E-ISSN 2250-0944
ISSN 2250-1150
doi: 10.31838/ijprt/10.02.02

Research Article

Fingerprint Based Watermarking Using DWT and LSB Algorithm

S.SIVAGANESAN[1*], M.GEETHA[2], T.GOWTHAMAN[3], M.PRADEEPA[4]
Assistant Professor[1, 2, 3, 4] Department of Electonics and Communication Engineering[1, 2,3], Department of Mechatronics Engineering[4], KIT-Kalaignarkarunanidhi Institute of Technology[1, 2, 3], RVS Technical Campus-Coimbatore[4]
Coimbatore-641402, Tamilnadu, India
E-mail id: sivaganesan.kannan@gmail.com
Received: 03.07.19, Revised: 03.08.19, Accepted: 03.09.19

ABSTRACT
Present age is the age of information and digital multimedia plays a very vital role in the representation, expression and propagation of the information. Equally important is to secure the information from being duplicated, altered and mutilated. Digital watermarking, hence has become a research topic to safeguard the copyright of the content. This work provides an innovative image watermarking scheme in two transform domains – Discrete Cosine Transform and Discrete Wavelet Transform. It is proved that DWT is more suited for authentication of fingerprints. DWT is better than DCT because the decomposition of images into three different levels. And concluded using the parameter mean square error, PSNR. From the study, it is obvious that DWT is better technique than DCT for the application of watermarking.

Keywords: Digital Watermarking, Discrete Cosine Transformation, Discrete Wavelet Transform, DWT, LSB

INTRODUCTION

Recent years have witnessed a rapid growth of digital media, and their propagation, especially images. This makes protecting multimedia information more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest and gradually has become a research hotspot in the field of information security. The idea of robust watermarking of images is to embed information fingerprint within the image with an insensible form for human visual system but in a way that protects from attacks such as common image processing operations. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key. Some of the applications of watermarking are broadcast monitoring, copy protection, data authentication and data hiding. Watermarks are classified after watermark embedding operation, whether they are visible to human visual system or not; visible watermarking and invisible watermarking. In real life, shading examples visible digital watermarking is the most common is to add "confidential" words in the word document, the visible watermarking is equivalent to a statement. Without visible digital watermarking is required in the visual perception cannot be aware of its existence, it is normally hidden embedded into the carrier, when the need to be extracted from the carrier. Unless there is a special statement, the objective of study of digital image watermarking is invisible watermark. This study presents a novel scheme of watermarking of digital images for copyright protection and authentication. In this study, we proposed methods of watermarking in frequency transformed techniques, Discrete Wavelet Transform (DWT). In DCT, embedded in the medium frequency region. It is a blind technique where we do not use the original image for extraction. In DWT, we embed in the LL region. Although, it is the most sensitive region, but embedding in this region proves resistance to various attacks especially compression. For DWT, non-blind technique is used.

Threats and Security Requirements

Threats are the conditions of possible specific actions that are enforced over the document that makes it counterfeit and illegal as against the wishes of the owner or creator. The most important threats which ought to be handled to ensure the security of the multimedia system are[1]:

Threat of Confidentiality

This threat represents the possibilities of accessing the data or document via unauthorized channels, with the growing usage of Internet, the chance of its occurrence is highly likely and is hard to get it dispelled out, unless effectively addressed[2,3].

Security Requirement

This requirement emphasizes the permit of only authorized access to the document or content and prevents the unauthorized access of resources.

Threat of Integrity

This is a threat to the content of the document by unauthorized entities, where the resource can be altered without any detection.

Security Requirement

It is required by this security requirement that the data be identically maintained from its source to destiny, and has not been accidentally or modified, altered, or destroyed, and remain unchanged right throughout the operations such as transfer, storage, and retrieval.

Existing Method

DCT BASED

The Algorithm for DCT based Digital Watermarking Embedding is proposed as below[1, 2, 3]: Read the watermark and the original image. Make the watermark image information into the 1Dimensional sequence. Input the original image into 8 x 8 sub-blocks, then do the DCT transform. Sort the coefficients of each sub-block after the DCT transforming, find two coefficients in the middle energy and then add fingerprint after binarization to it by add and shift method. According the principle above, compare the watermark information, exchange the coefficients if the relative doesn't match the watermark information

If i = 0; Make |P| > |Q|;

Else

Make |P| < |Q|;

a) Do the inverse DCT and form the watermark image.

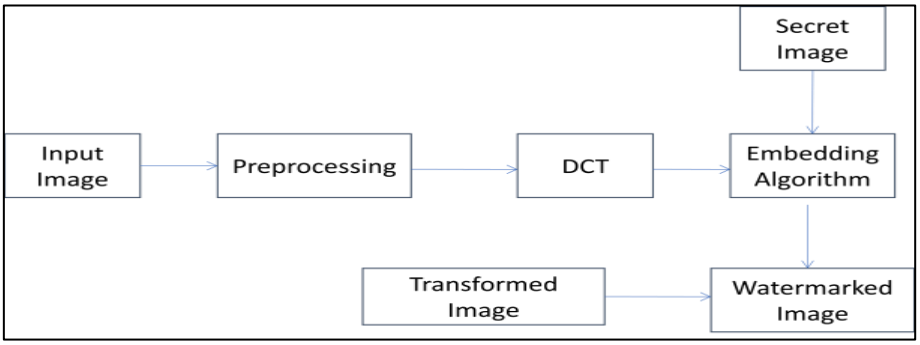

Fig.1: Add and Shift Method

The Algorithm for DCT based Digital Watermarking Extraction is proposed as below: On each 8 x 8 block of the watermarked image DCT is performed. Compare the middle frequency coefficients. If coefficient value is greater than another, then the message bit is 1; otherwise it is 0. Then form the 1_D sequence Re-organize the 1-D sequence into 2-D sequence and form the recovered watermark image.

Proposed System Dwt Based

The Algorithm for DWT based Digital Watermarking Embedding is proposed as below: Given a watermark, host image, watermark embedding inserts the watermark that is finger print into the target area of the host image. The cover image is decomposed into 3-level using DWT as the transform domain [2, 4, 6]. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. Here, we are using the Haar wavelet. The embedding is done in the LL region. So the altered host image i.e. watermarked image (LL) region (LL3) is LL3 = LL + k*w;

Where w watermark, and k is the embedding factor/strength. As watermark is directly embedded into some region, so far matrix addition to be feasible; we can concatenate zero's to watermark (in case watermark image is smaller than size if LL band). The cover images further reconstructed using inverse discrete wavelet transform

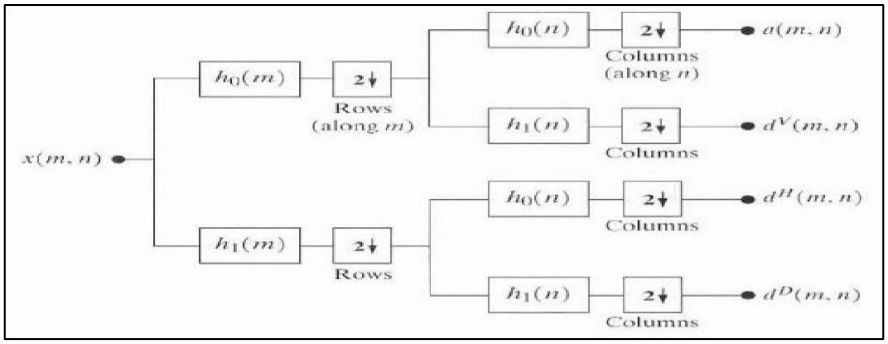

Fig. 2: DWT Method

Lsb Algorithm

There are many algorithms available for invisible digital watermarking. The simplest algorithm is Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is over written with a bit from the watermark. In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image[7,8,9]. This method is based on the pixel value's Least Significant Bit (LSB) modifications. The Algorithm for DWT based Digital Watermarking Extraction is proposed as below: The watermarked image is decomposed into 3 levels using DWT as the transform domain at the receiver end[10]. The extraction part is simply the inverse of the embedding procedure. Using the embedding strength and the original image, we can recover the watermark. After receiving the final watermarked image (may/may not be altered by attacks).

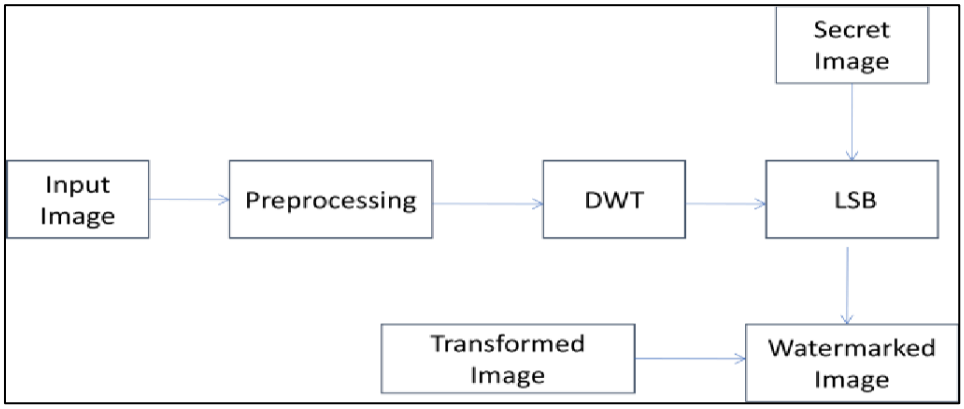

Fig.3 LSB Embedding

The below mentioned steps are followed to extract the watermark: Obtain the 3-level DWT of the watermarked image. The extraction part is as follows: $W_{rec}(i,j) = (LL_{wi}(i,j) - LL(i,j))/k$;

Where $W_{rec}(i,j)$ is the recovered watermark, $LL_{wi}(i,j)$ is the LL component of the watermarked image, $LL(i,j)$ is the LL component of host image and k is the embedding factor. If concatenation is done in the embedding part, the deconcatenation is required here to retrieve the watermark.

Implementation Results

Different images have been taking while analyzing various noise attacks and their effects on the original images and the recovered watermarks. It is not possible to display here all the results for all images. Fig-1 shows the original Lena image analyzed and the corresponding watermark. Using the standard Lena image (512 x 512) and watermarks.Fig-4b and Fig-3 show host image and fingerprint to be added as watermark, DWT based watermarked process. Fig-4 shows the recovered watermark which experienced region-based attack.

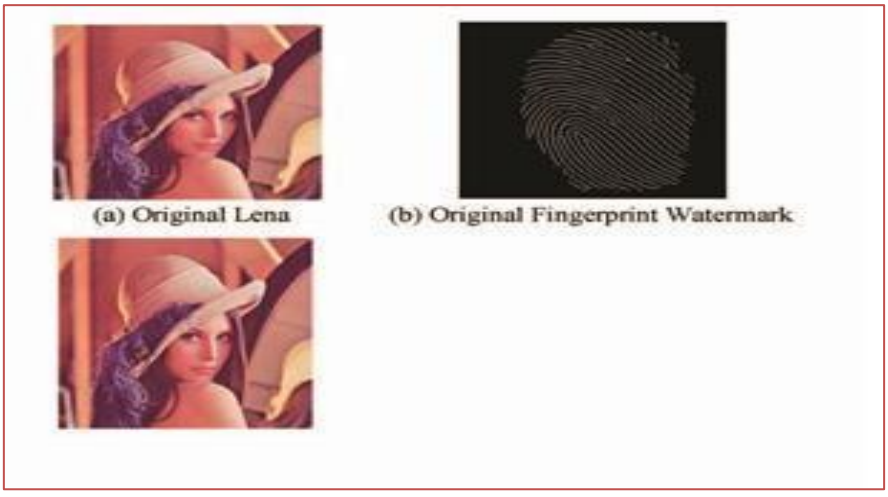

Fig.4: Original image (Lena) and corresponding watermark as fingerprint.

Mean Square Error (MSE) is a measurement of error introduced between two images. PSNR is inversely proportional to MSE.PSNR is measured between Original Watermark and extracted watermark. PSNR value without any attack is 32.50.PSNR is to determine the invisibility criteria. The following comparison shows DWT is better than DCT.

TYPES	EX-METHOD	PROPOSED SYSTEM
MSE	0.0242	0.1836

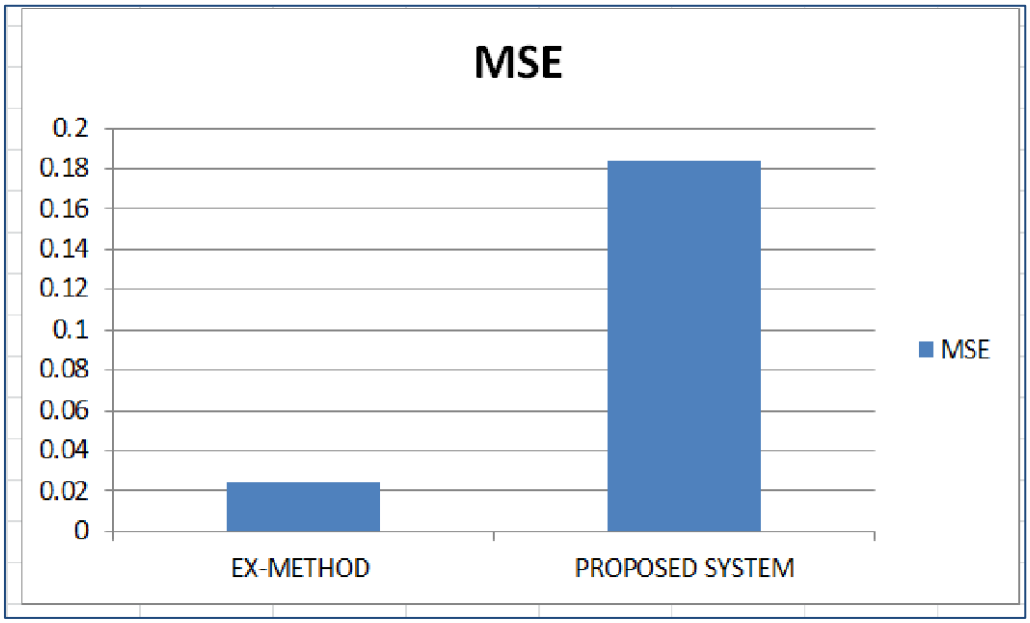

Fig.5.1: The figure shows the difference between MSE of Proposed and existing system.

TYPES	EX-METHOD	PROPOSED SYSTEM
PSNR	64.2953	55.4921

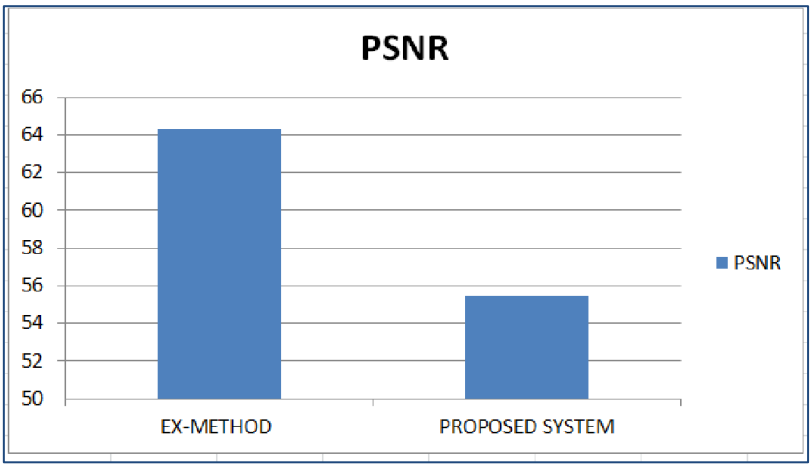

Fig.5.2: PSNR

CONCLUSION

This work provides an innovative image watermarking scheme in two transform domains – DCT and DWT. Both the domains are good enough to resist various attacks. It is proved that DWT is more suited for Human Visual System. DWT is better than DCT in various aspects and proved by the values of PSNR and MSE. From the study, it is obvious that DWT is better technique than DCT for the authentication of fingerprint .LSB algorithm makes

embedding more secure. The extracted watermark that is fingerprint is less effected by noise in DWT.

REFERENCES

1. Ashdown M., Flagg M., Sukthankar R., and Rehg J.M., A Flexible Projector-Camera System for MultiPlanar Displays, Computer Vision and Pattern Recognition (CVPR), pp. II-165 -II-172, 2014.
2. AkhilPratap Singh and Agya Mishra, "Wavelet based Watermarking on Digital image", Indian journal of Computer Science and Engineering, vol. 1, no. 2, 86-91.
3. Bo Chen and Hong Shen, "A new robust-fragile double image Watermarking algorithm", Third international conference on multimedia and Ubiquitous Engineering, IEEE-2009.
4. Brown M.S. and Seales W. A Practical and Flexible Tiled Display System 10th Pacific Conference on Computer Graphics and Applications (PG'02), pp. 194 –203, 2002.
5. Del Colle et.al, "DWT based Digital Watermarking fidelity and robustness evaluation", Journal of Computer Science and Technology, 4-1-2008.
6. Manzoor Ahmad Bhat, et.al, "Audio watermarking in images using wavelet transform", IJCST, vol.2, issue 4, Oct-2011.
7. Panyavaraporn, J.; Horkaew, P.; Wongtrairat, W., "QR code watermarking algorithm based on wavelet transform,"Communications and Information Technologies (ISCIT), 2013 13th International Symposium on , vol., no., pp.791,796, 4-6 Sept. 2013
8. Naderahmadian, Y.; Hosseini-Khayat, S., "Fast Watermarking Based on QR Decomposition in Wavelet Domain," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on , vol., no., pp.127,130, 1517 Oct. 2010.
9. Zhaoshan Wang, ShanxiangLv,YanShna (2012)"A Digital Image Watermarking Algorithm Based on Chaos and Fresnel Transform", 2012
10. M. Nithya, "Multimedia Security", IIT Bombay, 2005. Bo Chen and Hong Shen, "A new robust-fragile double image Watermarking algorithm", Third international conference on multimedia and Ubiquitous Engineering, IEEE-2009.