Survey Paper on Digital image watermarking

Ritu R Patel¹, Damini J Patel²,

¹Student, Computer Engineering, L.C.Institute of Technology, Gujarat, India
²Assistant Professor, Computer Engineering, L.C.Institute of Technology, Gujarat, India

ABSTRACT

Digital watermarking techniques have been developed to protect the copyright of multimedia objects such as text, audio, video, etc. So, we have proposed a hybrid Image watermarking technique which takes the advantages of different transforms like DWT, DCT, SVD and Arnold Transform, which enhances more security and provides robustness to the watermark. In this paper method, image is divided into several groups of frames, and one of the frames is selected where watermark will be embedded. Before embedding watermark in a selected frame it will be pre-processed with Arnold Transform which will provide security to it. The selected plane of Image are decomposed using DWT and high frequency band HH, middle frequency bands LH, HL are transformed with DCT. The DCT coefficients are SVD transformed which are embedded with corresponding transformed coefficients of watermarks along with Arnold Transform. The embedded watermark is extracted with inverse process of embedding. The proposed algorithm is tested with various Image sequences using MATLAB 2017a. The distortion quality of original image and watermark is controlled by the Peak Signal to Noise Ratio, Signal to Noise Ratio and Mean square error of the watermarked frame with original frame.

Keywords: -color components RGB, DWT, SVD, DCT, watermarking

1. INTRODUCTION

Digital watermarking is a technique that embeds data called watermark into a multimedia object so that watermark can be detected to make an assertion about the objects. It can be categorized as visible or invisible. Example of visible watermarking is the logo visible super-imposed on the corner of television channel in a television picture. On the other hand, invisible watermark is hidden in the object, which can be detected by an authorized person. Such watermarks are used for suit the author authentication and detecting unauthorized copying [6]. Protection of digital data has become a popular matter due to the quick development of the pervasive multimedia technology. Copyright protection of digital data has become a significant issue over increasing use of internet. Digital watermarking is that technology that provides security, data validation and copyright protection of the digital data. Digital watermarking is the process of embedding secret digital data, signal into the digital media such as image, video, audio and text [1].

1.2. Image Watermarking

Image Watermarking is the technique of embedding of owner copyright identification with the host image [9].

Figure 1: Watermark on Indian currency [9]
1.3. Discrete Cosine Transform (DCT)
The discrete cosine transform is a transformation technique based on digital water-marking algorithm and spatial domain technique. The discrete cosine transform is derived from discrete Fourier transforms and represents data in terms of frequency space rather than an amplitude space. The spatial domain technique can be transformed into the frequency domain, and the frequency domain technique can be transformed back to the spatial domain by using inverse discrete cosine transform. The discrete cosine transform (DCT) is a technique for converting a signal into effortless frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies [7].

1.4. Discrete Wavelet Transform (DWT)
The transformation product is a set of coefficients organized in the way that enables not only spectrum analyses of the signal, but also spectral behavior of the signal in time. This is achieved by decomposing signal, breaking it into two components, each concerned information about source signal. Filters from the filter bank used for decomposition come in pairs: low pass and high pass. Low pass filtered signal contains information about slow changing component of the signal, looking very similar to the original signal, only two times shorter in term of number of samples. High pass filtered signal be full of information about fast changing component of the signal [8].

1.5. Singular Value Decomposition (SVD)
The SVD is applied on the entire original image or some small part of it and then the singular matrix values are manipulated in order to insert the watermark in the image. SVD by principle is a method to detect algebraic features of an image and as their isn’t a huge change in the singular values upon adding small perturbations SVD based watermarking is particularly robust to geometric based attacks [2].

1.6. Applications of Watermarking [9]
- Owner Identification
- Copy Protection
- Broadcast Monitoring
- Medical Applications
- Finger Printing
- Data Authentication

2. LITERATURE REVIEW

2.1 “A Secure and robust image watermarking system using wavelet domain” [1].
A hybrid of DWT- SVD techniques has been proposed to embedded watermark in the image. The properties of DWT and SVD were found to be complementing each other as the proposed methods reveals good transparency and robustness. During experiments, The PSNR value for all test images above 30db indicates good perceptual transparency of the system.

Future scope: Hybrid of DWT – SVD techniques using better result but future scope of another method are apply to excellence performance.

2.2 “Genetic Algorithm based optimized Color Image watermarking technique using SVD and DWT”[2].
A new optimized DWT-SVD based watermarking technique using Genetic Algorithm. The singular value component of the original Image is modified by adding the singular component of the watermark image along with a suitable scaling factor. This scaling factor is optimized by GA using the PSNR values as the fitness criteria in order to achieve high values or robustness without compromising the transparency of the watermark.

Future scope: Future scope of the further application based analysis by using the Noise Correlation as a fitness function to test for better results in robustness.
2.3 “An Image Watermarking Scheme using Threshold Based Secret Sharing” [3].
An idea for authenticating the actual ownership by embedding a share of the secret image invisibly into the host or the original image. Frequency domain Techniques such as DWT and SVD are used for embedding shares into the host image. In frequency domain, compared to the original image, the obtained watermarked image is less distorted which in turn creates an environment that makes the embedded share of secret image unavailable for any kind of misuse. The leftover share of secret image is used to prove the actual ownership.

Future scope: Future scope is more than watermarking technique using robust and improve performance image processing attacks.

2.4 “An Image security using watermarking based on DWT-SVD and Fuzzy Logic” [4]
Author have new concept of developing new image watermarking. It uses the Discrete Wavelet Transform and then develops a DWT, SVD approach. Even DWT have wide range of functionality but when SVD is combined with it will enhance the robustness of extracted image.

Future scope: Future work on proposed scheme can be done to resist against Steganalysis. Steganalysis is a method To detect whether content is being hidden with some information or not i.e. it is a steganography one or not. As watermarking is similar to steganography and also some algorithms have been developed to resist against steganalysis. But the proposed scheme is not being tested whether it is resisted against steganalysis or not.

2.5 “Robust Digital Image watermarking using DWT+SVD approach” [5]
Author have presented by proposed watermarking technique for color images. The proposed technique uses a unique combination of HL sub-band of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The singular matrices obtained by applying SVD to the DWT applied watermark image, are added to the singular matrices obtained by applying SVD to the DWT applied host image, in proper proportion. The quality of the watermarked image is estimated in terms of the Peak Signal to Noise Ratio (PSNR) and correlation coefficients.

Future scope: Future work can be to embed more information into an image with simultaneously preserving the original image quality. This work is in progress.

2.6 “A Robust Encryption and Digital Watermarking Scheme for Dicom Images Using Quaternion and DWT-SVD” [6]
Authors have consumed substantial processing time for the medical images. A new lossless encryption technique using quaternion can be adopted which reduces the processing time enormously. The quaternion technique is implemented using counter mode of encryption and modular arithmetic operations. The security of the medical image transmission can even be enhanced by incorporating digital watermarking which serves as an authentication of the sender and also reduces the difficulty in maintenance of multiple documents. The signature of the patient and the patient data are used as the watermark images and they are embedded in the DICOM image using DWT-SVD (Digital Wavelet Transform- Singular Value Decomposition).

Future scope: Future scope of the patient data can be used as the verification data in times when the documents are confused with one another that are solve are different techniques of digital watermarking.

The authors have used DIW using five level discrete wavelet transform (5DWT)-singular value decomposition (SVD) and stream cipher (SP) encryption with different attacks. Extensive experiments present that proposed watermarking algorithms have high robustness and a good imperceptibility to numerous usual image processing attacks, such as top-hat filtering, Gaussian blurring, Gaussian blur with noise and image adjustment attack. To evaluate the efficiency of the algorithm and the extracted watermark image quality, we used widely known image quality function measurements, such as signal-to-noise ratio (SNR) and root mean square error (RMSE). Results indicate the excellent invisibility of the extracted watermark image (SNR = 38.35dB), as well as exceptional watermark extraction (RMSE = 3.09).

Future scope: Future scope of digital watermarking using DWT SVD using of different parameter using system.
2.8 “Robust RGB Color Image Watermarking Scheme Based on DWT-SVD and Chaotic System”[8]

The Authors have used DWT, SVD and chaotic systems are used. DWT and SVD are separately applied on three color planes (R, G and B) of original color image and watermark image for embedding and extracting processes. DWT and SVD techniques are used in the proposed watermarking scheme to increase the information hiding capacity and perceptual similarity of watermarked image. At the same time, chaotic system is also used in the proposed watermarking method to ensure the security of the watermarking technique by scrambling the watermark image. In the embedding stage, the gray scale watermark information is separately embedded into three color planes of the original color image. On the other hand, in the extracting stage, the watermark information is separately extracted from three color components and the final watermark is obtained by calculating the average of extracted results from three color components.

**Future scope:** Future scope of digital watermarking using DWT SVD using of different parameter and method of RGB color using system.

2.9 “A Modified Blind Image Watermarking Scheme Based on DWT, DCT and SVD domain Using GA to Optimize Robustness” [9]

The authors have used on original host image using Haar wavelet and approximation (LL) sub-band is selected to split it into two sub images. DCT and SVD operations are performed in both sub images using 8x8 block size. Based on pixels values of binary watermark image, singular value of first sub image is modified referring singular value of second sub image to embed watermark. Genetic algorithm (GA) technique is adopted to optimize visual quality and robustness of watermarked image. Peak Signal to Noise Ratio (PSNR) and Normalized Cross correlation (NCC) are computed to evaluate imperceptibility and robustness of the watermarked image. Experimental results obtained confirm that the proposed method is efficient and more robust against different attacks, viz. noise insertion, filtering, JPEG compression, histogram equalization, gamma correction, bit plane removal, image sharpening and cropping attacks.

**Future scope:** In this paper using of GA algorithm techniques but future scope of various classified technique are apply are better result.

---

### Table-3 Table of Comparison

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Title</th>
<th>Method/algorithm</th>
<th>Drawback and future scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A Secure and robust image watermarking system using wavelet domain</td>
<td>DWT, SVD, Attacks</td>
<td>Hybrid of DWT – SVD techniques using better result but future scope of another method are apply to excellence performance.</td>
</tr>
<tr>
<td>2</td>
<td>Genetic Algorithm based optimized Color Image watermarking technique using SVD and DWT</td>
<td>Genetic Algorithm</td>
<td>Future scope of the further application based analysis by using the Noise Correlation as a fitness function to test for better results in robustness.</td>
</tr>
<tr>
<td>3</td>
<td>An Image Watermarking Scheme using Threshold Based Secret Sharing</td>
<td>DWT, SVD, Secret shares</td>
<td>Future scope is more than watermarking technique using robust and improve performance image processing attacks.</td>
</tr>
<tr>
<td>4</td>
<td>Image security using watermarking based on DWT-SVD and Fuzzy Logic</td>
<td>Fuzzy Logic , SVD, DWT</td>
<td>Stegno analysis is a method To detect whether content is being hidden with some information or not i.e. it is a steganography one or not. As watermarking is similar to steganography and also some algorithms have been developed to resist against stegno analysis. But the proposed scheme is not being tested</td>
</tr>
</tbody>
</table>
5. CONCLUSION
In this survey paper we provided a recent research in the watermarking field. In this paper we have offered various characteristics for digital watermarking like basic of watermarking, techniques, applications, attacks that affects watermarking system. Copying photos from the Internet is just a matter of right clicking on a photo and saving it on the computer hence the security and authenticity of the image or data are cracks. The watermark is required to prevent the original images and other documents over the internet.

5. REFERENCES