# A robust algorithm for 3D Mesh Watermarking using NBR technique

Sheenu Gupta Manshi Shukla Rimt-Iet,Mandi Gobindgarh

#### Abstract

With the rapid development and wide use of Internet, information transmission faces a big challenge of security. People need a safe and secured way to transmit information. Digital watermarking is a technique of data hiding, which provide security of data. This paper presents a watermarking technique which least significant bits (LSB) NBR and Mesh watermarking, its steps and its process with matlab images.

*Keywords* watermarking ,LSB, NBR, Mesh.

## **1. Introduction**

Watermarking is a technique used to hide data or identifying information within digital multimedia. Our discussion will focus primarily on the watermarking of digital images, though digital video, audio, and documents are also routinely watermarked. Digital watermarking is becoming popular, especially for adding undetectable identifying marks, such as author or copyright information. The digital watermarking process embeds a signal into the media without significantly degrading its visual quality. Digital watermarking is a process to embed some information called watermark into different kinds of media called Cover Work [10,2]. Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. Digital watermarking involves embedding a structure in a host signal to "mark" its ownership [12]. Digital watermarks are inside the information so that ownership of the information cannot be claimed by third party [8]. While some watermarks are visible [5], most watermarks are invisible. [11].

## 2. Classification of Watermarking

Digital Watermarking techniques can be classified as:

- Text Watermarking
- Image Watermarking
- Audio Watermarking

Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

I. Visible watermark

II. Invisible-Robust watermark

III. Invisible-Fragile watermark

## 3. Techniques of Watermarking

A. Frequency Domain Watermarking: These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture.[4]

B. Spread Spectrum:

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image [1].

C. Spatial Domain Techniques:

Techniques in spatial domain class generally share the following characteristics:

The watermark is applied in the pixel domain.

No transforms are applied to the host signal during watermark embedding.

Combination with the host signal is based on simple operations, in the pixel domain.

The watermark can be detected by correlating the expected pattern with the received signal.

Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame. Let us denote a

picture to be watermarked by P and values of its pixel color samples by Pi, a watermarked version of picture P by P \* and values of its pixel color samples by P \* i. Let us have as many elements of watermark W with values Wi as number of pixels in picture P. Watermark W hereby covers the whole picture P. Further, it is possible to increase the watermark strength by multiplying watermark

element values by weight factor a. Then the natural Formula for Embedding Watermark W into Picture P Is: P\*i = P i + aWi

The most common algorithm using spatial domain watermarking is LSB

## 4. Applications of watermarking

The main applications of digital watermarking are presented as: *A. Copyright Protection:* Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.



Figure 1 Applications in Copyright

*B. Content Archiving:* Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems.



Figure 2 Applications in Contents Archiving

*C. Meta-data Insertion:* Meta-data refers to the data that describes data. Images can be labelled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records.

*D. Broadcast Monitoring:* Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. This has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

*E. Tamper Detection:* Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.



Figure 3 Applications in Digital Fingerprinting

*F. Digital Fingerprinting:* Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital data. Hence a single digital content can have different fingerprints because they related to different users.

### 5. Watermarks and Watermark Detection

There are mainly two types of watermarks that can be embedded in an image.

A. Pseudo-Random Gaussian Sequence: A Gaussian sequence watermark is a sequence of numbers contains 1 and -1 and which has equal number of 1's and -1's is denoted as a watermark. It is consider as a watermark with zero mean and one variation. Such watermarks are used for original data detection using a correlation measure.

B. Binary Image or Grey Scale Image Watermarks: Some watermarking algorithms embed meaningful data like

logo image instead of a pseudo-random Gaussian sequence. Such watermarks are considered as binary image watermarks or grey scale watermarks. Such watermarks are used for original data detection. Based on the type of watermark embedded, an appropriate decoder has to be used to detect the existent of watermark.

#### 6. Image Watermarking Embedding Domain

Based on domain used for watermark embedding process, the watermarking techniques can be classified into the following types:

### 1) Spatial watermarking

Spatial watermarking can also be applied using colour partition such that the watermark appears in only one of the colour bands. However, the watermark appears when the colours are separated for printing. Spatial domain process involves addition of fixed amplitude pseudo-noise into the image. These approaches modify the least significant bits of original contents. The watermark can be hidden into the data to assume that the LSB data are visually irrelevant.

2)Transformation based watermarking There are many techniques proposed based on transformation based watermarking. Watermarking can be applied in the transform domain; including such transforms are discrete Fourier, discrete cosine, and wavelet. In this first the host or main data is transformed and then modifications are applied to transformed coefficients. Watermark is embedded in DFT, DCT and DWT domain coefficients.

## 7. Proposed Work



Flow Chart of proposed Work

## 8. Results





Fig 4 described about the PSNR value of image after the embedding of watermark. It has shown that the psnr value in proposed is better than that of existing approach.





Fig 5 described about the MSE value of image after the embedding of watermark. It has shown that the mse value in proposed is better than that of existing approach.



Fig 6: Contrast

Fig 6 described about the contrast value of image after the embedding of watermark. It has shown that the contrast value in proposed is better than that of existing approach.



Fig 7: Energy of an image

Fig 7 described about the energy of image after the embedding of watermark. It has shown that the energy in proposed is better than that of existing approach.

## 9. conclusion

In this paper we survey the current literature on digital image watermarking,. We classified watermarking algorithms based on the transform domain in which the watermark is embedded. Also, study the watermarking properties, applications and techniques used. This paper proposed the robust techniques and generate results which can prevent attack on the watermark using LSB, NBR technique.

#### References

- [1]. Avani Bhatia, Mrs. Raj Kumari"Digital Watermarking Techniques".
- [2]. B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011
- [3]. Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" University Salzburg, pp. 9 – 17, Jan 2000.
- [4]. Chiou- Ting Hsu; Ja-Ling Wu; Consumer Electronics "DCT-based watermarking for video", IEEE Transactions on Volume 44, Issue 1, Feb. 1998 Page(s):206 – 216
- [5]. Cox, Miller and Bloom, "Digital watermarking", 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher
- [6]. DarshanaMistry "Comparison of Digital Water Marking methods"(IJCSE) International Journal on Computer Science and EngineeringVol. 02, No. 09, 2010, 2905-2909
- [7]. Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", AlpVision, Switzerland, pp 1 – 4M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116.
- [8]. H.Arafat Ali, "Qualitative Spatial Image Data Hiding for Secure Data Transmission", GVIP Journal, Volume 7, Issue 2, pages 35- 37, 2, August 2007
- [9]. Max Sobell"LSB Digital Watermarking", CPE 462
- [10]. Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark

data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518

- [11]. R.AARTHI, 2V. JAGANYA, &3S.POONKUNTRAN "Modified Lsb Watermarking For Image Authentication" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012
- [12]. Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.
- [13]. Yeuan-Kuen Lee1, Graeme Bell2, Shih-Yu Huang1, Ran-Zan Wang3, And Shyong-JianShyu "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding" Springer-Verlag Berlin Heidelberg 2009