SECURE HYBRID WATERMARKING USING DISCRETE WAVELET TRANSFORM (DWT) & DISCRETE COSINE TRANSFORM (DCT)

Neetu Rathi¹ and Dr. Anil Kumar Sharma²

M. Tech. Scholar¹, Professor & Principal²
Department of Electronics & Communication Engineering,
Institute of Engineering & Technology, Alwar-301030 (Raj.), India

ABSTRACT

Digital image watermarking is a technique used for copyright protections of digital data. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. This paper presents an efficient hybrid digital watermarking technique using DWT & DCT for copy right protection. In addition, a concise introduction about digital marking is presented along with its properties, techniques & attacks. The simulation results show that this algorithm has good robustness for some common image processing operations & also gives improved results in terms of PSNR & Correlation coefficients.

Keyword: Attacks, Authentication, DCT, DWT, PSNR.

1. INTRODUCTION

Everyday tons of data is embedded on digital media or distributed over the internet. The data so distributed can easily be imitated without error, putting the rights of their owners at risk. Even when encrypted for distribution, data can easily be decrypted and copied. One way to discourage illegal duplication is to insert information known as watermark, into potentially vulnerable data in such a way that it is impossible to separate the watermark from the data. These challenges motivated researchers to carry out intense research in the field of watermarking. A watermark is a form, image or text that is impressed onto paper, which provides indication of its authenticity. Digital watermarking is an extension of the same concept. Digital watermarking is the process of embedding information into digital multimedia content such that the information can be extracted or detected at the later stage for a variety of purposes including copy prevention and control [1]. A digital
watermark is used for this purpose which is a digital signal inserted into a digital image and may also serve as a digital signature [2]. Digital watermarking is also to be contrasted with public-key encryption, which also transforms original files into another form. Unlike encryption, digital watermarking leaves the original image uncontaminated and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software. Further, decrypted documents are far from any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent retransmission or dissemination. There are two types of watermarks: visible watermark and invisible watermark. In this paper we have concentrated on implementing watermark in image. The main factor of consideration for any watermarking scheme is its robustness to various attacks. Watermarking dependency on the original image increases its robustness but at the same time we need to make sure that the watermark is imperceptible.

2. CLASSIFICATION OF WATERMARKING

The classification of watermarks and watermarking techniques is very broad. These are divided into various categories [5, 6, 7] based on different criterions as shown in Fig. 1. According to the type of Document it can be divided into four categories i.e. Text Watermarking, Image Watermarking, Audio Watermarking and Video Watermarking.

![Fig. 1: Classification of watermarking Techniques](image)

On the basis of domain used for watermarking the techniques fall in two categories: those which use spatial domain and those which use transform domain. Spatial-domain watermarking technologies change the intensity of original image or gray levels of its pixels. This kind of watermarking is simple and with low computing complexity, because no frequency transform is needed. However, there must be trade-offs between invisibility and robustness, and it is hard to resist common image processing and noise. Transform-domain watermarking embeds the watermark into the transformed image. According to the human perception [5, 6, 9], it can be divided into Visible watermark, Invisible-Robust watermark, Invisible-Fragile watermark and Dual watermark. According to the application it is either source based or destination based. Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination -based watermark could be used to trace the buyer in the case of illegal reselling. Several different methods enable watermarking in the spatial domain. The simplest is just to flip the lowest-order bit of chosen
pixels. This works well only if the image is not subject to any change. A more robust watermark can be embedded by superimposing a symbol on picture. The resulting mark may be visible or invisible, depending upon the intensity value. Picture cropping, e.g., (a common operation of image editors), can be used to remove the watermark.

Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to identify under regular viewing. However, the mark appears immediately when the colors are separated for printing. This renders the document useless for the printer unless the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stockhouse before buying unmarked versions. Watermarking can be applied in the frequency domain (and other transform domains) by first applying a transform like the Fast Fourier Transform (FFT). In a similar manner to spatial domain watermarking, the values of chosen frequencies can be altered from the original. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture. Since watermarks applied to the frequency domain will be dispersed over the whole of the spatial image upon inverse transformation, this method is not as vulnerable to defeat by cropping as the spatial technique. However, there is more a trade-off here between invisibility and decodability, since the watermark is in effect applied indiscriminately across the spatial image.

3. ATTACKS ON WATERMARKS

A watermarked image is likely to be subjected to certain manipulations [2, 13], some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. The main type of attacks is as follows.

- **Active Attacks**: Here, the hacker tries intentionally to remove the watermark or simply make it unnoticeable. This is a big issue in copyright protection, fingerprinting or copy control for example.

- **Passive attacks**: In this case, the attacker is not trying to remove the watermark but simply trying to determine if a given mark is existing or not. As the reader should understand, protection against passive attacks is of the greatest importance in covert communications where the simple knowledge of the presence of watermark is often more than one want to grant.

- **Collusion attacks**: In collusive attacks [2], the goal of the hacker is the same as for the active attacks but the process is somewhat different. In order to remove the watermark, the hacker uses several copies of the same data, containing each different watermark, to construct a new copy without any watermark. This is a problem in fingerprinting applications (e.g. in the film industry) but is not the widely spread because the attacker must have access to multiple copies of the same data and that the number needed can be pretty important.

- **Forgery attacks**: This is probably the main concern in data authentication. In forgery attacks, the hacker aims at embedding a new, valid watermark rather than removing one. By doing so, it allows him to make change in the protected data as he wants and then, re-inserts a new given key to replace the destructed (fragile) one, thus making the corrupted image seems genuine.
4. PROPOSED ALGORITHM AND SIMULATION

In this work an algorithm is proposed for secure hybrid digital watermarking using DWT & DCT. For this a word “Hi” is used as a watermark & the image “lena” is used as a cover image. This watermark is first decomposed into equal parts in the form of binary matrix (0,1). Then the size of watermark image or message image is checked in comparison to the cover image. The size of the watermark should not be greater than that of cover image so that it can hide behind the cover image. Next the DWT is applied & the cover image is decomposed into its approximation coefficient’s. After applying DWT we get low frequency components of the cover image (cA1) & next we set a key=1982 for security purpose & a value of factor=10 which can vary. Then the watermarked image is to be hide behind the cover image in an encrypted manner (i.e. changing pixel value of cover image according to the watermark image). Afterwards extracting of the watermark image is done in a decrypted manner using DCT so that only a known receiver can decode it. Then PSNR & Correlation Value are computed for the recovered watermarked image. Fig. 2 shows the steps of simulation.

(a) Cover image “Lena”  
(b) Watermark Image “Hi”  
(c) Decomposed Watermark  
(d) Watermarked Image
Here we have observed that for Original Image Vs. Extracted Watermark Image, the value of PSNR = 56.7416, Correlation Value = 1. Next we are going to simulate the process with Attacks of Gaussian Noise as shown in Fig.3.
Here we have observed that the For Original Image Vs. Extracted Watermark Image,
The value of PSNR = 56.7109, Correlation Value = 0.9964
Next we go for compression attack as shown in Fig. 4.

![Decomposed Watermark](image1)

![Extracted Watermark](image2)

**Fig. 4: Simulation with Compression Attack**

Here we have observed, The value of PSNR = 56.7416, Correlation Value = 1
Next we carry out the Simulation with Salt & Pepper Attack as shown in Fig. 5.
Fig. 5: Simulation with Considering Salt & Peeper Attack

Here we have observed that for Original Image Vs. Salt & Peeper Attacked Watermark Image, the value of PSNR = 54.1684, Correlation Value = -0.036327

Observation: From Table-1 we can see that with reference to previous work we obtain much better result in terms of PSNR & Correlation Coefficient. Both parameters are improved for different cases i.e. without attack & on application of attack.

Table-1: Summary of Results as Compared to Previous Work

<table>
<thead>
<tr>
<th>Various Results</th>
<th>Results of Previous Work</th>
<th>Result 1 using Hybrid Technique without Attack</th>
<th>Result 2 using Hybrid Technique with Attack</th>
<th>Result 3 using Hybrid Technique with Attack</th>
<th>Result 4 using Hybrid Technique with Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR</td>
<td>31.552</td>
<td>56.7416</td>
<td>56.7109</td>
<td>56.7416</td>
<td>54.1684</td>
</tr>
<tr>
<td>Correlation Coefficient</td>
<td>0.9965</td>
<td>1</td>
<td>0.9964</td>
<td>1</td>
<td>-0.036327</td>
</tr>
</tbody>
</table>
5. CONCLUSION

The purpose of this paper is to provide a Hybrid Techniques i.e. combination of DWT & DCT which provides much security & robustness. The results obtained from the algorithm have provided simpler and a faster approach to find out the extracted images. The algorithm being proposed here has been shown to have good efficiency, but it is good enough to extract information from noisy environment in many application cases as: Biomedical signal processing, Image Processing, Image de-noising, Satellite Image Resolution, speech processing. Thus using MATLAB Hybrid Watermarking Techniques are implemented. Then Noise is added to the images in the form of Attacks. The noise is later removed & the base & watermark images are separated from the watermarked image. Finally a benchmarking of original & recovered image is done based on PSNR & correlation values.

REFERENCES