A Novel Watermarking Scheme using Otsu's Thresholding

[1]Neha Solanki, [2]Dr. Mayank Patel
[1]M.tech Scholar, [2]Associate Professor
[1]Computer Science & Engineering
[1]Geetanjali Institute of technical studies (GITS), Dabok, Udaipur, India.
[2]Geetanjali Institute of technical studies (GITS), Dabok, Udaipur, India.

Abstract: Now a day the popularity of digital video based applications is accompanied by the call for copyright guard to prevent unlawful copying and allotment of digital video. Copyright protection adds verification data such as rights information and logo in the digital media without affecting its perceptual class. In case of any dispute, validation data is extracted from the media and can be used as a soundproof to prove the possession. As a way of copyright protection, digital video watermarking has recently emerged as a significant field of attention and a very active area of research. In this work the targeted invisible watermarking is approached using Haar Wavelet functions, the watermark or message embedded into the cover image, before it, image segmentation approach is utilized here to extract the object of interest in the news and secret an 8bit or 16-bit message information to the one-bit binary message. The embedding is performed in odd and even blocks of LH and HL bands, by modulation the corresponding band value by the proposed embedding rule set. The retrieved results from the recommended experimental setup reveal that embedding a watermark can be performed faster and more robust than the existing methodologies.

Keywords:- Cover Image, Watermarking, Image Segmentation, Wavelet Function, Entropy.

1. INTRODUCTION

The employ of digital video has full-grown severely in new times. Digital video applications contain video-on-demand, video-conferencing, digital cinema, digital television, distance learning, entertainment, and advertising. Many users experience digital video when they watch a motion picture recorded on a digital video disc (DVD) or downloaded over the internet. The proliferation of digital video into more applications is encouraged by improving compression technology, better authoring and editing tools, capture and display devices at low cost; and more available bandwidth in digital communication networks. The duplicate, manipulation and the distribution of digital multimedia (images, audio, and video) via networks become faster and more comfortable. Therefore, owners and creators of digital products are worried about illegal copying of their product. As an outcome, security and copyright protection are becoming vital issues in multimedia applications and services.

1.1 THE NEED OF WATERMARKING:

The aim here is to access the ownership or integrity of some pieces of information named after the watermark. In the use of a watermark, the watermark should be unobtrusive (perceptually invisible), robust, universal, i.e., should apply to all three media under consideration, resilient to general signal processing and geometric distortions and intentional attack. Intentional attacks include forgery and offenses using one or more domain and in the spatial area.

Constant efforts are being complete to device an efficient watermarking schema, but techniques planned so far do not look to be robust to all imminent attacks and multimedia data processing operations. Watermarking sudden increase in interest is most likely due to the rise in concern over IPR. Generally, the watermarking of a still image, video, and audio demonstrate certain familiar basic concepts. Reported more than a few watermarking applications in the literature to depend on the services we wish to support.

2. DIFFICULTY FORMULATION FOR HAAR BASE INVISIBLE EMBEDDING

This thesis resolves many issues:

ISSUE 1: Till now there is no "Generic" nature in the watermarking algorithms available. More precisely, if the specific advance is applicable for a gray level image, the same move toward does not work for the other formats of an image.

ISSUE 2: Even if the gray color image watermarking algorithms are extended for RGB color images, the maximum work has been done for (y- luminance) color channel only because human eyes are less responsive to detect the changes in (y- luminance) color channel. No attack impact which may affect the analysis of the color channels, i.e., a particular attack, has been carried out

[1-2]. Therefore, separately from choosing digital Image Watermarking as a critical problem, we have decided to identify the suitability of a color channel concerning attack (if any) for multi-color channel images (True color windows BMP and uncompressed JPEG). We also decided to discover the ways such that attack impacts may be minimized before the watermark embedding process.

ISSUE 3: In most of the research paper, a watermarking scheme is finalized, it is applied to all test images. Each image is different and then some characteristics, and after embedding the watermark data by an exacting watermarking scheme, its performance against a particular attack may not be similar to another image. No study is conducted to create the embedding scheme based on some image characteristics. So we decided to explore the relationship between the performance of watermarking scheme and the cover image characteristics itself.

ISSUE 4: Most watermarking schemes are developed in a means that first a system is generated based on the extension of previously presented one and then check its performance against the common image manipulations and known attacks. There are substantial financial implications of watermarking schemes (say fingerprinting), but no plan has been developed, which is, by the device, resistant to at least single attack, to make sure that, a particular raid (having most economic issues) cannot be conducted by an enemy. Therefore we determined to plan watermarking schemes such that an inherent nature can be embedded to guarantee that at least one acute attack having most financial implications cannot be conducted on watermarked images.

2.1 DIGITAL WATERMARKING

Digital watermarks are pieces of information additional to digital data (audio, video, or still images) that can be detected or extracted later on to assert the data. This information may be textual data the author, its copyright, and so on; or it can be an image itself. Be hidden information is embedded by manipulating the contents of the digital data, allowing someone to identify original owner, or in the case of unauthorized duplication of purchased material, the buyer is involved. These digital watermarks stay intact under transmission/transformation, allowing us to protect our proprietary rights in digital form.

2.2 INVISIBLE/VISIBLE DIGITAL WATERMARKING

Visible and invisible are the two essential types of digital watermarking, and the digital watermark can be careful as either visible or invisible. Visible digital watermarking is a system by which anyone can put visible information in digital signals; the information is frequently a logo which identifies the owner of the digital signal. For example, a television broadcaster typically adds its logo to the corner video; it is a generally visible digital watermark. Invisible digital watermarking is a technique by which anybody can hide information in the digital signal, and the data will not be perceived. Since it is invisible, and invisible digital watermarking has a Used extensively.

2.3 SPATIAL DOMAIN TECHNIQUES

The simplest example of spatial domain watermarking techniques to insert data into digital signals in noise-free environments is least significant bit coding. There are several variants of the methods. Mostly involves embedding watermark by replacing the least significant bit of the image data with a bit of the watermark data [3]. The most straightforward approach to embed a watermark into an image in the spatial is to add a pseudo-random noise pattern to the luminance values of its pixels. Schyndel, [5] proposed a method based on bit plane manipulation of the least significant bit (LSB) which offers easy and fast decoding. Macq LSB inserts the watermark around image contours [6].

2.4 TRANSFORM DOMAIN TECHNIQUES

Generally, Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) are used as the methods of data changes. In these methods, a watermark that one needs to embed distributive in the overall domain of an original data, and the watermark, is hardly being destroyed once fixed.

The main strength offered by transform domain techniques is that they can take advantage of the unique properties of alternate domains to address the limitations of pixel-based methods [3]. While there are a lot of robust watermarks in the DCT domain, there are relatively less offered data hiding watermarking techniques in DCT domain [7]. Kim, [8] embed watermark bits as pseudo-random sequences in the frequency domain. Langelaar, [10] hide watermarks by removing or retaining selected DCT coefficients. Borg, [9] hide a watermark in JPEG images by forcing selected DCT blocks to satisfy satisfied linear or circular constraint. A little embeds watermark patterns in the quantization module after DCT [14] or in blocks chosen based on human

visual models. Choi, utilize inter-block correlation by forcing the DCT coefficients of a block to be higher or lesser than the average of the neighboring blocks [11].

In 1995, Cox developed a new algorithm of using spread spectrum to embed a mark [4] To improve Cox method, Lu, [12] to promote the watermark using Cocktail the robustness and second-hand Human Visual System (HVS) to maintain high fidelity of the watermarked image. Hsu et al. [13] Embed watermark bits by editing the polarity of DCT and DWT coefficients and use a meaningful logo image as the watermark. While most schemes embed only a single watermark, some allow for multiple watermarks embedding [1] a few embed orthogonal watermarks and extend the separate watermark algorithms for multiple watermarks [12].

After that, the inverse transform should be applied to obtain the watermarked image. Since watermarks applied to transform domain will be dispersed over the entirety of the spatial model upon inverse transformation, this technique is more robust to cropping than the spatial technology.

The transform techniques commonly used for watermarking purposes are respectively: the Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT) and the Discrete Wavelet Transform. They are also less known approaches implementing the Complex Wavelet Transform (CWT) and the Fourier-Mellin Transform (FMT). With the consistency process of JPEG2000 and the shift from DCT- to wavelet-based image compression methods, watermarking schemes operating in the wavelet transform domain has become even more interesting.

3. TENTATIVE SETUP AND RESULT EXAMINATION

3.1 ALGORITHM FOR WATERMARKING USING DWT

A) Algorithm 1: Embedding Procedure

Step 1. relate 1-Level DWT on an M*N host image.

Step 2. partition the HL and LH subband into non-overlapping blocks of size 2*2 and pick blocks in regular columns of HL and blocks in a strange column of LH for embedding watermark.

Step 3. For each selected block B(m, n) and a watermark bit w.

Calculate mean value M(m, n) of four coefficients in B(m, n)

$$M(m,n) = \frac{\sum_{i=0}^{1}\sum_{j=0}^{1}(x_{m+i,n+j})}{4} \quad (1)$$

Embed watermark tiny piece w

R: = M(m, n) mod 6;
for i := 0 to 1
for j: = 0 to 1
if 0 ≤ R < 3 then
if w = 1 then xm+i,n+j := xm+i,n+j + (3-R);
if w = 0 then xm+i,n+j := xm+i,n+j - R;
if 3 ≤ R < 6 then
if w = 1 then xm+i,n+j := xm+i,n+j + (3-R);
if w = 0 then xm+i,n+j := xm+i,n+j + (6-R);

Step 4. execute IDWT on the embedded image to obtain a stego image.

B) Algorithm 2: Extraction Procedure

Step 1. be relevant 1-Level DWT on an M*N stego image.

Step 2. separate the HL and LH subband into non-overlapping blocks of size 2*2 and choose blocks in even columns of HL and blocks in odd columns of LH for extracting the watermark.

Step 3. For each block B(m, n). estimate mean value M(m, n) of four coefficients in B(m, n)

$$M(m,n) = \frac{\sum_{i=0}^{1}\sum_{j=0}^{1}(x_{m+i,n+j})}{4} \quad (2)$$

Extract watermark bit w

R: = M(m, n) mod 6 ;

if $0 \leq R < 1.5$ then w:= 0;

if $1.5 \leq R < 4.5$ then w:= 1;

if $4.5 \leq R < 6$ then w:= 0;

3.2 SUBSTANTIATION OF THE RESULT

The MSE (Means Square Error) and NC (Normalized Coefficients) values are calculated for the watermarking procedure. Moreover, the criterion of the proper watermarking technique is, lower should be the MSE value and higher should be the NC value. MSE represents the similarity index of the original image in comparison to the watermarked image. While NSE represents the index that shows the deterioration or harm of extracted watermark when compared to unique watermark which was used for hiding in the previous stage. The resemblance of the watermarked image or attacked frame to cover (original image). Better is resemblance better is a watermarking scheme

(A) PSNR: The Peak-Signal-To-Noise Ratio (PSNR) is worn to evaluate deviation of the attack of the watermarked and the original
frame video frames and is defined as:

PSNR := 10 Log10 (2552 / MSE) , measured in dB(decibels) units
(3)

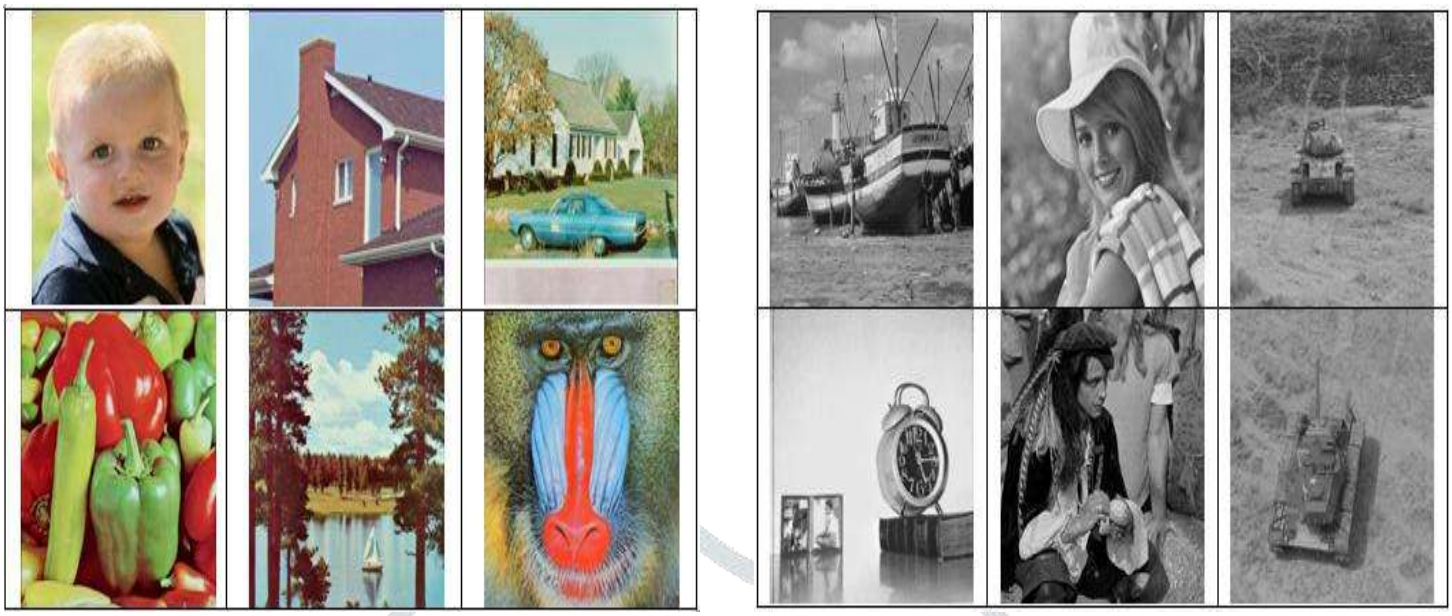
Where MSE (mean squared error) between original and distorted frames (size m x n) is clear. MSE is the sum of squared difference between the original and watermarked frame.

(B) NC: The Normalized Coefficient(NC) gives a evaluate of the robustness of watermarking. NC can be ranged between 0 to1: W and W‟ represents the original and extracted watermark respectively.

$$NC = \frac{\sum W_{i,j} * \sum W'_{i,j}}{\sqrt{\sum (W_{i,j})^2 * \sum (W'_{i,j})^2}} \quad (4)$$

3.3 RESULTS AND PARAMETERS

Digital watermarking skill is an emerging field in computer science, cryptology, signal processing, and communications. The watermarking research is more exciting as it needs collective concepts from all the tracks along with Human Psycho visual analysis, Multimedia and Computer Graphics. The watermark may be of a visible or invisible type, and each has got its applications.
The Fig.3.3.1 (a) & (b) represents the cover images and watermark images set.



(a) Cover Images (b) Message / Watermark Images

Fig.3.3.1 Cover and Message Image set

The segmentation result for the message images using Otsu method is depicted as below:

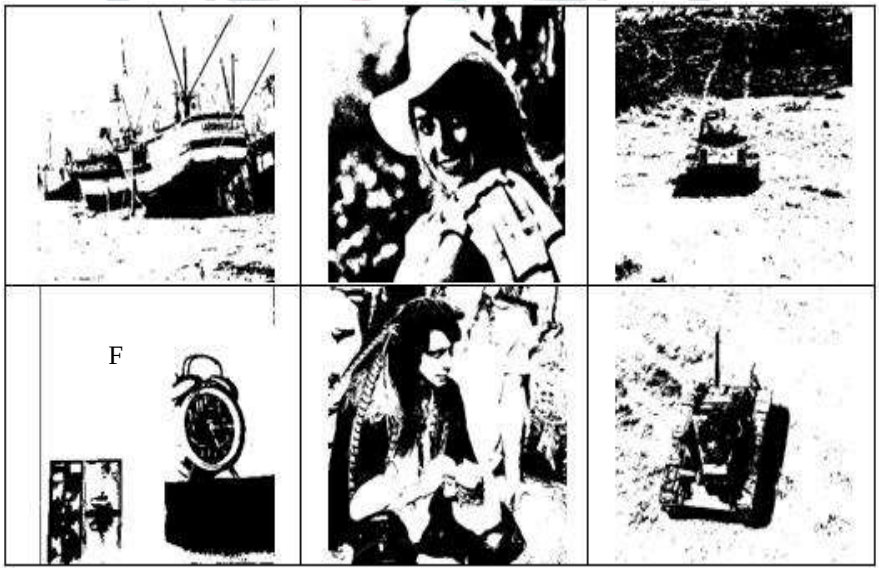


Fig. 3.3.2 The binary conversion of watermark images

The watermarked images resulted from embedding algorithm applied individually on six messages is represented by below figure, where binary message bits are embedded into LH and HL band of cover images,

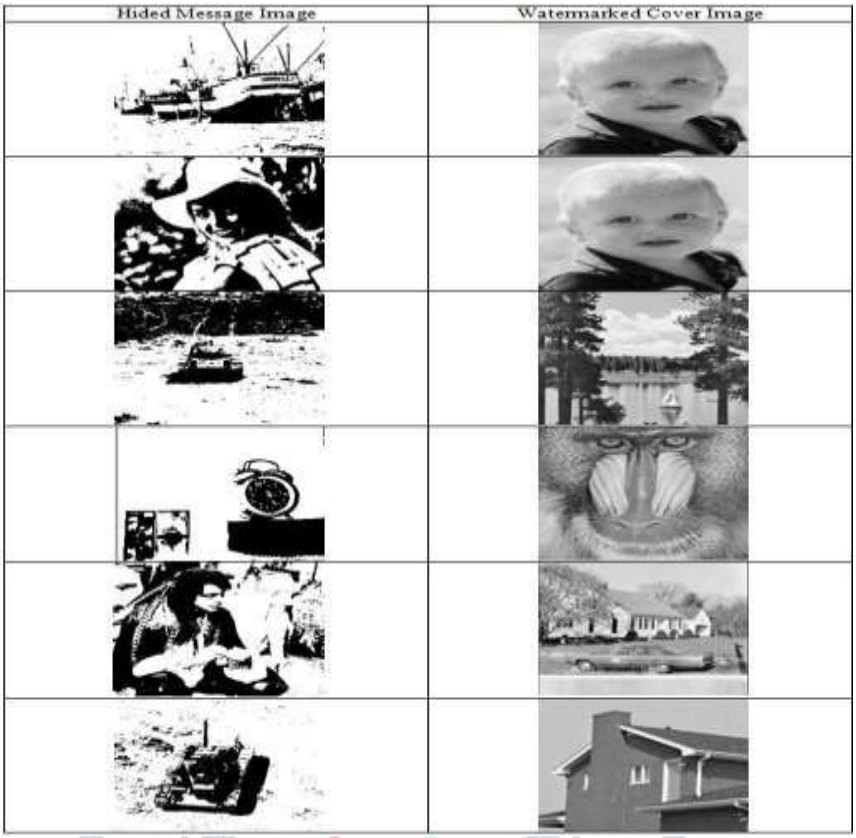


Fig. 3.3.3 the watermarked cover images

Extracted watermarks at user end using Algorithm2 is depicted by below figure:-

Fig 3.3.4 The extracted watermark or message at user-end.

4. CONCLUSION

Safer Digital watermarking system can be implemented by combining the Cryptography and digital watermarking. Here, we applied a simple model of watermarking technique, which It has the skill to insert an invisible watermark into a spatial domain of a base image. This technique yields marked-images with high imperceptibility and robustness quality. We are interested in the spatial domain watermarking due to its most comfortable modeling into hardware and for its economical features. Therefore we are planning to implement our proposed algorithm as a hardware chip as soon as possible in the nearest future. The suggested embedding scheme can be extended to video watermarking, where watermarked frames will be an add-on secrecy point.

REFERENCES

[1] S. Voloshynovskiy, S. Pereira, T. Pun, "Watermark attacks," Erlangen Watermarking Workshop 99, October 1999.

[2] G. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking Digital Image and Video Data: A State of - Art Overview, IEEE Signal Processing Magazine," vol., pp. 20-46, Sep. 2000.

[3] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Processing, 1998, vol. 66, no. 3, pp. 283-301.

[4] J. Lee et al., "A survey of watermarking techniques applied to multimedia," IEEE International Symposium on Industrial Electronics, vol. 1, pp. 272-277, 2001.

[5] Cox et al.,: "Digital watermarking: principal and practice," Morgan Kaufmann, 2002.

[6] J. Meng, and S. Chang, "Embedding Visible Video Watermarks in the Compressed Domain,"International Conference on Image Processing, ICIP 98, Proceedings, vol.1, pp. 474-477, 1998.

[7] Sourav Bhattacharya, T. Chattopadhyay, and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis concerning" H.264/AVC".

[8] Vivek Kumar Agarwal, "Perceptual watermarking of digital video using the variable temporal length 3D-DCT,"IIT, Kanpur, 2007.

[9] C. Navya Latha, K. Sumanth, „ Digital Video Watermarking." International Journal of Scientific & Engineering Research", Volume 4, Issue 7, July-2013

[10] Fernando Perez- Gonzalez and Juan R. Hernandez, "A tutorial on Digital Watermarking". Conference: Conference: Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999.

[11] Y. R. Lin, H. Y. Huang and W. H. Hsu, "An embedded watermark technique in the video for copyright protection," 18th International Conference on Pattern Recognition-ICPR "06,20-24 August 2006, pp. 795-798, Hong Kong.

[12] Nisreen I. Yassin 1, Nancy M. Salem2 and Mohamed. El Adawy National Research Centre, Cario, Egypt, "Block-Based Video Watermarking Scheme Using Wavelet Transform and Principal Component Analysis," IJCSI International Journal of Computer Science Issues,vol. 9, Issue 1, no. 3, January 2012.

[13] X. Kang, WenjunZeng, J. Huang, "A Multiband Wavelet Watermarking Scheme." International Journal of Network Security", vol.no. 2,pp. 121-126,Mar 2008.

[14] T. Khatib, A. Haj, L. Rajab, H. Mohammed," A Robust Video Watermarking Algorithm," Journal of Computer science, vol.4,pp.910-915, 2008.