Survey of High Secure Digital Image Watermarking using Different Transform Technique

Himalaya Shrivastava 1* and Prof. Sandip Nemade 2

1M. Tech. Scholar, Department of Electronics and Communication TIT, Bhopal.
2Associate Professor, Department of Electronics and Communication TIT, Bhopal.
*Corresponding author email id: himalaya2691@gmail.com

Date of publication (dd/mm/yyyy): 22/06/2019

Abstract – Telemedicine is well known application where enormous amount of medical data need to be transferred securely over network and manipulate effectively. Security of digital data, especially medical images, becomes important for many reasons such as confidentiality, authentication and integrity. Digital watermarking has emerged as a advanced technology to enhance the security of digital images. The insertion of watermark in medical images can authenticate it and guarantee its integrity. The watermark must be generally hidden does not affect the quality of the medical image. In this paper, we study of digital watermarking based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). This method can be used for authentication and data hiding purposes. The future work can be extended to hybrid DWT and single value decomposition (SVD) method to improve the robustness of the watermark.

Keywords – Discrete Wavelet Transform, Haar Wavelet, JPEG Image Encoding, Peak Signal to Noise Ratio.

I. INTRODUCTION

Watermarking in the frequency domain is more preferred over the spatial domain watermarking because in spatial domain watermarking direct modifications are made into the image pixels while in the frequency domain watermarking, modifications are made into the transform coefficients. Also some transforms have properties like energy compaction which are very useful in the watermarking [1]. It has been shown that watermarking process is analogous to the communication system and the watermarked image is equivalent to the channel in the communication system. Similar to channel, which has the maximum probability of noise occurrence, a lot of distortion or error could affect the watermarked image. The cause of this distortion could be lossy compression, geometric operations like scaling or cropping, image enhancement operations like increasing of contrast and histogram equalization, resampling, requantization, A/D and D/A conversions etc.

Using any type of image property or characteristic for embedding of the watermark is called image-adaptive or image dependent watermarking [2, 3]. Spread spectrum watermarking is done in the transform domain by which the watermark is spread across a large number of transform coefficients. Therefore in any one frequency component the watermarking content is very negligible and could not be determined. But as the location and content of the watermark is known to the watermarking process, it is possible to extract the complete watermark at the receiving end. Perceptual models or masks designed by using the limitations of the Human Visual System (HVS) are also used in image-adaptive watermarking. By using the perceptual models or masks those regions in the visually significant parts of the image are known that can bear some additional data without being perceptible. The watermark is then embedded in those regions.

This information carrying ability varies from one coefficient to another [4]. Strength factor in the watermarking process determines how much a frequency coefficient can be modified in accordance with its information carrying ability so that it does not affect the perceptual fidelity of the data [5].
Main use of watermarking is in the copyright/ownership protection of the digital content. Robust watermarking is used in this application. Most of the research work in robust watermarking is being done in frequency domain as watermarking in the frequency domain is more robust and secure than spatial domain watermarking. In the frequency domain, watermarking could be done using spread spectrum method or Quantization Index Modulation (QIM). But the watermarking using QIM is found to be very sensitive to the scaling of signal and hence very feebly resistant against the probable malicious attacks. On the other hand, spread spectrum based watermarking poses much stronger resistance against the malicious and non-malicious attacks. Also spread spectrum based watermarking has lesser complexity level and multiple watermarks could be embedded using it. Therefore robust watermarking using spread spectrum method is more preferred over the QIM method. As the internet has now become accessible to a large population of the world, necessity of robust watermarking to protect the copyrights of the content owners is increasing day by day. So, there is still a wide scope of research in this area [6, 7]. A lot of image-adaptive watermarking techniques are being proposed by the researchers as they are more robust than the non-image-adaptive techniques. There is a need to thoroughly study these techniques. There is a scope to find out more watermarking techniques where many image-adaptive measures could be applied simultaneously to obtain better robustness of the extracted watermark against a large number of watermarking attacks [8].

II. LITERATURE REVIEW

N. Senthil Kumaran et al. [1], Image security is a relatively very young and fast growing. Security of data or information is very important now a day in this world. In this paper proposed to advantages and that working functionalities. This algorithm is verified on different watermarking images. And it’s providing robust and secure results. To measure the effectiveness of this algorithm is provide embedding and extracting images. PSNR and MSE also calculated the embedding watermarking images. In this DWT watermarking embedding result images provide the good, secure and robust. In this paper proposed to how to process LSB technique.

Aase et al. [2] briefly discussed the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provided a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, their method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours.

Ahmed et al. [3] described a method that adds or subtracts small random quantities from each pixel. Addition or subtraction is determined by comparing a binary mask of bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. The watermark is subtracted by first computing the difference between the original and watermarked images and then by examining the sign of the difference, pixel by pixel, to determine if it corresponds to the original sequence of additions and subtractions. This method does not make use of perceptual relevance, but it is proposed that the high frequency noise be pre-filtered to provide some robustness to low-pass filtering. This scheme does not consider the problem of collusion attacks.

Akhaee et al. [4], digital watermarking has been investigated deeply for its technical and commercial feasibility in all media types like, digital photographic image, printed materials or document images and video.
It is a proven method for reducing content piracy and improving the ability to identify, track and manage digital media. It is widely used in applications like rights management, remote triggering, filtering/classification and e-commerce. It is a technique that is used to balance the need for content security with best possible consumer experience to enable media and entertainment industries to adapt the advanced facilities of the modern digital revolution while reducing the threat of content theft.

Ali et al. [5], proposed two schemes where the first was fragile watermarking and was used to authenticate the digital content, while the second was used to reconstruct the region where the integrity verification fails.

The watermark embedding procedure even though efficient reduced the quality of the reconstructed image when the strength of attack was increased. Different decomposition levels grant the tamper detection within the image in localized spatial and frequency domain. The aim is to present an authentication technique that hides watermark into some wavelet sub-bands of the to-be-authenticated image. This scheme is capable of detecting malicious and incidental manipulations. Furthermore, security is of particular concern that is often overlooked. It is extremely difficult for an attacker to create a faked image that appears to be authentic.

### III. Digital Watermarking

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means 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 [9].

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise [10].

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal [11].

![General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions.](image)

### IV. Discrete Wavelet Transform

An image can be analyzed in the DWT by exposing it first to an analysis filter bank and then later on applying a down-sampling operation on it. At every decomposition stage the analysis filter bank has a low pass and high
pass filter. The signal which goes from these filters gets divided into two bands. The low pass filter associated
with mean operation, brings out the most important information of the signal. The high pass filter associated
with a subtraction operation, brings out the complete details of the signal information. The resultant signal after
the filtering operation is then down-sampled by two. A two-dimensional transform is obtained by applying two
different one-dimensional transforms. In the beginning, image is filtered along the row and down-sampled by
two. Obtained sub-image is then filtered along the column and down sampled by two. In this process the image
gets divided into four bands called as HH, HL, LH and LL, as shown in Figure 2. Here LL represents the least
resolution approximation component while HL represents the horizontal, LH represents the vertical and HH
represents the diagonal component respectively. The LL sub band can subsequently be decomposed to achieve
one more decomposition level.

![DWT Diagram]

Fig. 2.2 Levels for DWT. Where G, H are the high-pass and low-pass filter coefficient.

The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level
of decomposition (remaining two samples, in this case). The DWT will then have the same number of
coefficients as the original signal.

V. METHODOLOGY

A. Watermark Embedding

For this process firstly we apply 2 level DWT on host image decomposes the image into sub-images, 3 details
and 1 approximation. The approximation looks just like the original. The same manner 2 level DWT is also
applied to the watermark image. For this Haar wavelet is used. Then technique alpha blending [8] is used to
insert the watermark in the host image. In this technique the decomposed components of the host image and the
watermark are multiplied by a scaling factor and are added. Since the watermark embedded in low frequency
approximation Component of the host image so it is perceptible in nature or visible. Alpha blending: formula of
the alpha blending the watermarked image is given by

\[ WMI = k \times (LL3) + q \times (WM3) \]

where WM3 = low frequency approximation of Watermark, LL3 = low frequency approximation of the original image, WMI = Watermarked image, k, q - Scaling factors. After embedding the watermark Image on cover image Inverse DWT is applied to the watermarked image coefficient to generate the final secure watermarked image.
B. Watermark Extraction

For this firstly we applied 2 levels DWT to watermarked image and cover image which decomposed the image in sub-bands. After this we apply alpha blending on low frequency components. *Alpha blending:* Formula of the alpha blending extraction for Recover watermark is given by

\[
RW = \frac{(WMI - k \times LL3)}{q}
\]

Where

- \( RW \) = Low frequency approximation of Recovered watermark,
- \( LL3 \) = Low frequency approximation of the original image,
- \( WMI \) = Low frequency approximation of watermarked image.

After extraction process, Inverse discrete wavelet transform is applied to the watermark image coefficient to generate the final watermark extracted image. Fig. 4 shows the watermark extraction process.

C. Discrete Cosine Transform

The development of many fast algorithms for the efficient implementation of the DCT has greatly helped to make this transform very popular. The main advantage of DCT is that it eliminates the redundancy between neighboring pixels of an image. As a result uncorrelated transform coefficients are obtained which can be encoded independently. Energy is bundled by DCT in the low frequency coefficients keeping the total energy of the image conserved.

Therefore some high frequency coefficients could be abandoned without any appreciable loss of quality. That's the reason for a very prominent use of DCT in the compression of images.

Distributed source coding (DSC) mainly depends on the principle of independent encoding and joint decoding. ‘Distributed’ in DSC points to the distributed nature of encoding operation, not the location as in distributed computing. DSC regards the compression of correlated information resources that do not communicate with each other (1). DSC models the correlation between multiple sources together with channel code and hence able to shift complexity from encoder to decoder. Hence DSC, DVC in current context, can be used to develop the devices having complexity-constrained encoder.
VI. CONCLUSION

A 2 level DWT based image watermarking technique has been implemented. This technique can embed the invisible watermark into the image using alpha blending technique which can be recovered by extraction technique. Experiment results shows that the quality of the watermarked image are dependent only on the scaling factors k and q and the recovered watermark are independent of scaling factor. Results shows that the recovered images and the watermark are better for 2-D discrete wavelet transform then 1 & 2 level discrete wavelet transform.

REFERENCES


AUTHOR’S PROFILE

Himalaya Shrivastava is currently pursuing the Master of engineering degree in digital communication and engineering from the Technocrats Institute of Technology, Bhopal, India. His research interests include image processing and cyber security.