

Robust Watermarking for Color Images using Discrete Wavelet Transform

T. Ravindra

M.Tech, Roll no: 17021D8016

Department of Electronics & Communication Engineering,
UCEK, JNTUK Kakinada, East Godavari, A.P, India

Abstract:- This paper presents a robust blind dual water marking mechanism for digital colour images in which invisible robust watermarks and fragile water marks are embedded in special and frequency domains for copy right protection and authentication. In robust watermarking the water mark is inserted in luminance channel that is y channel and all and the remaining chrominance channels i.e. Cb Cr are concatenated with y channel to form the robust market image and for fragile water mark the water mark is going to be inserted in each of the red channel, green channel and blue channel by least significant bit algorithm so that any modification in the original image is easily visible for the owner of the digital content. The embedded watermark is tested by applying various signal processing attacks such as image noise, image crop, image zoom, image rotate, etc for checking the property of robustness involved in our scheme.

Key Words: Authentication, Copy right protection, discrete wavelet transform (DWT), least significant bit (LSB), water marking, noise parameters.

1. INTRODUCTION

With rapid increased in technology the digitalized material which has been

Transmitted over internet has no protection of ownership and security. So these digitalized materials has been taken by the Unauthorized users which losses the ownership of the original author so for this purpose digital water marking has become a relatively focus technique aimed at providing a reliable way to authenticate at images and protect copyright protection. The main purpose of robust water marking in is to protect the ownership of host images by embedding the water mark using discrete wavelet transform of original image and placing a water mark in sub bands of original water mark without disturbing the quality of original image i.e cover image. These operations are carried out in frequency domain or temporal domain so that all features of an image i.e. horizontal features, vertical features and diagonal features are easily extracted without any disturbance. Robustness is one of the major concern in which the extracted water mark should be robust enough so that any signal processing attacks done by the unauthorized users must

be negligible i.e holding the property of robustness however for the sack of increasing robustness of water marked image, the previous robust water marking techniques of an alter the significant areas of post image which can cause serious distortion of the quality of water mark image. This distraction may help the malicious attackers identify which data are valuable allowing them to perform cryptanalysis and acquire the confidential data therefore we have to develop a robust water marking scheme that can deliver outstanding robustness while maintaining good visual quality of water marked images. On the other hand the fragile water mark embedded in the original cover image is included in each of the highly correlated channels i.e red channel, green channel; blue channel is easily identifiable to the author if any hacker has made a attack. Previously the watermarking is applicable to only gray scale images which lies in the range of 0 to 255 pixels values but the technology has increased to processing and transmission of watermarked colour images in information oriented society. The discrete wavelet transform is used to represents the signal in more redundant form and can keep a track of continuous time and frequency this is similar to Fourier analysis and widely used in digital signal processing and image compression it can recover week signals from noise for certain classes of signals and images wavelet analysis provide more precise information about signal data and other techniques.

2. WATERMARK EMBEDDING

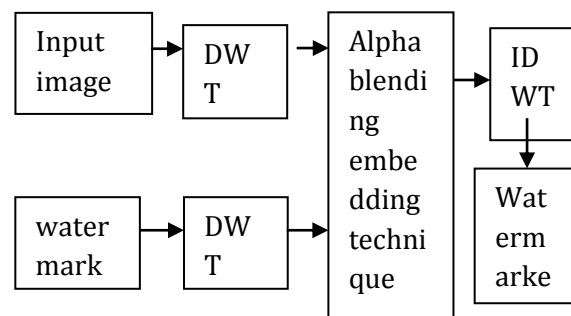


Fig-1: Watermark embedding procedure.

3. WATERMARK EXTRACTION

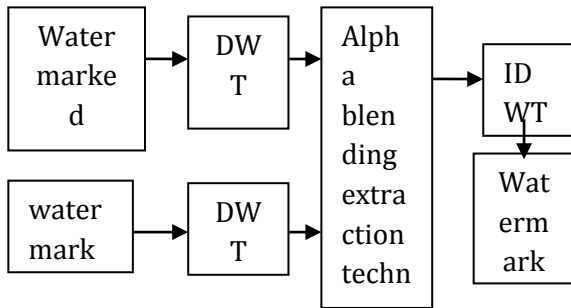


Fig-2: Watermark extracting procedure.

4. ROBUST WATERMARK

The water marks which are detectable even after some image processing operations such as image scaling, bending, cropping, rotating, zooming, adding of noise etc has been performed on water marked image are called robust water marks.

The original cover image i.e colour image Lena of 512*512 images is first divided into YCbCr colour space which consist of luminance channel y and chrominance channel chroma-blue and chroma-red channels. Luminance refers to brightness and chrominance refers to colour of an image. YCbCr colour space is again divided individually into Y,Cb, Cr channels and now we have to consider the y channel and apply doubiches wavelet transform on it which gives rise to sub bands of LL, HL, LH, HH, where, LL represents approximate part of input image LH extracts horizontal features of an image HL represents vertical features of image and HH extracts the diagonal features of an image. Now the LL band is divided by luminance quantization table and the resultant Q-LL band is placed in HH sub band so that any attacks on the image cannot affect the water mark placed in HH sub band. Now the resultant water mark is added after one level DWT to the Q-LL and replaced as water marked Q-LL i.e WQ-LL. Now the inversed DWT is applied to the sub bands finally concatenating the Y' CbCr channels forming the original colour image with robust water marked image.

5. FRAGILE WATERMARK

A digital water mark is called fragile if it is fails to be detectable after slightest modification a fragile water mark is destroyed if anybody attempts to tamper with object in which it is embedded i.e the modifications to original work are easily noticeable.

The robust water marked image is again divided into each of the highly correlated red channel, green channel, blue

channel and fragile water mark is embedded into each of the channels by least significant bit substitution scheme and ternary modulation property the fragile watermarked bit scheme is represented by W_F and the inserted water mark is represented by W'_F now these three channels R',G',B' are concatenated to finally form the fragile water marked image which is consisting of robust water mark image finally forming blind dual marked image of colour images.

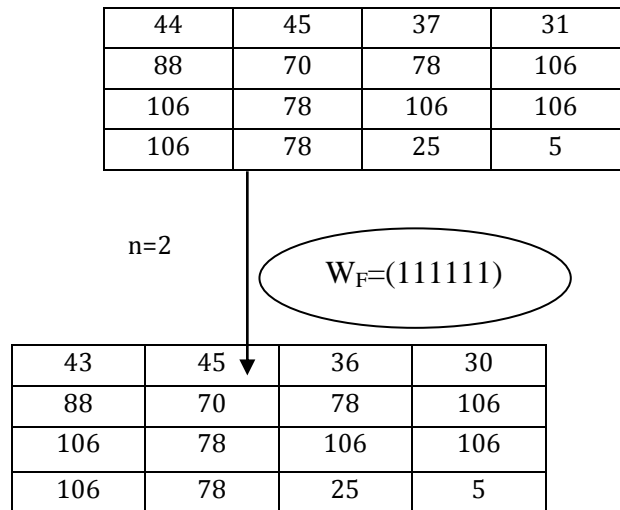


Fig-3: Example of embedding fragile water mark.

Extraction of blind dual watermark i.e robust water mark and fragile watermark is the reverse process of embedding water mark after the extraction of robust water mark bits have been extracted from the water mark image the owner of the image can be identified. The extraction of robust water mark is a blind i.e it doesn't required the original image or ant information regarding water mark, now for fragile water mark the W_F and W'_F bit streams are compared with each of the RGB channels and if any difference in pixels is observed they are marked as dark colour so therefore the integrity of an image can be detected and tampered area can be located accurately.

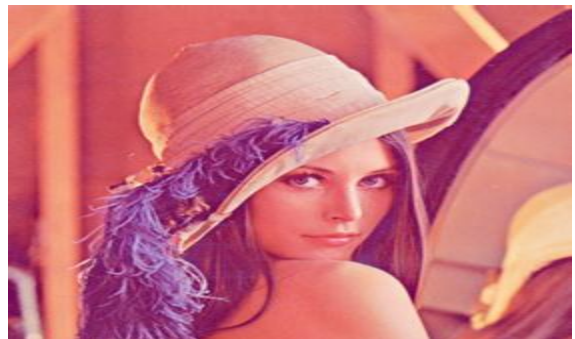


Fig-4: Dual watermark.

6. DUAL KEY MECHANISM

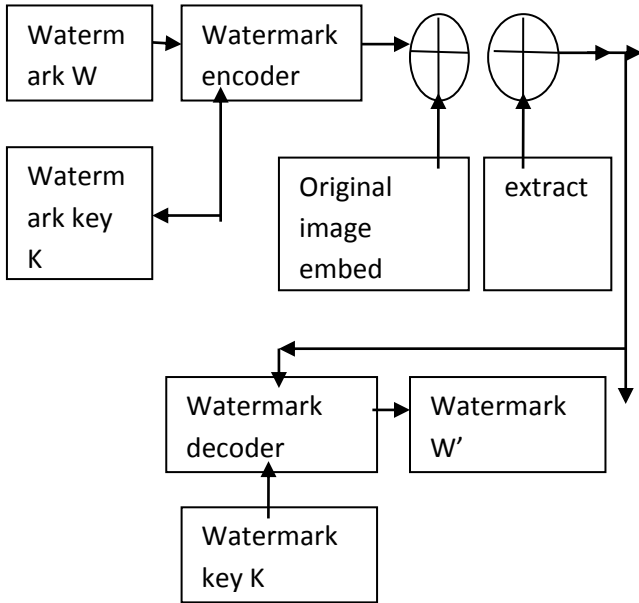


Fig-5: Dual key mechanism insertion.

Now we are going to propose a dual key water mark embedding and extractions scheme which is composed of authentication centre and a secret key it solves the problems of water mark in interpretation attack. The general robust blind water marking system is embedded and extracted of the water mark information under the control of single key K.

The design scheme of dual secret key digital water mark mainly includes the generation of secret key and embedding extraction of water mark which is based on one dimensional discrete wavelet transform. The water mark W and the original image I are used as input to the system and the extracted water mark W' is used as output of the system if $W=W'$ the system is considered as strong anti jamming which has strong robustness; if W and W' has the greater difference the description of the robustness of the system is poor. The transmitter key should be matched with a receiver key so that it displays the input cover image and the water mark inserted in it

7. PERFORMANCE PARAMETERS & RESULTS

The peak signal noise ratio PSNR and the structural symmetry SSIM are they performance parameters used to measure the quality of the water marked image relatively with the embedded water mark strength K.

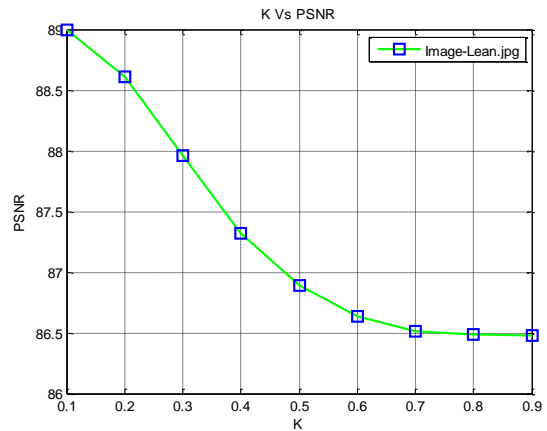


Chart-1: K versus PSNR.

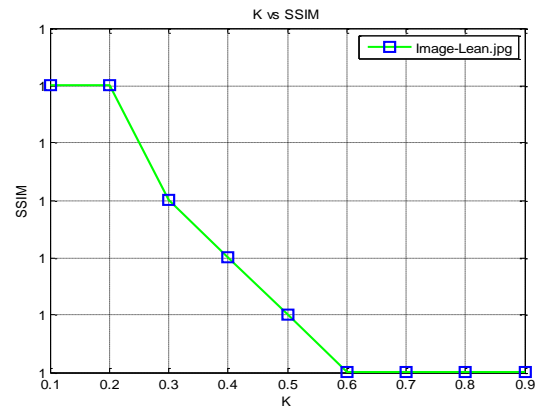


Chart-2: K versus SSIM.

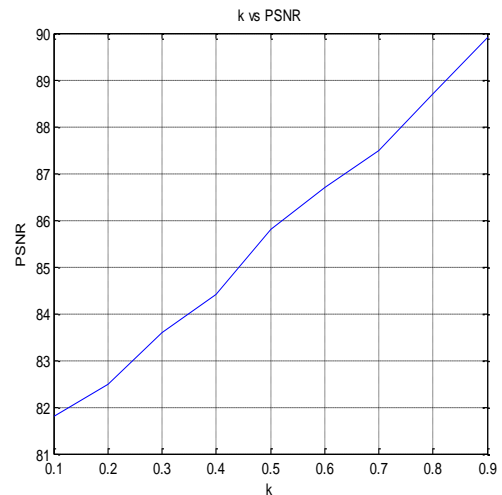


Fig . K versus SSIM

Chart-3: K versus PSNR in noise.

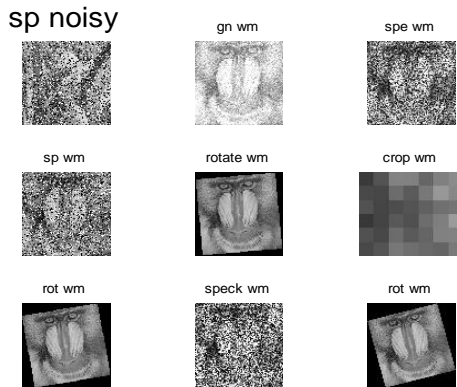


Fig-6: Various attacks on watermark.

8. CONCLUSION

In this paper we have proposed a robust blind dual watermarking using double key authentication in which the robust and fragile water mark are embedded in frequency and special domains to protect the authentication of the images and copy right protection. The experimental results PSNR, SSIM shows that the proposed water marking mechanism can with stand various signal processing attacks such as zooming, cropping, rotating, noisy etc and provides the robustness of the watermark of the system. And dual key provides the further safety of the system when compared to the other mechanisms.

REFERENCES

- [1] M. Yeung, F. Mintzer, "An invisible watermarking technique for image verification," Proceedings of the International Conference on Image Processing, vol. 2, pp. 680-683, 1997.
- [2] C. C. Chang, Y. P. Hsieh, C. H. Lin, "Sharing secrets in stego images with authentication," Pattern Recognition, vol. 41, no. 10, pp. 3130-3137, 2008.
- [3] A. Khan, S. A. Malik, "A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection," Information Sciences, vol. 256, pp. 162-183, 2014.
- [4] W. J. Chen, C. C. Chang, T. H. Ngan Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, pp.3292-3301, 2010.
- [5] 5Q. Su, Y. Niu, H. Zou, X. X. Liu, "A blind dual color images watermarking based on singular value

decomposition," Applied Mathematics and Computation, vol. 219, no. 16, pp. 8455-8466, 2013.

BIOGRAPHY



T. Ravindra received the B.Tech degree from GIET Engineering college , India, in 2016. he is currently a final year M.Tech student of C&SP in Jawaharlal Nehru Technological University Kakinada. his primary research interest is in medical imaging and Image Forensics