala P. S3

Abstract—Watermarking is a technique of embedding imperceptible signal in to a digital content mainly for protecting authentication information of content owner. It adds a layer of security to the content and helps in identifying unauthorized access. fight by making use of hidden copyright information. It is also helps to protect the content from several attacks on it. In this paper we use transformation domain technique using scene change detection with visual cryptography. Here we divide the watermark image in to smaller parts and applying visual cryptographic technique on each part. and embedding each part in to DCT coefficients to prove it to be more robust and secure method.

Index Terms— Robust, DCT, Visual Cryptography, Transformation Domain Technique.

1. INTRODUCTION

Digital watermarking is a technology used for hiding information. It is a process by which copyright information such as logo can hidden behind the digital content in visible or invisible way. The success of watermarking depends on technology used for inserting watermark and choice of watermark structure. The two main issues involved in watermarking are those of maintaining the robustness of the watermark information and keeping visual perception of the original image intact. Apart from copyright protection and copy control digital watermarking is also useful in the areas of broadcast monitoring, fingerprinting, indexing, medical application, content authentication etc.

There are many technologies used in the areas of data hiding such as Cryptography, Steganography and Watermarking. Cryptography deals with scrambling message into a code to protect its meaning. This is done with the secret key. The same secret key is used to decrypt the message at the receiving end. Steganography deals with protecting the message or its value using some clever hiding technology. Whereas in Watermarking technology additional information is directly embedded into the original content or host signal. Ideally, there should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host signal.

There are many technologies used for watermarking insertion such as

1. Spatial domain technique
2. Transformation domain technique

In Spatial domain technique, the pixel values of directly modified.

In transform domain technique, the transform coefficients are modified. For the extraction of watermark inverse transformation is performed. Some common transform domain techniques are:

1. Discrete Cosine Transform (DCT)
2. Discrete Fourier Transform (DFT)
3. Discrete Wavelet Transform(DWT)

Here we are using DCT method for watermarking.

The paper is organizes in the following manner. In section that is section II deals with the literature survey different Watermarking technologies. Section III deals with proposed method of this system. Section IV deals with the methodology that has been implemented in this paper. In Section V Experimental results are described in Section 6 contains conclusion remarks of the experiment conducted.

2. LITERATURE REVIEW

There are many watermarking techniques are in use now a day's which can resist many possible attacks against it using different domains such as spatial and transform domains.

a) Transform Domain Techniques

Compare to spatial domain techniques transform domain techniques are more applied. Here we insert the watermark in to spectral coefficients.

2.1 DCT

In this technique signal will be converted in to elementary frequency components. In a 2D DCT matrix, leftmost corner of a matrix represent lowest frequency coefficients where the bottom most corner represent the highest frequency coefficients. Watermarking with DCT is more robust compare to spatial domain techniques. This can be divided in to

- *Jyoti V. Prasad, pursuing M.Tech.in Computer Networks Engineering, Mangalore Institute of Technology & Engineering, Moodabidri (DK), under Visvesvaraya Technological University, Belgaum-590014, (Karnataka) (e-mail: jyoth.prasad@gmail.com).*
- *Prof. Padmashree G, working as Senior Assistant Professor, Department of Computer Science and Engineering in Mangalore Institute of Technology & Engineering, Moodabidri (DK), under Visvesvaraya Technological University, Belgaum-590014, (Karnataka) (e-mail: padmashree@mite.ac.in).*
- *Prof. Venugopala P.S., Working as Assoc. Proffessor, Department of Computer Science and Engineering in NMAMIT, Nitte, Karkala, Udupi Dist, (email: venugopalaps@gmail.com)*

1. Global DCT Watermarking
2. Block based DCT watermarking

In a system proposed by Vani Bhat[1], used a blind watermarking algorithm on uncompressed video. She embeds bit-plane watermark bits into the luminous pixel value for each video frames. Scene change detection algorithm is used for detecting scenes in the video. In each scene same bit plane image is embedded and different scene contains different bit plane image. The extraction process she used is a blind and the watermark can be extracted without any distortion from the watermarked frame. The system is robust against attacks such as frame dropping, temporal shifts and addition of noise. The robustness can be further be improved.

In this case according to the energy regions spectral regions are separated and transform is applied to all part of the image. V.M. Potdar, S.Han and E. Chang [8] uses, segmentation of the image into non-overlapping of 8 x 8 blocks. Forward DCT is applied to each of these blocks. Block selection criteria and coefficient selection criteria is used to select particular block. Finally watermark is embedded by modifying the selected coefficients and apply inverse DCT transform on each block.

A block based method called Optional differential energy watermarking of DCT encoded images and video is proposed by Langelaar and Langendijk [8]. A block which composes of several 8x8 DCT blocks is inserted with a watermark bit by dividing the block into two parts. In order to produce an energy difference in the two parts of the same block, where the energy difference is determined by the watermark bit, the High frequency DCT coefficients in the compressed bit stream are selectively discarded. The number of 8x8 DCT blocks in a block, JPEG quantization, step size, and a minimal cut-off index for watermarking are the three parameters in this technique.

2.2 DWT

Cheng et al. [4] proposed an algorithm which was based on embedding the watermark image in three times at three different frequency bands, namely, low, medium and high and It is proved that, watermark cannot be totally destroyed by any type of filter.

S.Faragallah presents an efficient and robust video watermarking approach based on singular value decomposition performed in DWT domain [11][9]. Video frames are transformed with DWT using two resolution levels, high frequency (HH) and middle frequency (LH, HL) to embed the watermark data, making it robust against video characteristic and image processing attacks.

2.3 Visual Cryptography

Noar and Shamir[10][12][13][14] proposes visual cryptographic mechanism based on pixel level. This is used to hide information by dividing the picture in to shares of black image and white image. White pixel is divided into 4 sub pixels and black pixel is shared in to complementary sub pixel layouts. For security purpose layout will be randomly chosen. Each pixel has 2 black and 2 white pixels

Pixel	Probability	Share1	Share2	Share1 × Share2
	50%			
	50%			
	50%			
	50%			

Figure 1: Visual cryptography Pixel expansion technique

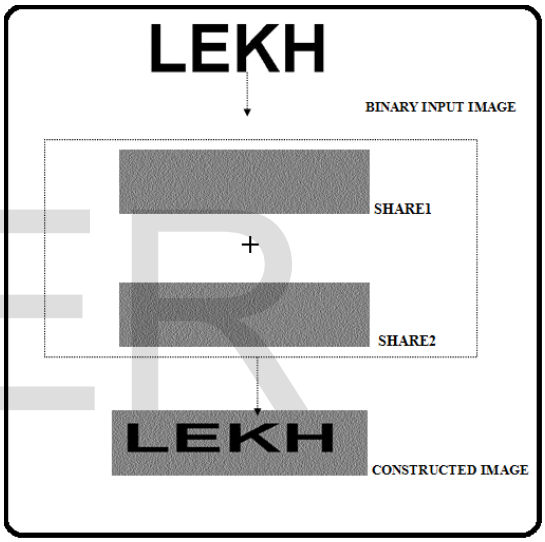

Figure 2: Process of Visual Cryptography

3. Proposed System

In a proposed method we use DCT based watermarking. Here scene detection[1] is used and the watermark image will be divided into smaller parts and each part is converted in to binary image. Visual cryptography[9][5] is applied to each part. and 2 shares are generated for each part. Each share is embedded into successive scenes to make system more robust. As the scene change detection occurs the different shares are embedded. Blind extraction is used where no reference picture is used. After extraction the received part will be re-arranged. This is to make the watermark more robust and secure.

This system uses MATLAB application. It mainly contains 3 modules.

Module Description:

i. Watermark creation module.
ii. Watermark embedding module.
iii. Watermark extraction module.

i) Watermark creation module:

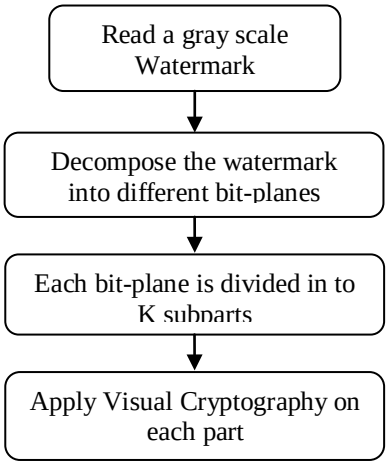

Figure 3: Watermark Creation Process

To make system more robust against attacks, it uses watermark creation in mainly 3 phases.

1. Extract the image in to bit-planes.[1]
2. Divide each bit-planes into K subparts
3. Apply visual cryptography on each subparts. [5]

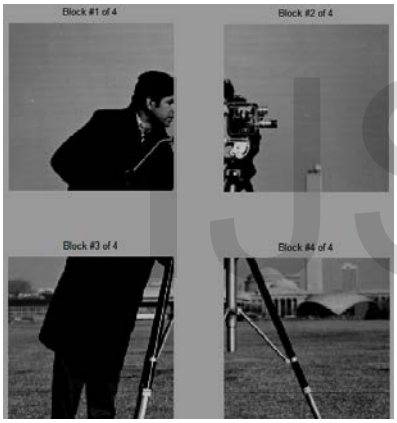

Figure 4: Dividing an Image in to smaller parts

ii) Watermark Embedding Module

This module mainly uses scene change detection algorithm by calculating histogram difference between 2 consecutive frames. The histogram difference is calculated by defining certain threshold value. If the difference exceeds the threshold value, it will be treated as scene change.

Video which is to be used in watermarking process will first be converted in to frames. Each frame is converted in to picture. Each picture is than converted from RGB in to Ycbcr [1] format. In that luminous channel is chosen and used for embedding.

For embedding[1] the shares generated from the visual cryptographic function and it will be adjusted with the intensity value of video frame. For this it also uses similarity measure. [1]

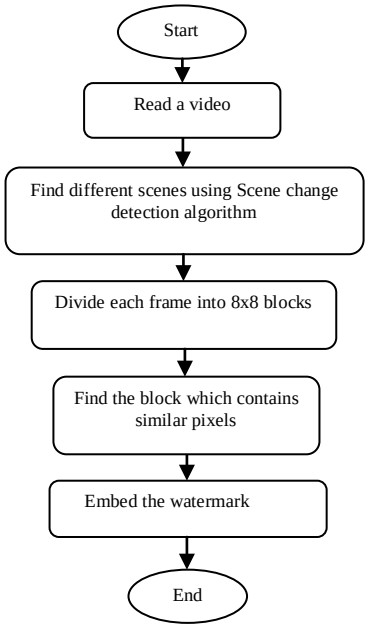

Figure 5: Watermark Embedding Process

iii) Watermark Extraction Module

This module uses blind extraction method where there is no reference picture is used. It uses extraction process by taking watermarked video[1]. Each share extracted from the first frame of each scene, rejoined and rearranged

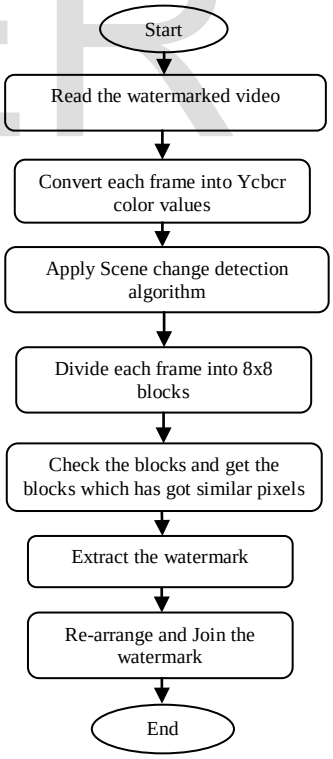

Figure 6: Watermark Extraction Process

4 The system is implemented using MATLAB 2010a environment. A grayscale image is taken as a watermark and divided in to vertically and horizontally 4 smaller parts. Visual cryptography is applied to each part. Since by using visual cryptography the pixel expansion is done, the size of the image will increase horizontally. The

uncompressed AVI video used is 144x176 and 7 watermark bits can be embedded into each 8×8 block, so the maximum capacity of each video frame in the proposed watermarking algorithm is 2772 watermark bits at most. Therefore, gray scale image of size 21x21 is chosen. I have experimented this with 2 video files of 8841KB and has 119 frames with the duration of 7 seconds.

Since the proposed method uses a series of watermark signals which are divided into smaller parts makes system more robust. If an attacker want to get watermark image he need to get all the video frames. Even in the case of some of the frames dropped or all the frames dropped due to attack and only one frames remains per scene, we are able to get back the watermark inserted, since one part is embedded in each successive individual scene, this makes it more robust against attack by frame dropping.

Visual cryptography gives more security on the authentication information, because one can identify an image

Figure 9: Shares generated using Visual cryptography

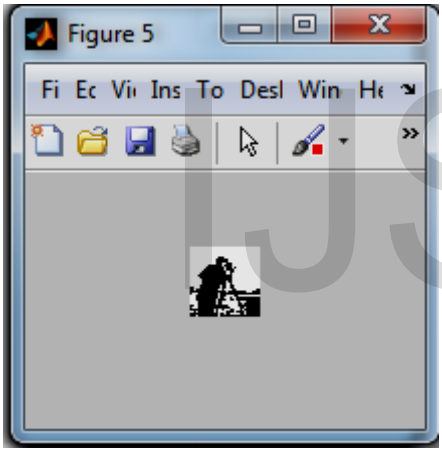

Figure 7: MSB bit-plane of cameraman picture

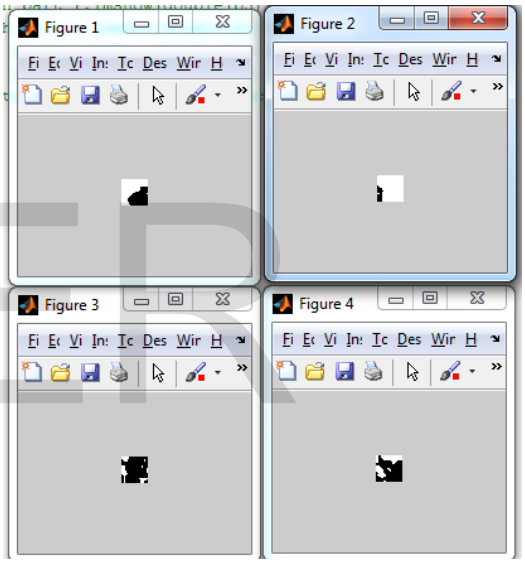

Figure 10: Extracted parts

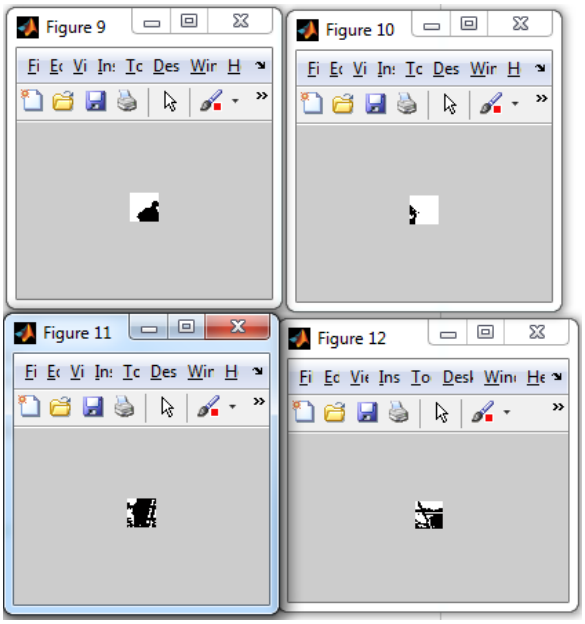

Figure 8: Snapshots of bit-plane image part

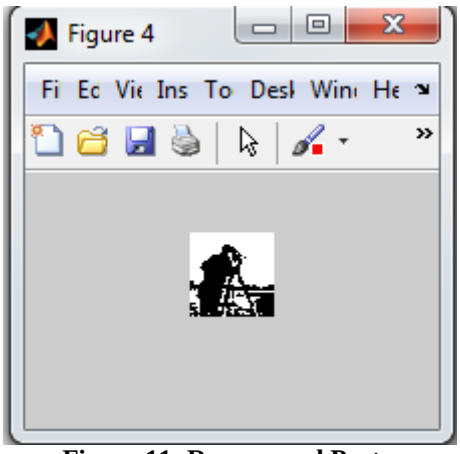

Figure 11: Rearranged Parts

It does not considerably affect the quality of the video after watermarking. Following figure shows the first frame of the video before and after watermarking.

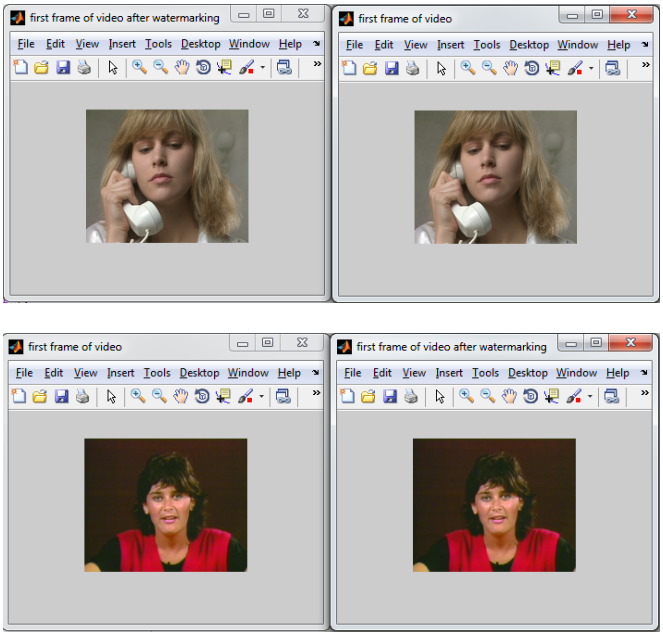

Figure 12: First Frame Before and after watermark

5. Conclusion And Future Work

With the gaining popularity of multimedia on Internet preserving a copyright information of owner of multimedia is an important matter. The proposed method uses watermarking of uncompressed video. It successfully embeds watermark bits by dividing the image into smaller parts and by applying the visual cryptography on each parts. It is able to reconstruct the embedded part successfully . It uses blind extraction technique. With the experimental results we can come to know that the system is more robust against certain attacks.

This can also be improved by combing audio watermarks. It can also use some advanced visual cryptographic concept with coloured images. This will certainly reduces the chances of attacks and loss on the copyright information.

References

[1] Video Watermarking by Adjusting the Pixel Values and Using Scene Change Detection, Vani Bhat, Dept of Computer Science, NMAMIT, Nitte, Venugopala P SAsst. Professor, Dept of CSE, NMAMIT, Nitte

[2] Optimization of Bit Plane Combination for Efficient Digital Image Watermarking, Sushma Kejgir Department of Electronics and Telecommunication Engg. SGGS Institute of Engineering and Technology, Vishnupuri, Nanded, Maharashtra, India.

[3] Video Water Marking Using Abrupt Scene Change Detection, Kintu Patel, Mukesh Tiwari, Jaikaran Singh

[4] Performance Comparison of Digital Image Watermarking Techniques: A Survey, Namita Chandrakar Department of Electronics and Telecommunication Shri Shankaracharya Technical Campus Bhilai, India

[5] A Visual Cryptographic Technique to Secure Image Shares Jagdeep Verma, Dr.Vineeta Khemchandani

[6] Comparison of Digital Water Marking methods, Darshana Mistry Computer Engineer Department Gandhinagar Institute Of Technology Gandhinagar, India

[7] Recursive Information Hiding in Threshold Visual Cryptography Scheme, Lekhika chettri1, Sandeep Gurung2, Department of Computer Science & Engg., Sikkim Manipal Institute of Technology

[8] A Review of Different Techniques on Digital Image Watermarking Scheme, Y. Shantikumar Singh1, B. Pushpa Devi2, and Kh. Manglem Singh3, 1 Department of ECE, 3Department of CSE, 1, 3 NIT, Manipur, India

[9] Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography Manoj Kumar1 and Arnold Hensman2, School of Informatics and Engineering, Institute of Technology Blanchardstown, (ITB), Blanchardstown, Dublin

[10] M. N. a. A. Shamir, "Visual cryptography," In EUROCRYPT, pp. 1-12, 1994.

[11] OsamaS.Faragallah, "Efficient Video Watermarking based on singular value decomposition in the discrete wavelet transform domain," International Journal of Electronics and Communications (AEU), vol. 67, no. 3, pp. 189-196, 2013.

[12] An Overview of Visual Cryptography based Video Watermarking Schemes: Techniques and Performance Comparison Adrita Barari 1, Sunita Dhavale 2 1 Dept. of Electronics Engineering, Defence Institute of Advanced Technology, Pune- 411025, India. Email: mailadrita@gmail.com, 2 Dept. of Computer Engineering, Defence Institute of Advanced Technology, Pune- 411025, India,

[13] Visual Cryptography Scheme Based On Pixel Expansion for Black & White Image, Lekhika Chettri Dept of Computer Application, Sikkim University, India

[14] Visual Cryptography, Moni Naor*and Adi Shamir, Department of Applied Math and Computer Science, Weizmanu Institute, Rehovot, 76100, Israel.