IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 3 (Mar. 2013), ||V3|| PP 01-09

Digital Watermarking Algorithm for Color Images

Mr.P.B.Khatkale, Prof.D.G.Lokhande, Asst.Prof.Srescoe,
ME Electronics (Digital System) SRESCOE, Kopargaon Kopargaon

Abstract: Digital watermarking methods describe the technologies that allow hiding of information in digital media such as images, video and audio. Watermarking techniques embed information in images by introducing changes that are imperceptible to the human eye but recoverable by a computer program. Generally, the watermark is a code to identify the owner of the image. The locations in which the watermark is embedded are determined by a secret key. Doing so prevents possible pirates from easily removing the watermark. Furthermore it should be possible to recover the watermark from an altered image. Possible alterations of watermarked images include compression, filtering and cropping. These alterations are referred to as attacks. The first watermarking application that might come to mind is related to copyright protection of digital media Watermarking algorithms have been proposed to protect varieties of content, such as official documents.

Keywords: *Compression, Cropping, Digital Watermark, Hiding, Secret key*.

I. INTRODUCTION

A watermarking system must allow for a useful amount of information to be embedded into the image. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

The process of digital watermarking involves the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes. The embedding method must leave the original data perceptually unchanged. The major technical challenge is to design a highly robust digital watermarking technique, which discourages copyright infringement by making the process of watermarking removal tedious and costly. [12]

A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection algorithm. In multimedia applications embedded watermarks should be invisible, robust and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark. The literature survey explains robustness is the resistance of an embedded watermark against intentional attacks such as noise. Capacity is the amount of data that can be represented by an embedded watermark.

II. BLOCK DIAGRAM

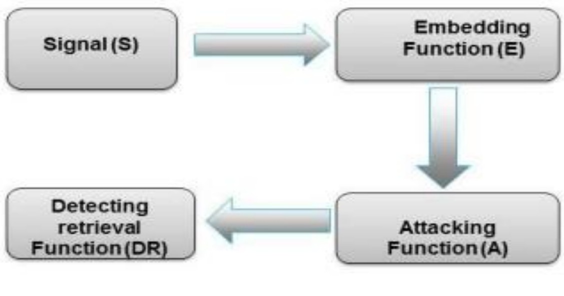

Fig.1 Basic Watermarking Procedure

Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead. In this paper plan to present a new image watermarking technique that can embed more number of watermark bits in the cover image without affecting the imperceptibility and increase the security of watermarks. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video. In this paper image is the host signal and embedding the secret data and the extract the same. In this process enhancing the network security. [7]

2.1 Embedding stage:-

One of the most important features that make the recognition of images possible by humans is color. Color is a property that depends on the reflection of light to the eye and the processing of that information in the brain. The color is used every day to tell the difference between objects, places and the time of day. Usually colors are defined in three dimensional color spaces usually colors are defined in three dimensional color spaces. These could be RGB (Red, Green, and Blue), HSV (Hue, Saturation, and Value) or HSB (Hue, Saturation, and Brightness). The last two are dependent on the human perception of hue, saturation, and brightness [6]. Color represents the distribution of colors within the entire image. This distribution includes the amounts of each color, but not the locations of colors.

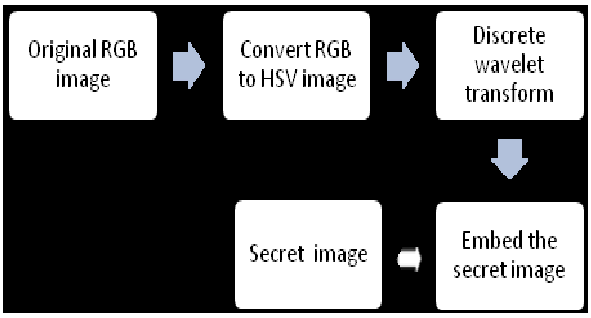

Fig.2 Embedding Stage

2.2 Extracting stage:-

In a digital watermarking scheme, it is not convenient to carry the original image all the time in order to detect the owner's signature from the watermarked image. Moreover, for those applications that require different watermarks for different copies, it is preferred to utilize some kind of watermark-independent algorithm for extraction process i.e. dewaters marking. Its robustness against many attacks including rotation, low pass filtering, salt n paper noise addition and compression. [9]

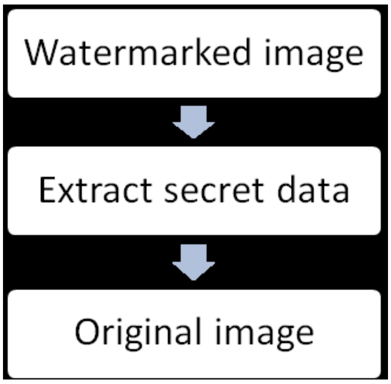

Fig.3 Extracting Stage

III. PROPERTIES

For better activeness, watermark should be acoperceptually invisible within host media, statistically invisible to unauthorized removal, readily extracted by owner of image, robust to accidental and intended signal distortion like filtering, compression, re-sampling, retouching, crapping etc. For a digital watermark to be effective for ownership, it must be robust, recoverable from a document, should provide the original information embedded reliably and also removed by authorized users

3.1 Robustness:

The watermark should be robust such that it must be difficult to remove. The watermark should be robust to different attacks. The robustness describes whether watermark can be reliably detected after performing some media operations. [10]

3.2 Perceptual transparency:

This property describes that whether watermark is visible or invisible to human sensor organ. Perceptible watermarks are visible to human while imperceptible are not. Imperceptible watermarks are such that content remains same after applying digital watermarking technique.[2]

3.3 Security:
Security property describes that how easy to remove a watermark. This is generally referred to as attack on watermarking. Attack refers to detection or modification of watermark. [4]

3.4 Complexity:
This is important property which is to be considering in real-time applications like video. Complexity property is concerned with amount of effort needed to extract or retrieve the watermark from content. [7]

3.5 Capacity:
Capacity property of digital watermarks refers to amount of information that can be embedded within the content. The important point is that more data is used in watermark, watermark will become less robust. In addition to these properties, watermarks are having some extra properties as unambiguity, tamper resistance, inseparable from the works and able to undergo some transformation as works. [1]

IV. CLASSIFICATION

Digital watermarks are classified according to their applications. The watermarks are classified as perceptible watermarks and imperceptible watermarks, robust and fragile, public and private. This classification of watermarks is broadly described in following sections.

4.1 Perceptible watermarks and imperceptible watermarks:
Perceptible watermarks are visible to human eye while imperceptible watermarks are invisible. The perceptible watermarks are useful for primary application i.e. for statement ownership or authorship. So for this reason it should be visible. On the other hand imperceptible watermarks are useful for complex applications such as document identification in which content being watermarked must appear in unchanged form Examples of visible (perceptible) watermarks are logos on TV, IBM watermark and that of invisible (imperceptible) watermarks are ATT, NEC/MIT, UU etc. Perceptible watermarks i.e. visible one are extension of the concept of logos. They are applicable to images only. These watermarks are embedded into image. They are applicable in maps, graphics and software user interface. Imperceptible watermarks i.e. invisible one remains hidden in the content. They can be detected only by authorized agency. These watermarks are useful for content or author authentication and for detecting unauthorized copier. [4]

4.2 Robust watermarks and fragile watermarks:
Robust or fragile is nothing but degree to which watermarks can withstand any modifications of any types caused due to the transmission or loss compression. Perceptible watermarks are more robust in nature than imperceptible one. But meaning of this is not that imperceptible watermarks are fragile one. Robust watermarks are those watermarks which are difficult to remove from the object in which they are embedded. Fragile watermarks are those watermarks which can be easily destroyed by any attempt to tamper with them. Fragile watermarks are destroyed by data manipulation. [5]

4.3 Private watermarks and public watermarks:
Private watermarks requires at least original data to recover watermark information Public watermarks requires neither original data nor embedded watermarks to recover watermark information. Private watermarks are also known as secure watermarks. To read or retrieve private watermark, it is necessary to have secret key. Public watermark can be read or retrieve by anyone using specialized algorithm. In this sense public watermarks are not secure. Public watermarks are useful for carrying IPR information. They are good alternatives to labels. [3]

V. DIGITAL WATERMARKING FOR COLOUR IMAGE

Full-size images require large amounts of disk space to store and bandwidth or time to transmit and display. In many applications, a smaller version of an image is sufficient. There are many ways in which a large image can be reduced in size.

5.1 Techniques of Image size Reduction:
5.1.1 Cropping:
The simplest way, in which to reduce an image's size is by cropping, i.e. choosing only a certain portion of the image to view. This works well if one region of an image contains all of the interesting information. Even then, it requires a determination of what part of the image is important. This may be an easy task for a human, but is very difficult for a computer.[8]

5.1.2 Pixel Skipping:

To eliminate the above problem, we can reduce the size of an image by throwing out pixels evenly throughout an image. For example, if we wanted to reduce the size of an image by half in each dimension, we could throw out every other pixel. This method is fairly fast, but may produce artifacts, especially in color images. If an image is dithered, for example, it may have a regular pattern of two or more colors adjacent to each other in order to produce the illusion of a different color (which wasn't available in the color palette.) If we happen to throw out all of one of those colors, the perceived color, and thus the overall look, of the image will change drastically [10].

5.1.3 Pixel Averaging:

In order to eliminate the problem of color artifacts as described above, we can average adjacent pixels together instead of simply throwing them out as in Pixel Skipping. However, this will take more time and may tend to blur the image [11].

5.1.4 Frequency Domain Processing:

A different approach to image size reduction involves looking at an image in the frequency domain in the hopes that the useful information will be more easily selected. For example, if an image was composed entirely of low frequency components, the high frequency components would all be very small in the frequency domain and we could truncate them. When the image was transformed back to the spatial domain, it would be reduced in size by the same factor as in the frequency domain. Note that for this example, the net effect would be the same as Pixel Averaging. The advantage of Frequency Domain Sampling is that it could also reduce the size of images with only high-frequency content. In addition, if the frequency domain image was sampled as in Pixel Skipping, then the image in the spatial domain would also be reduced in size. The exact effects of this on the image are not obvious [1].

5.1.5 Wavelet Decomposition:

The 2-D Discrete Wavelet Transform (DWT) offers another possible approach to image size reduction. The DWT is a decimating transform which produces a segmented image with different segments containing coefficients corresponding to different levels of detail in the image. Each level of the DWT produces four segments. The next level of the DWT operates on that smoothed version [1].A color image can be thought of as three grey-scale images (Red, Green, and Blue). Any of the above algorithms must be applied to each of these images separately, after which the images can be re-combined to form the complete image [1].In order to investigate the above algorithms, several platforms are recommended. For Cropping, Pixel Skipping, and Pixel Averaging, XV is used, an image display and manipulation package. XV includes hooks for programmers to add their own code. This allowed writing the appropriate routines without having to worry about writing code to load and display images. XV already implemented Cropping, and added Pixel Skipping and Pixel Averaging [1].

5.2. Arnold Transform

The security of watermarking can be enhanced by scrambling or encrypting before watermarking is embedded. In this paper, the extended Arnold transform is used to scramble watermarking of copyright protection. Initial Arnold transform equation is as follows:

$$\begin{cases} x_{n+1} = (x_n + y_n) \mod 1 \\ y_{n+1} = (x_n + 2y_n) \mod 1 \end{cases} \quad \textbf{(1)}$$

mod 1 denotes that takes the fractional part only, namely
x mod1=x-[x]. So the phase space of *(xn, yn)* is restricted in square [0, 1] X [0, 1]. It transforms (1) to matrix form.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = C \begin{pmatrix} x_n \\ y_n \end{pmatrix} \mod 1 \quad \textbf{(2)}$$

Formula (2) defines matrix C. Taking note of the determinant ICI =1 , Arnold mapping has a fixed area(no attractile gene). At the same time it is all mapped. That is to say, every point in unit matrix uniquely transforms to another point. The character is very important. With it each watermarking pixel in different places can get a different place to embed. Arnold mapping has two typical factors to generate chaotic motion. One is tensile (multiplied by the matrix C to make x and y larger), and another is folding (make x and y retract unit matrix by modulus). In fact, Arnold mapping is also a chaotic mapping. Generalize Arnold mapping as follows.

Firstly, generalize phase space to {0,I,2, ... ,M-I} X {0,I,2, ... ,M-I}. That is, only take positive integers from °to M-I. Secondly, generalize the equation as most common two-dimensional and fixed area.

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = C \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod M \quad \textbf{(3)}$$

In the formula, a, b, c and d are all positive integers. Its fixed area requires leI =*ad* - *be* =1. In this conditions, a=1, b=r, c=p and d=rP+l. So only rand p parameters are independent. Formula (3) can be replaced by (4).

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & r \\ p & rp+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod M \quad \textbf{(4)}$$

Formula (3) still has the characteristics of chaotic mapping. Therefore, take use of generalized Arnold mapping (3) to generate the corresponding scrambling location of every pixel point of watermarking. Take every pixel coordinate (x, y) of watermarking as the initial value; take three independent parameters of coefficient matrix C and the times of iterations(k) as secret key; and take the result of iteration(x', y') as the corresponding location where (x, y) is scrambled. Since the chaotic characteristics of mapping, the corresponding location of any two adjacent pixels scrambled of watermarking will be a great deal of separation. And because it is a one by one mapping, the scrambling location got by different iteration of watermarking coordinates is different. Thus, scrambling location does not produce a conflict. [13]

5.2 Algorithms for Implementation:

The advantages of watermarking are its imperceptibility and robustness. Also, an effective watermarking approach should satisfy the requirements of security, unambiguity and low computational complexity. Dependent on the processing domain of the host image, current image watermarking techniques can be divided into two categories:

- Spatial domain watermarking methods
- Transform domain water marking schemes

For spatial domain methods watermark embedding is achieved by modifying the pixel values of the host image with computational efficiency. For transform domain schemes, the host image is first converted into frequency coefficients by a transformation method such as the discrete cosine transform (DCT), discrete Fourier transform (DFT) or discrete wavelet transform (DWT) etc. [2].For the DWT, S-Plus is used with the Wavelets toolkit. Here we had to split the color images up into their R, G, and B components in order to run the DWT on them. We need to add routine to XV to save images to separate files which S-Plus could read (1 file for each of the three color components R, G, and B), also added a routine to load images which had been saved by S-Plus. [14]

5.3 Multi-level Wavelet Decomposition Of Image:

The discrete wavelet transform (DWT) is a new signal analysis theory in recent years. It is a new analysis method in time domain and frequency domain, which is widely used in many fields. The basic idea of DWT is to separate frequency detailed, which is multi-resolution decomposition. One time of decomposition can divide main image to four subgraphs as the size of a quarter. They are a low frequency approximate subgraph and three horizontal, vertical and diagonal directions high frequency details subgraph. Fig 3.1 is a schematic diagram of three-level DWT decomposition [4].

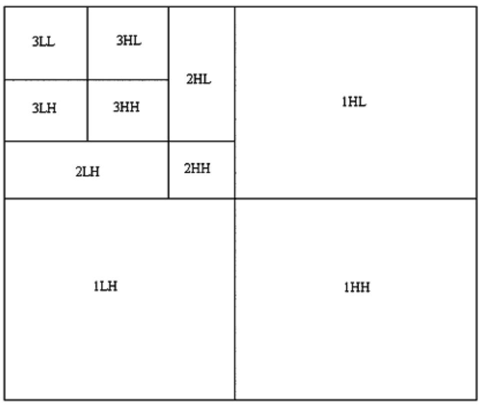

Fig.4 Three-level DWT decomposition

In the wavelet transform domain, high frequency part represent details information as image's edge, contour and texture and so on. Embedding watermarking in these places, people are not easily conscious of it. But after processing or attacking, it has poor stability. Most energy of image is centralized in low frequency. The amplitude coefficient is larger than it of detail sub graph. By the brightness of shadowing of human visual model, we know that background brightness is brighter so that the just noticeable difference (JND) of signal embedded is higher. That is, low frequency approximate sub graph has larger capacity of people's perception. It is equivalent to a strong background, in which more watermarking information can be. As long as the watermarking information embedded is below JND value, people are not able to feel the signal. Low frequency coefficients are nearly unchanged to common attack so that watermarking information embedded in low frequency coefficients has better robustness [3].

In Matlab, the realization of two-dimensional multi-level DWT decomposition of image is the function Wavedec2 (). Its form of call syntax is:

[C, S]=Wavedec2 (matrix of image, N, typename) (5)

For example, the image described with matrix A takes three-level DWT decomposition (N=3) by haar wavelet (wavelet type called haar). The expression of decomposition is as follows:

[C, S]=Wavedec2 (A, 3, haar) (6)

The wavelet coefficients after decomposition are all stored in a one-dimensional row vector C. Every coefficient of wavelet sub graph is ordered in row vector C. Its form is as follows:

$$C=[LL_N,HL_N,LH_N,HH_N,HL_{N-1},LH_{N-1},HH_{N-1},\ldots ,HL_1,LH_1,HH_1]$$

In it LL_N, HL_N, LH_N, HH_N is row vector listed in the order of priority of separately the N level low-frequency sub graph, detail sub graph of horizon, vertical and diagonal directions.

The other HL_i, LH_i, HH_i, (i=1, 2... N-l) is row vector listed in the order of priority of separately the i level detail sub graph of horizon, vertical and diagonal directions. The vector C and S after wavelet decomposition can be reconstructed with two-dimensional inverse DWT function Waverec2 (). For example, the formula corresponding to Eq.6 of initial image reconstructed by wavelet coefficients is as follows:

A'=Waverec2(C', S', haar') (7)

When the right coefficients C' and S' of Eq. 7 are same with the coefficients C and S of Eq.6 the image A' reconstructed by Eq.7 is same with the initial image A by decomposition Eq.6.

5.3.1 Embedding Algorithm of Digital Watermarking:

Because two different kinds of watermarking will be embedded in wavelet domain of color image, first of all, the problem considered is the order of the two kinds of watermarking embedding. The influence between them should be minimized to the best of its abilities. Generally speaking, for the order of adding two kinds of watermarking, there are three options to select.

a. Firstly embed fragile watermarking. Secondly embed robust watermarking.
b. Firstly embed robust watermarking. Secondly embed fragile watermarking.
c. Embed robust and fragile watermarking at the same time.

Comparison of three kinds of embedded sequence, first option is most not feasible because fragile watermarking is very sensitive to distortion. If embed fragile watermarking in advance, robust watermarking embedded later will destroy the fragile watermarking. So fragile watermarking will lost its role completely. In the option b, embed robust watermarking earlier and fragile watermarking later. The fragile watermarking will influence robust watermarking to some extent. It reduces the performance of robust watermarking and makes anti-interference ability of robust watermarking difficult to play out completely. In this paper, take the use of option c. It embeds two kinds of watermarking in different locations at the same time. Therefore, two kinds of watermarking can play its roles independently. And robustness and sensitivity are all better [8].

The two kinds of watermarking both use binary image seal in the same size. If W is binary image watermarking, its size is Ml x M2. Usually in order to calculate easily, let Ml = M2. To robust watermarking, in order to abolish space relation of pixel of watermarking image and improve its security, encrypt robust watermarking with chaotic encryption algorithm. To fragile watermarking, take use of Arnold transformation to transform binary image watermarking and then encrypt it with RSA public key encryption algorithm [8].

The flow chart of algorithm is as follows:

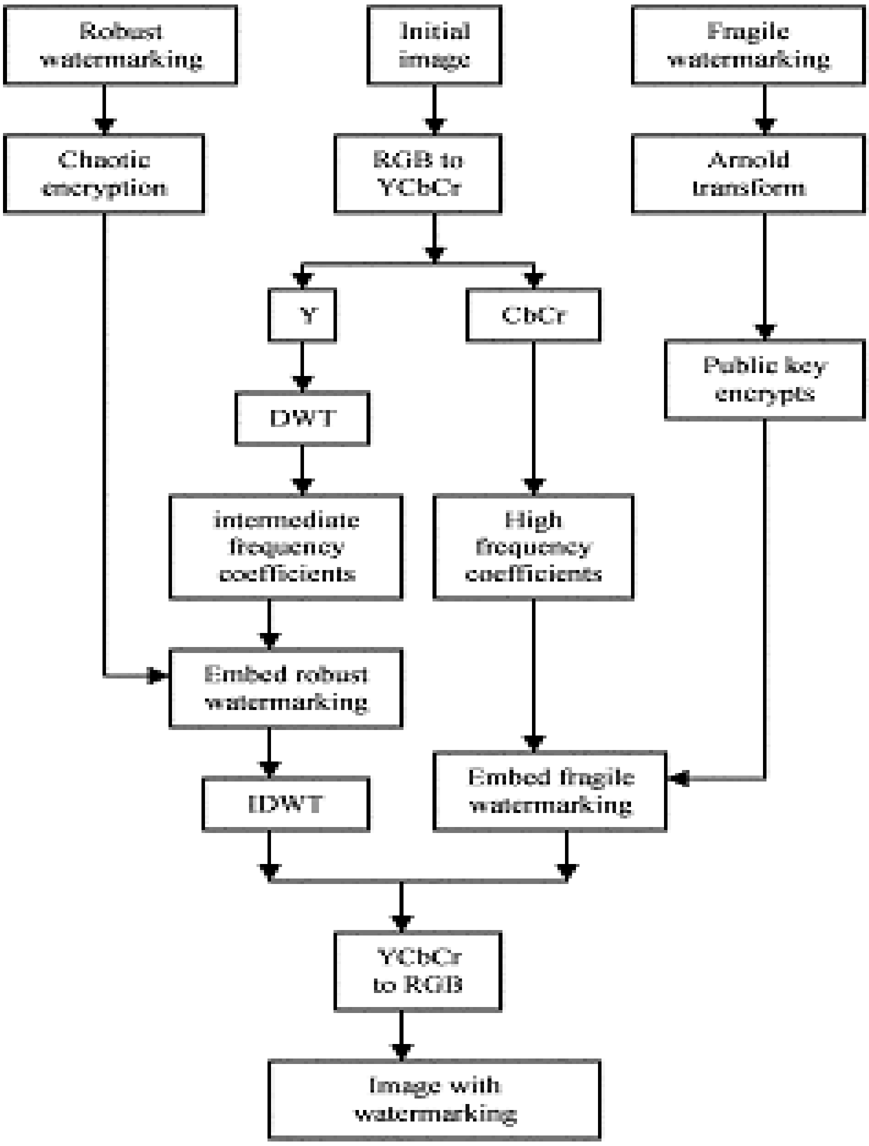

Fig. 5 Flow Chart of Embedding Watermark

The embedding steps are as follows:
Step 1: Chaotic encryption algorithm is used to robust watermarking.
Step2: Use Arnold transformation to transform fragile watermarking, and then encrypt it with RSA public key encryption algorithm.
Step3: Use (9) to switch initial image's room.
Step4: Use DWT to switch Y component in YCbCr domain. Information embedded is less as decomposition levels of DWT get more. So use four-level DWT to Y component in this paper, and then embed robust watermarking by chaotic encryption in the intermediate frequency coefficients and fragile watermarking in high frequency coefficients of CbCr.
Step5: Use IDWT to switch Y component. Switch YCbCr room to RGB room. Then get color image embedded with watermarking.

5.3.2 Extraction Algorithm of Digital Watermarking:
Extraction of watermarking is inverse process of embedding.
The flow chart of algorithm is as follows:

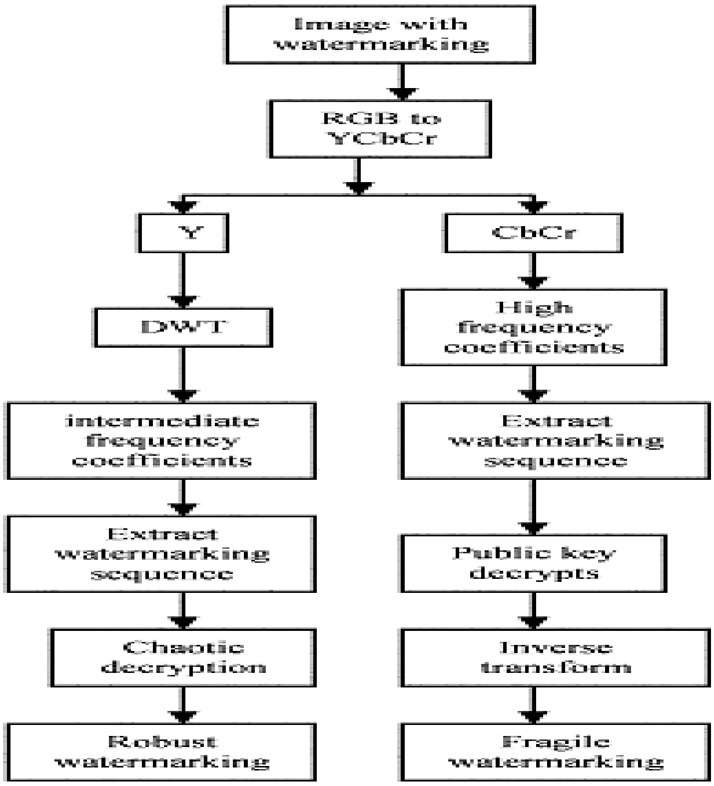

Fig. 6 Flow Chart of Extracting Watermark

Its steps are as follows:
Step 1: Switch the room of image which watermarking is embedded. Y component, Cb component and Cr component can be got.
Step2: Take four-level DWT to Y. Extract watermarking with secret key in its intermediate frequency coefficients. Then take chaotic decryption to get robust watermarking. Because the fragile watermarking is encrypted by owner's private secret key, all users can use the public key to decrypt. They can get the watermarking information and then verify it.The fragile watermarking can be got by decrypting high frequency coefficients of Cb and Cr components [11].

VI. RESULTS

Image	PSNR with JPG Attack	PSNR with MAL Attack	PSNR
Lena	44.7707	58.7355	48.0026
Rice	42.7809	59.7543	48.0091

VII. CONCLUSION

In this paper a new frequency domain algorithm for color digital image watermarking is presented, this algorithm uses the green channel for watermarking embedding. From result we can conclude that the signal to noise ratio with JPG attack is less as compared to MAL attack. By comparing our algorithm to others, we can conclude that the maximum numbers of bits that can be hidden and recovered successfully from the watermarked images have been increased. Excellent performance for the embedding process is achieved for an embedding stage. It has also been demonstrated that for this embedding strength the signature is immune to a variety of attacks, including filtering, contrast balancing, compression, and geometrical transforms such as resizing. Image Adaptive Self Embedding Watermarking proved robust against various attacks performed. The use of semi-fragile property helps to detect the location of fraud in the image. This technique is having a great scope of opportunities; especially in the field of cyber frauds, court evidences and certificate or identity forgery and even in the preservation and transmission of cultural heritage images. The large need of networked multimedia system has created the need of *COPYRIGHT PROTECTION*. It is very important to protect intellectual properties of digital media. Internet playing an important role of digital data transfer. Digital watermarking is the great solution of the problem of how to protect copyright. Digital watermarking is the solution for the protection of legal rights of digital content owner and customer.

REFERENCES

[1] Y.I.Song, RZ.Liu, and T.N.Tan, "Digital Watermarking for Forgery Detection in Printed Materials" in International Symposium on Multimedia Information Processing, Beijing, China, October 24-26, 2001 .

[2] Anumol T.J. & P.Karthigaikumar," DWT based Invisible Image Watermarking Algorithm for color Images" in IJCA Special Issue On "Computational Science- New Dimensions & Perspectives"NCCSE,2011.

[3] P.S.Huang, C.S.Chiang, C.P.Chang and T.M.Tu,"Robust Spatial Watermarking technique for colour images via direct saturation adjustment "in IEE Proc.-Vis.Image Signal Processing Vol-152, No-5, October 2005.

[4] Yu Wei, Yanling Hao and Yushen Li,"A Multipurpose Digital Watermarking Algorithm of Color Image", Proceedings of the 2009 IEEE in" International Conference on Mechatronics and Automation" August 9-12 Changchum-China.

[5] Rafael C.Gonzalez, Richard E.Woods, Steven L.Eddins, "Digital Image Processing Using MATLAB" Pearson Education ISBN 81-297-0515-X, 2005.

[6] B. Verma, S. Jain, D. P. Agarwal, and A. Phadikar, "A new color image watermark scheme Infocomp. Journal of computer Science. vol. 5, pp. 37-42, 2006.

[7] S. Armeni, D. Christodoulakis, I. Kostopoulos, Y. Stamatiou, and M. Xenos, "A Transparent Watermarking Method for Color Images," in 1st IEEE Balkan Conference On Signal Processing, Communications Circuits and Systems, Maslak, Istanbul, Turkey, 2000 .

[8] I. nasir, Y. weng, and J. Jiang, "A new robust Watermarking Scheme for color Image in spatial domain," in IEEE the 3rd international conference on signal-image technology & internet based systems, 2007.

[9] W. Luo and G. L. Heileman, "A fast and robust watermarking method for JPEG images," in Computer modeling & new Technologies, 2004, pp. 39 47.

[10] Y. Y. CHUNG, "High Capacity Digital Watermarking Systems ," in proceedings of world academy of science, engineering and technology, April 2004.

[11] M.Bami, F.Bartolini, A. D. Rosa, and A. Piva, "Capacity of the Watermark-Channel: How Many Bits Can Be Hidden Within a\ Digital Image?" in Proc. of SPIE, 1999.

[12] A. AI-Gindy, H. AI-Ahmad, R Qahwaji , and A. Tewfik , "Enhanced OCT based technique with shuffle scheme for robust Image watermarking of handwritten signatures.," in proceeding of ICCCP'07 International conference for communication,Computer and Power, Muscat, Oman, 2007, pp. 450-451

[13] Z. Wang, A. Bovic, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," in IEEE Transactions on Image Processing, 2004, pp. 600-612.

[14] I.J.Cox et. al.,"Secure Spread Spectrum Watermarking of Images, Audio and Video", Proc IEEE International Conf on Image Processing, ICIP-96, Vol.3, pp 243-244