ISSN No: - 2456 – 2165

A Review of Image Watermarking Methods

SumanVerma
M.Tech Scholar
MACERC
Jaipur, Rajasthan, India

Manish Mathuria
Professor
MACERC ,
Jaipur, Rajasthan, India

Abstract: - By the gradual support & enhancement in usage of internet, several issues are faced with respect to security.A safe & secure technique is needed to transmit the data. Digital watermarking is the method that ensures hiding of information & security. Watermarking is the method that hides the content or either detects the information in a digitized multimedia. Main focus of this discussion is on the watermarking of digitized audio, video & documents that are watermarked on a routine. This methodology has gained attention, particularly for indulging unidentifiable marks like copyright information about an author. This process includes a signal in a media that downgrades the visual ability of media.In this document, a watermarking method based on DWT is presumed to secures the data of an image & enhance the quality also.

Keywords:-Digital watermarking, Spatial domain, Least Significant Bit (LSB), Frequency domain, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT).

I. INTRODUCTION

Digital image processing is a rapid increasing section with several implementing applications in the branch of computer science engineering. It is one of the major research subject as well as this methodology can be implemented in different kinds of fields such as medical research, human & computer interface, enforcement of law, enhancement & restoration of picture & digitization watermarking for the purpose of security. Digital image processing possesses several advantageous assets over processing of analog pictures. Digital image processing also supports several operations of computers for the purposes like improvising the quality of picture & removal of noise from pictures. The digitized picture [1] is presented by the 2-D pictures such as a finite group of digital figures which are defined as pixels. So, processing of a picture of digital format by a computer is termed as digital image processing.

The digital technology used for the purpose of communication like internet deals that has various kinds of problem associated to security & privacy of content. Some security measures are needed to prevent the access of information illegally without acknowledgement any 3rd party. So there is a high need to save the information in this internet world. There are several methodologies for that secure the digitized information which comprises encryption & decryption, steganography, cryptography & digitized watermarking. This methodology of digital watermarking is explained in this document.

Digital watermarking is a method used for hiding the data. Several numbersof methodologies are used for hiding of information in digitized formats like video, audio, pictures, audios & texts. In general, digital watermarking is that methodology that helps to invade the information secretly& some extra information in a cover picture that can be either extracted & used for the purpose of authentication, identification, protection of copyright & contents. At various levels, the factor of scaling if implied for invading a watermark in cover picture. This digital watermarking technique is mainly implemented to produce the digitized data & protection of information from some hackers & gives the right of ownership for digitized information. Other characteristics of this method are termed as robustness. It also possesses imperceptibility confronting various types of attacks or manipulation of picture like filtering, cropping, compression, rotation & scaling. The robustness watermark that is includedcomputes the effectiveness of the implemented algorithm of digital watermarking. The methodology of digital watermarking is implemented for improvisation in ownership of picture which that is done by invasion of signals that are of low level into the picture. This method can also be employed for protecting the picture from tampering & validation [2].

Digital watermarking is a highly emerging technology that is implemented to attain various kinds of applications with success. Digital watermarking is been implemented in various kindsof methodologies that are used for image processing. Main target of the application is to provide appropriate security paths to digitized form data. The applications of digital watermarking are comprised of Broadcast Monitoring [3], Digitized Fingerprint [4], Transaction Tracking [5], Protection of Copyright [6], Detection of Tempering [7], Hiding of Information [8] & Authentication of Content [9] &many more.

Every methodology of digital watermarking is comprised of two algorithms: one of them is detecting algorithm while other is the embedding algorithm. These algorithm processesare executed in a same fashion for every method of watermarking. The figure 1

ISSN No: - 2456 – 2165

presents the embedding process of watermark where watermark is included into cover picture by making use of embedding algorithm. While,figure 2 presents the process of detection of watermark where the invaded watermark is obtained by algorithm of detection.

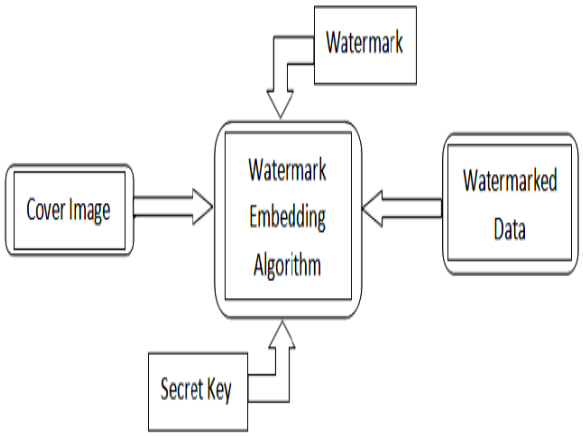

Figure 1. Watermark Embedding Process

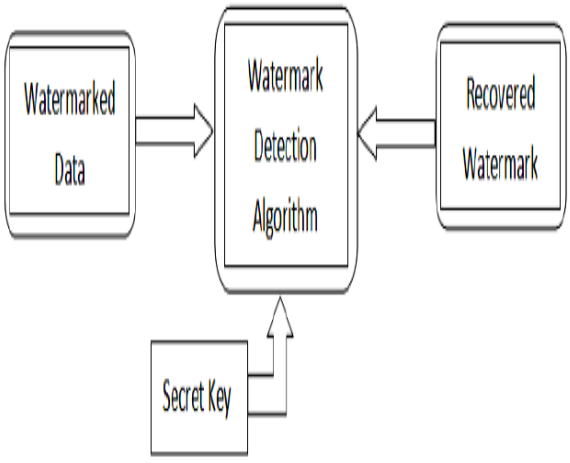

Figure 2. Watermark Detection Process

II. DIGITAL IMAGE WATERMARKING WORKING

Digital Watermarking is that kind of methodology employed in digital signal processing of the provided data that is hided into some other data of multimedia format. This data can be barely seen while a extractor or detector is able to sense the data. The digitized pictures are used for the purpose of digital picture watermarking to invade the data in secret form. The images bearing a watermark are generated. These watermarked pictures provide high level of robustness confronting the attacks. Several level of digital watermarking is presented in diagram 3. The working of digitized picture watermarking is presented in three stages [10]:

A. Embedding Stage

Embedding stage is the starting level where watermark is invaded into the actual picture by the embedding algorithm & a secret key. After this a picture that is watermarked is produced. After this, the watermarked picture gets distributed over whole network.

B. Distortion/Attack Stage

At this level the information gets spread into complete network. And it also indulges some noise in watermarked pictures or the picture confronts some kind of attacks. So, the data that is watermarked is demolished or either modified.

C. Detection/Retrieval Stage

On this level, watermark is either identified or withdrawn by a definite from the pictures that are watermarked by implementing an identification algorithm & a secret key. Furthermore, it also helps to identify any kind of noise.

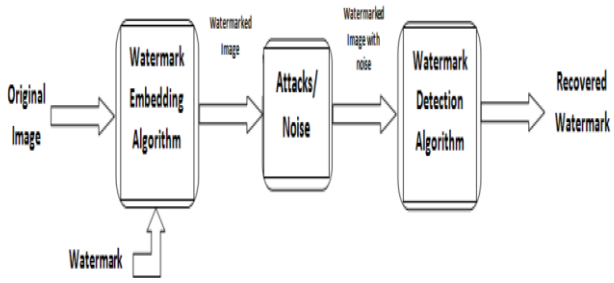

Figure 3. Stages in Digital Image Watermarking

III. DIGITAL IMAGE WATERMARKING TECHNIQUES

In the domain of digital watermarking, digitized picture watermarking has got more attraction of researchers for mainly two reasons: one is that it is readily available & the other is that it is able to transmit a lot of redundant data that can be implied to produce some kind of watermarks [11]. Digitized watermarking contains several methodologies that help to ensure security of digitized information. The complete digitized picture watermarking methodology functions into two domains in either transformation & spatial domain. The spatial domain methodology can be implemented directly over pixels. The watermark is invaded by transforming the pixels. LSBs are the spatial domains that are required in general. Transformation domain methodologies invade the watermark by modifying the coefficients transformation domain. This domain is generally incorporated in DCT, DFT & DWT. These methodologies are proven to b helpful in gaining robustness & imperceptibility in

contrast to spatial domain. Later on, explanation & the implementation of these domains are provided.

A. Least Significant Bit (LSB)

LSB is defined as a basic method for watermarking in spatial domain that incorporate a watermark in least significant bits of pixels that are selected on a random basis in a cover picture. The LSB is illustrated as [12]:

Image:
10010101 00111011 11001101 01010101….
Watermark:
1 0 1 0…..
Watermarked Image:
1001010**1** 0011101**0** 1100110**1** 0101010**0**…..

The steps opted to invade a watermark in real picture through LSB is [13]:
1) The RGB picture is transformed to gray scale.

2) The double precision are generate of the picture.

3) The MSB is shifted to the LSB of watermarked picture.

4) The LSB of hosted picture should be made zero.

5) Shifter version (as in step 3) is added to watermarked pictures to transform (as in step 4) hosted picture.

The main advantages of this technique are that it is highly easy to implement this on a picture. It also provides more perceptual transparency. No degradation in quality is observed when watermark is incorporated through LSB. The disadvantages of this technique is that it possess less robustness for general processing of signals as it is very easy to eliminate watermarks by some attacks that are done for on processing of signals. It is not so prone to noise & attacks as it is imperceptible.

B. Limitations of spatial domain watermarking

Watermarking performed over spatial domain possess more ease in contrast to transformation domain. The disadvantage occurred over spatial domain is for robustness. It don't generally implied with basic steps such as invading the noise & cropping. Other disadvantages of this technique are that this method doesn't allow sub sequential processing for improvisation of robustness in watermark.

C. Transform Domain Watermarking

The watermarking of transform domain has gained much popularity in contrast to watermarking over spatial domain. The picture is presented in terms of frequency in this domain. The watermarking methodologies working on this domain works as, initially the actual picture is transformed by a defined transformation. A watermark is invaded in the transformed picture on transforming coefficients. Lastly, inverse transformation is executed for attaining picture that is watermarked [14]. The DCT (Discrete Cosine Transform) is main implemented transforming domain technique along with DFT & DWT.

D. Discrete Cosine Transform

DCT is implemented to process the signals. It helps to transform the spatial to frequency domain. DCT is also implemented in various regions for identifying the patterns, compression of information & processing of signals. More robustness is observed in watermarking by DCT contrasting the spatial domain. The main steps included in this are [11]:

1) Segmenting the picture into non-overlapping blocks of 8x8.

2) Implementation of forward DCT to every of these blocks.

3) Implementing some of the selection criterions of block like HVS.

4) Implementing some of the selection criterions on coefficients like highest.

5) Placing watermark by transforming the chosen coefficients.

6) Implementing some of the inverse DCT transformation over every block.

As by invading the information related to watermark in a DCT, image is segmented into various bands of frequency. As shown by the figure 4. FL displays minimal frequency constituents in a block, as FH displays the constituents of higher frequency which is chosen for provided regions. Higher level of robustness is achieved by discrete cosine transformation contrasting various attacks on processing of signal. The reason is selecting the perceptual significant frequency domain coefficients.

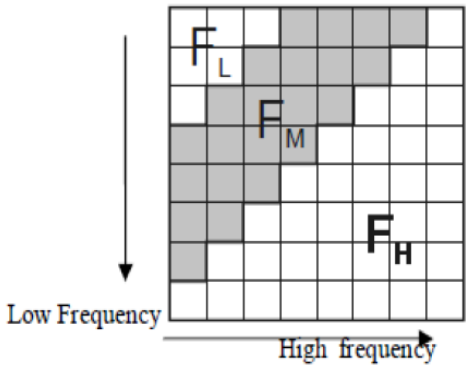

Figure 4. Discrete Cosine Transform Region

Going buy the terms of DCT, DFT, edge of picture is seen over to edge of an even function. It is the simplest transformation

over other linear transformations in the technique for processing of digitized signal. The 2D-DCT is stated as:

$$F(jk) = a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (1)$$

A relative inverse transformation (is its 2D1DCT) is stated as

$$F(mn) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (2)$$

E. Discrete Fourier Transform

DFT elaborated as Discrete Fourier Transformation furnish several challenges related to geometry, translation, scaling, testing etc. This images is segmented into sine & cosine terms by DFT. Such watermarking techniques that are formulated over DFT incorporate two types: one of the embedment is formed over a template while other is done straightly. A technique that invades the watermark straightly is executed by transformation of magnitude of DFT & coefficients of phase.This technique to embed is based upon templates that elaborate the working of templates. A template is that structure that is incorporated in domain of DFT for approximation of DFT to estimate the transformational factor. By the transformation of image, resynchronization of picture takes place & a detector is allotted that will extract the invaded spread spectrum watermark [11]. The DFT is used for periodic & digitized signals on function of f(x) i.e. discrete time. The DFT obtained for signal having a period M is [1]:

$$F(u) = \sum_{x=0}^{M-1} f(x)e^{-\frac{j2\pi ux}{M}}$$

IDFT i.e. Inverse Discrete Fourier Transform is presented as:

$$f(x) = \frac{1}{M}\sum_{u=0}^{M-1} F(u)e^{\frac{j2\pi ux}{M}}$$

IV. PROBLEM STATEMENT

By rapid enhancement & application of Interne, several issues are faced up during the transmission of data as they possess a threat to security. A secure & safe path is preferred by the users to relay any data. Here, the digital watermarking method proves to be a fine method to hide the data that ensures its security also. A method of watermarking is presented in this base document that LSB, steps & process with MATLAB pictures. This technique is worth noting for ensured watermarking. There is a scope of improvisation in its performance.

V. PROPOSED METHODOLOGY

The technique of digital watermarking is incorporated for hiding the data in a signal that cannot be extracted over a 3rd party. Its main application is to protect the copyright of digitized data. There is a difference in this & encryption is that viewing, accessing & interpretation of signal is possible in this methodology but retains the ownership of information. The base document explains a methodology for watermarking that is termed as LSB (least significant bit), its procedure & process with pictures of MATLAB. A watermarking technique is based on DWT for retaining the quality & security of pictures.

A.Discrete Wavelet Transform

Discrete Wavelet Transformation of an image that is also termed as DWT presents a picture in different resolutions. The representation of multi-resolution explains a general layout to clarify the information contained in a picture. The signals incorporated in multi-resolutions were classified by DWT. The image is diversified in quadrants of low & high frequency with the help of SWT. Also, the quadrant of low frequency is further segmented into high & low frequencies & this process goes on till the time the complete signal don't get decomposed totally.

A single DWT segments a 2D image in four quadrants. One of the regions comprises low frequency of actual image; right top is comprised with the information regarding horizontal way of image, left bottom region contains the information regarding vertical path & right bottom comprises greater frequency of real image. Robustness is observed in coefficients of lesser frequencies with invaded watermarks as it comprises a lot of data about the real image [2]. Reforming the real image from distorted image is performed by IDWT [16].

Scaling of digitized wavelet is performed. DWT is majorly implemented in the watermarking of digitized images as it has gradual spatial localization & multi resolution techniques. It is highly convenient to detect a region in cover image by characteristics of spatial localization by which invasion of watermark is performed very technically.

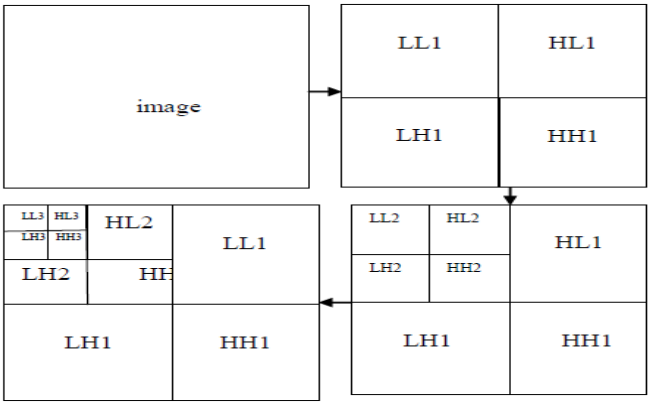

Fig 5:- Discrete Wavelet Decomposition

B. Walsh-Hadamard Transform

Walsh in 1923 introduced a complete set of orthonormal square wave functions to represent these transforms. The computational simplicity of the Walsh function is real and takes only two values which are either +1 or -1. It can be applied to only for images when $N = 2^n$.This is one of the important orthogonal transform .FWHT had been found in many areas of digital filtering, face recognition, image watermarking and communications, for example multicarrier Code Division Multiple access(CDMA) and multiband OFDM(Orthogonal frequency Division multiple access).[4]. HT is useful in signal and image processing applications in which real time implementation become a crucial issue. It has the lowest computational cost among all the existing discrete orthogonal transforms. Forward Walsh-Hadamard transform kernel is given as

$$g(x, y, u, v) = \sum_{i=0}^{n} (-1)^{[b_i(x)b_{n-1-i}(u) + b_i(y)b_{n-1-i}(v)]}$$

Inverse Walsh-Hadamard transform kernel is given as

$$h(x, y, u, v) = \sum_{i=0}^{n} (-1)^{[b_i(x)b_{n-1-i}(u) + b_i(y)b_{n-1-i}(v)]}$$

Walsh transform has the advantage of less computational complexity and nearly identical forward and inverse Kernels and it is computed by a fast successive doubling methods. The algorithm shows robustness against compression at low quality factor. The orthogonal rows and columns are independent . Walsh is robust for image modification than other popular transforms because i latter the values of pixels in block are changed by different amount due to the multivalve kernels. So it is better suited for real time implementation in hardware. The Discrete Walsh- Hadamard transform is used in literature for watermarking images. In Ref. [13], it is mentioned that Hadamard transform packs most of the energy into the upper left corner of the transformed matrix . In that paper, it is made clear that in high frequency band, Hadamard coefficients are more immune to noise and many high frequency coefficients of Hadamard transform have the values of lower or middle band coefficients of DCT. So only room left for watermark embedding in middle and high frequency bands of transformed image. The watermarking is done based on Multi-resolution Walsh-Hadamard transform and SVD. It describes about how to decompose an image using Multiresolution Walsh- Hadamard Transform (MR-WHT) and then middle singular values of high frequency sub-band at the finest and the coarsest level are modified with Singular values of watermark. The process of watermark embedding involves, performing L-level MRWHT at the finest level and then apply SVD on both HH sub-band and watermark image. Modify the middle singular values of the HH sub-band and perform inverse SVD to construct the watermarked HH sub-band and it is placed in its original position and Llevel inverse MR-WHT is performed to get the watermarked image. The limitation of the scheme is even after and before embedding watermark in mutiresolution Walsh transform it is observed that the peak signal to noise ratio remain fixed. An adaptive invisible watermarking scheme is proposed in DCT domain in which the scaling parameter is calculated through empirically chosen value.

The number of salient regions to be captured and the size of each region are fixed adaptively for each image. An improved quantization is used to embed the watermark in the DC coefficients. Finally, an edge map of one of the ROI is embedded into DWT domain of the watermarked image. The major contribution of the work is that it uses adaptive mathematical model using sigmoid function that inserts watermark either visibly or invisibly based on user's requirements by adjusting the controlling parameter.

C. Singular Value Decomposition

It is a mathematical tool widely used in image compression, retrieval and watermarking. According to it, every real matrix A can be decomposed into a product of three matrices, U, S, V where $UU^T = I$, $V V^T = I$ and S is a diagonal matrix containing largest singular values. The singular values above rank of matrix is zero.

$$A = USV^T$$

In SVD singular values represent the luminance of the image layer and singular vectors represent the geometry of the image. The main advantage of the SVD is the largest singular values preserve most of the energy and are resistant to small perturbations and there by immune to most of the signal processing and image compression operations. Multiresolution Walsh Hadamard transform is obtained by Zigzag scanning of the Walsh Hadamard transform coefficients as shown in Fig. 6.The transformed image after application of zigzag scanning is shown in Fig. 6. In Walsh transform the sequency is in ascending order. Sequency means the number of transitions in each row or column. This is analogues to frequency in Discrete Fourier transform. Zero sequency corresponds to DC and high sequency corresponds to AC components of image. A walsh transform can cause DC or low frequency components on upper triangle and arrange the remaining coefficients in zig-zag sequence from low frequency to high frequency. Low frequency component of image packs most of the energy and low sequence middle singular values are suitable for robust hiding of watermark.

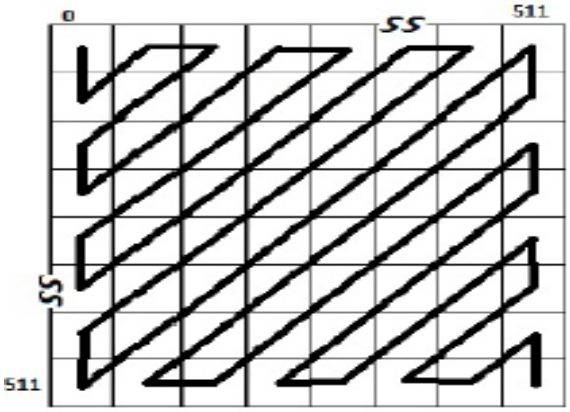

Fig. 6.Zig-Zag Scanning of Walsh-Hadamard Coefficients

Fig. 7. Multi Resolution image Obtained after zig-zag Scanning of pixel Coefficients in Lena image

It has been observed that similar to [18] as in DCT, the low frequency band coefficients of Walsh-Hadamard transform are in upper triangle and high frequency components are in lower triangle. The coefficients of FWHT2 is divided into 4 quadrants Q1, Q2, Q3 and Q4 and they represent frequencies in lower to higher frequencies-LL, LH, HL and HH bands as shown in 3 In this paper, entropy is used for selecting appropriate blocks for robust embedding of watermark. It is a statistical measure of randomness and a measure of texture in image.

$$E = -\sum PlogP$$

C. Watermark Concealing Algorithm

The step by step watermark concealing algorithm is illustrated in Fig.8

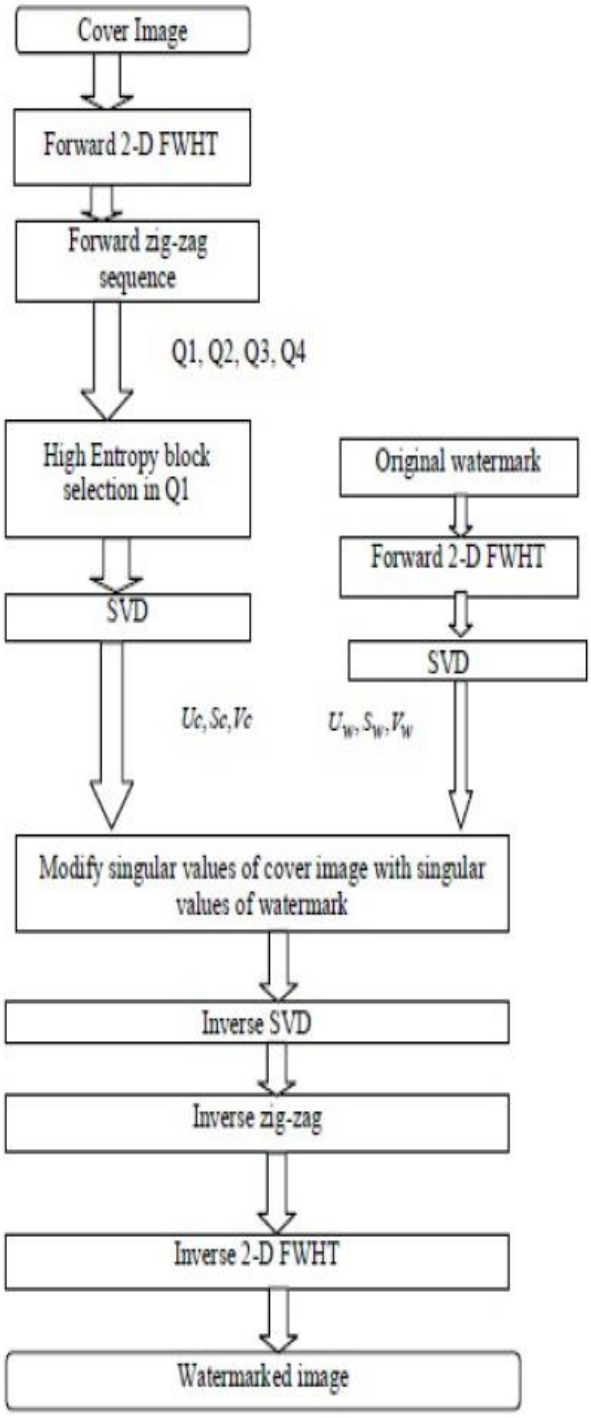

Fig. 8. Watermark Concealing Algorithm

Step 1:- Apply fast Walsh-Hadamard transform to host image A.

$$B = FWHT2(A)$$

Step 2:- Arrange coefficients in zigzag sequence and map them into 4 quadrants: Q1, Q2, Q3, and Q4.

Step 3:- Divide Q1 block into non overlapping blocks of 64 × 64.

Step 4:- Apply Singular value Decomposition for high entropy blocks.

$$[Uc, Sc, Vc] = SV D(B)$$

Step 5:- Apply fast Walsh-Hadamard transform to the whole visual watermark W .

$$C = FWHT2(W)$$

Step 6:- Apply SVD to the Walsh-Hadamard coefficients of watermark.

$$[Uw, Sw, Vw] = SV D(C)$$

Step 7:- Singular values of watermarked image is obtained by singular values of B and singular values of watermark using the equation below

$$S_{wa} = S_c + k \times S_w$$

Step 8:- Apply inverse SVD.

$$B_{new} = U_c S_{wa} V_c^T$$

Step 9:- Apply inverse Walsh-Hadamard transform.

$$A_w = IFWHT2(B_{new})$$

D. Watermark Extraction Algorithm

The step by step watermark extraction algorithm is illustrated in Fig.9

Step 1:- Apply fast Walsh-Hadamard transform to host image A and watermarked image $A*$.

$$B* = FWHT2D(A*)$$

Step 2:- Arrange coefficients in $Q*$ into zigzag sequence and map them into four quadrants: Q1W, Q2W,Q3W and Q4W.

Step 3:- Divide Q1W block into non overlapping blocks of 64 × 64.

Step 4:- Apply Singular value Decomposition for high entropy block in Q1W.

$$[Uwa, Swa, Vwa] = SV D(Q1W)$$

5) Obtain singular values of watermark from singular values of watermarked and host image.

$$S_{we} = (S_{wa} - S_C)/K$$

6) Apply inverse SVD.

$$W_{ext} = U_w S_{we} V^T_w$$

7) Apply inverse Walsh-Hadamard transform.

$$W_{ext1} = IFWHT2(W_{ext})$$

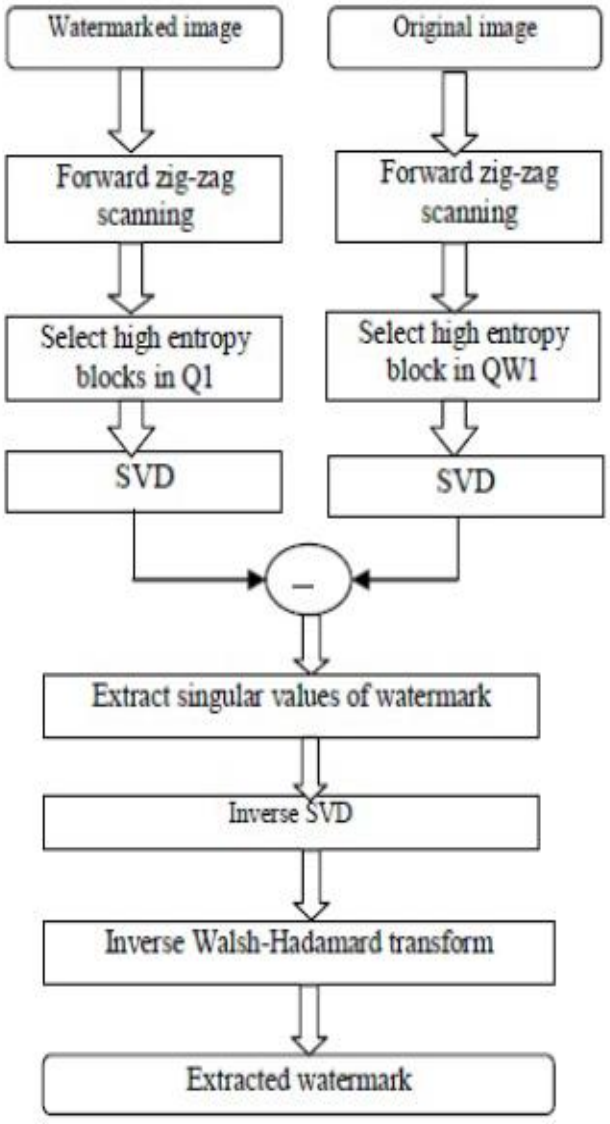

Fig. 9. Algorithmic steps for watermark Extraction algorithm

VI. CONCLUSION

Several numbers of methodologies are implemented in watermarking for the purpose of security.Spread Spectrum, Spatial domain&Frequency domain. In the base document, a spatial domain technique is implemented LSB to secure the pictures, that is simple & easy & puts more impact. This LSB process is very easy to use when it is incorporated with LSB.The different picture in MATLB explains a different type of process step & it outcome. In coming future, various other sorts of data & tests can be performed by LSB on several pictures. The technique of DWT watermarking will be implemented for enhancement of performance of watermarking from base document.

REFERENCES

[1] Avani Bhatia, Mrs. Raj Kumari"Digital Watermarking Techniques".

[2] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011

[3] Brigitte Jellinek, "Invisible Watermarking of Digital Images for Copyright Protection" University Salzburg, pp. 9 – 17, Jan 2000.

[4] Chiou- Ting Hsu; Ja-Ling Wu; Consumer Electronics "DCT-based watermarking for video", IEEE Transactions on Volume 44, Issue 1, Feb. 1998 Page(s):206 – 216

[5] Cox, Miller and Bloom, "Digital watermarking", 1st edition 2001, San Fransisco: Morgan Kaufmann Publisher

[6] DarshanaMistry "Comparison of Digital Water Marking methods"(IJCSE) International Journal on Computer Science and EngineeringVol. 02, No. 09, 2010, 2905-2909

[7] Dr. Martin Kutter and Dr. Frederic Jordan, "Digital Watermarking Technology", AlpVision, Switzerland, pp 1 – 4M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, International Journal of Modelling and Simulation, 18(2), 1998, 112-116.

[8] H.Arafat Ali, "Qualitative Spatial Image Data Hiding for Secure Data Transmission", GVIP Journal,Volume 7,Issue 2 , pages 35- 37, 2, August 2007

[9] Max Sobell"LSB Digital Watermarking",CPE 462

[10] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9 (September 2012) ISSN 2229-5518

[11] R.AARTHI, 2V. JAGANYA,&3S.POONKUNTRAN "Modified Lsb Watermarking For Image Authentication" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012

[12] Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[13] Yeuan-Kuen Lee1, Graeme Bell2, Shih-Yu Huang1, Ran-Zan Wang3, AndShyong-JianShyu "An Advanced Least-Significant-Bit EmbeddingScheme for Steganographic Encoding" Springer-Verlag Berlin Heidelberg 2009.