ISSN:0975-9646
Saraswathi.M , / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011, 1109-1113

Lossless Visible Watermarking for Video

Saraswathi.M

No.51,Devanumbut Village,Latheri, Katpadi, Vellore-632202, Chennai, India.

Abstract— Nowadays worldwide research activities and the industrial interest in digital watermarking methods are growing tremendously. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data. Our aim in the project is to work on the aspects of visible watermarking videos with lossless recovery.

Through this work, visible watermark is applied to video using mapping function which is reversible. The size of the watermark is arbitrary. It can embed different types of watermark During Extraction video is recovered without any loss.

Keywords— Digital Watermarking, Visible Watermarking, Attacking Watermarking Schemes.

I. INTRODUCTION

With the growing popularity of digital medias through the World Wide Web, intellectual property needs copyright protection, prevention of illegal copying and verification of content integrity. One way for copyright protection is digital watermarking[1].Digital watermarking is defined as a process of embedding data, called a watermark, into a multimedia objects(host signal) such that the embedded watermark can be detected or extracted later to make an assertion about the objects. The multimedia objects can be text, image, audio, video and their compositions. If the host signal is represented by x and the watermarked signal by y, then the watermark, represented by w, is defined as w , y − x, i.e., the difference between the watermarked and the host signal. A simple example of a digital watermark would be a visible seal placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material. [2].

II. ATTACKING WATERMARKING SCHEMES

The different types of attack on watermarking systems include common signal processing operations, geometric attacks and other intentional attacks [3]. Few attacks are discussed below.

1) Noise attacks

As the communication channel is noisy in nature, noise addition attack is considered as most common attack in digital watermarking. Gaussian noise distribution function is given in Eq. 1[9].

$$f_g(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(x-a)^2}{2\sigma^2}} \quad -(1)$$

Speckle noise is a granular noise that inherently exists in and degrades the quality of the images. It adds multiplicative noise to the image I, using the equation J = I+n*I, where n is uniformly distributed random noise with mean 0 and variance v.

The Poisson distribution is a discrete probability distribution that expresses the probability of a number of events occurring in a fixed period of time if these events occur with a known average rate and independently of the time since the last event. Poisson noise distribution function is given in Eq.2

$$f_p(x) = \frac{e^{-a}a^x}{x!} \quad -(2)$$

An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions.

2) Filtering Attacks

The marketed image may undergo several filtering operations in the course of enhancement techniques. Such filtering operations include low pass, high pass, median or Gaussian filtering. It is absolutely necessary for the watermarked information to be resistant to all such filtering processes.

3) Geometric attacks

Rotation attack rotates an image by an angle of certain degrees in a counter clockwise direction about its center point. To rotate the image clockwise, a negative value for angle must be specified. The equations for y axis rotation is given in Eq.3

$z' = z\cos\phi - x\sin\phi \qquad x' = z\sin\phi + x\cos\phi \qquad y' = y \quad (3)$

The watermark is also prone to be distorted or lost while the watermarked image is rescaled. Scaling factor a and b is used to produce the transformed coordinates (x',y') . The equation for scaling is given in Eq.4

$x' = x \cdot sx \qquad y' = y \cdot sy \qquad z' = z \cdot sz \qquad (4)$

The watermark is distorted after applying translation attack to the watermarked image. Transformation equation translates

a two dimension point by adding translation distance x0 and y0, to the original coordinate position (x,y) to move the point to a new position (x',y'). The equation for translation is given in Eq.5 [4]

$$x' = x + tx \qquad y' = y + ty \qquad z' = z + tz \tag{5}$$

III. VISIBLE WATERMARKING

Visible watermarking is a type of digital watermarking used for protection of publicly available images [5]. Visible watermarking schemes are important intellectual property rights (IPR) protection mechanisms for digital images and videos that have to be released for certain purposes but illegal reproductions of them are prohibited. Visible watermarking techniques protect digital contents in a more active manner, which is quite different from the invisible watermarking techniques. Digital data embedded with visible watermarks will contain recognizable but unobtrusive copyright patterns, and the details of the host data should still exist. The embedded pattern of a useful visible watermarking scheme should be difficult or even impossible to be removed unless intensive and expensive human labors are involved. [6]

In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. A television broadcaster adds its logo to the corner of transmitted video; this is also a visible watermark. Visible watermarking has been more popular in the case of protecting digital images due to the fact that it allows users to easily identify their content due to the property of the scheme without the need for an explicit extractor. This also allows owners to prevent the unauthorized usage of their images. Visible watermarks change the signal altogether such that the watermarked signal is totally different from the actual signal, e.g., adding an image as a watermark to another image. Stock photography agencies often add a watermark in the shape of a copyright symbol ("©") to previews of their images, so that the previews do not substitute for high-quality copies of the product included with a license. [7]

1) Three major requirements for visible watermarking

1. Visibility: The watermark must be easily identified.
2. Transparency: The watermark must not significantly obscure the image details beneath it.
3. Robustness: The original pixels in the watermarked areas should not be easily recovered.

2) Characteristics of visible watermarks

- A visible watermark should be obvious in both color and monochrome images.
- The watermark should be spread in a large or important area of the image in order to prevent its deletion by clipping. The watermark should be visible yet must not significantly obscure the image details beneath it.
- The watermark should be applied automatically with little human intervention and labor.[8]
- The watermark must be difficult to remove; removing a watermark should be more costly and labor intensive than purchasing the image from the owner.

A) Related Theory

A group of techniques, named *reversible* watermarking [9], allow legitimate users to remove the embedded watermark and restore the original content as needed. However, not all reversible watermarking techniques guarantee *lossless image recovery*, which means that the recovered image is identical to the original, pixel by pixel.

Lossless recovery is important in many applications where serious concerns about image quality arise. Some examples include forensics, medical image analysis, historical art imaging, or military applications.

Yip et al. [10] proposed the importance of lossless visible watermarking. Watermark is inserted to the host image using algorithms, Pixel Value Matching Algorithm (PVMA) and Pixel Position Shift Algorithm (PPSA). PVMA uses mapping function for embedding but it treats both the low variance region and high variance regions as the same. In order to overcome this disadvantage PPSA is introduced. The secret key is introduced during mapping to enhance the security. The embedding procedure is original image and watermark image will be taken as input, depending on the input region either PVMA or PPSA algorithm is used and the mapping will be done.

As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region [11].

Yonggian et al. [12] presented the visible watermarking technique in Discrete Wavelet Domain(DWT). DWT is applied for both input image and the watermark image and it is decomposed into four structures which is taken for finding the scaling factors. Then the result is added to produce the Visible Watermarked image.

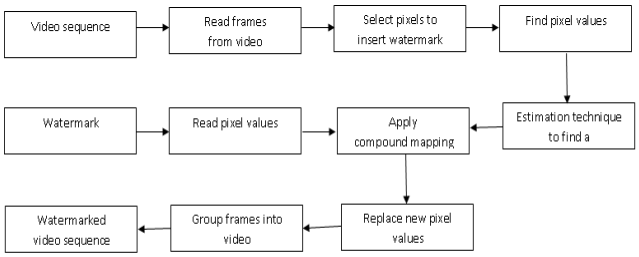
Tsung et al [13] proposed a generic lossless visible watermarking approach where the generic property leads to embed different types of visible watermarks which include opaque monochrome and translucent full color ones. The method is based on one to one compound mapping which replaces the pixels of original image by watermark image to produce the watermarked image. Security protection measures were introduces for avoiding illicit recoveries. Lemmas are proved for compound mapping. Embedding, extraction procedures were explained.

B) Embedding procedure

Keeping generic lossless visible watermarking approach as the base paper, it implemented watermarking for image, the procedure has been extended to video with that extraction

module has one for module for extracting the watermark. Attacks against visible watermarking are regarded as common image recovery problems. To make watermark more useful, must care about its robustness against a various kind of possible attacks. These include robustness against noise addition such as salt & peeper, Gaussian noise and speckle noise and compression attack such as scaling and aspect ratio changes, rotation, cropping, row and column removal, filtering, cryptographic and statistical attacks, as well as insertion of other watermarks.

Different types of geometric and signal processing attacks were checked against watermarked video and the PSNR value is calculated to find the quality of the video.

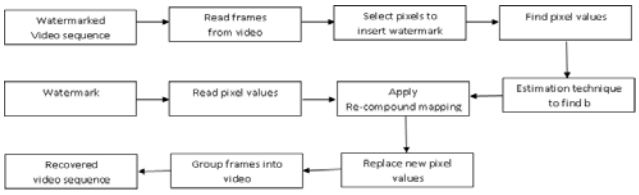


Watermark Embedding Process

- Select input video for embedding watermark
- Select watermark image
- Read the number of frames in video
- Select the single frame from the input video
- Find the size of the watermark
- Find the size of the singleframe
- Get the input from the user whether the watermark should be inserted in 'center, top left, top right, bottom left or bottom right'
- Based upon the user input set values for 'xl,xh,yl,yh' - select watermark area
- For frame 1 to number of frames do the following.
- Read frame 'singleframe'..
- Set the value of watermarking area to be singleframe(xl:xh,yl:yh)
- Copy the single frame as watermarked frame W.
- For the selected watermark area conduct the following steps
- Read the pixel values of neighbouring pixels of selected watermarking area a
- Read the pixel value of watermark b
- Read the pixel value of Watermarking area p
- Apply compound mapping q=(p-a)+ (b)
- Replace the selected watermark area in W by q.
- Group the watermarked frames into video
- Save the movie for extraction.
- Play the movie 'watermarked movie.avi'
- Apply different types of attack to the watermarked movie and store the results

C) Extraction procedure

- Select input video for extracting original video
- Select watermark image
- Read the number of frames in video
- Select the single frame from the input video
- Find the size of the watermark
- Find the size of the single frame
- Get the input from the user whether the watermark is inserted in 'center, top left, top right, bottom left or bottom right'
- Based upon the user input set values for 'xl,xh,yl,yh' to select watermarked area
- For frame 1 to number of frames do the following.
- Read frame 'single frame'..
- Set the value of watermarked area to be single frame(xl:xh,yl:yh)
- Copy the single frame as extracted frame E.
- For the selected watermark area conduct the following steps
- Read the pixel values of neighbouring pixels of selected watermarked area a
- Read the pixel value of watermarking area p
- Read the pixel value of Watermark b
- Apply Re - compound mapping q=(p-(b))+a
- Replace the selected watermark area in E by q.
- Group the watermarked frames into video
- Save the movie.
- Play the movie 'extractedmovie.avi'.
- Check the PSNR value by comparing extracted movie with original movie.



Watermark Extraction Process

D) Procedure for Extracting the Watermark

- Select original video
- Select watermarked video
- For frame 1 to number of frames do the following.
- Read frame 'singleframe'.
- Find the difference between the watermark area of watermarked video and the original video
- Show the extracted watermark

E) Results and Discussions

A series of experiments implementing the proposed methods were conducted in MATLAB. To measure the effectiveness of the method, the performance metrics is measured. The quality of a watermarked video is measured by the peak signal-to-noise ratio (PSNR)

Input video	**:**	xylophone.mpg
Size	**:**	240*320
No. of frames	**:**	141
Input Watermark	**:**	vit5.jpg
Size	**:**	50*80

Embedded and extracted sample video clips were shown under Fig.1 and Fig.2.

Embedded and Extracted Video clips

Fig.1 Emdedded Video clip

Fig.2 Extracted video clip

F) Attacks and PSNR values:

Different types of attacks which include signal processing operations, geometrical attacks were applied to the watermarked video and the PSNR value is calculated against original video and the extracted video to check the quality of the extracted video.

The different types of attacks applied to watermarked video include salt & pepper noise, Gaussian noise, speckle noise, Poisson noise, rotation, translation and cropping. Table1 shows the embedded and extracted video clip with its psnr value. Table 2 shows the attacked video clip and extracted video clip with its psnr value.

Attack Type	PSNR value	Attacked Video Clip	Extracted Video Clip
Salt & pepper	26.8631		
Gaussian	22.2584		
speckle	26.8661		
Poisson	26.1101		
Rotation	21.2546		
Translation	26.8627		
cropping	17.5277		

Table. 1 Attacks and their PSNR values

IV.CONCLUSION

A number of techniques have been proposed for visible watermarking digital images. However, the embedding distortion of visible watermarking is usually larger than that of invisible watermarking. In order to reduce the distortion many papers included the concept Lossless image recovery. Visible watermarking algorithm for video is analysed. The embedding algorithm takes input video and watermark as input and produces watermarked video. The extraction algorithm takes watermarked video and watermark as input and produces extracted video as output. Attacks are introduced to the watermarked video and the PSNR value is checked against input video and extracted video.

The future work can be carried out to check the quality of the extracted watermark by checking the normalized correlation coefficient.

REFERENCES

[1] *S* Samuel and WT Penzhom, ―Digital watermarking for copyright protection, IEEE AFRICON 2004**,** pp.953-958.

[2] Yanqun Zhang, Digital Watermarking Technology: A Review, ETP International Conference on Future Computer and Communication,2009,pp. 250-252.

[3] K.Murugesan, P.Santhi ―Probability and Queueing Theory ―, 2nd edition, Anuradha Publications, 2007.

[4] C.-H. Huang and J.-L.Wu, ―Attacking visible watermarking schemes,IEEE Trans. Multimedia, vol. 6, no. 1, pp. 16–30, Feb. 2004.

[5] Pei-Min Chen,# A Visible Watermarking Mechanism using a Statistic Approach, Proceedings of ICSP, 2000, pp.910-913

[6] J. Meng and S. F. Chang, ―Embedding visible watermarks in the compressed domain,#Proc. of ICIP 98.

[7]G. W. Braudaway, K. A. Magerlein, and F. Mintzer―Protecting publicly-available images with a visible imagewatermark,# in Optical Security and Counterfeit Deterrence Techniques, vol. 2659, R. L. van Renesse, Ed. San Jose, CA: S&T and SPIE, 1996, pp. 126–133 .

[8] I. J. Cox and M. L. Miller, ―A review of watermarking and the importance of perceptual modeling,# in Human Visionand Electronic Imaging II, vol. 3016B, SPIE, 1997.

[9] Y. J. Cheng and W. H. Tsai, "A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks," presented at the Int. Computer Symp.—Workshop on Cryptology and Information Security, Hualien,Taiwan, R.O.C., Dec. 2002.

[10] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, ―Lossless visible watermarking,#in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2006, pp. 853–856.

[11] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, ―A DCT domain visible watermarking technique for images, in Proc. IEEE Int. Conf. Multimedia and Expo., vol. 2, 2000, pp. 1029–1032.

[12] Munesh Chandra, Shikha Pandey ―A DWT Domain Visible Watermarking Techniques for Digital Images, International Conference on Electronics and Information Engineering,Vol.2, 2010.

[13] Tsung-Yuan Liu, Student Member, IEEE, and Wen-Hsiang Tsai, Senior Member, IEEE, Generic Lossless Visible Watermarking A new approach, IEEE transaction on image processing, vol. 19, no. 5, may 2010.

.