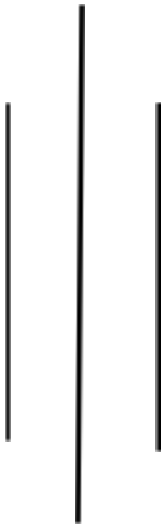
9 Jan, 2021

SRM UNIVERSITY AP
Andhra Pradesh

3D Image Watermarking using Horizontal Line Embedding



By:

- Rakush Rimal (AP17110010129)
- Cyrus Maharjan (AP17110010130)

Mentor:

- Dr. Shuvendu Rana, SRM AP

3D Image Watermarking using Horizontal Line Embedding

Abstract:

Watermarking is one of the techniques of information hiding. Basically, a watermark is the text or image impressed onto paper which provides evidence of its authenticity. For example if you place the money in light, you can see an image which is not found in duplicate one. Digital watermarking is the extension of the watermarking concept in the digital world. It is defined as the pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information. The watermarking algorithm holds the host image and data to embed and produces a watermarked image. The goal of digital watermarking is to avoid third party users removing or replacing the hidden data or message. The most important advantage of digital watermarking is that it provides copyright to the content owner. It also helps to avoid illegal copying of the information over the network. Digital image safety falls upon one of the important aspects in today's world. Digital watermarking is a famous technique which is used for copyright protection and authentication. This paper presents a method of 3D image watermarking by finding DC coefficients of a horizontal line which provide image security to the owner.

Introduction:

Watermarking is one of the three techniques of information hiding, steganography and cryptography are the other two. Basically, a watermark is the image or text that is impressed onto paper which provides evidence of its authenticity. For an example, visible when money is put into light, unique mark in the paper during manufacture.

Digital Watermark is an extension of the watermarking concept in the digital world. A Digital watermark is defined as the pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information. For example, we can see "Getty Image" in the images when we search in google.

The first and most important feature of digital watermarking is that it provide the copyright to the content owner. Even if your information is made of multiple copies and shared, only you can claim its ownership. It also helps to avoid illegal copying of the information. Digital watermarking also helps in authentication.

Digital Image Watermarking is one of the method to protect the rightful ownership and tamper detection of the image. In digital watermarking image some secret information is embedded into image in such a way that it maintains its originality and can be tracked for ownership and tamper detection when it is needed. After data embedding, the output image can or not necessarily be similar to its original image, but the watermark should be encrypted in such a way that the unauthorized person shouldn't able to modify or temper the image.

Digital watermarking has three phases. They are:

1. Embedding
2. Attack
3. Detection

1. Embedding
   In embedding, an algorithm holds the host and the data to be embedded and produces the watermarked image.

   Input: watermark, cover data and optional key
   Output: Watermarked data

2. Attacks
   The watermarked digital image is normally transmitted to another person over the internet. If that person makes the modification, it is called an attack.

3. Detection:
   Detection or extraction is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it or measure the confidence measure.

   Input : original data or watermark W, watermarked data, key (if applied)
   Output: watermark or confidence measure

   Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

   The information to be embedded in a signal is called a digital watermark. It can also be defined by the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

3D imaging is a technique to develop or create the illusion of depth in an image. 3D imaging has become a very useful factor for industrial applications to assist in quality control processes. 3D imaging is the process of manipulating 2D data into three-dimensional formats, creating the illusion of depth.

Block Diagram:

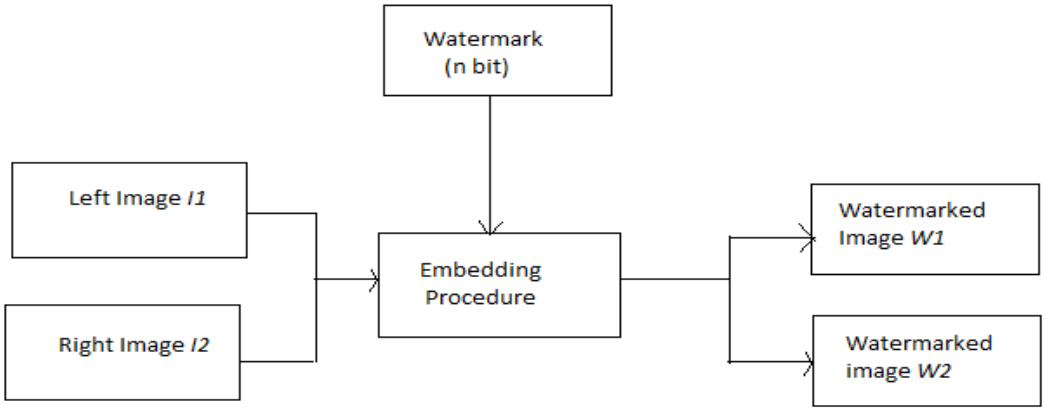


Fig: Watermarking Block Diagram

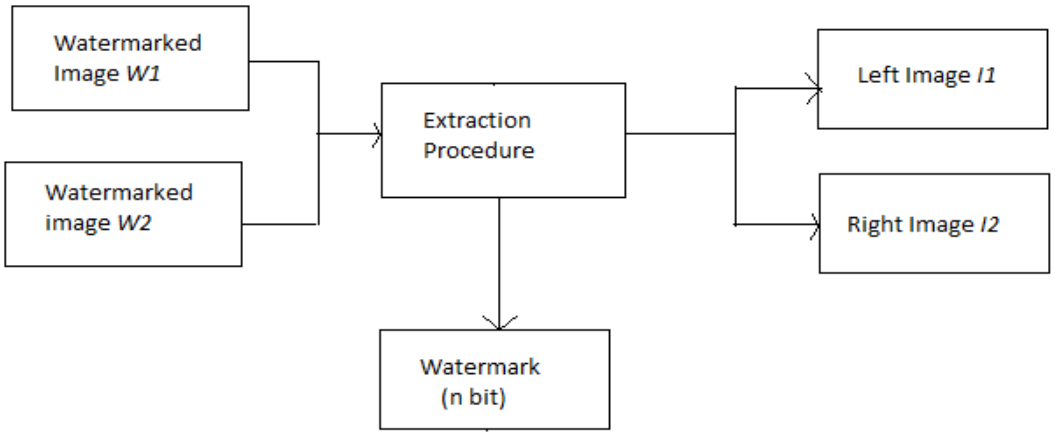


Fig: Extraction Block Diagram

Literature Review:

Researchers have done much research in the field of digital watermarking in the last two decades. S.Shrivastava and S.Choubey [1] present a general method to improve watermark robustness by exploiting the masking effect of surface roughness on watermark visibility. Watermark technology has been successfully used for this purpose for other kinds of media such as images and video, but, a lot of work is again necessary to reach robustness and industrial applicability for 3D watermarking. In this paper they have treated a specific aspect of 3D watermarking technology: the visual quality of the watermarked model. In particular, after a panoramic on 3D watermarking technology they have presented some ideas about this issue, and they have proposed a method based on multi resolution analysis to improve this aspect in future watermarking algorithm.

Khare and Vinay[2] proposed a medical image watermarking with focus on robustness and imperceptibility by utilizing homomorphic transform(HT), redundant discrete wavelet transform (RDWT) and singular value decom-position (SVD) transforms.HT is used to obtain the reflectance component of medical host image, on which RDWT decomposition and SVD are applied.The watermark image is processed similarly using RDWT and SVD.Watermark image is then embedded into the host image using singular values(Svs).After embedding, chaotic encryption is applied for extra security.The described technique can be extended for multiple watermark of real time applications.

Tjokorda et al.[3] proposed a reversible medical image watermarking method using LSB modification for tamper detection and recovery in ROI. Reversibility is achieved by using run length encoding(RLE) to embed the original LSBs into the RONI for higher embedding capacity.
Thanki et al.[4] proposed a fast discrete curvelet transform(FDCuT) and discrete cosine transform(DCT) based medical image watermarking scheme. In this scheme, a watermarked bit is embedded into the HF of FDCuT-DCT of the host image using white gaussian noise(WGN) sequence. Recovery of watermark data is performed by correlation of WGN sequences at extraction. The limitation of this scheme is the presence of noise in the extracted watermark image.
Ritu and Manisha[5]developed a medical image watermarking algorithm for e-diagnoses using M-ary modulations where the diagnosis part(ROI) is extracted using Fuzzy C-means and the electronic patient record (EPR) as a watermark is embedded in mid-band discrete cosine transform(DCT) coefficients using M-Ary modulation in RONI. The use of M-ary modulation improves the robustness of the system but the result of this scheme is limited to only brain medical images.
A technique proposed by Kumar et al.[6] uses second level DWT to generate different frequency components of the host image. The selected component is further treated with SVD and the watermark to be embedded is secured using arnold transform. An embedding approach is then used to embed the encoded watermark into the host image. Set partitioning in hierarchical tree (SPIHT) is used to further compress the watermarked image. This method can further be expanded to include various multimedia such as audio and video.
Sabbane and Tairi[7] suggested a watermarking scheme for providing security, reliability, and authenticity of medical information which consist of numerical information into the original image. The main idea behind this work is the use of polynomial transform to decompose an image into two parts called the structure and the texture component. The texture component is used for embedding. The capacity and

robustness of their model can be improved by combining transforms such as SVD, DFT and DWT, another limitation is that the work did not include color medical images.
Secure and robust fragile medical image watermarking for authentication and self recovery proposed by Elhoseny et al.[8] where the host image is transformed into 4x4 blocks and SVD is applied by inserting LSB of image pixels.Survival of attacks is taken care of by two authentication bits called block authentication and self recovery bits.Arnold transform is used to insert the self recovery bits.As a limitation,this scheme cannot detect non-fragile tampers.

Proposed Algorithm:

Algorithm 1: Proposed watermarking scheme		
Input	:	A left image *I1* and a right image *I2* both have size of $R \times C$ pixels and a watermark bit sequence *D*.
Output	:	Two watermarked images *W1 & W2* having size of $R \times C$ pixels which contain the hidden watermark *D*
Step 1	:	Read the left image *I1*. Read the right image *I2*.
Step 2	:	Convert both the images *I1 & I2* into grayscale images.
Step 3		Read the ‘n’ bit watermark to embed into the image.
Step 4	:	Take a line or a horizontal matrix of size (1,:,:) in both left and right images.
Step 5	:	Perform the DCT (1D) operation for both left image line and right image line.
Step 6	:	Take the DC coefficients (DCL and DCR) of both the images.
Step 7	:	Embed the watermark bit such that 1 for DCL>DCR and 0 for DCL<DCR
Step 8	:	Perform inverse DCT to get the original image.

Extraction Algorithm:

Algorithm 2: Proposed watermark extraction and image recovery scheme		
Input	:	Two watermarked images *W1 & W2* having size of $R \times C$ pixels which contain the hidden watermark *D*
Output	:	A left image *I1* and a right image *I2* both have size of $R \times C$ pixels and a watermark bit sequence *D*.
Step 1	:	Read the left watermarked image *W1*. Read the right watermarked image *W2*.
Step 2	:	Convert both the images *W1 & W2* into grayscale images.
Step 3	:	Take a line or a horizontal matrix of size (1,:,:) in both the images.
Step 4	:	Perform the DCT (1D) operation for both left image line and right image line.
Step 5	:	Take the DC coefficients (DCL and DCR) of both the images.
Step 6	:	If DCL>DCR then watermark bit is 1 otherwise the watermark bit is 0.
Step 7	:	Extract n bit watermark.

Future Work:

1. We're going to compare the work with existing schemes.
2. Implementing different 3d attacks and image processing of a video processing attacks so that robustness of this scheme can be justified.
3. Going for paper publication after completion of the work.

Conclusion:

In digital watermarking, a watermark is a digital code that is integrated into a digital media, which is inseparably attached to it. This data could be utilized to validate ownership, detect unauthorized users, provide image security and so forth. 3D digital watermarking is very important due to the onward rapid development of the digital media information in business more especially in the field of medical, industrial and entertainment fields. This will solve the problem of having the 3D file to be duplicated, which will ensure the confidence of transmitting 3D data over any communication channel without being duplicated by unauthorized users. This paper deals with reading of 3D image file and then slice it into two part, left image and right image. A sequence of binary data is embedded as a watermark using DCT and the same is then extracted at the receiver.

References:

1. S. Shrivastava and S. Choubey, "A Secure Image Based Watermark for 3D Images," 2011 International Conference on Communication Systems and Network Technologies, Katra, Jammu, 2011, pp. 559-562, doi: 10.1109/CSNT.2011.119.
2. Khare, P., & Srivastava, V. K. (2020). *A Secured and Robust Medical Image Watermarking Approach for Protecting Integrity of Medical Images. Transactions on Emerging Telecommunications Technologies.*
3. Tjokorda, A. B. W., Adiwijaya, & Permana, F. P. (2012). *Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and run length encoding (RLE) compression.* doi:10.1109/comnetsat.2012.6380799
4. Thanki,R.,Surekha,B.,Vidvyas,D., & Borisagar,K(2017).An efficient medical image watermarking scheme based on FDCuT–DCT .https://www.sciencedirect.com/science/article/pii/S2215098617304287?via%3Dihub.

5. Ritu,A., & Manisha,S(2016).Medical Image Watermarking Technique in the Application of E-diagnosis Using M-Ary Modulation. https://www.sciencedirect.com/science/article/pii/S187705091630597X
6. Kumar, C., Singh, A. K., & Kumar, P. (2019). *Dual watermarking: An approach for securing digital documents. Multimedia Tools and Applications.* doi:10.1007/s11042-019-08314-5
7. Sabbane,F., & Tairi,H.(2019).*Medical image watermarking technique based on polynomial decomposition*.https://doi.org/10.1007/s11042-019-08134-7
8. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., & Hou, G. (2018). *Secure and Robust Fragile Watermarking Scheme for Medical Images. IEEE Access, 6, 10269–10278.* doi:10.1109/access.2018.2799240
9. M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," in Proc. 1996 IEEE Int. Conf. Image Processing, vol. 3, Lausanne, Switzerland, Sept. 1996, pp. 211–214.
10. A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Performance analysis of watermarking schemes based on skew tent chaotic sequences," in Proc. IEEE-EURASIP Workshop Nonlinear Signal Image Processing (NSIP 2001), Baltimore, MD, June 2001.
11. G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: A framework," IEEE Comput. Graph. Applicat., vol. 19, no. 1, pp. 18–24.
12. S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "On the invertibility of invisible watermarking techniques," in Proc. IEEE Int. Conf. Image Processing (ICIP'97), vol. 1, Santa Barbara, CA, Oct. 1997, pp. 540–543. [3] N. Nikolai