Extended Performance of Digital Video Watermarking using Hybrid Wavelet Transform with Haar, Cosine, Kekre, Walsh, Slant and Sine Transforms

Tejas S. Kulkarni
Department of
Information Technology,
PCCOE, Pune, India

ABSTRACT

Video piracy has become an important issue nowadays as digital data has improved over decades. With advancement of technology, it is important to find a way to propose ownership over digital videos. To solve this issue, one can consider use of watermark. A watermark is an image which can serve as content which can be extracted from a video to claim ownership of digital video. Video watermarking is applied in either spatial domain or transform domain till now in research methodologies. This paper proposes new method of watermarking which is based on hybrid wavelet transform. Proposed method has illustrated that use of hybrid wavelet transform for Cosine-Walsh transform generates better results as compared to Cosine transform and other hybrid wavelet transforms. System is analyzed against attacks such as cropping, salt and pepper and Gaussian attack.

Keywords

Hybrid wavelet transform, Cosine transform, Haar transform, Kekre transform, Walsh transform, Slant transform, Sine transform

1. INTRODUCTION

The quality and quantity of digital data is both improved and increased after rapid advancement of technology. As digital data has increased, the need to protect one's proprietary digital data has gained interest in current research areas. One of the methods to secure digital data is watermarking. Digital watermarking is a technique to ensure ownership of digital data by application of watermark on digital data such as images and videos. Video piracy is becoming more and more difficult issue, as anyone can make as many copies of digital videos and share them. Such illegal acts cannot be determined by existing techniques which are only based on cryptography which provide only confidentiality, integrity and authenticity of data. In this scenario one can consider use of digital video watermarking [1].

1.1 Types of digital watermarking

According to how watermark is applied on image, watermarking techniques are classified into various ways as shown in fig. 1.Based on human perception, watermarking can be visible or invisible [2]. Visible watermarking ensures that watermark is visible to the user while invisible watermarking hides the very presence of watermark from user or attacker. Invisible watermarking can be robust or fragile. Robust watermark is a watermark which should be robust against various attacks and fragile watermark gets destroyed even because of slightest change in signal or any attack.

Based on type of cover medium, watermarking is divided into Textual, video, image and audio watermarking. Textual watermarking is used to protect important documents of one's organization such as articles in journal and digital libraries which are present in digital format. Video watermarking consists of extracting frames from video and applying watermark on those frames. Image watermarking consists of a watermark which is embedded on cover image. Audio watermarking uses the characteristics of human ear which tells that with presence of strong audio signal with weak one, human ear cannot tell the difference in these two.
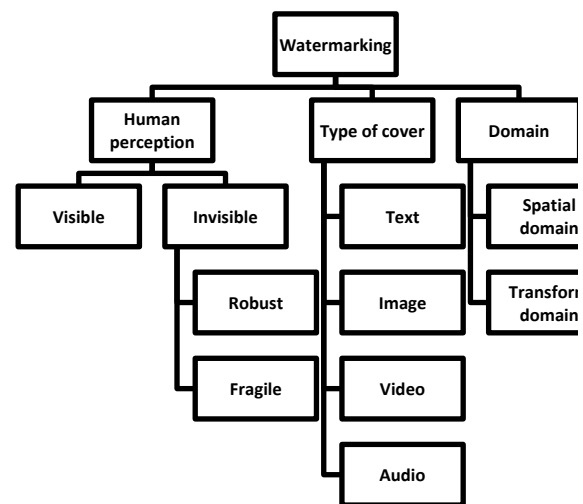

Fig 1: Types of watermarking

Based on domain, watermark can be embedded in spatial domain or transform domain [3]. In spatial domain, watermark is embedded on cover image by directly changing the pixel values It's a simple technique and its computation.

$T_{st}=$	$S_{11}\begin{bmatrix}t_{11}\\t_{21}\\\vdots\\t_{b1}\end{bmatrix}$	$S_{12}\begin{bmatrix}t_{11}\\t_{21}\\\vdots\\t_{b1}\end{bmatrix}$	...	$S_{1a}\begin{bmatrix}t_{11}\\t_{21}\\\vdots\\t_{b1}\end{bmatrix}$	$S_{11}\begin{bmatrix}t_{12}\\t_{22}\\\vdots\\t_{b2}\end{bmatrix}$	$S_{12}\begin{bmatrix}t_{12}\\t_{22}\\\vdots\\t_{b2}\end{bmatrix}$	...	$S_{1a}\begin{bmatrix}t_{12}\\t_{22}\\\vdots\\t_{b2}\end{bmatrix}$	...	$S_{11}\begin{bmatrix}t_{1b}\\t_{2b}\\\vdots\\t_{bb}\end{bmatrix}$	$s_{12}\begin{bmatrix}t_{1b}\\t_{2b}\\\vdots\\t_{bb}\end{bmatrix}$	...	$S_{1a}\begin{bmatrix}t_{1b}\\t_{2b}\\\vdots\\t_{bb}\end{bmatrix}$	b rows
	S_{21}	S_{22}	...	S_{2a}	0	0	...	0	...	0	0	...	0	b rows
	0	0	...	0	S_{21}	S_{22}	...	S_{2a}	...	0	0	...	0	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	0	0	...	0	0	0	...	0	...	S_{21}	S_{22}	...	S_{2a}	
	S_{31}	S_{32}	...	S_{3a}	0	0	...	0	...	0	0	...	0	b rows
	0	0	...	0	S_{31}	S_{32}	...	S_{3a}	...	0	0	...	0	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	0	0	...	0	0	0	...	0	...	S_{31}	S_{32}	...	S_{3a}	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	S_{a1}	S_{a2}	...	s_{aa}	0	0	...	0	...	0	0	...	0	b rows
	0	0	...	0	S_{a1}	S_{a2}	...	s_{aa}	...	0	0	...	0	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	.	.	.	.	.	.	.	.	.	.	.	.	.	
	0	0	...	0	0	0	...	0	...	S_{a1}	S_{a2}	...	s_{aa}	

Fig 2: Generation of Hybrid wavelet transform

cost is less compared to watermark embedding using transform domain. One of the examples is Least Significant Bit (LSB) modification. In LSB technique, a Pseudo random number generator is used to generate a key which enables program to find locations of pixels where watermark bits will be embedded directly on them. This kind of watermark can be embedded on a single cover image multiple times [1].

In transform domain [4], watermark is embedded in frequency domain. A transform is applied on cover mediumand watermark bits are embedded. Inverse transform is applied to get back original image. One of the advantages of using transform domain is that it provides invisible and robust watermarking. There are various transforms used to achieve watermarking .Most popular of them are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT)[5][6]. After application of DCT image is broken down into frequency components and middle frequency component is used to embed watermark. DWT breaks down image into four energy components LL, LH, HL and HH and watermark is embedded on them

1.2 Characteristics of watermarking System

For system to be effective, a watermark system should possess certain characteristics as robustness, imperceptibility, speed and capacity [2][8]. Robustness is a property of watermark which implies that a watermark should not get destroyed under attacks or during transfer of cover data in communication channel or processing of cover image by receiving application. Imperceptibility is property which tells that any attacker should not be able to detect watermark in the video or image and watermark should be invisible.

Watermark embedding should not take long time to get embedded on cover medium. Speed of embedding watermark can be improved by use of effective algorithm and dedicated hardware [4].

Capacity refers to maximum number of bits that can be embedded on cover image. The watermark should be of much significant size that it can easily detect the ownership of data easily and it should be enough small that its presence should be well hidden from attacker.

1.3 Attacks on a watermark System

Attacks on digital watermark system can be classified into various categories such as active and passive attack, removal and geometric attack [3].

Active attacks are attacks in which attacker tries to hamper watermark present in the cover image so that it will be impossible to retain original watermark. Such attacks are hazardous to applications where ownership of the media is crucial. Passive attacks are attacks in which attacker simply tries to know if watermark is present in system or not.

In removal attack, watermark is tried to be removed from the watermarked video. The goal of attacker is to destroy watermark present in watermarked video. Attacker may or may not know the key or algorithm used for watermark embedding. The attacks used are denoising, remodulation, collusion attack and quantization [9].

In geometric attacks, distortions are added to the video frames so that system should not be able to detect the watermark which is present in cover object. The attacks often change geometric structure of cover image by attacks such as cropping, rotation, scaling and spatial shifting.

In proposed system for embedding of watermark, hybrid wavelet transform is used. Generation of hybrid wavelet transform is as below.

2. GENERATION OF HYBRID WAVELET TRANSFORM

For generation of hybrid wavelet transform, at least two orthogonal transforms is needed, say S and T. For calculating first b rows of Hybrid Wavelet Transform; simply take kronecker product of each row element of orthogonal transform S with each column of orthogonal transform T [7].

The Resultant size of HWT will be L=pxp. If orthogonal transform S is axa and orthogonal transform T is bxb then p=a*b.

For generation of next b rows of HWT, second row of transform S is shift rotated and appended with zeros as shown in Fig 2. Similarly all remaining rows are calculated by repeating shift rotation.

$$S = \begin{bmatrix} s_{11}s_{12}\cdots s_{1a} \\ s_{21}s_{22}\cdots s_{2a} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ s_{a1}s_{a2}\cdots s_{aa} \end{bmatrix} \quad T = \begin{bmatrix} t_{11}t_{12}\cdots t_{1b} \\ t_{21}t_{22}\cdots t_{2b} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ t_{b1}t_{b2}\cdots t_{bb} \end{bmatrix} \quad (1)$$

In proposed method, Hybrid wavelet transform is formed from various orthogonal transforms such as Cosine , Haar, Walsh, Slant, Kekre and Sine.

3. PROPOSED METHOD

In proposed method, a video is taken as cover object over which a watermark is to be embedded. Video is then partitioned into frames and hybrid wavelet transform is applied on it. Watermark is embedded in transform domain and original video is regenerated by application of inverse hybrid wavelet transform.

3.1 Watermark embedding

Following is the method used by proposed system to embed watermark in video frames.

1. Input a video from user

2. Partition video into frames.

3. Extract every 20th frame

4. Input a watermark from user of BMP format

5. Apply hybrid wavelet transform on both video frames and watermark.

6. Embed watermark bits in transform domain

7. Apply inverse hybrid wavelet transform to regenerate original video

Watermark embedding process is shown in figure 3

3.2 Watermark extraction

Following is the method used by proposed system to extract watermark from video frames.

1. Partition into frames an already watermarked video

2. Select every 20th frame and apply hybrid wavelet transform

3. Copy watermark bits

4. Output as extracted watermark
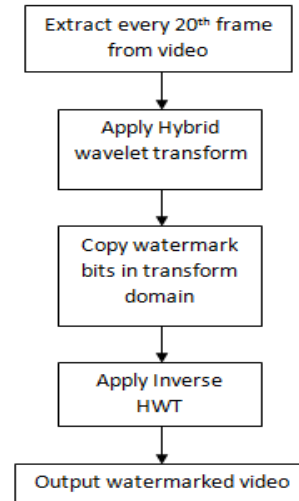
Watermark embedding process is shown in figure 4

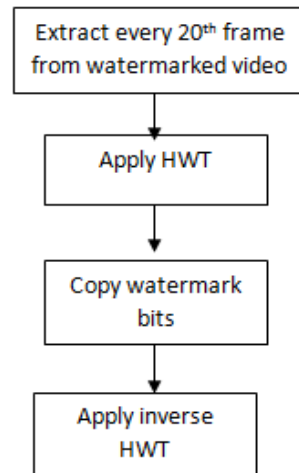**Fig 3: Process for embedding a watermark in video**

Fig 4: Process for extracting a watermark from video

4. RESULTS
4.1 Results of Hybrid wavelet transform

Proposed system is tested for 15 videos and 15 watermarks. Videos are of AVI format and each video is of 16 seconds length. Watermark is of BMP format. Watermark is of 128*128 pixels and video frames are of 512*512 pixels. For evaluating performance of system, mean square error is used as similarity measure. Mean square error (MSE) is cumulative squared error between reference image and target image [10]. Lower the MSE, more similar are the two images and higher the MSE, less similar are the two images.

For evaluating results, various proportions of hybrid wavelet transform such as 1:8, 8:1, 1:4, 4:1, 1:2 and 2:1 are used. Following tables show results for minimum MSE between original-retrieved video frame and watermark using varying proportions of constituent transforms.

Table 1. Mean square error for original-retrieved video frame, original-retrieved watermark using varying proportions of hybrid wavelet transform

Name of Transform	Proportion for original image and original watermark	Mean Square error for original-retrieved video frame	Mean Square error for original-retrieved watermark
Cosine - Haar hybrid wavelet transform	2:1,2:1	0.62	1979
Cosine - Kekre hybrid wavelet transform	8:1,1:2	0.66	1913
Cosine - Walsh hybrid wavelet transform	8:1,8:1	0.66	1662
Cosine - Slant hybrid wavelet transform	2:1,1:2	0.62	2036
Cosine - Sine hybrid wavelet transform	8:1,2:1	0.66	1783
Cosine transform		0.73	9041

Table 1 shows MSE values between original-retrieved video frame and original-retrieved watermark for hybrid wavelet transform using Cosine transform and Haar, Kekre, Walsh, Slant and Sine transforms.

From results, it is clear that Cosine-Walsh with 8:1 proportion for original- retrieved video frame and 8:1 proportion for original- retrieved watermark gives minimum MSE for retrieved watermark.

Table 2. Mean square error for original-retrieved video frame, original-retrieved watermark using varying proportions of hybrid wavelet transform

Name of Transform	Proportion for original image and original watermark	Mean Square error for original-retrieved video frame	Mean Square error for original-retrieved watermark
Walsh-Cosine hybrid wavelet transform	8:1,8:1	0.77	2044
Walsh-Haar hybrid wavelet transform	8:1,1:2	0.77	2042
Walsh-Kekre hybrid wavelet transform	8:1,1:2	0.77	1808
Walsh-Slant hybrid wavelet transform	1:2,2:1	0.69	2161
Walsh-Sine hybrid wavelet transform	2:1,2:1	1.59	1945
Cosine transform		0.73	9041

Table 2 shows MSE values between original-retrieved video frame and original-retrieved watermark for hybrid wavelet transform using Walsh transform and Haar, Kekre, Cosine, Slant and Sine transforms.

From results, it is clear that Walsh-Kekre with 8:1 proportion for original- retrieved video frame and 8:1 proportion for original- retrieved watermark gives minimum MSE for retrieved watermark.

4.2 Results against attacks
System is checked against various attacks such as cropping, salt and pepper and Gaussian attack. Results are shown in table 3.

From table 3, results show MSE for original-retrieved watermark for Cosine-Walsh is minimum compared to other hybrid wavelet transforms and cosine transform for cropping attack, Salt and pepper attack and Gaussian attack.

Table 3. Performance of system against attacks such as Cropping , Salt and pepper and Gaussian attack

Name of Transform	MSE of watermark for Cropping Attack	MSE of watermark for Salt and pepper Attack	MSE of watermark for Gaussian Attack
Cosine	20281	12149	14557
Cosine-Walsh	3717	3851	5241
Walsh-Kekre	4460	4255	7187
Sine-Haar	4216	4500	4912

5. CONCLUSION
In this paper, a new technique of video watermarking is proposed by help of hybrid wavelet transform. A watermark is embedded on every 20th video frame by application of hybrid wavelet transform and results are evaluated in terms of mean square error. It is observed that hybrid wavelet transform using Cosine-Walsh for 8:1 proportion of video frame and 8:1 proportion of watermark gives better result for MSE compared to other combinations of hybrid wavelet transforms as well as Cosine transform. Results also show that Cosine-Walsh gives minimum MSE for original-retrieved watermark for cropping, salt and pepper and Gaussian attack.

In future, self mutated hybrid wavelet transform can be considered for application of video watermarking in place of hybrid wavelet transform.

6. REFERENCES

[1] S.Elango, Dr.G.Thirugnanam, R.Shankari, 2015. A Survey of Digital Video Watermarking Techniques for Copyright Protection and Authentication.

[2] Dr.V.Seenivasagam.2014. A Survey on Video Watermarking and Its Applications.

[3] Gopika V Mane, G. G. Chiddarwar. 2013 Review Paper on Video Watermarking Techniques

[4] Alka N. Potkar, Saniya M. Ansari ,2014. Review on Digital Video Watermarking Techniques

[5] M. Sundararajan, G.Yamuna, 2013 .DWT BASED SCHEME FOR VIDEO WATERMARKING.

[6] ShaikhShoaib,Prof.R.C.Mahajan,2015.Authenticating Using Secret Key in Digital Video watermarking Using 3-Level DWT

[7] Sudeep D. Thepade and Jaya H. Dewan "Image Compression using Cosine – Slant Hybrid Wavelet Transform with Assorted Color Spaces,"

[8] Swati Patel Anilkumar Katharotiya Mahesh Goyani A Survey on Digital Video Watermarking, IJCTA-2011

[9] Ankita A. Hood , Prof. N. J. Janwe, Robust Video Watermarking Techniques and Attacks on Watermark – A Review, International Journal of Computer Trends and Technology

[10] Sudeep.D.Thepade Nikhil Bankar ,Akansha Raina, Shreyas Deshpande,Abhijeet Kulkarni Novel Method for Keyframe Extraction using Block Truncation Coding and Mean Square Error, Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference