Digital Color Image Watermarking using DWT and SVD for Data Security

Ayushi Potfode
M.Tech Scholar
Ec(Dc)
Nirt,Rgpv,Bhopal,India

Deepak Kourav
Assi. Professor
Ec(Dc)
Nirt,Rgpv,Bhopal,India

ABSTRACT
Now a day's internet plays a vital role in carrying information from one place to another .This information which is transmitted is digital multimedia which include images audio and also video .Attacking of digital data is very easy and easily monitored by anyone through the internet .Therefore in order to protect these attacks several intellectual rights have been introduced nearly fifty years ago. This results in the evolution of digital watermarking. Watermarking of images can be done in various domains such as spatial domain, frequency domain, and wavelet domain. In watermarking is a technique of embedding a secret message in a cover message. When media is watermarked the secret message is usually a copyright message.

Watermarking does discourages intellectual property theft and help us to prove ownership when such a theft occurs. This survey paper describes digital watermarking in detail and explains theory, techniques and its applications especially to digital libraries. This paper tells about digital image watermarking scheme with blind detection for copyright verification. The binary watermarks are embedded in the wavelet domain of an image using the discrete wavelet package transform (DWPT) and quantization of the selected dominant coefficients. In our algorithm largest value of coefficients is at same blocks of watermark embedding process will be selected during the watermark extraction. Therefore we doing need the original image for watermark extraction process. It is a blind detection technique. It saves time and space for transferring of original image respectively experimental result show that the proposed techniques are robust to Gaussian noise and jpg compression. These propose method is designed robust against these attacks and based on blind detection, Therefore it can be used in copyright verification effectively.

Keywords
Color, wavelet, watermark, DWT.

1. INTRODUCTION
In the internet world the volatile growth of digital technologies, a large number of applications in the field of multimedia communications and multimedia networking have been enabling over the past decade. It's a necessary concern for the authentication and the copyright protection from unauthorized manipulation for digital images, like audio, video data. Digital image watermarking techniques is planned to include some water marks in the field of multimedia data which authenticates the authorized copyright holder which cannot be manipulated or removed without damaging a multimedia data. There is large number of applications in digital watermarking. It has impressive performance it shows transparency, strength, sensitivity, and blind detection in different applications, the two schemes were introduced for water marking which is based on wavelet watermarking technique [1] and the second one technique is based on image-adaptive watermarking. In 1997, X I a et al. the next technique were introduced in watermarking field is multi resolution method for digital images. All the above methods are based on discrete wavelet transform (DWT)[1] ,which insert a pseudorandom codes to huge coefficients at high-frequency band and middle-frequency band of DWT of an image. DWT method is strong for some general image compressions but in DWT watermark detection technique detection is reliant on the noise level of an image. Hsu et al. Proposed a method which is based on multi resolution for converting digital watermarks into digital images. Ju et al. Proposed a method for digital image watermarking which is a combination of discrete wavelet transform (DWT) and the independent components analysis (ICA). Inoue et al. introduce a watermarking method by making a group of wavelet coefficients into insignificant or significant coefficients by using zero or a tree and after that embedding a watermark in the place of insignificant coefficients or in the place of the threshold significant coefficients. Hu et al. Proposed a watermarking which used pixel-based scaling method. For the pixel-method the scaling factor were adaptively determined by the luminance effect and the local spatial characteristics. Taskovski et al. offered low resolution [9] content based watermarking method. In the process embedding, the watermark is set in the lowest resolution of the three-level wavelet decomposition incorporated with a visual modeling of the local image characteristics. Wei et al. proposed a technique which is based on perceptually watermarking technique for an image. The watermark is set in the wavelet coefficients and in its amplitudes which are controlled by wavelet coefficients so that the watermark noise does not exceed they just-noticeable distinction of each wavelet coefficient. Barni et al. introduced a watermarking algorithm [5], based on masking of watermark according to the characteristics of human visual system (HVS). Kundur et al. And Tuetal. Both were presented a watermarking approach named as Fragile watermarking approach which embeds a watermark in to the discrete wavelet domain of an image or an audio by quantizing the consequent coefficients. Though, the performance of compression is unknown for their approaches like JPEG and they uses less adaptive discrete wavelet transform (DWT).

2. METHOD
There are several methods were proposed in digital watermarking field.

2.1 Digital Watermarking
This is a technique, which allows an individual to include hidden copyright notice or an any other messages for verification to the digital media. In this case the group of bits is messages which describe the information about the signal

or for the author too. Watermarking is the process which is defined for embedding of unremarkable marks or for labels which represent the bits in the digital content. In the message the embedded marks are generally hidden but it can be detected or extracted from the image.

2.2 TYPES of WATERMARKS

2.2.1 Visible Watermark

In these watermark the signal get completely changed which means the output signal were differ from the original signal.

2.2.2 Invisible Watermark

In these watermark signal does not change completely some minor variations were present in the output signal.

In our paper we proposed a watermarking technique which is based on DWT

2.2.3 Wavelet watermarking techniques

Wavelet domain is another possible field for watermark embedding [2]. Wavelet is a great tool in an image processing area which is widely used for image compression. We represent an image in various area by using 2d wavelet transform. This image is divided in to four different bands LL, HH, LH, HL these bands provided an information about the image.

The DWT separates an image into a lower resolution (LL), horizontal resolution (HL), vertical resolution (LH) and in also diagonal resolution (HH). The separation process can be repeated to compute multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform [1] shown below in figure1

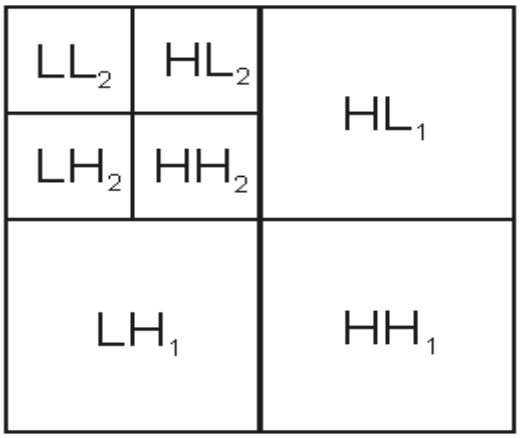

Figure:1 2Scale 2-Dimensional Discrete Wavelet Transform

Discreet wavelet transform has many advantages one of its is that it assumed more accurate model of HVS as compared to FFT or DCT. These methods also use watermarks of higher power in the region where HVS is less sensitive. In this region watermark embedding [2] allows to raise the strength of our watermark, with no additional impact on image quality. It is one of the simplest techniques which use a similar embedding technique to that which used in the DCT, the embedding of a CDMA sequence in the detail bands according to the equation shown below.

Embedding of a CDMA Watermark in the Wavelet Domain.

Where Wi denotes the coefficient of the transformed image, xi is the bit of the watermark to be embedded, and a scaling factor. To identify the watermark we make the pseudo-random sequence as same we used in CDMA generation and its determination with its correlation with the help of two transformed bands. If the correlation exceeds some threshold T, the watermark is to be detected.

2.3 Discrete Wavelet Packet Transform

It is simply an extension to DWT which provides multi resolution.

It can be achieved by increasing level of decomposition in dwt domain. Wavelets are powerful tool in image processing used extensively for image compression .the 2d wavelet transform [1] is used to represent image in various resolutions. The

$$I_{W_{x,y}} = \begin{cases} W_i + \alpha |W_i| x_i, & u, v \in HL, LH \\ W_i & u, v \epsilon\ LL, HH \end{cases}$$

image is decomposed into four bands LL, LH, HL, HH which give description of the image in these resolutions [4]. 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. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in figure

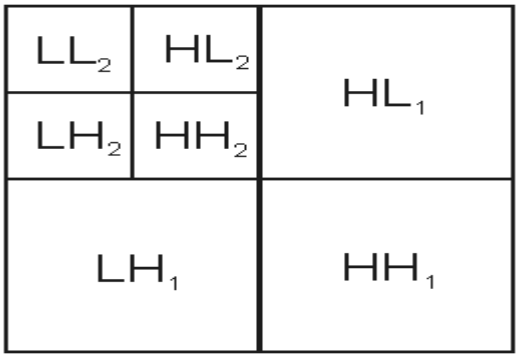

Figure2: 2Scale 2-Dimensional Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, and HH). Embedding [2] watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality

3. PROPOSED METHOD

In the digital image watermarking we proposed a method, in which the watermark is positioned in discrete wavelet packet domain [1]; in these both have a spatial information and a frequency information. By the help of discrete wavelet domain characteristic, the different modification like compression of JPEG and the adding of Gaussian noise will be detect more probable. This proposed method is specially designed for robust against all these attacks it is based on blind detection. As a result, these proposed method more effectively used for copyright verification.

In digital image watermarking a watermark is a familiar image or a pattern in the paper it becomes lighter when it is seen by help of transparent light. In the process of digital watermarking the information is embedding in another object or signal[2]. Watermarking is a process which is more

commonly used since an earlier time mainly it will used in the currency notes or in the cheques. In the digital media digital watermarking technique is used for the protection of author's right on digital documents. The two terms which is linked with watermarking but it differ from watermarking are steganography and cryptography [7]. Steganography is that art which is used for the purpose of writing the hidden messages. Cryptography is used for the study of message privacy.

4. STRUCTURE OF A TYPICAL WATERMARKING SYSTEM

All the watermarking system mainly consists at least two different units: first one is watermark embedding [2] unit and second one is watermark detection and extraction unit.

4.1 Watermark Embedding Unit

In embedding unit we passes an unmarked image through a perceptual analysis block which detect number of altered pixels because of this the output result is differ from the original one[2]. It should be noted that the sensitivity of a human eye shows a change in smooth areas and it shows a slightly changes on edges because of high tolerance. After performing this we suppose that a perceptual-mask has been computed, with the help of this mask the hidden information is created and it will spread everywhere on original image. The interleaving which is used in another application and it involves the coding like storage in compact disc is similar to the spreading method. We use compact disc storage to protect our information from the scratch and harsh dust particle. In this case the spreading is mainly used to make sure that the unseen information which survives from cropping of an image. The way of spreading is depend upon secret key, so it is not easy to improve the hidden information if it is not in the form of key. In actuality, a similar method is used in spread spectrum systems like in Code-Division Multiple Access to take out the most wanted information from noise. In an Addition the key will depends on the uncertainty and It can be introduced in the pixel amplitudes form (remember that the perceptual mask impose only an upper limit). As a result, watermark is added to the original image.

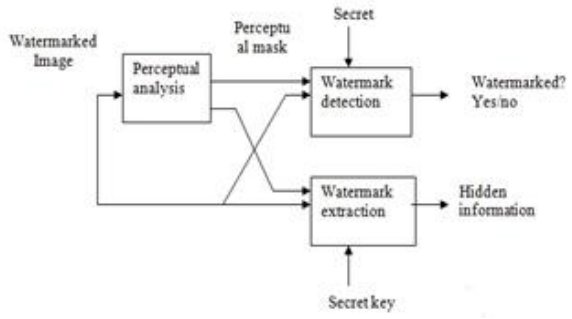

Figure3: Watermark Embedding Unit

4.1.1 Proposed Algorithm for DWPT Watermark Embedding and Extraction

Digital watermarking base on process of embedding is shown in the following figure4

In watermark embedding method the main process is that to embedded random binary string in to the discrete wavelet domain with the help of DWPT during the process of embedding [2]. The owner is the only one who knows this watermark. Also we can do that the watermark is fixed in to the selected coefficient of the selected block by quantizing the coefficient with the particular user defined quantization parameter. During the process of embedding the main steps are as follows:**1.** Discrete wavelet packet transform (DWPT) is applied [1]. A fully wavelet packet structure, same as shown in Figure 2, is used in our proposed method. A m scale, full wavelet packet decomposition is apply thus 2 ^2m blocks show during the embedding process.

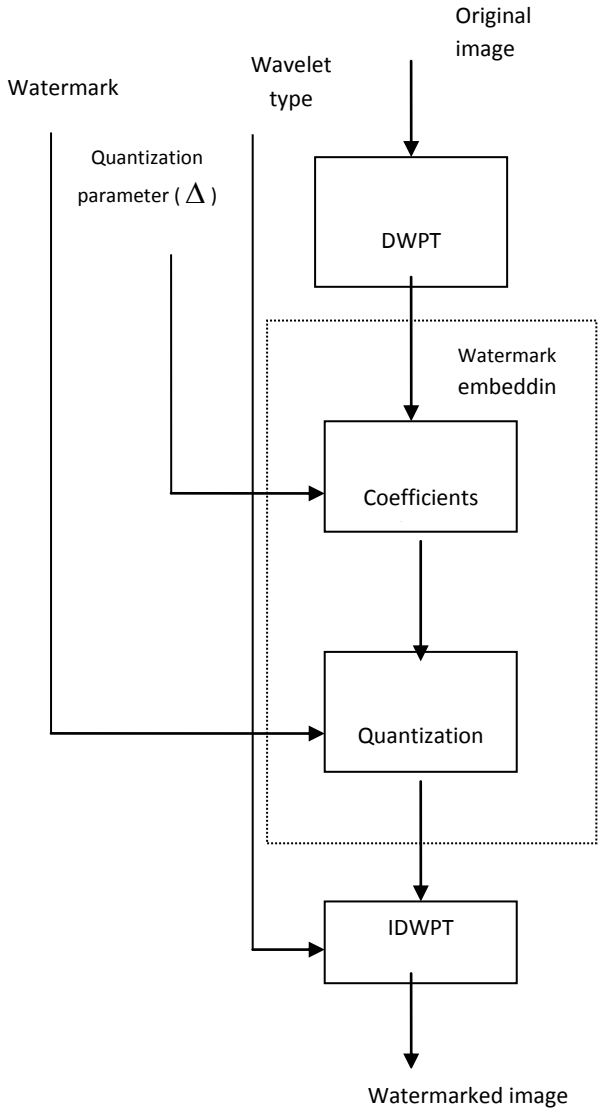

Figure4: Watermark Embedding Procedure

2. The largest absolute value of coefficients will be selected. The amount of the selected coefficients is according to the row size of the selected blocks. In our method, one row of largest absolute value of coefficients will be selected. One block embeds one watermark bit. In this case, all m-level horizontal blocks are selected. The coefficients, which are embedded watermark bits, are selected among these blocks by using the quantization parameter Δ.

3. All the elected coefficients c will be divided by Δ. The mathematical equation is as follows:

$$Q(c) = \begin{cases} 1, & if \ \frac{c}{\Delta} = k \qquad k = k \pm 1, k \pm 3, k \pm 5..... \\ 0, & if \ \frac{c}{\Delta} = k \qquad k = k \pm 2, k \pm 4, k \pm 6..... \end{cases}$$

4. After this we compare every watermark bit mW with the Q(c) of all the selected coefficients in the corresponding block. If the Q(c) = Wm, condition satisfies the coefficient c remains unchanged. If Q(c) ≠ Wm, condition occur the coefficient c = c + Δ.

5. Next we applied a Inverse discrete wavelet packet transform (IDWPT) method after every watermark bits. Finally, a watermarked image appears.

5. RESULT AND SIMULATION

Figure5: Data Image

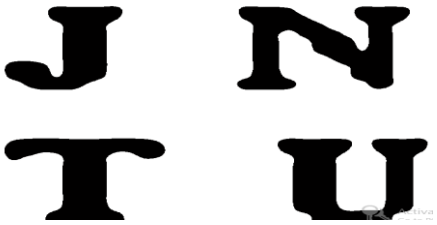

Figure6: Watermark image

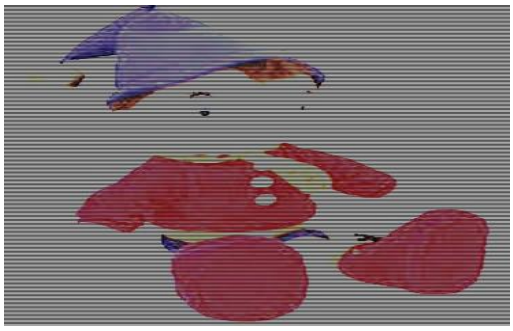

Figure7: Extracted Data Image

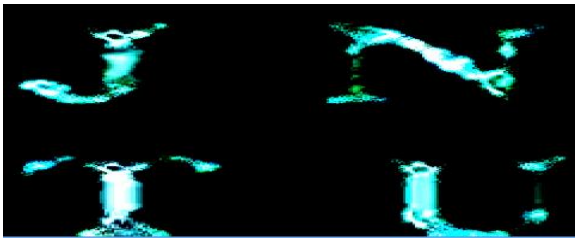

Figure8: Extracted Water Mark

6. CONCLUSIONS

In this paper we discuss about the watermarking technique in which the watermark is set in the wavelet domain with the discrete wavelet packet transform (DWPT) [1] and quantization of the selected dominant coefficients, in this method blind detection of watermark is useful. These method helps in to saves the time and space in the process of transferring an original image and saving an original image. The proposed technique shows an experimental result that technique is robust [3] against JPEG compression and Gaussian noise. The strength of watermark will be effect by the different value of quantization parameter these watermarks is used in the algorithm which is user defined. We need to perform number of experiments for making an decision of suitable value. The capacity is also an important part of digital watermarking will also be developed in our future work.

7. REFERENCES

[1] Qing Liu ,TianshuiGrayscale Image Digital Watermarking Technology Based on Wavelet Analysis 2012 IEEE Symposium on Electrical & Electronics Engineering (EEESYM).

[2] AnamitraMakur, Nikhil Narayan S.”Tamper-Proof Image Watermarking using Self Embedding” Electrical & ElectronicNanyang Technological University, Singapore, acm-2012.

[3] V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli “Robust Watermarking of Compressed and Encrypted JPEG2000 Images” Member, Ieee Transactions On Multimedia, Vol. 14, No. 3, June 2012.

[4] XiangbinFeng ,Yonghong Chen.Digital Image Watermarking Based on Super-Resolution Image Reconstruction9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012),978-1-4673-0024-7/10, IEEE-2012.

[5] Bin Zhang, Yang Xin, Xin-XinNiu, Kai-Guo Yuan, Hui-Bai Jiang,“A Near Reversible Image Watermarking Algorithm” Proceedings Of The Ninth International Conference On Machine Learning And Cybernetics, Qingdao, 11-14 July 2010.

[6] ME Haroutunian, S.A Tonoyan, "Random coding bound of information hiding E-capacity," Proc. IEEE Symp. International Symposium on Information Theory, IEEE Press,Jun. 2008: 536.

[7] A Menezes, P. Orschot, S. Vanstone. "Handbook of Applied Cryptography," London: CRC Press, pp.454 - 4591996.

[8] D. Johnson, A Menezes, S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," International Journal of Information Security, voL I, pp. 36-63, 200 I.

[9] B. He, "A Digital Watermarkinging Algorithm Based on Radon Transform Invariant Moments and Wavelet Lifting," Computer & Digital Engineering, vol. 39, pp.124-128, 2011.