

A Review On GUI Implementation of Efficient Robust Digital Watermarking using 3-Discrete wavelet Technique

Ravi Kumar¹, Garima Garg²

Abstract:

The great success of internet that allows the transmission, very wide distribution, and access of digital data in an easy manner. The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Like traditional watermarks,.

Keywords —Digital Video Watermarking, Discrete Wavelet Transform, 3-D digital water marking, Video Frame, Watermark, MATLAB.

I. INTRODUCTION

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of computer-aided information hiding in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark

distorts the carrier signal in a way that it becomes perceivable, it is of no use.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time.

Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal.

Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. Such a message is a group of bits describing information pertaining to the signal or to the author of the signal (name, place, etc.). The technique takes its name from watermarking of paper or money as a security measure. Digital watermarking can be a form of steganography, in which data is hidden in the message without the end user's knowledge.

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. Types Of Video Watermarking

2.1 VISIBLE WATERMARKING

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.

Visible watermarks can be used in following cases:

- * Visible watermarking for enhanced copyright protection.

In such situations, where images are made available through Internet and the content owner is concerned that the images will be used commercially (e.g. imprinting coffee mugs) without payment of royalties. Here the content owner desires an ownership mark, that is visually apparent, but which does not prevent image being used for other purposes (e.g. scholarly research).

- * Visible watermarking used to indicate ownership originals.

In this case images are made available through the Internet and the content owner desires to indicate the ownership of the underlying materials (library manuscript), so an observer might be encouraged to patronize the institutions that owns the material.



Fig 1: Visible Water marking

1.2 INVISIBLE WATERMARKING

Invisible watermarks do not change the signal to a perceptually great extent, i.e., there are only minor variations in the output signal. An example of an invisible watermark is when some bits are added to an image modifying only its least significant bits. Invisible watermarks that are unknown to the end user are steganographic. While the addition of the hidden message to the signal does not restrict that signal's use, it provides a mechanism to track the signal to the original owner.

It is an overlaid image which cannot be seen, but which cannot be detected algorithmically.

- Embedding level is too small to notice.
- It can be retrieved by extraction software.
- Application :

Authenticity, copyrighting, etc.

Invisible watermark is classified into three parts:

- Robust
- Semi- Fragile
- Fragile
- Invisible robust watermark is embedded in such a way that alterations made to the pixel value are perceptually not noticed.
- Invisible fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

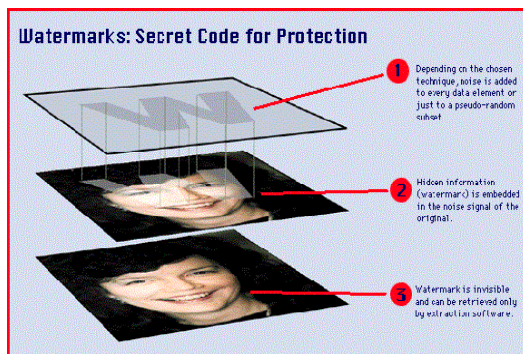


Fig. Invisible Watermarking.

3. METHODOLOGY

3.1 INPUT AND OUTPUT:

User has to browse a video as input to the application and perform the watermarking technique on the extracted frames then reconstruction of frames and displays the result as in form of watermarked video.

3.2 STEPS OF DIGITAL VIDEO WATERMARKING

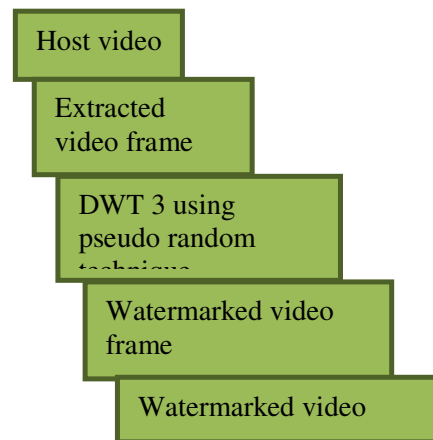


Fig. 3 Steps of Digital Video Watermarking

4. Technique Used

i. Uniform Pseudo Random Number

The function rand generates pseudorandom numbers with a uniform distribution over the range of (0, 1). The uniform distribution is commonly used to generate random numbers over an interval.

Rand :It generates arrays of random numbers uniformly distributed in the interval (0,1).

$$Z = \text{rand}(m,n)$$

or

$$Z = \text{rand}([m n])$$

which returns an m-by-n matrix of random entries.

$Z = \text{rand} \%$ returns a scalar.

$Z \sim U[0,1]$, uniform over the interval.

$Y = (\text{max}-\text{min}) * Z + \text{min} \% Y \sim U[\text{min}, \text{max}]$

$\text{height} = 1/(\text{max}-\text{min}) .$

4.1 Comparison of PRNG and TRNG

References:

[1]. Nanchang, P. R. China, May 22-24, 2009, pp. 104-107, A Digital Watermarking Algorithm Based On DCT and DWT.

[2]. International Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011, Comparative Performance Analysis of DWT-SVD Based Color Image Watermarking Technique in YUV, RGB and YIQ Color Spaces.

[3]. International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153, Review Paper on Video Watermarking Techniques.

[4]. Int. J. Communications, Network and System Sciences, 2012, 5, 490-495 <http://dx.doi.org/10.4236/ijcns.2012.58059>
Published Online August 2012 (<http://www.SciRP.org/journal/ijcns>), A Dynamic Multiple Watermarking Algorithm Based on DWT and HVS.

[5]. International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 4, No. 3, September, 2011, Image Compression Using DCT and Wavelet Transformations.

[6]. IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 12, NO. 7, NOVEMBER 2010, Digital Cinema Watermarking for Estimating the Position of the Pirate.

[7]. International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013, A Survey of Digital Watermarking Techniques, Applications and Attack.

[8] M. Alvarez-Rodriguez and F. Perez-Gonzalez. Analysis of pilot-based synchronization algorithms for watermarking of still images. Signal Processing - Image Communication, 17(8):611–633, 2002.

[9] Manuel Alvarez Rodríguez and Fernando Pérez-González. Analysis of pilot-based synchronization algorithms for watermarking of

Characteristic	Pseudo-Random number Generators	True Random Number Generators
Efficiency	Excellent	Poor
Determinism	Deterministic	Nondeterministic
Periodicity	Periodic	Aperiodic

still images. Signal Processing: Image Communication, 17(8):611 – 633, 2002.

[11] D.N. Arnold, R.S. Falk, and R. Winther. Finite element exterior calculus, homological techniques, and applications. Acta Numerica, 15:1–155, 2006.

[12] Nicolas Aspert, Diego Santa-cruz, and TouradjEbrahimi. Mesh: Measuring errors between surfaces using the hausdorff distance. pages 705–708, 2002.