Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Efficient Colour Image Watermarking using Factor Entrenching Method

K.G.S. Venkatesan
Associate Professor, Dept. of CSE
Bharath University, Chennai
Tamil Nadu – 600 073, INDIA

G. Julin Leeya
Department of C.S.E.
Bharath University, Chennai
Tamil Nadu – 600 073, INDIA

G. Dayalin Leena
Teaching Fellow, Dept. of CSE
University College of Engg, **Arni,**
Tamil Nadu, INDIA

Abstract - Digital Imaging has been a boon to mankind in recent years because of its valuable advances especially in the World Wide Web. Even though the advance helps in digital field, there are certain intruders who use these advances maliciously. Lots of digital imaging techniques have been proposed so far to triumph over the intruders. The vital purpose is to afford a competent watermarking technique for image safety where digital image should not be destroyed by any adversary if published over the network. For past few years scientists have turned out their attention towards Discrete Wavelet Transform (DWT), a prevailing technique used to secure digital image watermarking. This technique works by decomposing the host image into various sub-bands and using the decomposed sub-bands for further watermarking purpose leaving the host image harmless. Discrete Wavelet Transform based watermarking schemes are highly robust and defend against most digital image manipulations. A transform named Arnold's Cat Map (ACM) provides secondary security in digital image watermarking. ACM works by shuffling the given image in to unidentified collection of pixels. We use both the above techniques to provide high security in watermarking. Watermarking has been done with a set of images which in turn produced very good performance ratios in terms of Peak Signal to Noise Ratio (PSNR).

Key Words : Digital Imaging, Discrete Wavelet Transform, Arnold's Cat Map, PSNR, Watermarking.

I. INTRODUCTION

Due to the quick spread of Internet facilities all over the world in these modern years, the necessity of digital technology has been evidently amplified. Digital technology includes digital images, digital media, text etc. Since most of the organizations, publishers, artists post their models, images, secrets via internet; security has to be provided to greater extent. Security nowadays has become a question among the users who publish their resources. Security can be of different forms such as detecting the mall practices, blocking the unauthorized users, providing measures to prove the ownership etc. Security system that will handle all the attacks should be developed. Digital Image Processing has paved the way for digital images to be processed and handled. Here images to be published are taken as the input. Using certain developed techniques, transforms or applications those images are protected from malicious attackers.

Steganography is the knack of concealing information inside digital carriers. The information need to be protected is embed or hide within a digital carrier so that the information reaches its destination without any security issues. Watermarking is a small part in steganography. Steganography is used for data encryption where as Watermarking is used for data hiding within a host carrier.

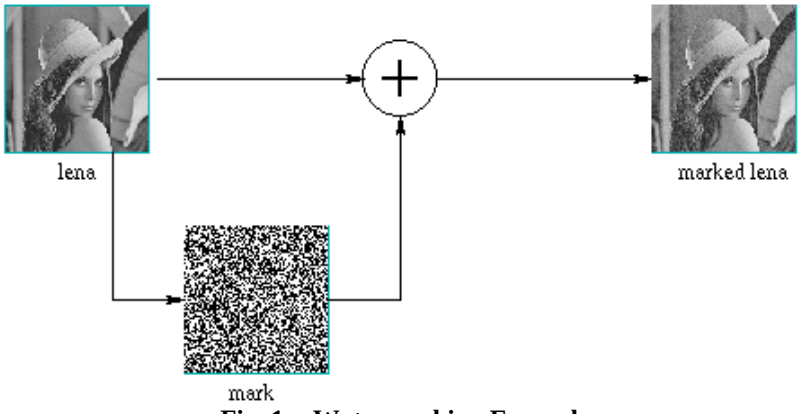

Fig. 1 : Watermarking Example

Watermarking may be either visible or invisible. If only authentication is needed then it is wise to go for visible watermarking but if both authentication and security are needed then better go for invisible watermarking methods. Robustness is a parameter used in watermarking technique. A watermarking technique is robust if and only if the watermarking withstands the general image processing attacks such as rotation, scaling, noise, etc.

A novel chaos primarily based watermarking theme for image authentication and tamper detection is projected . This theme provides each integrity and legitimacy for digital watermarking. Extracting the proper watermark is just potential if somebody has correct keys. Since chaotic maps are sensitive to initial values, they're used as key during this theme. someone with wrong keys won't be ready to forge the watermark. so as to thwart counterfeiting attacks it's essential to interrupt constituent wise freedom, this theme employs chaotic maps to interrupt the corresponding position relation between pixels within the watermarked image and therefore the watermark. Provides hi-fi and is capable of localizing changed regions in watermarked image [1]. Watermark embedding research has been initiated in 1990 [2]. With the redundancy of the medium as design and influence, digital watermarking technology is to use the digital embedding method to hide the watermarking information into the digital products of image, visible and video. Seen from the field of signal process, the watermarking signal being embedded into carrier is as a feeble signal to add into a strong background. As long as the intensity of watermarking is lower than the contrast restriction of human visible system (HVS) or the apperceive restriction of human audio system (HAS), the watermarking signal won't be felt by HVS or HAS. With these unique characters and important application, digital watermarking technology has been got more and more attention [3-4]. Discrete wavelet transform in frequency domain is preferred among all the other techniques because of its unique characteristics such as perceptivity, security and robustness [5]. Robust image watermarking against noise and pepper attack is clearly defined in [6]. Biometric images using salient region-based authentication watermarking is proposed for self-recovery and tamper detection and also it recover the damaged data of original biometric images with hidden information based on tampering detection [7]. An adaptive digital image watermarking algorithm based on non-linear wavelet transform and Morphological Haar Wavelet Transform used. Human Visual System (HVS) is adaptively embedded into the original image in different resolutions [8]. The extraction of watermark can be done in the decrypted domain. Stream cipher is used to propose encryption algorithm. The phase DWT and inverse DWT (IDWT) in the encrypted domain, perform an analysis of data development and quantization errors under the frame. The problem of data development can be solved by reducing data development. In the case that multilevel DWT/IDWT can be performed with less data growth in homomorphic encrypted domain [10]. supported appropriate performance for those content-preserving geometric deformations and image process operations, as well as JPEG compression, low pass filtering, cropping and RBAs. Scaling the dimensions of pictures, freelance of the element position within the image plane, proof against cropping, sturdy to interpolation errors throughout geometric transformations, and customary image process operations. [11]. A second-order statistics (SOS)-based image quality metric, that considers the feel masking result and therefore the variation sensitivity in Karhunen–Loève rework domain. It improves the robustness in return . The gradient direction watermarking can be used for uniform quantization for the direction of gradient vectors. The watermark bits are entrenched by quantizing the angles of large gradient vectors at multiple wavelet scales .

II. PROPOSED SYSTEM

A. System Architecture

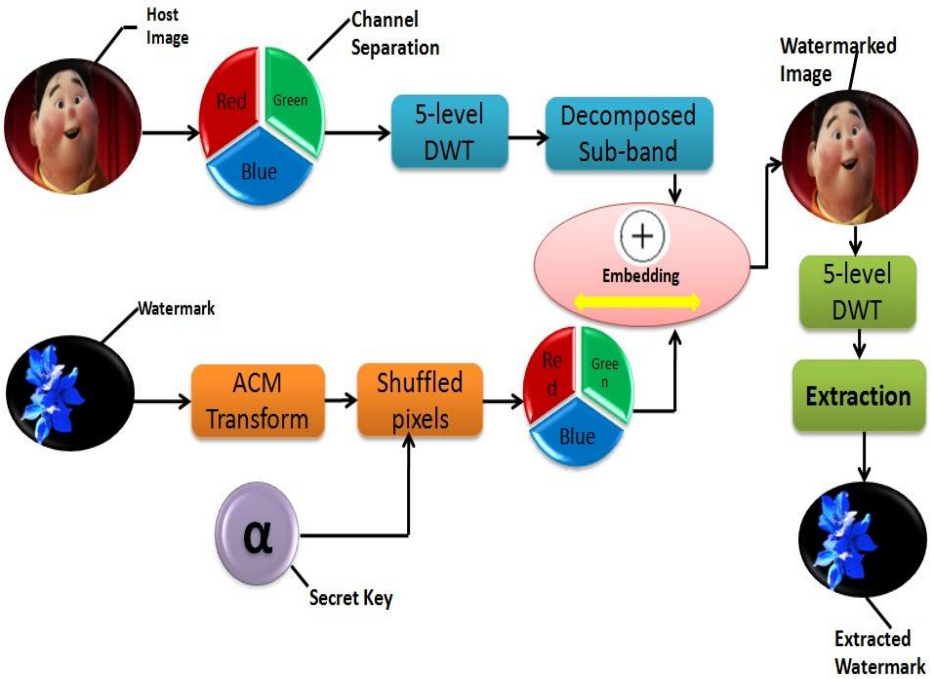

Fig 2 : Watermarking System Architecture

In the embedding process, colour image is given as host image. The host image is separated in to red, green and blue channels in which each separated channels forms a gray image. 5-level discrete wavelet transform is applied on each of

gray image. The gray image is now decomposed into four different sub-bands. Colour image of any size is taken as the watermark or the information to be hidden inside the host image. Arnold's cat map transform is applied on the watermark which converts the original watermark into a collection of pixels. This shuffled watermark is then implied with a secret key 'α' which is the strength/key of the watermark. It is then separated into red, green and blue channels.

Each separated channel is embedded with the decomposed gray image. Inverse discrete wavelet transform is applied on the embedded coefficients to get the watermarked image. Reverse process of embedding is applied for extraction process. Here the input is the watermarked image and watermark is extracted without any image quality degradation after the extraction process.

B. Discrete Wavelet Transform

Wavelet analysis consists of decomposing a signal or an image into a hierarchical set of approximations and information. The levels in the hierarchy often correspond to those in a dyadic scale. From the signal analyst's point of view, wavelet analysis is a decomposition of the signal on a family of analysing signals, which is usually an orthogonal function method. From an algorithmic point of view, wavelet analysis offers a harmonious compromise between decomposition and smoothing techniques [8]. Unlike conventional techniques, wavelet decomposition produces a family of hierarchically organized decompositions. The selection of a suitable level for the hierarchy will depend on the signal and experience. Often the level is chosen based on a desired low-pass cut-off frequency. At each level j, we build the j-level approximation Aj, or approximation at level j, and a deviation signal called the j-level detail Dj, or detail at level j. We can consider the original signal as the approximation at level 0, denoted by A0. The words approximation and detail are justified by the fact that A1 is an approximation of A0 taking into account the low frequencies of A0, whereas the detail D1 corresponds to the high frequency correction.

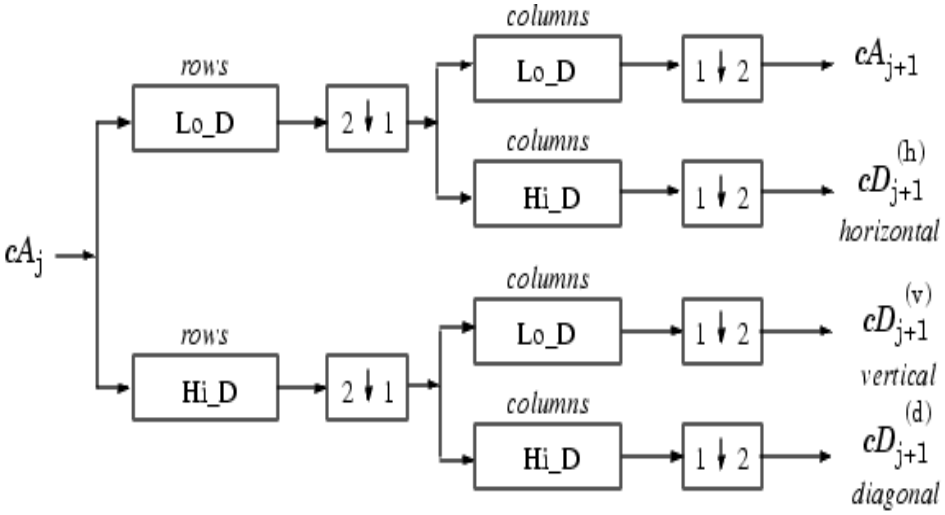

Fig 3 : DWT Decomposition

One way of understanding this decomposition consists of using an optical comparison. Successive images A1, A2, A3 of a given object are built. We use the same type of photographic devices, but with increasingly poor resolution.

$$A_2 = A_3 + D_3 = A_4 + D_4 + D_3$$

The Matlab algorithm for discrete wavelet transform (DWT) is, in fact, a classical scheme in the signal processing community, known as a two channel sub-band coder using conjugate quadrature filters. The decomposition algorithm starts with signal s, next calculates the coordinates of A1 and D1, and then those of A2 and D2, and so on. The reconstruction algorithm called the inverse discrete wavelet transform (IDWT) starts from the coordinates of AJ and DJ, next calculates the coordinates of AJ-1, and then using the coordinates of AJ-1 and DJ-1 calculates those of AJ-2, and so on [9].

C. Arnold's Cat Map Transform

There are two variants of encryption, Arnold Cat Map and Chen's chaotic system. Arnold Cat Map takes concepts from linear algebra and uses them to change the positions of the pixel values of the original image. The effect after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image. Chen's chaotic system will then take the image produced from the Arnold Cat Map and change the actual grey scale values of the pixels with a weight of watermark, the result will be the final encrypted image.

Mathematically the Arnold Cat Map, (ACM), can be represented as: The Arnold Cat Map is a discrete system that *stretches and folds* its trajectories in phase space.

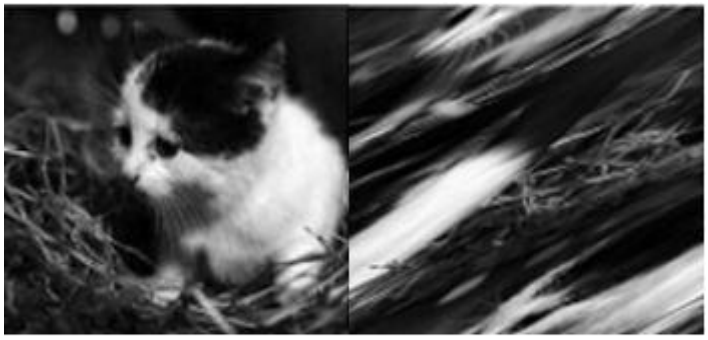

Fig 4. (a) : ACM Example

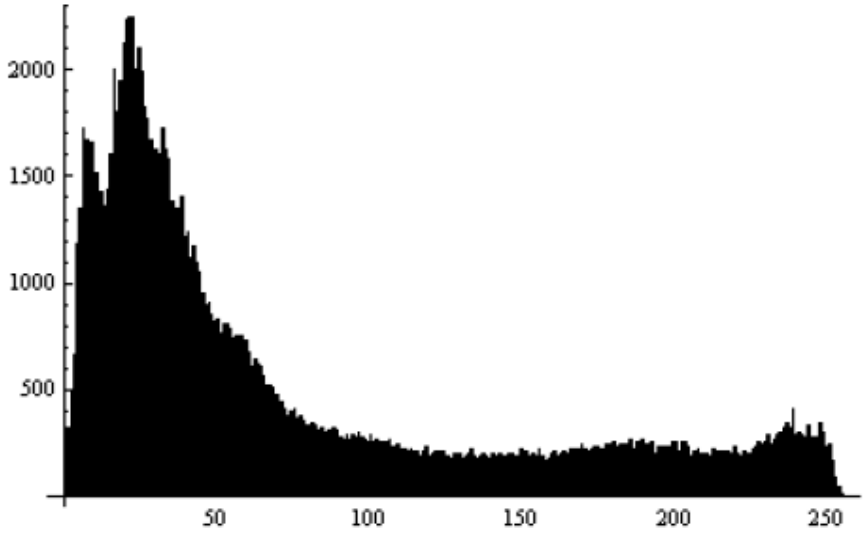

Fig 4. (b) : Histogram of Shuffled Image

III. WATERMARKING PROCESS

A. Watermark Embedding Algorithm

- Colour image of any size/format is taken as the host image and the watermark.
- The host image is separated into three basic colour components.
- Each component is employed with single level 2-dimentional discrete wavelet transform.
- Low-Low sub-band of single level decomposition is further decomposed into two level 2-dimentional discrete wavelet transform [8].
- Repeat the above step till the decomposition reaches its fifth level.
- The watermark is employed with Arnold's cat map transform which shuffles the original watermark with the same pixels.
- Encrypt the shuffled watermark with the secret key which is the weight factor in watermarking.
- Separate the encrypted shuffled watermark into three basic colour components.
- Embed each of decomposed host image component with the separated colour component of encrypted shuffled watermark.
- Inverse discrete wavelet transform is used at last to obtain the watermarked image.

B. Watermark Extraction Algorithm

- Watermarked image from embedding process is the host image to be extracted.
- The host image is separated into three basic colour components.
- Each component is employed with single level 2-dimentional discrete wavelet transform.
- Low-Low sub-band of single level decomposition is further decomposed into two level 2-dimentional discrete wavelet transform.
- Repeat the above step till the decomposition reaches its fifth level.
- Extraction process is applied to the decomposed host image components. Shuffled watermark components are extracted from this process.
- The shuffled watermark components are employed with inverse Arnold's cat map transform to get the original watermark without any image quality degradation.

IV. IMPLEMENTATION RESULTS

A. Host Images and Watermarks

More than a dozen colour images are taken and tested for watermarking performance. Six among them are displayed here in figure 5. These images are of different sizes such as 512*512, 650*560, 1200*980 etc., and of various formats such as jpg, bmp, png, gif etc. These images are given as the input to embedding process.

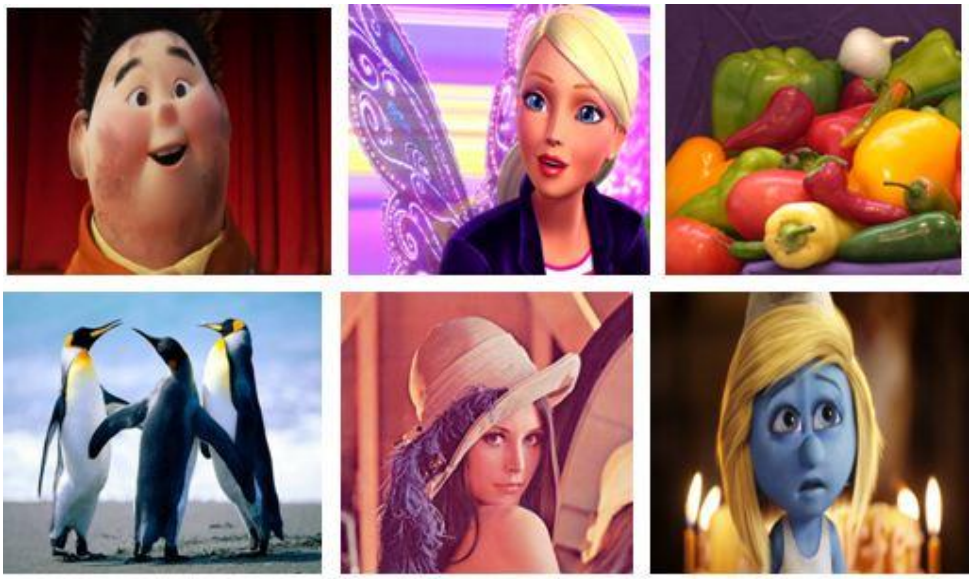

Fig 5 : Host Images

Colour images of different sizes are taken as watermarks. The size of watermark is altered based on the size of the host images. Few of watermarks are shown below in Fig 6.

Fig 6 : Watermark Images

B. Channel Separation

Host image is separated into the three basic colour components namely red, green and blue components. Fig. 7 shows the separated channels of host image.

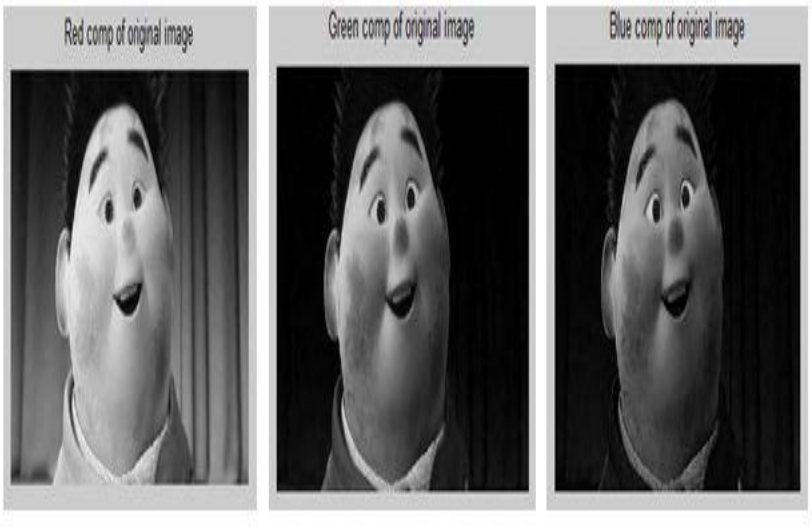

Fig 7 : Channel Separation – Host Image

The watermark after employed with Arnold's cat map transform is encrypted with the weight factor of watermarking. Then it is separated into the three basic colour components as in the host image. Fig. 8 shows the separated shuffled watermark components.

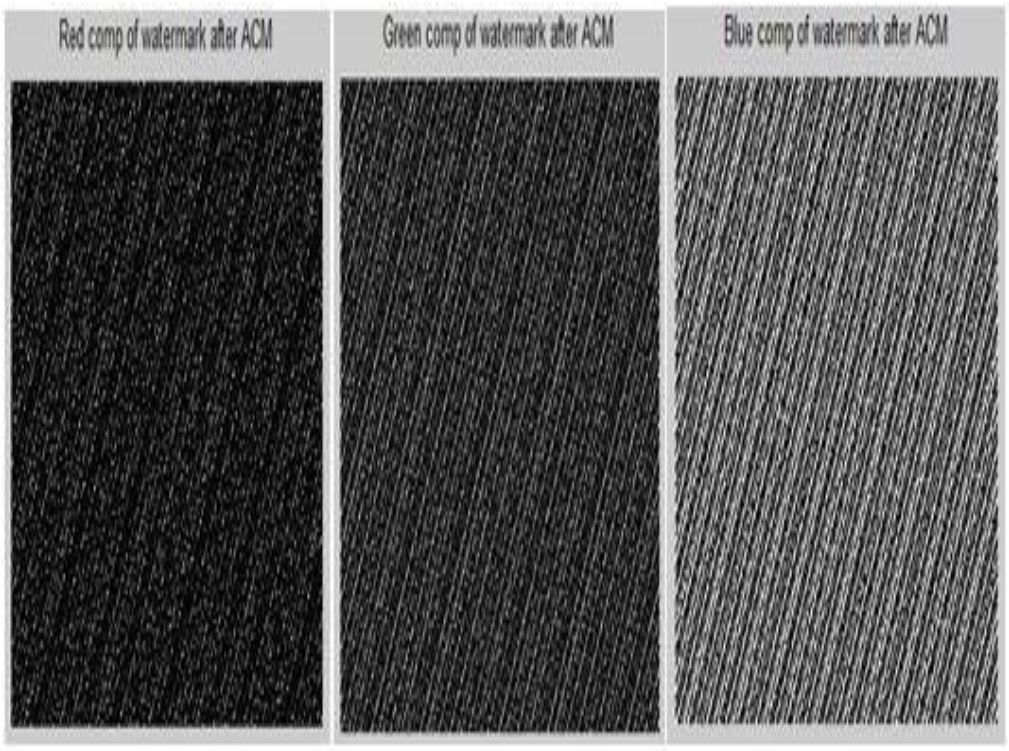

Fig 8 : Channel Separation – Shuffled Watermark

C. DWT Decomposition – Host Image

The separated component of host image is then employed with 5 – level discrete wavelet transform. DWT use Haar, which is the oldest yet efficient wavelet as their wavelet for decomposition process. The components are decomposed into four different levels of sub-bands namely the Low-Low level which is also known as the approximation level [10], the Low-High level which is also known as the horizontal level, the High-Low level which is also known as the Vertical level and the High-High level which is also known as the diagonal level. Fig. 9 shows the different decomposed levels of host image components.

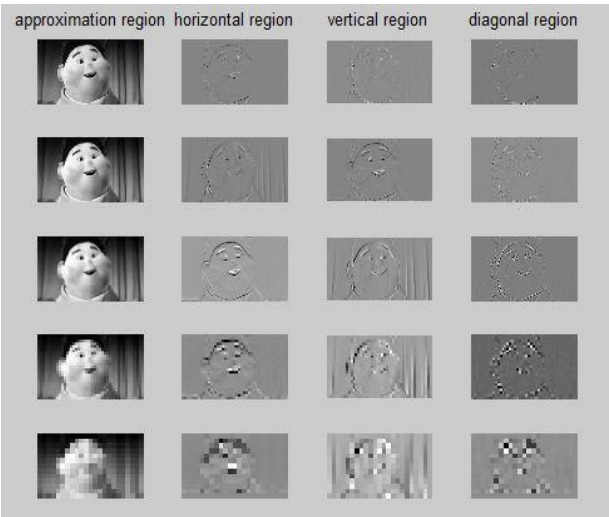

Fig. 9 : Decomposition – Host Image Components

D. Embedding Result

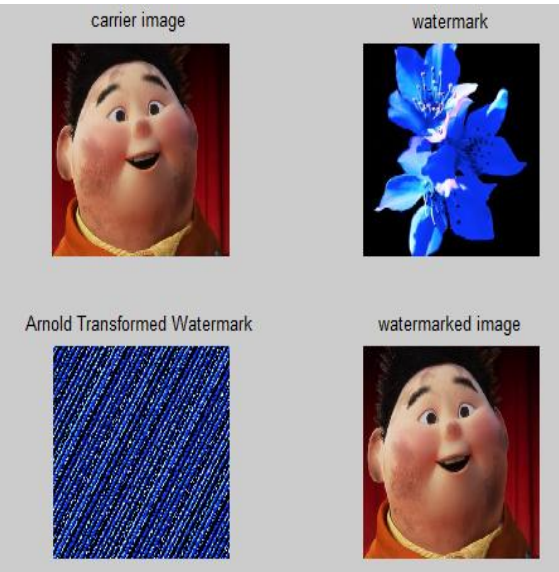

Fig. 10: shows the result of embedding process.

E. Extraction Result

Watermarked image is separated into the basic colour components and are employed with 5 – level discrete wavelet transform. Extraction process is applied on the decomposed watermarked colour components. Fig. 11 shows the extraction results.

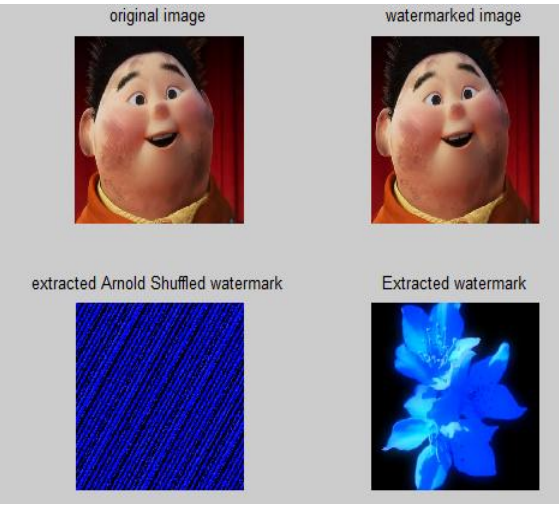

Fig 11 : Extracted Watermark

V. EXTRACTION OF WATERMARK FROM ATTACKS

A. Noise Attack

Digital images are prone to a variety of types of sound. Noise is the result of errors in the photograph acquisition process that result in pixel values [9]. There are more than a few ways that noise can be introduced into an photograph, depending on how the photograph is created. Noise is one of the major attacks which are used frequently by the unauthorized users intending to damage or destroy the owner's pictures. The noise added here is Gaussian noise. Fig. 12 shows the attacked watermarked image and the extracted watermark from noise attack.

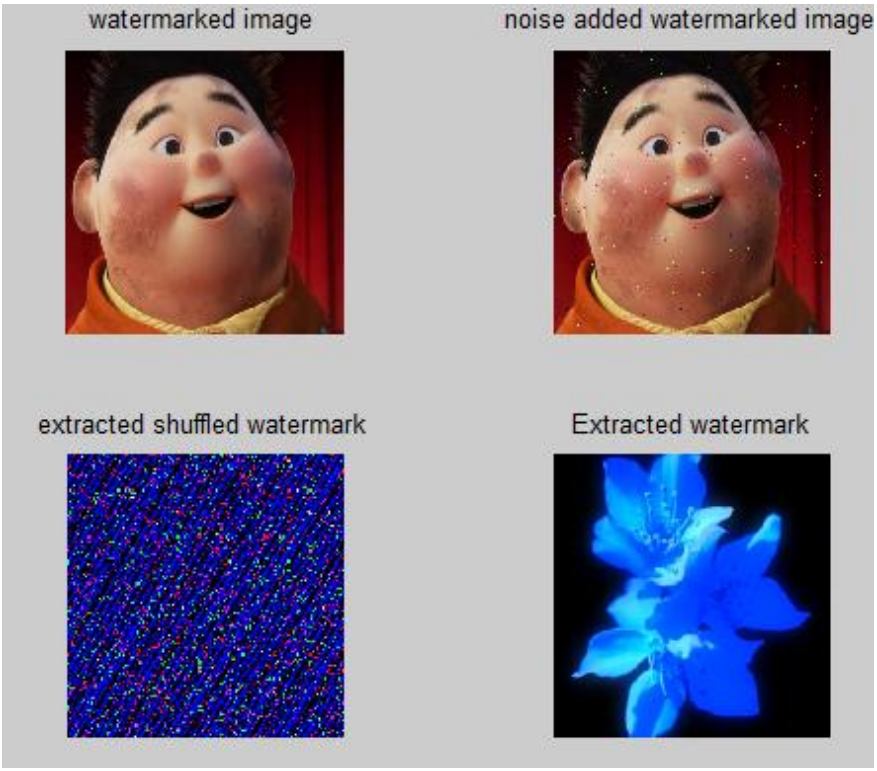

Fig. 12 : Extracted Watermark from Noise

B. Scaling Attack

Scaling is another attack which is vulnerable. Attackers scale a small part of the published image and claim to be their own image. A robust watermarking scheme should withstand all the scaling attacks performed to the watermarked image. Fig. 13 shows the scaled watermarked image and the extracted watermark from the attack.

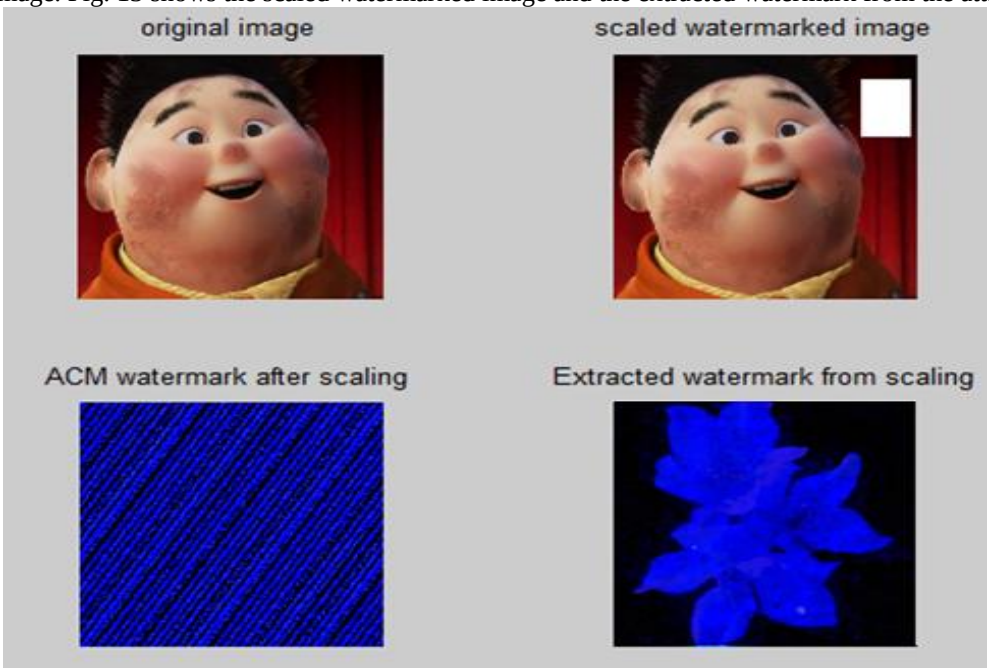

Fig. 13. Extracted Watermark after Scaling

C. Performance Measures

The performance measure in our scheme is calculated using a parameter called PSNR ratio. Peak signal-to-noise ratio (PSNR) between images is to compute the noise ratio between the original watermark and the extracted watermark. Higher the PSNR rate, lower the error rate [11]. The PSNR rate of the extracted watermark in our scheme is 96.7439 which is near to the original watermark rate. The PSNR rate of the extracted watermark after adding noise attack is 86.8961 and after adding scaling attack is 72.4330.

VI. CONCLUSION

Our scheme has enhanced the image watermarking technique and produced a good result in terms of PSNR ratio. Security is achieved by hiding the watermark encrypted with weight factor along with ACM shuffling. Robustness is achieved to maximum extent after adding attacks like noise and scaling. This scheme can be further enhanced by extracting the watermark perfectly from scaling attack and other image manipulations not tested here.

Acknowledgment

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, Principal, HOD of Computer Science & Engineering, Dr. K.P. Kaliyamurthie, Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank Dr. A.Kumaraval for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

[1] Sanjay Rawat and Balasubramanian Raman, "*A chaotic system based fragile watermarking scheme for image tamper detection"*, Int. J. Electr. Commun, Vol. 65, pp. 840-847, 2011.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "*Techniques for data hiding*", *IBM. Syst. J.*, vol. 35, pp. 313-335, 1996.

[3] ChangHong Dong, "*The use of MATLAB for imagery processing and applies*" , Beijing: The publishing of defence industry, 2004, pp. 33-37.

[4] Rohith. S, Dr. K. N. Haribhat, "*A Simple Robust Digital Image Watermarking against Salt and PepperNoise using Repeition Codes"*, ACEEE 2011.

[5] Chunlei Li , Yunhong Wang , Bin Ma and Zhaoxiang Zhang, "*Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme"*, Computer Standards & Interfaces, Vol. 34, pp. 367-379, 2012.

[6] Xiaosheng Huang and Sujuan Zhao, "*A Digital Image Watermarking Algorithm Based on Haar Wavelet Transform"*, Physics Procedia, International Conference on Solid State Devices and Materials Science, Vol 25, pp. 568-575, 2012.

[7] . Subramanyam, Sabu Emmanuel Mohan S. Kankanhalli, "*Robust Watermarking of Compressed and Encrypted JPEG2000 Images"*, IEEE Transactions on Multimedia, Vol 14, No 3, pp. 703-716, 2012.

[8] Peijia Zheng and Jiwu Huang, "*Discrete Wavelet Transform and Data Expansion Reduction in Homomorphic Encrypted Domain*", IEEE Transactions on Image Processing, Vol 22, No 6, pp. 2455-2468, 2013.

[9] Shijun Xiang, Hyoung Joong Kim and Jiwu Huang, "*Invariant Image Watermarking Based on Statistical Features in the Low-Frequency Domain*", on Ckts. and Systems for Video Technology, Vol.18, No 6, pp. 777-790, 2008.

[10] Fan Zhang, WenyuLiu, WeisiLin and King Ngi Ngan, "*Spread Spectrum Image Watermarking Based on Perceptual Quality Metric*", IEEE Transactions on Image Processing, Vol 20, No 11, pp. 3207-3218, 2011.

[11] Ehsan Nezhadarya, Z. Jane Wang and Rabab Kreidieh Ward, "*Robust Image Watermarking Based on Multiscale Gradient Direction Quantization*", IEEE Transactions on Information Forensics and Security, Vol 6, No 4, pp. 1200-1213, 2011.

ABOUT THE AUTHOR

G.Julin Leeya received her B.E degree in Computer Science & Engineering from Jei Mathaajee College of Engineering, Kanchipuram and now currently pursuing her M.Tech. Final Year in Computer Science & Engineering from Bharath University, Chennai. She has secured Second Rank Holder in College and many Cultural activities certificates in the schools and colleges.

	**K.G.S.Venkatesan** received his B.Tech degree in Computer Science & Engineering from JNT University, Hyderabad and received his M.Tech degree in Computer Science & Engineering from Bharath University, Chennai. He is currently pursuing his Ph.D in Computer Science & Engineering at Bharath University, Chennai. He has 10 years of Teaching experience and has guided many B.Tech and M.Tech projects. He is having Membership in Indian Society of Technical Education (MISTE). He attended **HIGH IMPACT Teaching Skills** Programme conducted by WIPRO MXLA (Mission 10X Learning Approach).
	**G.Dayalin Leena** received her B.E degree in Computer Science & Engineering from Rajiv Gandhi College of Engineering, Sriperambudur and received her M.E. degree in Computer Science & Engineering from Jerusalem College of Engineering, Chennai. She is currently working as Teaching Fellow in Computer Science and Engineering Department in University College of Engineering Arni, a Constituent College of Anna University Chennai. Her area of interest is Image Processing and Web Technology.

