An Extensive Review on Color Image Watermarking using Transform Techniques

Prince Sharma[1], Prof. Amarjeet Kumar Ghosh[2]

[1]*M.Tech.Scholar,* [2]*Research Guide*

Department of Electronics and Communication Engg., VIST, Bhopal

Abstract- Digital image watermarking has gained a great interest in the last decade among researchers. Having such a great community which provides a continuously growing list of proposed algorithms, it is rapidly finding solutions to its problems. However, still it is a challenging issue to concern. Therefore, more and more people are entering the field to make the watermarking idea useful and reliable for digital world Of these various watermarking algorithms, some outperform others in terms of basic watermarking requirements like robustness, invisibility, processing cost, etc. In spite of a great variety of digital watermarking methods, characteristics of robustness and transparency are the most universal and important for any of them. A degree of robustness of the watermark data defines how immune it is against modifications and/or malicious attacks. Another important characteristic is the perceptual transparency of the watermark. Artifacts introduced through a watermarking process may reduce the commercial value of the watermarked data. In examination, the performances of watermarking algorithms have revived for Colour Image Watermarking based on literature survey.

Keywords- Information Security, Image Watermarking, Digital Image Watermarking, Entropy, SVD, QR.

I. INTRODUCTION

Digital data hiding has received increasing attention from information technology community from 1990's. With popularization on the World Wide Web and ease of data transferring over the Internet, copyright and security concerns have emerged. As computational performance has become cheaper it is nowadays cheaper to copy and distribute digital media than make one. In order to protect digital media from piracy, unauthorized use and other illegal actions, watermarks are used. Most of the demand for watermarking comes from movie, music and picture industries, where piracy is a big concern.

Watermarking is a method used in computer security where identifiers of the signal holder are embedded in the host signal for keeping track where the signal comes or who are the copyright owners. Signal carrying the information before watermark is embedded into is called cover signal or host and the data holding copyright ID is referred as watermark. When some digital media file is received, watermark can be extracted from it and it can provide authentication to digital media and protect the copyright.

Recent advances in multimedia production, delivery and processing have also created new opportunities for the dissemination and illegal consumption of multimedia content. Digital Rights Management (DRM) is the practice of imposing technological restrictions on actions with regards to digital media. The task of DRM is to provide "remote control" and "persistent protection" for digital content. On the other hand, some information about the protected content should be available to everyone, which limits usage of cryptographic tools. Driven by the requirements of DRM, the last two decades have seen the development of new tools to tackle the problems in media security. Secure Media Technologies (SMT) is the concept encompassing a wide range of diverse technological areas including watermarking, steganography, cryptography, biometrics, fingerprinting, network security and digital forensics. Digital Watermarking is one of the most promising, versatile and fast developing areas of SMT.

Digital Watermarking incorporates means of securing the rights of the owner of the digital data, providing authentication of the source or originality of the digital data. The hidden message (watermark) signifies information that can be detected and retrieved by authorized personnel or systems designed for that purpose. Methods of Digital Watermarking can be applied to many types of content such as text, audio, images, video, 3D meshes, software programs and network packets.

There are several algorithms of watermarking; most of them are intended for dealing with grayscale watermarks. Two types of watermarks exist, visible watermarks and invisible ones. In visible mode, as the name implies, it can easily see the watermark, which is usually some visual message or a company logo. Visible watermarks should be protected against removal by unauthorized parties. At the same time the watermarks have to resist falsification, meaning that, since it is relatively easy to insert this type of watermark into an image, to provide a method to insure that the watermark was inserted by the owner of the image. In invisible mode the watermarked image is perceptually identical to the original one. The watermark in such an image, depending on the embedding procedure, can be extracted using a special algorithm along with additional data (key image). Fig. 1.1 shows stages involved in digital image watermarking algorithm.

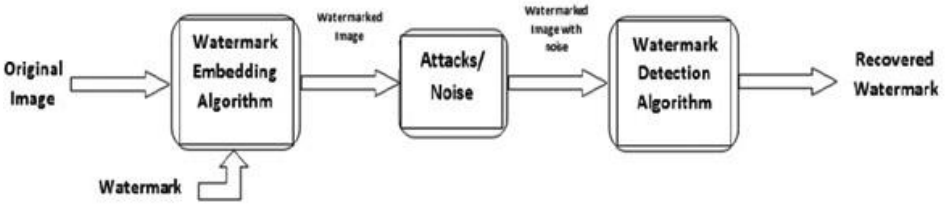

Fig. 1.1 digital image water marking algorithm steps.

II. DISCRETE WAVELET TRANSFORM

Discrete wavelet transform is a method for transforming a digital image by decomposing it into a set of frequency channels. DWT is a time-scale representation of digital signal. It is obtained with digital filtering techniques and it is calculated by successive high-pass and low- pass filtering of the discrete time-domain signal. Graphical representation of DWT is presented in Fig. 2.1.

There are various filters available. However, the most commonly used are Haar Wavelet Filter, Daubechies Bi-Orthogonal Filters and Daubechies Orthogonal Filters. When the input sequence is constant, decomposition in the Haar basis eliminates high frequency terms, hence Haar function is used when images have high contrast of black and white. Haar filter is a special case of Daubechies filter family, it is Daubechies filter of order 1. Daubechies filter construction is based on calculating the frequency response function for the filter coefficients fulfilling moment and orthogonality conditions. Orthogonality and asymmetry are the main features of Daubechies family. Four bands of data, low- frequency band (LL), vertical mid-frequency band (LH), horizontal mid-frequency band (HL) and high-frequency band (HH) are produced in 1-level 2-dimensional DWT. In n-level 2- dimestional DWT, the LL subband is subject of being decomposed into further subband images by applying DWT n-1 times. Due to multi-resolution characteristics, watermark can be embedded into each of those bands. Generally watermark is added into LL because it is more robust against attacks. Modifying HH band is not reducing imperceptibility so much that human eye can detect it, but the robustness is compromised.

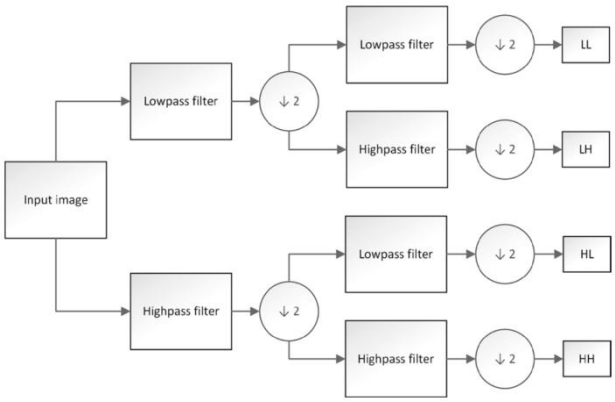

Fig. 2.1 Graphical representation of DWT.

DWT has many good characteristics. Input image is decomposed into three spatial directions, namely, horizontal, vertical and diagonal in wavelet transform. That's why wavelets reflect more precisely anisotropic properties of the human visual system. Using simple filter convolution, wavelet transform can be easily implemented and it is computationally efficient. In the lower resolution, watermark detection is also computationally effective, since there are few frequency bands involved at every successive resolution level. High resolution subbands can be used to detect edges and texture patterns in an image.

III. PRIOR WORK

SR. NO.	TITLE	AUTHORS	YEAR	APPROACH
1	Colour image watermarking based on wavelet and QR decomposition,	P. Rasti, G. Anbarjafari and H. Demirel,	2017	A new image watermarking algorithm on colour images is proposed
2	A novel non-blind watermarking scheme for color image using PCA transform and histogram matching technique	A. Saboori and S. A. Hosseini,	2016	A novel method is proposed for color image watermarking using PCA transform and histogram matching technique
3	Comparison of hybrid watermarking technique on different color spaces	N. Fatima and D. J. Tuptewar,	2016	This examination gives comparative study of digital watermarking technology based on DWT and SVD on various color spaces

4	A robust color image watermark scheme using kinoform	G. Yang, C. Zhao and H. Xie,	2015	A robust color image watermark scheme using kinoform is proposed
5	Color image watermarking in YUV color space based on combination of DCT and PCA,	A. Saboori and S. A. Hosseini,	2015	A new method is proposed using a combination of the DCT and PCA transform in order to use the low-frequency band for the color image in YUV color space
6	Reliable RGB color image watermarking using DWT and SVD,	R. Islam and J. Kim,	2014	A reliable RGB color image watermarking which uses discrete wavelet transform (DWT) and singular value decomposition (SVD)
7	Robust Color Image Watermarking Approach Based on Shape-Specific Points,	C. Y. Yang and W. F. Wang,	2014	a watermarking scheme with high perceived quality for color images by using the Euclidean distance of radius-weighted mean (RWM) and centroid.
8	A New Watermarking Algorithm for Color Satellite Images Using Color Logos and Hash Functions	A. Kunhu and H. Al-Ahmad,	2013	a new robust and fragile watermarking algorithm which embeds 3bit index map of color logo watermark in the frequency domain

P. Rasti, G. Anbarjafari and H. Demirel, [1] In this work, a new image watermarking algorithm on colour images is proposed. The proposed algorithm divides a cover image into three colour bands of red, green and blue. Then the following tasks are done on all three channels separately. First, Each colour band is divided into patches of small sizes then the entropy of each patch is calculated. At this step a threshold is found based on the average entropy of all patches and following is applied to all patches which have entropy lower than the threshold. A wavelet representation of each patch is given by applying a discrete wavelet transform. Then Singular value decomposition, orthogonal-triangular decomposition, and a chirp z-transform are used to embed a watermark on the cover image. Several signal processing attacks are applied on watermarked images in order to robustness of the algorithm. The Proposed algorithm is compared with one conventional and two state-of-the-art algorithms. Experimental results show superiority of the proposed algorithm compare with other algorithm in the area of image watermarking.

A. Saboori and S. A. Hosseini,[2] In this examination, a novel method is proposed for color image watermarking using PCA transform and histogram matching technique. First the color cover image is transformed into YUV from RGB space. Next, the luminance component(Y) is divided into non-overlapping blocks. Then, the values of each block are placed in the matrix data (X) and PCA transform will be applied to it. Finally, the watermark (grayscale image) is embedded into the first component of the PCA after histogram matching to it. Also the proposed method is compared to other methods in spatial domain. Our method is robust and increases the capacity of watermarking.

N. Fatima and D. J. Tuptewar, [3] Due to the advancement of digital media, data authentication and security has become a major issue. Digital watermarking comes as a solution to it. This examination gives comparative study of digital watermarking technology based on DWT and SVD on various color spaces. The same technique is applied on various color spaces like RGB, YUV and YCbCr in case of color image. The quality of watermarked image is measured using PSNR and the quality of extracted watermark is measured using Pearson's correlation coefficient. It was observed that the quality of watermarked image is acceptable. Robustness of the algorithm was tested for different attacks. It was observed that the color space YCbCr gave the best results among the three color spaces.

G. Yang, C. Zhao and H. Xie, [4] A robust color image watermark scheme using kinoform is proposed. The kinoform has relatively less information than regular computer-generated hologram (CGH) as a watermark image embedded in a color Lena. The kinoform is transformed into a non-cascade iterative encrypted kinoform watermark with non-cascade phase retrieve algorithm and random fractional Fourier transform. This kinoform watermark is embedded in the color cover image, which can be extracted with the only right phase key and right fractional order, and reconstructed to represent original watermark image. In color image, our experimental results have been shown in high security, good imperceptibly, and robustness to resist attacks, such as noise, compression, cropping and so on.

A. Saboori and S. A. Hosseini,[5] In the color image watermarking in DCT domain, the watermark bits are inserted into a range of DCT coefficients of the cover

image. The watermark embedding into the low-band is not suitable in term of invisibility of the watermark and the quality of the watermarked image. In this examination a new method is proposed using a combination of the DCT and PCA transform in order to use the low-frequency band for the color image in YUV color space. The color image is transformed into YUV from RGB color space and the luminance (Y) component is divided into non-overlapping blocks and the low-band coefficients of each block are placed in the matrix data, the PCA transform will be applied to it. The first component of the PCA (PC1) has the maximum energy concentration, So the watermark is placed within it, because the watermark is more resistant against attacks. Also the our method is compared to other DCT methods. Our method is robust and keeps the quality of the cover image.

R. Islam and J. Kim, [6] This examination proposes a reliable RGB color image watermarking which uses discrete wavelet transform (DWT) and singular value decomposition (SVD) for embedding and extracting watermark. The DWT and SVD applied on the watermark image increase information hiding capacity and perceptual similarity of the watermarked image. In the watermarking embedded stage, the processed watermark information using the proposed method is embedded into three color components (R, G and B) with an optimum watermarking scaling factor (α). In the extraction stage, the resultant watermark is calculated by averaging the three extracted watermarks from R, G and B components. The experimental results show that the proposed method achieves high normalized correlation (NC) of the extracted watermark and high peak signal to noise ratio (PSNR) of the watermarked image after several image processing attacks. In addition, the proposed method outperforms other conventional methods in terms of perceptual similarity, robustness, and detection rate.

C. Y. Yang and W. F. Wang, [7] In this examination, a watermarking scheme with high perceived quality for color images by using the Euclidean distance of radius-weighted mean (RWM) and centroid has reported. Based on spatial domain, the proposed watermarking scheme can effectively embed a secret message in host images. Simulations demonstrate that the marked images generated by the proposed watermarking scheme are tolerant of versatile attacks such as color reduction, compression, cropping, lens-blurring, noise addition, pixel-truncation, and so on. Above all, the extracted watermarks are recognized when the marked images suffered from attacks such as JPEG2000 compression with a high CR attack and large-scale noise-addition attacks.

A. Kunhu and H. Al-Ahmad, [8] This examination deals with a new robust and fragile watermarking algorithm which embeds 3bit index map of color logo watermark in the frequency domain and fragile information in the spatial domain of 24bit satellite color images. The color logo is used for copyright protection and the hash functions are used for checking the authenticity of the satellite image. The new algorithm caused minimal invisible distortion to the images demonstrated by high peak signal to noise ratio and similarity structure index measure values. The new watermarking technique has been successfully tested on a variety of satellite images. The robust watermarking scheme survived many attacks such as JPEG compression, resizing and rotation while the fragile watermark is very sensitive to the slightest modification to any RGB pixel, also it can accurately locate the tampered areas on the satellite color images.

IV. PROBLEM STATEMENT

In Digital Image Watermarking (DIW), the robustness-transparency trade-off depends on several aspects such as: a domain chosen to embed a watermark; a technique used to modulate the coefficients in that domain; a type of attack that might occur; a measure of transparency for the watermarked image. Several domains are traditionally used for DIW. Among them there are spatial as well as basis transform domains where each domain has its advantages under different types of attacks and transparency measures.

Nowadays, a great variety of image processing tools can be applied to editing of watermarked images with the aim of their enhancing or compression. For an embedded watermark, this can be qualified as an attack which might be combined with intentional/unintentional noising (additive or multiplicative in nature). Definitions of transparency and quality for watermarked images are subjective in principle and may differ depending on the application.

Therefore, the quality of the technique is determined using some properties like robustness, transparency and capacity. The watermarking technique is robust, if the watermark is not significantly affected when exposed to various attacks like the compression, scaling, rotation and noises then watermarking scheme is robust. The transparency or imperceptibility means after embedding the watermark, the original data should not be distorted. The capacity means the size of watermark which is inserted into original data. More capacity means it can hide large size of information.

- The high robustness of watermark techniques against the various attacks like the compression, noise, cropping, rotation and scaling.
- The high transparency or imperceptibility for watermark image after insertion the watermark image into original image.
- The security of the watermark image using encryption technique (Arnold transformation).

V. CONCLUSION

In this work an extensive survey of literature on colour image watermarking based on wavelet and QR decomposition has presented. In recent years with the fast growth of technology and the increasing use of the internet for data transfer shall provide for the protection of communication systems. Where, the controlling and protecting sensitive or confidential documents and images has become next to impossible. Therefore, the world today is based on the provision of many of the techniques of information security, such as encryption and digital watermarking. Digital watermarking is one of the most influential techniques to detect misappropriated data and ensure copyright protection for the digital content like texts, images, audios and videos from illegal manipulations.

REFERENCES

[1]. P. Rasti, G. Anbarjafari and H. Demirel, "Colour image watermarking based on wavelet and QR decomposition," 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, 2017, pp. 1-4.

[2]. A. Saboori and S. A. Hosseini, "A novel non-blind watermarking scheme for color image using PCA transform and histogram matching technique," 2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Prague, 2016, pp. 1-5.

[3]. N. Fatima and D. J. Tuptewar, "Comparison of hybrid watermarking technique on different color spaces," 2016 Conference on Advances in Signal Processing (CASP), Pune, 2016, pp. 13-17.

[4]. G. Yang, C. Zhao and H. Xie, "A robust color image watermark scheme using kinoform," 2015 IET International Conference on Biomedical Image and Signal Processing (ICBISP 2015), Beijing, 2015, pp. 1-5.

[5]. A. Saboori and S. A. Hosseini, "Color image watermarking in YUV color space based on combination of DCT and PCA," 2015 23rd Iranian Conference on Electrical Engineering, Tehran, 2015, pp. 308-313.

[6]. R. Islam and J. Kim, "Reliable RGB color image watermarking using DWT and SVD," 2014 International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, 2014, pp. 1-4.

[7]. C. Y. Yang and W. F. Wang, "Robust Color Image Watermarking Approach Based on Shape-Specific Points," 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kitakyushu, 2014, pp. 65-68.

[8]. A. Kunhu and H. Al-Ahmad, "A New Watermarking Algorithm for Color Satellite Images Using Color Logos and Hash Functions," 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, 2013, pp. 251-255.

[9]. F. Guerrini, M. Okuda, N. Adami, and R. Leonardi, “High dynamic range image watermarking robust against tone-mapping operators,” Information Forensics and Security, IEEE Transactions on, vol. 6, no. 2, pp. 283–295, 2011.

[10]. X. Xue, M. Okuda, and S. Goto, “μ-law based watermarking for HDR image robust to tone mapping,” 2011.

[11]. H. Park, S. H. Lee, and Y. S. Moon, “Adaptive video watermarking uti- lizing video characteristics in 3d-dct domain,” in Digital Watermarking, pp. 397–406, Springer, 2006.

[12]. E. Elbas¸i, “Robust multimedia watermarking: Hidden markov model ap- proach for video sequences,” Turkish Journal of Electrical Engineering & Computer Sciences, vol. 18, no. 2, pp. 159–170, 2010.