IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 6, June 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Discrete Wavelet Transformation a Method for Digital Watermarking

Ifra Iqbal Khan[1], M.A. Rizvi[2],

[1] Department of computer Technology and Application, National Institute of Technical Teachers' Training and Research, Bhopal, M.P., India

[2]Department of computer Technology and Application, National Institute of Technical Teachers' Training and Research, Bhopal, M.P., India

Abstract
In today's era the need for watermarking is felt to protect the data from being illegally copyrighted, the digital watermarking has got its multiple use for protecting data over the network as it does not involve the medium in which data is travelling it deals directly with the message which carries the hidden message to keep the secrecy of message a priority. There are several techniques involved in digital Watermarking but one main and important technique being evolved is Discrete Wavelet Watermarking (DWT) as mark produced by it is most robust of the all present techniques. It involves the wavelet decomposition mechanism for embedding the mark and inverse technique is applied to retrieve it. The discreet wavelet transformation is one of the most popular and secure technique which provides full-fledged robustness regarding any kind of attack, this technique can be made more efficient by reducing the levels of decomposition and making faster in computation.

Keywords: *Content Control, Data obfuscation, Digital Watermarking, DWT, Forensic Construction, Robust*

1. **Introduction**

Digital watermarking is the field in image processing which allows a secure way of transmission of the message, by being hidden in another data; it may any media like image file, video file or audio file. The watermarking in a broader sense can be taken as a content controller which is useful for tracking the individual assets moreover it is a security tool which enhances the security of a particular data in fact an organization giving full copyrights to owner, to embed its mark in an media along with a key which only desired recipient can have otherwise data hidden is not visible to the non-authentic users [4]. The watermark contains the owner's identification mark that is the creator of the data, also if piracy occurs it can track back the malicious users. According to different forms of watermarking digital watermarking comprises of Spatial domain and frequency domain , Discrete Wavelet Transformation (DWT) comes under the category of frequency domain, this domain provides a very important property of the watermarking which is robustness , this technique is strongly robust against attacks like transformation and other noise attacks. It forms an invisible and imperceptible; also many copies of watermark on copies of data are possible to provide unique identity to the data. The digital watermarking comes under the category of steganography which involves the hiding secret message or data in these host media whether it may be audio, video or still image, main thing is only the sender and intended recipient knows that the message even exists and which is only essential for retrieving the message[4].

2. Digital Watermarking

In digital watermarking the image is evaluated according to pixels present that is pixel by pixel in context to this the image has got low frequency and high frequency pixels. Then data is encoded by using an encoder its encoders choice whether to encode a 0 or a 1 after encoding by using any domain technique the watermark is embedded in the media [1]. The recipient needs to extract the original message, they are like gray dots on a black background those gray dots will be the hidden image or media message which sender does not want to disclose to non-authentic users. The new technologies that are developed embeds code so that image can be altered by scaling, cropping and transcoding without losing the ability of extracting the watermarked data, they are not generic and also not standardized. The advantage of digital watermarking is that it does not allow extraction if key is absent, this process is very essential as it can be applied to n- number of files mark can be similar or dissimilar the example for this is fingerprinting.[2]The Requirements for Digital watermarking are :

- The image should not get distorted in the presence of mark also when the unique identifier is being extracted.
- The watermark should be easily available either with the help of a key or by some comparison norms between hidden image and carrier image, to extract mark from the host image.
- The watermark must be fully resistant and robust to all kinds of attacks.

3. Need for Watermarking

The use of digital content, media and many forms of data flow over the internet and other networks has felt the need to secure the data, to secure the privacy of owner that is the reason for digital watermarking being the most popular technique to hide the data also to provide copyright authentication, protection has given rise to this invisible watermarking technique. Today, it is easily possible to manipulate data for example a scanner can be easily accessed so it can tamper data easily hence watermarking provides the solution to all such problems regarding owners' rights protection and securing the data[1][2].

4. Literature Review

In 2016, **Min Chien Yu** et. Al. [3]In "Improving Security and Privacy of Images on Cloud Storage by Histogram Shifting and Secret Sharing" cited that difference of Peak Signal to Noise Ratio(PSNR) of watermarking and masking in context to the data stored on cloud, as these are more prone to attacks this threat of attacks can be reduced by the invisible marking that is digital watermarking. This work carried out contains the comparison based study which focused on increasing the security of the data in a leakage prone environment. They proposed a secret key which prevented the malicious users from attacking the content stored on cloud.

In 2016, **Arezou Soltani Panah** et. al. [4] In "The properties of non-media Digital Watermarking : A Review of State of Art Techniques" proposed that strength of watermark lies within its capability of being visible that is how much easily it is visible to the user, they have focused on the imperceptibility of watermark. The invisibility they have define is for human intervention that how a data or content can be secured by the use of digital watermarking. They have also included that this technique is used to enhance data with the hidden information to make data more trust worthy. One difficulty that was encountered is that one cannot count on the large noise bandwidth and sensitive data such as salary, property co-ordinates and biological data cannot tolerate even a slightest distortion.

In 2016, **Pei Yu Lin** [5] in "Distributed Secret Sharing Approach based on QR Code" have proposed a designed QR sharing approach to protect the private QR data a reliable and secure means of distributed system, this approach is quite different from related QR code it uses some of its characteristics for achieving secret sharing so as to resist any print and scanning operation without permission. This reduces the threat of attacking the data stored at the backend of the QR database only desired recipient can read the data.

In 2013, **Rui Li** et.al.[6] in "A Digital Watermarking Approach to Secure and Precise Range Query Processing in Sensor Networks" have suggested the methods which works on two-tiered wireless sensor networks to be protected from the attackers, main vulnerable and sensitive area of network at which most attack took place was node so it became vital point of research so it was preserved by the sensor named se link watermarking scheme so as to protect data they have clustered the data with watermark embedded into links in order to prevent any distortion.

In 2009, **Jyotsna Singh** et.al. [7] in "Watermarking of unified Multimedia Data Types, Audio and Image" they have studied the audio, video and image conversion into randomized spectral divisions by using the two dimensional discrete fractional random transformation which has got a key utilized for embedding process and for decryption same key is required by the receiver. They have found out that by this randomization technique, on watermarking two different data types reduces number of computations and signal that was recovered after decryption and watermark extraction process which was found to be deviated from the host signal.

5. Properties

Robustness : A watermark is robust if it has got immunity to the attacks such as noise distortions and transformation which are cropping, scaling and other geometric transformations and conversions such as analog to digital conversions and digital to analog conversions[9][10][8].

Tamper Resistance: The watermark should be tamper proof it means data should not be manipulated by any external or internal source. The authority should not be handed over to non-desired recipients that is why we use watermarking which protects any change in data without the secret key encrypted by owner of data[9][8].

Fidelity: The watermark must be imperceptible, if fidelity is high then it is difficult for human eye to perceive changes in the signal without the consent of owner [10][8].

6. Applications

Copyright protection: The owner has got rights to authenticate the data and the secret key to be distributed to the user of its data which can only extract the message by use of that key. It gave authentication privileges to data owners to protect the data [8][9].

Authentication : This prevents any changes in data and watermark does not allow illegal copyright of data, tampering in such cases is impossible as hidden data is imperceptible to human eye, if data is not seen it cannot be manipulated[8][9][10].

Broadcast Monitoring : It concerns with distribution of data over the internet, managing rights over tele-media , cinema radio and other means that video and audio signals the data can be protected by the watermarking being applied to media for example the channel logo seen on side of the television screen so as to save data from being theft and copied by attackers, this prevents illegal copying of media[8][9].

Digital Signature: They are for authentication of documents; it uses a private key cipher text of a compressed string derived from the object. It can be used with any kind of message whether it is encrypted or not.

Proof of Ownership : It provides the owners identity, multimedia owners may want to use watermarks which not only identify copyright ownership, but actually proved the ownership[8][9].

Transactional Watermarks: It provides the monitoring and owner identification applications in which the owner places the same watermark in copies of same content and for distribution different watermark is embedded to track the piracy [9].

Data Obfuscation: This concerns with mining of data how data can be mined by keeping privacy in mind or to protect large and bulk data before applying mining the data undergoes digital watermarking technique to prevent its illegal distribution over the network [8].

Forensic Construction: It involves indexing of data so that the data under invigilation is easily identified by the auditor, in this embedded information is present in the data structure and not in the data set. The places it can used for forensic construction inn cases of investigation like that concerning cyber security, medical imaging and remote sensory images [8].

7. Discrete Wavelet Transformation (DWT)

The technique which is categorized under the frequency domain is known as Discrete Wavelet transformation. This transformation technique involves wavelet coding which is done by transforming the coefficients that defines the pixel of an image, it provides the more efficient method of watermarking, due to the this the coefficients can be quantized coarsely to zero providing minimal distortion to image which is imperceptible to human eye[2][4]. The transformational methods which are prevalent for wavelet coding are Huffman coding and Laplacian transformation etc. They provide simpler statistics of transformational data as the computed data carry little visual information. Huffman coding provides a lossless environment coding to provide a platform for conducting a comparative study by different weights assigned to the coefficient. The wavelets are chosen on the basis of coding and decoding of the transformation, in between when encryption is done the computational complexity becomes low as the refined transformation function like scaling to implement the embedding of mark in image [1]. It adds an advantage to the system that when we divide pixel into small number of components the transform is able to recompress and reconstruct the coefficient. The coding involves Discrete Wavelet Transform to embed the message and for recovering the message the algorithm uses inverse wavelet transforming this the image gets decomposed into different decomposition levels the two level decomposition means that levels are decided by number of operations involved for the computation of forward and inverse transformation which on other hand increases the level of decomposition also quantization increases the lower scale coefficients that result in more levels of decomposition[1]. The Discrete Wavelet Transform (DWT) occurs when a function gets expanded as a sequence of number then the coefficients which are obtained as results are known as Discrete Wavelet Transform.

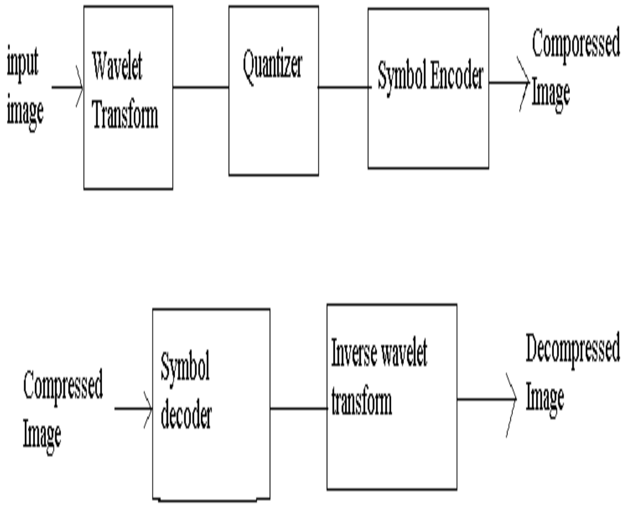

Fig 2 : A wavelet coding system

Basic Approach involved in two dimensional Wavelet transform are as follows[2]:

- For an image compute the two dimensional wavelet transform
- Take the transformed image and alter it.
- Now evaluate the inverse transform an apply it to the image to get the original signal

The Discrete Wavelet transform (DWT) have got scaling and wavelet vectors that are used as low pass and high pass filters [1][2]. In this process image produced is of multiresolution the frequency gets divided into high and low values according to the pixels then for a clear and more precise watermark we further divide the low frequency quadrant into again lower and higher frequency values that is called decomposition and embedding is carried out in the lower and higher frequency overlapping quadrants, after this inverse wavelet transformation is applied to get the message hidden in the host image in place of the transformed coefficient.

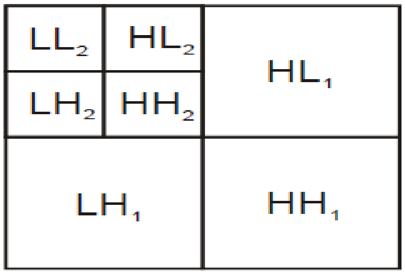

Fig 3: 2-level Discrete Wavelet Transform

8. Advantages and Disadvantages

The below table gives the advantages and disadvantages of the several techniques which are used for digital watermarking.

Table I
Advantages and Disadvantages of different techniques of watermarking [13]

Algorithm	**Advantages**	**Disadvantages**
DWT	• Provides time and frequency computation. • Good localization id provided in time and frequency domains. • Compression Ratios are higher making the watermark imperceptible to human eye.	• More time consuming. • Cost of Computation is high. • Compression takes time. • Noise near edges is observed while doing the experiment.
LSB	• Implementation with Ease. • Image Quality does not gets degrade easily. • Watermark is Transparent to Human eye.	• It is not robust. • Prone to noise and geometric transformational attacks.
DCT	• Embedding takes place in	• Invariance properties of

	middle frequency range of an image or media visibility remains unaffected. • Watermark is not easily removed by any attack.	image get eliminated. • During quantization higher frequency components gets suppressed.
DFT	• Geometric Transformations like rotation and scaling can be recovered by this method. • Method eliminates risk of transformational attacks.	• Implementation is complex. • Cost of computation found out to be higher than other methods.

9. Conclusion

The DWT is based on time and frequency tools it is time consuming but by using Discrete Wavelet Transform(DWT) the robustness is assured , it also involves the Fourier transformation to save the entire message being attacked or get affected by any geometrical transformations. In the technique of digital watermarking the embedding algorithm takes the secret key and watermark bits as inputs and converts the data set into a digitally watermarked set so as to prevent any further modification in the media.

References

[1]. Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", Pearson, Third Edition, 2013.

[2]. Madhuri A. Joshi , "Digital Image Processing : An Algorithm Approach"PHI Learning, Fifth Edition, June 2010

[3]. Min-Ying Wu, Min Chein Yu, Jenq-shiou Leu, Sheng-Kai Chen, Improving Security And Privacy of Images on Cloud Storage by Histogram Shifting and Secret Sharing, IEEE, 2016.

[4]. Arezou Soltani Panah, Ron Van Schyndel, Timos Sallis, Elisa Bertino. "On The Properties of Non-Media Digital Watermarking : A Review of State of the Art Technique",pp2670-2704, Volume 4, 2016.

[5]. Pei Yu Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code". IEEE Transactions on Industrial Informatics, Vol 12 No. 1, Feb. 2016.

[6]. Yequin Yi, Rui Li, Fei Chen, Alex X Liu, Yaping Liu "A Digital Watermarking Approach to secure and Precise Range Query Processing in sensor Networks ", Proceedings IEEE Infocom, pp 1950-1958, 2013.

[7]. Jyotsna Sing, Parul Garg, Alok Nath, "Watermarking of Unified Multimedia Data types, audio and image" IEEE, 2009.

[8]. Ingeman J.Cox, Matt L. Miller, Jefferry A. Bloom, "Watermarking Applications and their Properties", International Conference on Information Technology Las Vegas, 2000.

[9]. Preeti Arya, Dherendra Singh Tomar, Deepika Dubey, "A Review on Different Diigital Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition, 2015.

[10]. Prabhishek Singh , R S Chadha , "A Survey of Digital Watermarking Techniques", Applications and Attacks, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[11]. K.Sridhar, Dr. Syed Abdul Sattar, Dr. M Chandra Mohan , "Comparison of Digital Watermarking with OtherTechniques of Data Hiding" , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 350-353, 2014.

[12]. Er. Sanjeev Kumar, Dr. Tanu Preet Singh, "A Review of Digital Watermarking, Applications and its Techniques", International Journal of Computer & Organization Trends – Volume 10 Number 1, Jul 2014.

[13]. Aaquib Rashid, "Digital Watermarking Applications and Techniques: A Brief Review", International Journal of Computer Applications Technology and Research, Volume 5–Issue 3, 147-150, 2016.