International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

A New Color Image Watermarking Frame through Dwt and Alpha Channel

Veereshkumar Swamy
Department of Electronics & communication Engineering
M.U.I.M.T Engineering College Udgir
SRTM University Nanded, India
veereshswamy2@gmail.com

Sandeep Bawage
Department of Electronics & communication Engineering
Veerappanishtty Engineering College Shorpur
Vishveshwarayya Technical University, India
sandeepbawage@gmail.com

Abstract **- The huge success of the Internet allows for the transmission, wide distribution, and access of electronic data in an effortless manner. Content providers are faced with the challenge of how to protect their electronic data. This problem has generated a flurry of recent research activity in the area of digital watermarking of electronic content for copyright protection. Further in order to provide security to multimedia data, the digital watermarking techniques have been applied. So, we have proposed two methods for image watermarking. i.e. One is DWT based method and other is Alpha Channel based method, a watermarking algorithm for color images based on wavelet analysis is proposed and performance of the stego/watermarked image can be evaluated in terms of peak signal to noise ratio (PSNR) while passing through the AWGN channel. The simulation of proposed model is done by using MATLAB. And the experimental results demonstrate that, the proposed framework can assures the security of the watermark image and the watermark image has good invisibility and strong robustness for common signal processing and attacks.**

Index Terms **– Watermarking, DWT, Payload, Alpha channel, AWGN channel.**

I. INTRODUCTION

In recent years, the distribution of works of art, including pictures, music, video and textual documents, has become easier. With the widespread and increasing use of the Internet, digital forms of these media (still images, audio, video, text) are easily accessible. This is clearly advantageous, in that it is easier to market and sell one's works of art. However, this same property threatens copyright protection. Digital documents are easy to copy and distribute, allowing for pirating. There are a number of methods for protecting ownership. One of these is known as digital watermarking.

Digital watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal known as a watermark, can be used later to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work. Watermarks of varying degrees of obtrusiveness are added to presentation media as a guarantee of authenticity, quality, ownership and source. To be effective in its purpose, a watermark should adhere to a few requirements. In particular, it should be robust and transparent. There are a variety of image watermarking techniques, falling into two main categories, depending on in which domain the watermark is constructed.

A digital watermark is a digital signal or pattern inserted into digital content. The digital content could be a still image, an audio clip, a video clip, a text document, or some form of digital data that the creator or owner would like to protect. The main purpose of the watermark is to identify who the owner of the digital data is, but it can also identify the intended recipient. All the information handled on the Internet is provided as digital content. Such digital content can be easily copied in a way that makes the new file indistinguishable from the original. Then the content can be reproduced in large quantities.

Digital watermarks apply a similar method to digital content. Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies.

Currently there are various techniques for embedding digital watermarks. Basically, they all digitally write desired information directly onto images or audio data in such a manner that the images or audio data are not damaged. Embedding a watermark should not result in a significant increase or reduction in the original data.

To be effective in the protection of the ownership of intellectual property, the invisibly watermarked document should satisfy several criteria:

1. The watermark must be difficult or impossible to remove, at least without visibly degrading the original image.
2. The watermark must survive image modifications that are common to typical image-processing applications (e.g. scaling, color requantization, dithering, cropping and image compression).
3. An invisible watermark should be imperceptible so as not to affect the experience of viewing the image.
4. For some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decodability without requiring the recovery of property and subsequent prosecution.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

II. PROPOSED WORK

An image Watermark system consists of two modules: the embedding module and the retrieval module. The embedding module is used at the sender's end where the payload is embedded into the cover image to derive Watermark-image using any one of the Steganographic techniques, whereas the retrieval module is used at the receiver end to extract the payload from the Watermark-image by using inverse Steganographic technique as shown in the Figure 1.1.

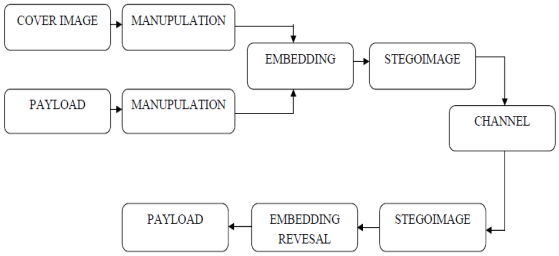

Figure 1.1: Block diagram of Watermark Model

At the transmitter end, cover image and the payload are applied to the Watermark-system encoder to generate Watermark image using certain steganographic techniques. At the receiver end Watermark system decoder extracts the payload by identifying the key which may be used between the transmitter and the receiver to provide security against intelligent attackers.

III PROPOSED ENCODING MODEL

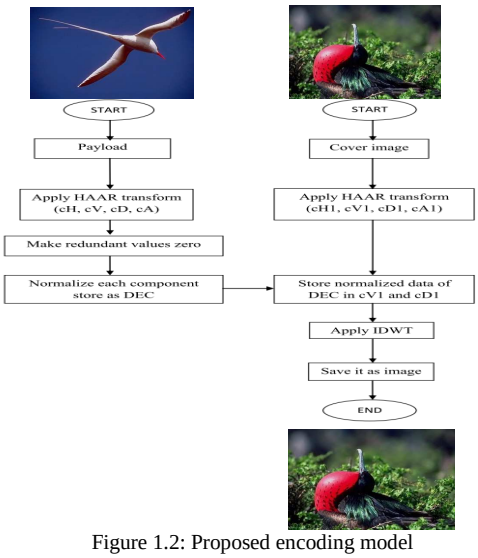

Figure 1.2: Proposed encoding model

A. ENCODING PROCESS (ALGORITHM)

1. Input the image to be hidden (img_hide).
2. Take wavelet transform with HAAR wavelet for img_hide and call the components: cA, cH, cV, cD respectively.
3. Make redundant values in the img_hide as 0.
4. Find the maximum of all the components and normalize each sub image by dividing it with the maximum values.
5. DEC is the data that contains normalized wavelet decomposed values of img_hide
6. Decompose the cover image, into cA1, cV1, cH1, cD1 components using HAAR wavelet.
7. Store the cA size, M1, M2, M3, M4 I first four values of cH1.
8. Store normalized img_hide data dec in cV1 and cD1.
9. Take IDWT of DEC1 which is nothing but idwt (cA1, cH1, cV1, cD1) and call it as S.
10. While saving the image S directly there may be loss during conversion so we normalize S.
11. Convert S to 16 bit format with the value M stored as the first pixel value. Where M=maximum (absolute(S)).
12. Calculate mean square error and calculate PSNR using
PSNR=$10LOG_{10}$ (255^2/mse).

IV DECODING MODEL

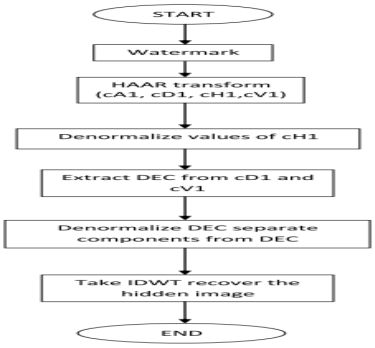

Figure 1.3: Proposed decoding model

A. DECODING PROCESS (ALGORITHM)

1. Read 1st pixel of Alpha channel.
2. Read message length.
3. For i=1: Length.
4. Read bits.
5. Normalize to 8 bit fragment.
6. For each 8 bit fragment, extract decimal.
7. Convert decimal to ASCII.
8. Display message.

V SIMULATION

The performance of the designed system is evaluated through MATLAB simulation. To analyze the performance of BER v/s PSNR and MSG LENGTH v/s BER & PSNR of watermarked image, passing through the AWGN channel.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Considering BER, PSNR as the performance parameters. The details of the signal and system a characteristic have been elaborated in this section.

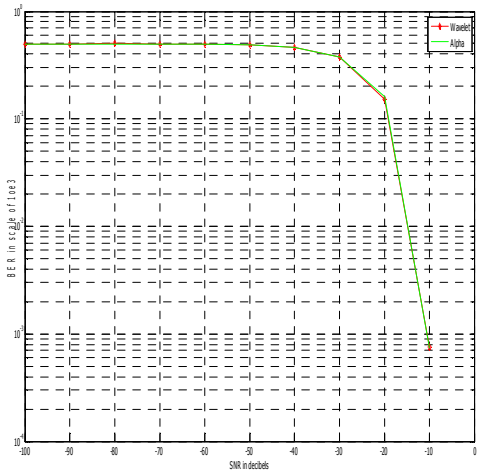

Figure 2.1 SNR v/s BER at -10 db

The graph 2.1 shows that when watermarked images are transmitted over channel, BER improves with improvement in SNR and is significantly good at -10db. Hence it is proved that the quality of performance is independent of channel noise and the performance is in accordance to channel performance for normal image transmission.

Once the image is zoomed, we get the detailed understanding of the behaviour. It is clear that wavelet based techniques are better susceptible to channel noise and hence approaches to optimum BER at relatively lower SNR than Alpha based technique.

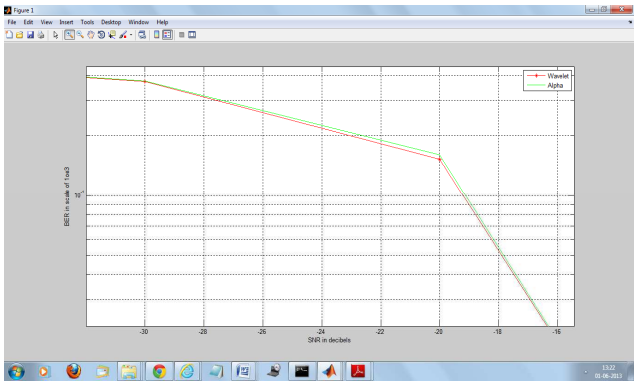

Figure 2.2 SNR v/s BER

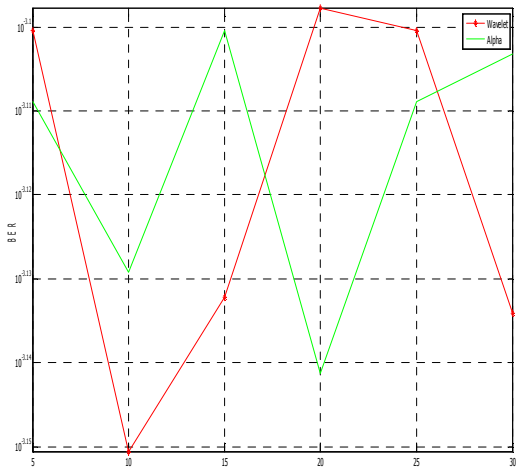

Figure 2.3 MSG LENGHT v/s BER at -10 db

While analyzing the graph (Fig 2.3) of Message length v/s BER, we emphasize that BER is not directly dependent on Message length the way it is dependent on SNR. Because probability of error remains same for a specific SNR irrespective of the length of the message. However when message length increases, probability of Burst error also increases. Under burst error wavelet performs better as wavelet coefficients are real valued in comparison to alpha channel values which are integers. Hence error probability for image watermarked with wavelet is lower than that of alpha based watermarking.

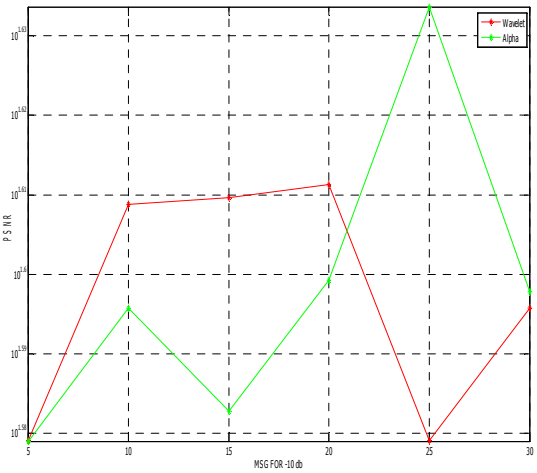

Figure 2.4 MSG LENGHT v/s PSNR at -10 db

While analyzing the graph (Fig 2.4) of Message length v/s PSNR, it is clear that Alpha channel technique clearly outshines its counterpart in image quality. Alpha channel deals with image transparency. Image quality to a large extend is independent of transparency. However as wavelet values are directly incorporated in the main image, they affect the PSNR values more directly.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

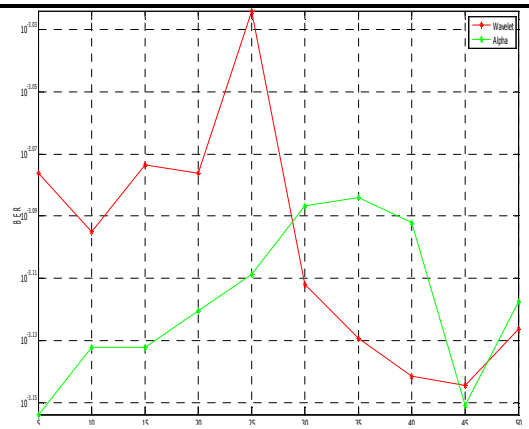

Figure 2.5 PASSWORD LENGTH v/s BER

The figure (2.5) presents that strength of password also has direct impact on the overall performance of the system. With the increase of password strength, BER is expected to increase. However for password length between 30 and 45 the trend is reversed which should be desirable result. This is due to the fact that with increase in data, domain of data gets more adoptive to channel noises. Hence it can be safely said that optimum password length is 30-40 for digital watermarking technique with any of wavelet or alpha channel based watermarking.

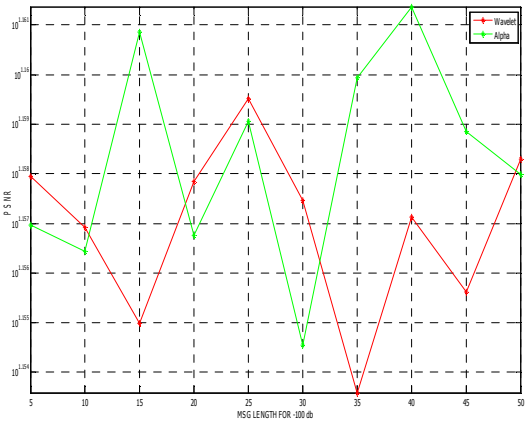

Figure 2.6 PASSWORD LENGTH v/s PSNR

Generally in figure (2.6) with increase of password strength, PSNR of the received image is decreased. However the opposite must be the desired feature from any suitable technique. The trend is observed for Password length between 30-40 which is also justified by BER graph. Hence it can be proved that for Image of size 256x256 and average message size bellow 50, optimal password strength is alphanumeric 30-50 characters long.

VI CONCLUSION

To conclude, we present a case of color image watermarking framework through DWT and Alpha channel transmission over AWGN channel. In first approach of wavelet (Discrete Wavelet Transmission), we can watermark payload (i.e. secret logo or messages) in detail band (i.e. highest frequency coefficient) of the cover image. And in second approach we can embed the message character in alpha channel of png (portable network graphics) image.

Further in order to provide security to the images, we have introduced a concept of image encryption using scan patterns and carrier images. Hence it provides an authenticity and integrity to the images and alpha channel is used for transparency of the images.

Thus we can safely say that either of wavelet based watermarking or alpha channel based watermarking present's identical characteristics and are both adaptive to channel noise. Alpha channel presents better image quality in terms of PSNR where as wavelet based technique produces better BER property. Both the techniques work best for average password length of 30-40. Both the techniques are independent of the message length (for average size messages). However wavelet based technique is better suited for very high message length. In addition, this method gives more capacity and high security to transfer images in communication field.

VII FUTURE CONTRIBUTION

In this paper we focused on data embedding and data extraction from an image using Discrete Wavelet Transform (DWT) algorithm and Alpha channel. And it's hidden the payload in detailed band of cover image. In future we will try out it in audio watermarking in the spatial or frequency domains when the embedding rate is less than the maximal amount.

REFERENCES

[1]. R. Wolfgang and E. 1. Delp, "A watermark for digital images, " Proceedings of IEEE International Conference on Image Processing, Vol. 3, pp.2 I 9-222, 1996.
[2]. Christine T. Podilchuk, "Image-Adaptive Watermarking Using Visual Models.", Proceedings of IEEE Journal on Selected Areas in Communications, Vol. 16, no. 4, May 1998.
[3]. Pradosh Bandyopadhyay, Soumik Das, Shauvik Paul Atal Chaudhuri and Monalisa Banerjee " Color Image Authentication through a Dynamic Fragile Watermarking Framework", @International Conference on Methods and Models in ComputerScience,2009.
[4]. Soumik Das, Pradosh Bandyopadhyay, Prof. Atal Chaudhuri, Dr. Monalisa Banerjee, "An Invisible Color Watermarking Framework for Uncompressed Video Authentication' "©2010 International Journal of Computer Applications (0975 – 8887)Volume 1– No.11.
[5]. Abrar Ahmed Syed & Dr.K.R.Rao "Digital watermarking".
[6]. Panduranga H.T & Naveen Kumar S.K "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images"@Panduranga H.T.et al./(IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 297-300.
[7]. G. Langelaar, I. Setyawan and R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol. 17, pp. 20-43, Sept. 2000.
[8]. H. Inoue,A. Miyazaki and T. Katsura, "An Image Watermarking Method Based on the Wavelet Transform", IEEE Conf. on Image Processing, Vol. 1, pp. 296-300, 1999.
[9]. J. Cummins, P. Diskin,S. Lau and R. Parlett, "Steganography and digital watermarking", School of Computer Science, The University of Birmingham, 2004.

[10]. M. Yeung, B. Yeo and M. Holliman, "Digital watermarks: shedding light on the invisible", IEEE Micro, Vol. 18, pp. 32-41. Nov. 1998.
[11]. X. Jian-hui, W. Li-na and Z. Huan-guo, "Wavelet based denoising attack on image watermarking", Wuhan University Journal of Natural Sciences.
[12]. M. Arnold, M. Schmucker and S. D.Wolthusen. "Techniques & Application of Digital Watermarking and Content Protection", Artech House Publications, Boston, London.