INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 5)
Available online at: www.ijariit.com

Novel approach for image watermarking in YC_BC_R color space using LWT and SVD

Ruchika Vashisth
ruchikavashisth@gmail.com
Matu Ram Institute of Engineering and Management, Rohtak, Haryana

Vijay Nandal
vijay.nandal@yahoo.co.in
Matu Ram Institute of Engineering and Management, Rohtak, Haryana

ABSTRACT

Now a day's with advancement in technology privacy is one of the concern-parameters. There are diverse techniques available to protect our crucial data safe from unauthorized person. Watermarking, cryptographic, steganography are few examples which help us to protect our information. Digital image (DI) authentication under varying transmission and acquisition conditions is very tedious and efficient watermarking is an effective method to rid of this problem. In this research paper, we propose a transform domain approach in YCbCr color space to enhance the performance of a watermarking system, employing the distinguish integration of Discrete Wavelet Transform, Discrete Fourier Transform, and Singular Value Decomposition. DWT stage selectively utilizes the horizontal and vertical detail coefficients of the 2–dimensional DWT of an image. The translation variance problem of the DWT is compensated in the following DFT stage, which also exploits the frequency characteristics of the image. Finally, SVD is used to embed the watermark data. The method gives superior results in terms of enhanced PSNR values and is able to withstand a diverse of image processing attacks for example blur attack and motion attack. In our research work, four types of attacks are used and we can say that image quality is robust against these attacks.

Keywords— *DWT, LWT, SVD, Domain, Fourier Transform, Coefficient, Color space*

1. INTRODUCTION

With the rapid advancement of network topology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identification are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over a communication network to steal information that they want. To deal with the security problems of secret images, we should develop some secure appropriate algorithm by which we can secure our data on the internet. Visual cryptography is a method of encrypting a secret image into shares such that stacks a sufficient number of shares reveal the secret image. We consider the security of shares in visual cryptography and generating more meaningful shares with respect to basic cryptographic approach. Basically, visual cryptography is used for the encryption of visual information like written materials, textual images, and handwritten notes, print and scanned materials etc. in a perfectly secure way so that the decryption can be performed by human visual system [8].

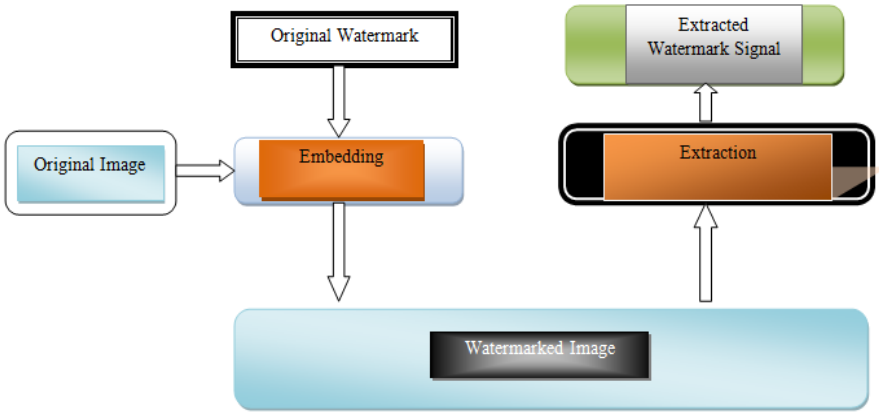

Fig. 1: Watermarking block diagram

Watermarking is the technique of embedding the secret image in a cover image without affecting its perceptual quality so that the secret image can be revealed by some process. Share generation for the visual cryptography can also be done by the concept of

watermarking using some watermarking technique. We can use these watermarked shares for retrieving the hidden information. This effort can generate the meaningful shares rather than some shares having no information. Here our proposed scheme will add the merits of both visual cryptographies as well as watermarking, where we will generate the shares using basic visual cryptography model and then we will watermark those shares using some cover images. The decryption will be the same as in the visual cryptographic model i.e. by the visual system.

2. LITERATURE SURVEY

Image authentication under various transmission conditions is a very challenging task and to solve this problem I must do a robust method for watermarking. In this paper, to enhance the performance of watermarking system we propose Walsh Hadamard Transform domain approach in YCbCr color space using the unique combination of 2–Level Lifting Wavelet Transform and Singular Value Decomposition. Every stage of the system is tested. YCbCr color space is used to make use of its decorrelation property to increase the correlation between the cover and watermarked final image. LWT stage selectively uses the detail coefficients of the 2–dimensional LWT of an image. After applying LWT we apply WHT to find the WHT coefficient and at the final, we apply SVD on each coefficient to get the final watermarked image. Through this method, we find the PSNR value is an increase. So, this method gives the better results in terms of increasing PSNR value and can withstand a variety of image processing attacks [1]. DIW is one of the ways that is resilient to various attacks on the image based digital media where data authentication is done with the aid of embedding a watermark in picture traits. This work incorporates a new approach for DIW using 3level lifting wavelet transform -Walsh Hadamard transform-Singular Value Decomposition in YCbCr color gap. Extensive experiments exhibit that the proposed watermarking algorithm has a good imperceptibility and high robustness to quite a lot of long-established image processing attacks, similar to motion blurring, and usual attack. To evaluate the effectivity of the algorithm and the fine of the extracted watermark image (WI), we used commonly recognized photo pleasant operate measurements, comparable to Peak signal-to-noise ratio (PSNR), executing time for embedding and root mean square error. Effect point out the acceptable invisibility of the removed WI, as good as quality watermark extraction [2]. The digital watermarking technique provides a superior and robust solution for the ownership problem. Considering the following issues in the existing system and the aim is to provide an excellent security to the image, the message is embedded within the image. Watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. Another issue is to use of digital watermark as a contents authentication and tamper proofing. In this paper, it gives reviews of many papers on digital watermarking techniques [3]**.**

3. PLANNING OF WORK/METHODOLOGY

In our research work, YCbCr color space is used for watermarking technique. This paper consists of three different techniques which give us superior result with respect to reference work. The wavelet transform is a time domain localized analysis method. It decomposes the image into the different spatial domain and independent frequencies. When the image is DWT transformed means transformed into frequency domain which is easy to analyze. It is decomposed into four districts namely LL which is a low-frequency district and three high-frequency districts namely LH (Level detail), HL (Upright detail) and HH (Diagonal detail). In this decomposition L stand for low-frequency component and H stand for the high-frequency component. Figure 2 shows the one level DWT decomposition process. But DWT having one disadvantage that it uses of larger wavelet filters produces blurring and also ringing noise near edges in images. LWT overcome the disadvantage of DWT. On another hand, LWT significantly diminishes the processing time and execution becomes faster. SVD is a factorization of a real or complex matrix into three matrices. Consider an m×n real or complex matrix M. Then the SVD is obtained as follows:

$$M = USV^T$$

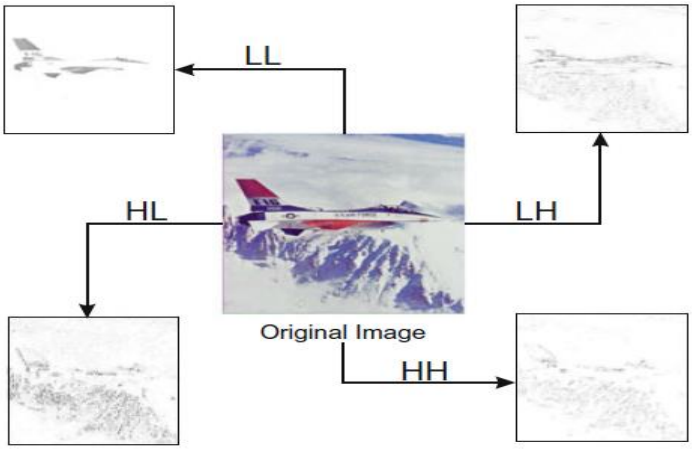

Fig. 2: Decomposition of the image into four components

3.1 Robustness against attacks

(a) Blurring: To evaluate the robustness of the proposed method, several attacks have been implemented in the watermarked image. Blurring is used in pre-processing steps, such as removal of small details from an image. Noise reduction can be accomplished by blurring with a linear filter and also by nonlinear filtering. The simulation results show that secret images have been extracted successfully from the blurred watermarked images.

(b) Motion blurring: The blurring of an image caused by the distance an object moves relative to the amount of camera motion. For computer graphics, this effect needs to be added artificially, either by 3D motion blur that is calculated during rendering or with a 2D motion blur that is applied as a post-process on the already rendered images. The simulation results obtained shows that the secret images have been extracted successfully from the motion blurred watermarked images.

(c) Sharpening: The principal objective of sharpening is to highlight fine details in an image or to enhance detail that has been blurred, either in error or as a natural effect of a particular method of image acquisition. The simulation results show that the secret images have been successfully extracted from the sharpened watermarked image. In this section, the system design with the proposed methodology has been explained. A stepwise methodology of the use of these three techniques – Visual Cryptography, Watermark embedding, and Watermark extraction is explained. The accuracy of the proposed approach is measured by using a descriptive measure such as a peak signal to noise ratio (PSNR).

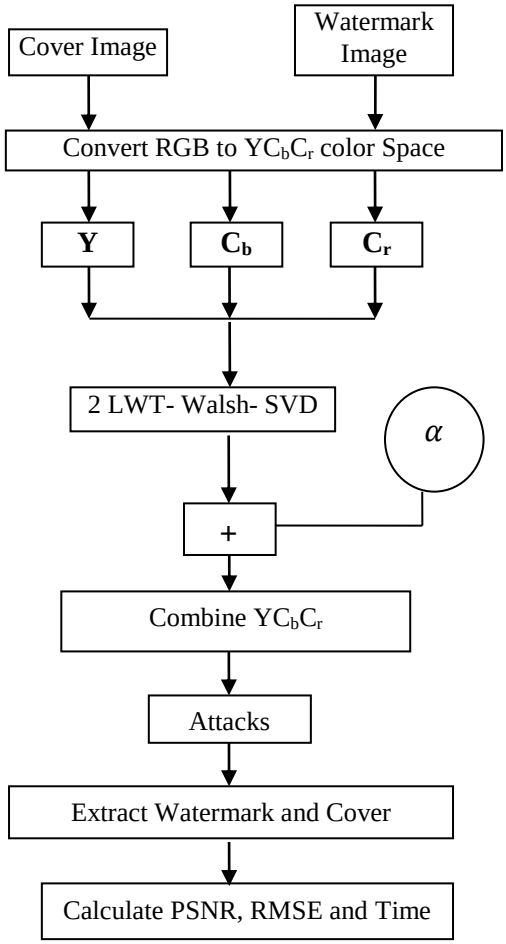

Fig. 3: Flowchart of algorithm

$$MSE = \frac{\sum[f(i,j) - F(i,j)]^2}{N^2}$$

$$PSNR = 20log_{10}\left(\frac{255}{RMSE}\right)$$

4. SOFTWARE USED AND SIMULATION RESULT

4.1 Software

Proposed scheme have developed in MATLAB 2015A tool. The scheme takes as input a secret image and two cover images. It first generates the two shares of the secret image using visual cryptography encryption. After encryption, both shares are watermarked in two cover images using digital watermarking. Then using a watermark extraction algorithm both shares are extracted from the watermarked images and then stacked together to reveal the original secret image. To run this scheme minimum hardware configuration is required with no extra specifications. The experiment was run in Windows 7 on a DELL laptop with Intel i5 2.4 GHz processor. In order to explore the performance of the proposed scheme, MATLAB platform is used and a number of experiments have been performed on different sizes of images, namely Lena, Pepper, Baboon, Barbara, Boat, and Fruit. Two binary images of different sizes have been used to generate the shares.

Fig. 4: Experimental dataset used to calculate PSNR and RMSE

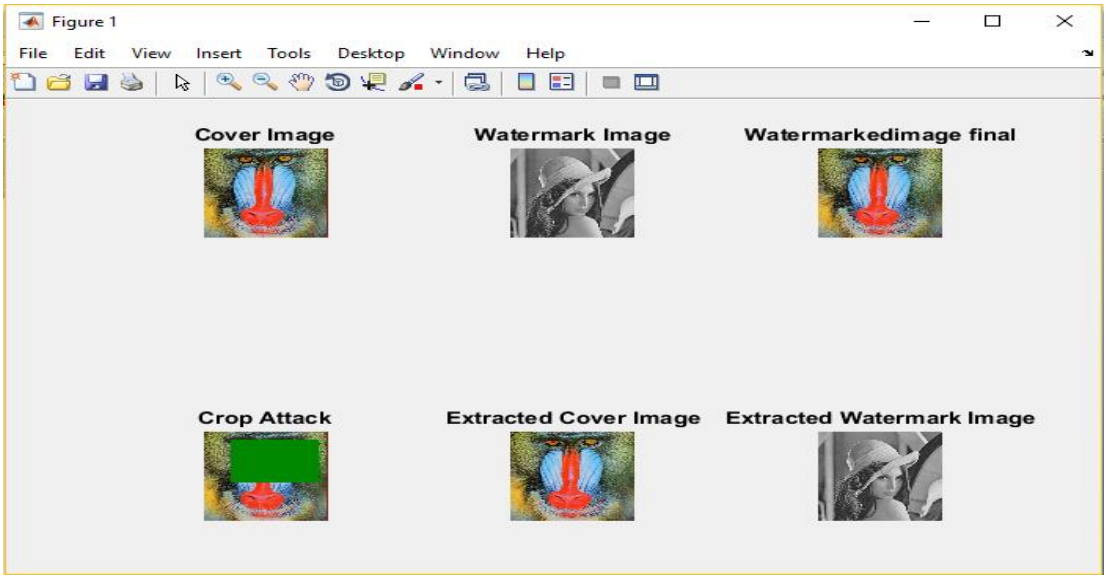

Fig. 5: Watermarked image and effects of crop attack

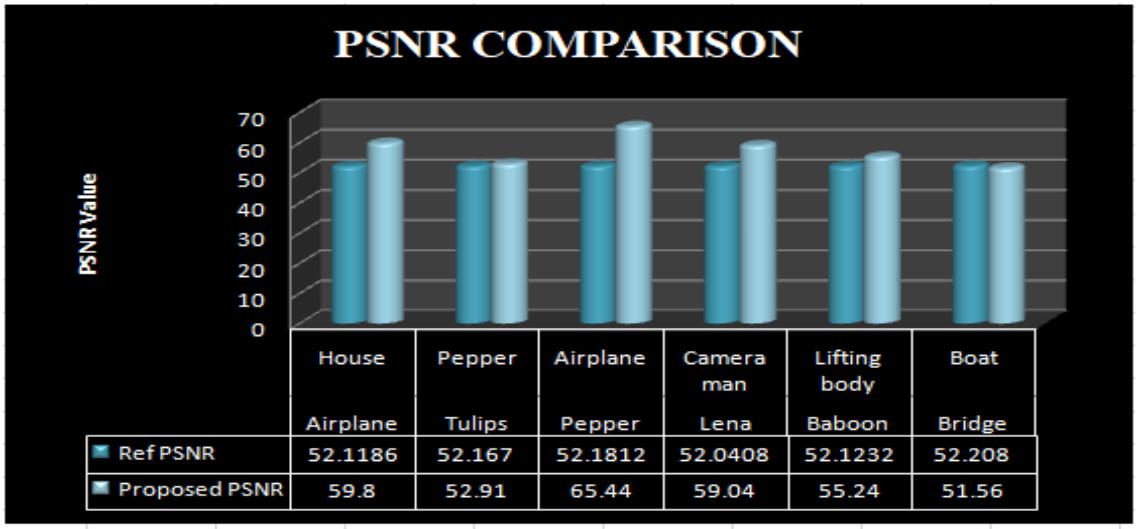

Fig. 6: PSNR comparisons between the reference and proposed technique

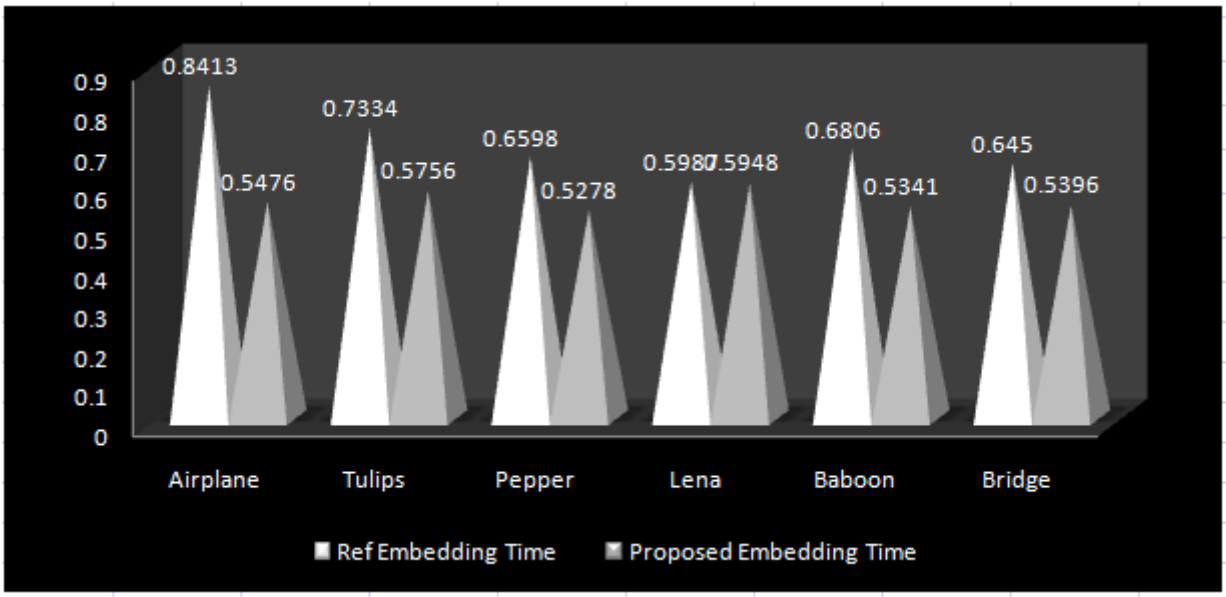

Fig. 7: Time comparisons between the reference and proposed technique

5. CONCLUSION

Various technologies are available which can be used to protect valuable information. In these days privacy becomes the main concern. Nowadays, tremendous improvement of the computerized mixed media revolution and the web authorize individuals to imitate, circulate and store information more effectively. Data or image interchange over open systems requires a standard protocol to give security to the picture, genuineness of the picture proprietorship and image integrity verification. Watermarking provided double security to shares by hiding them in some cover images. Watermarked images are robust against a number of

attacks like blurring, sharpening, cropping and Gaussian etc. The objective of the proposed research is digital image watermarking using LWT and SVD techniques in YCbCr Color Space. LWT is better than DWT due to Wavelet transform is a time domain localized analysis technique. Besides this diverse attack also used in our work and image quality is superior to these attacks (Crop attack, Blur attack). In final analysis proposed work having PSNR value in the range of 52 dB to 65 dB depending upon images but reference work having PSNR value around 52 dB for same images. The major areas of future scope are, we can enhance the visual quality of watermarked images, watermark the secret shares into the color images, and enhance the capacity of watermark so that large images could be watermarked.

6. REFERENCES

[1] Piyush Pandey, Rakesh Kumar Singh, "Novel Digital Image Watermarking Using LWT-WHT-SVD in YCbCr Color Space" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6, June 2017.

[2] Varsha Purohit1 Bhupendra Verma2," A New Approach for Image Watermarking Using 3LWT-Walsh Transform-SVD in YCbCr Color Space " IJSRD - International Journal for Scientific Research & Development| Vol. 5, Issue 02, 2017.

[3] Salma Hussainnaik, 2Farooq Indikar 3Reshma H Husennaik, "Review on Digital Watermarking Images" © 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.

[4] N.Vinay Kumar, Prof.A.Venkat Ramana, DR.C.Sunil Kumar and V.Raghavendra, "An Enhanced invisible Digital Watermarking Method for Image Authentication", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12016-1202.

[5] Mehdi Khalili and Mahsa Nazari, "Non Correlation DWT Based Watermarking Behavior in Different Color Spaces" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[6] Namita Chandrakar1 and Jaspal Bagga2, "Performance Analysis of DWT Based Digital Image Watermarking Using RGB Color Space" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 1, January 2015.

[7] D.Vaishnava, T.S.Subashinib, "Robust and Invisible Image Watermarking in RGB Colorspace using SVD" International Conference on Information and Communication Technologies (ICICT 2014).

[8] Amit Kumar Singh, Mayank Dave and Anand Mohan, "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain" The National Academy of Sciences, pp. 351–358 India 2014, 19 July 2014.

[9] Pravin M. Pithiya and H.L.Desai, "DCT Based Digital Image Watermarking, Dewatermarking & Authentication" International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 3 May 2013.

[10] Dr. H. B. Kekre, Dr. Tanuja Sarode, and Shachi Natu, "Performance Comparison of DCT and Walsh Transforms for Watermarking using DWT-SVD" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013.

[11] Anuradha, Rudresh Pratap Singh, "DWT Based Watermarking Algorithm using Haar Wavelet," International Journal of Electronics and Computer Science Engineering, Vol. 1, No. 1, 2012.

[12] Rahim Ansari, Mrutyunjaya M Devanalamath, K. Manikantan, and S. Ramachandran, "Robust Digital Image Watermarking Algorithm in DWT-DFT-SVD Domain for Color Images" 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India.

