Watermarking Embedding procedures in Middle Frequency Coefficients

[1]Mr. Kesava Reddy, [2]Prof. T. Bhaskara Reddy
[1]Research Scholar in Department of Computer Science and Technology, Sri Krishnadevaraya University Anantapur
[2]Professor in Department of Computer Science and Technology, Sri Krishnadevaraya University, Anantapur

Abstract: In this paper, a block DCT based algorithm is developed to embed the watermark into the images. Fig.2 will give complete idea of watermark embedding. Let X be the original gray – level image of size LI x La and the digital watermark W be a binary data of size $M_1 \times M_2$. During the embedding stage, the host image is first transformed to a spectral domain that facilitates data embedding by modifying the middle frequency range. For this process, the resolution of a watermark image W is assumed to be smaller than that of the original image X. For each 8 × 8 image block, only (64 X ($M_1 \times M_2$ / $L_1 \times L_2$) coefficients will be used for watermark embedding. The ratio of ($M_1 \times M_2$) and ($L_1 \times L_2$) determines the amount of information to be embedded into the images.

Key Words: DCT, Embedding, Watermark Image.

1.INTRODUCTION : Different watermarking applications have different requirements. In the following, we present some application scenarios described by Cox [8] and other authors. For image data authentication, the embedded watermark has to be invisible to a human observer and it should be altered (or broken) by virtually any intentional modification of the image[1]. Furthermore, it should be difficult to insert a false watermark and the watermarking scheme should be able to indicate regions where alterations in the image have taken place. Several image copyright protection application scenarios are possible. First, the owner of an image can embed an invisible, robust and quickly extractable watermark to identify unauthorized copies. Finally, the copyright holder (the seller of an image) might also want to know which customer leaked an unauthorized copy of the data. Here, fingerprinting and circulation tracking techniques come into play to identify not only the seller but also the buyer of an image.(by using image tagging technique) To this aim, some additional requirements are necessary.

1.1Water Marking Process : Image watermarking imperceptibly embeds the data into a original image (host image). The general process of image watermarking is depicted in fig. 1. The original image (host image) is modified using binary data to create the watermarked image. In this process, some error, (or) distortion is introduced. To ensure transparency of the embedded data, the amount of image distortion due to the watermark embedding process has to be small. The watermarked image is then distributed and may circulate from legitimate to illegitimate customers. Thereby, it is subjected to various kinds of image distortion. Image distortion may result from e,g, lossy image compression, re–sampling (or) from specific attack on the embedded data.

Note, that we do not discuss visible watermarking in this work. The methodology for visible is very different from invisible watermarking. Our focus is on invisible or, better, imperceptible watermarks.

The extraction process may (or) may not depending on the nature of application, require knowledge of the original host image to estimate hidden binary data from the distorted image that is received. The

watermark is recovered from the watermarked image. It is desired that the difference between the extracted and original watermark is as low as possible.

In order to see the different aspects of the watermarking problem, depending on the particular application and the application' requirements, we have to refine the general watermark model (fig.1) and have a closer look at the successive stages of the watermarking problem[2]. These stages comprise The Embedding stage (fig. 2) The extraction stage (fig. 6) The distribution stage The decision stage

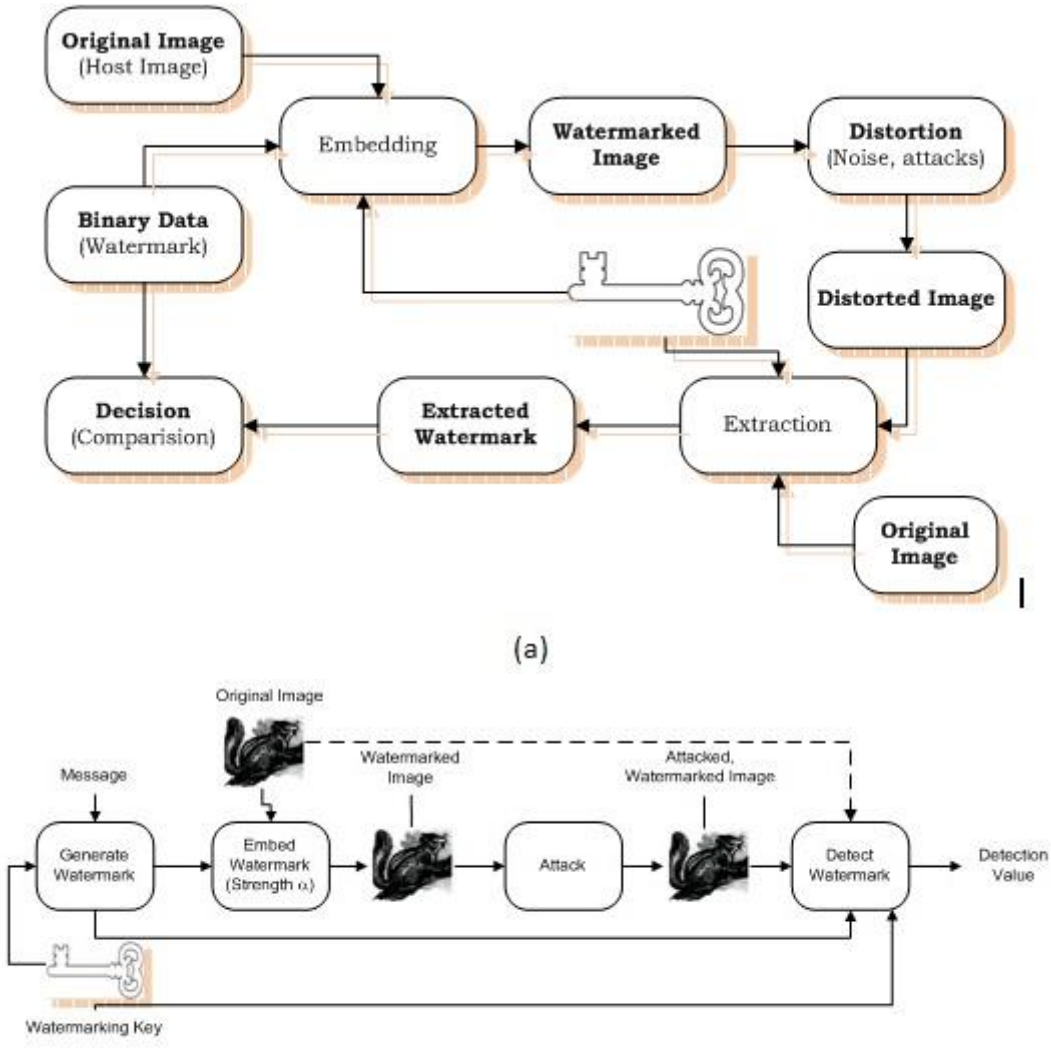

Fig.1 : The Data–Hiding model a general overview

1.2. Embedding stage : Except for some very early watermarking schemes (Spatial domain methods), all robust watermarking schemes operate in a transform domain that offers access to the frequency components of the host image. By omitting the transform step and performing data embedding step in the spatial domain, one can design a simple and computational efficient algorithm for watermarking.

In the embedding stage, the host image is therefore first transformed to a domain that facilitates data embedding. This work exclusively considers the DCT(discrete cosine transform)[3] . Other commonly used frequency domain representations can be obtained by the Wavelets or the DFT (discrete Fourier transform). Section 2.10.2. discusses some of the rational that makes an image's frequency representation a favorable playground for watermark embedding.

The original watermark may be a signature data (also called the message), a small image (a "logo") and a binary data. In this work binary data as our watermark. (size of the watermark must be less than the original size of the image)

Next, the subject of the transform coefficients is modified according to the binary data. Optionally, we can employ a model of human perception to weight the strength of the embedding modification. Note that by choosing a suitable frequency transform domain and selecting only certain coefficients (middle – frequency range). The better the image transform approximates the properties of HVS, the easier is to put more energy in the embedded signal without causing perceptible distortion. (see section 1.3. for more details about modeling certain properties of the human visual system) Finally, the inverse transformation is applied on the modified transform domain coefficients to produce the water marked image.

1.2.1 Watermarking Embedding procedures : In this stage, a block DCT based algorithm is developed to embed the watermark into the images. Fig.2 will give complete idea of watermark embedding.

Let X be the original gray – level image of size LI x La and the digital watermark W be a binary data of size $M_1 \times M_2$. During the embedding stage, the host image is first transformed to a spectral domain that facilitates data embedding by modifying the middle frequency range. For this process, the resolution of a watermark image W is assumed to be smaller than that of the original image X. For example, for each 8 × 8 image block, only (64 X ($M_1 \times M_2$ / $L_1 \times L_2$) coefficients will be used for watermark embedding. The ratio of ($M_1 \times M_2$) and ($L_1 \times L_2$) determines the amount of information to be embedded into the images.

The original image X and digital watermark W are represented as

$$X = \{x(i, j), 0 \leq i < L_1, 0 \leq j < L_2\} \quad (3)$$

Where $x(i, j) \in \{ 0, \text{-------} \text{-------}, 2^L - 1\}$ is the intensity of pixel x (i, j) and L is the number of bits used in each pixel.

$$W = \{w(i,j), 0 \leq i < M_1, 0 \leq j < M_2\}$$

Where $w(i,j) \in \{0, 1\}$

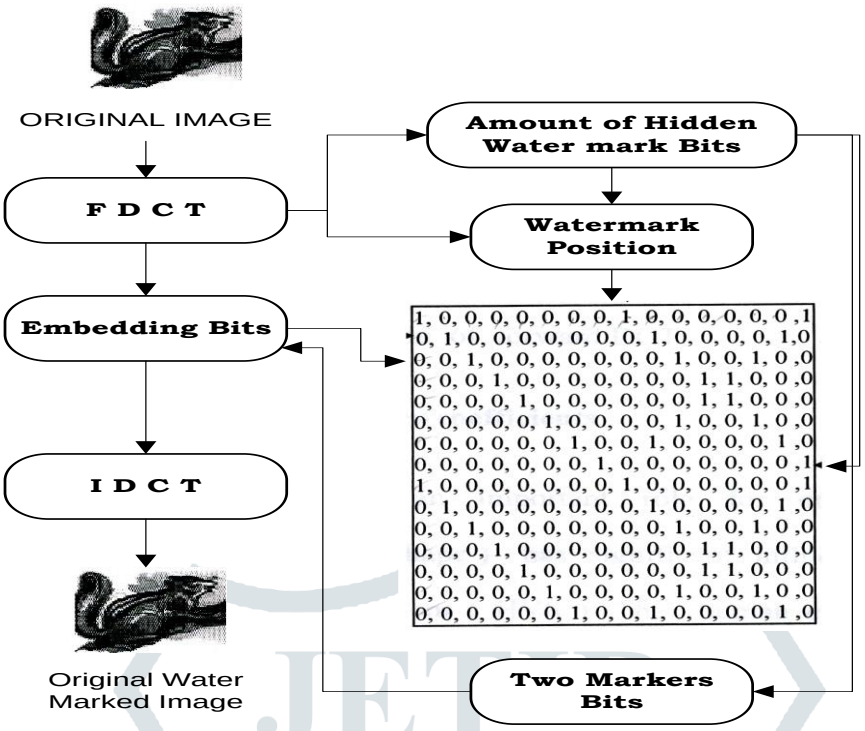

Figure 2 : WATER MARK EMBEDDING PHASE

In X, there are $L_1/8 \times L_2/8$ image blocks with size 8×8. To obtain the same number $L_1/8 \times L_2 / 8$ of blocks as the image X, the water mark W is decomposed into several blocks with size $(M_1 \times 8/ L_2) \times (M_2 \times 8/ L_2)$. For example if $M_1 = L_1/4$ and $M_2 = L_2/4$, the block size of the watermark is 2×2 and if MI = Li/8 and $M_2 = L_2/8$, the block size of the watermark block is 1×1. The extra columns and rows might be added to complete each image and watermark blocks.

1.2.2 Block Transformation of the Image

The commonly used frequency domain transform is discrete cosine transform (D C T) which was used by JPEG[5]. The input image X is divided into blocks of 8x8, and each block is DCT transformed independently. That is

$$Y = FDCT(X)$$

Where FDCT denotes the operation of forward DCT.

1.2.3. Choice of Middle – frequency coefficients

Human visual system plays an important role for embedding of watermark. The spatial frequency (shape) has significant influence on the sensitivity of Human Visual System (HVS) . The human eye is more sensitive to low – frequency noise. In contrast, high – frequency noise is less visible. However, the energy

of most natural images are concentrated in the lower frequency range, and the information hidden in the higher frequency components might be discarded after quantization operation of lossy compression. In order to embed the watermark that can survive lossy data compression a reasonable trade – off is to embed the watermark into the middle – frequency range . Only '2' coefficients are selected out of 64 DCT coefficients from each 8x8 image block of image size ($L_1 \times L_2$).

$$Yr = Reduce\ (Y)$$

Where

$$Y = \{y(k \times 8 + i, 1 \times 8 + j), 0 \le k < L_1 / 8, 0 \le 1\ L_2/8, 0 \le i < 8, 0 \le j < 8\ \}$$

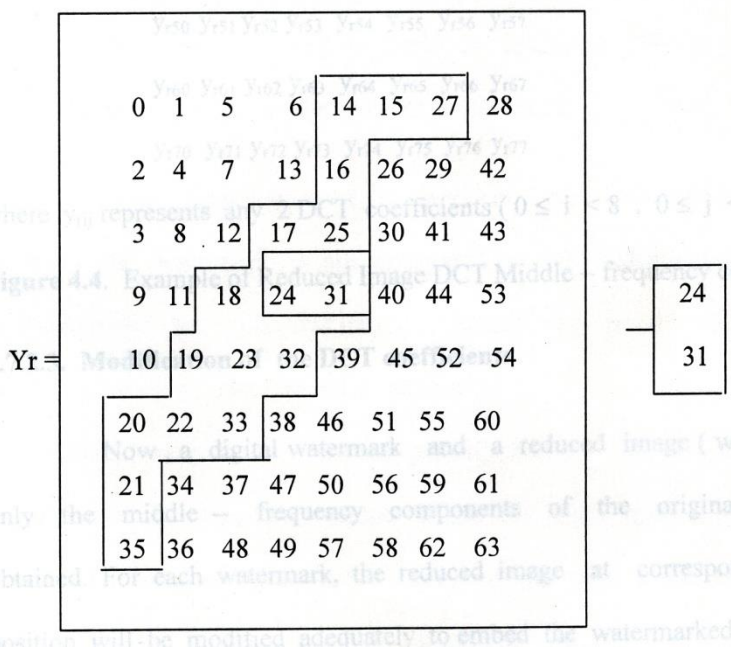

Figure 3 Example of defining the middle frequency coefficients (inner box region)

From the inner box region any two coefficients are selected from each 8 x 8 image block of original image size (LI x LI). In this paper (3,3) & (3,4) coefficients are selected. This can be done for entire original image as follows

$$Yr = \begin{matrix} y_{r00} & y_{r01} & y_{r02} & y_{r03} & y_{r04} & y_{r05} & y_{r06} & y_{r07} \\ y_{r10} & y_{r11} & y_{r12} & y_{r13} & y_{r14} & y_{r15} & y_{r16} & y_{r17} \\ y_{r20} & y_{r21} & y_{r22} & y_{r23} & y_{r24} & y_{r25} & y_{r26} & y_{r27} \\ y_{r30} & y_{r31} & y_{r32} & y_{r33} & y_{r34} & y_{r35} & y_{r36} & y_{r37} \\ y_{r40} & y_{r41} & y_{r42} & y_{r43} & y_{r44} & y_{r45} & y_{r46} & y_{r47} \\ y_{r50} & y_{r51} & y_{r52} & y_{r53} & y_{r54} & y_{r55} & y_{r56} & y_{r57} \\ y_{r60} & y_{r61} & y_{r62} & y_{r63} & y_{r64} & y_{r65} & y_{r66} & y_{r67} \\ y_{r70} & y_{r71} & y_{r72} & y_{r73} & y_{r74} & y_{r75} & y_{r76} & y_{r77} \end{matrix}$$

where y_{rij} represents any 2 DCT coefficients ($0 \le i < 8, 0 \le j < 8$)

Fig. 4. Example of Reduced Image DCT Middle – frequency coefficients

1.2.4. Modification of the DCT coefficients

Now, a digital watermark and a reduced image (which contains only the middle -- frequency components of the original image) are obtained. For each watermark, the reduced image at corresponding spatial position will be modified adequately to embed the watermarked pixels[6].

In our opinion, embedding each watermarked pixel by modifying the polarity between the corresponding pixels in the neighboring blocks is an effective approach too achieve the invisibility and survival for compression

1.3. Residual polarity reversing

In most related literature, the water mark bits are added to the selective coefficients of the transformed image. The watermark can only be "detected" by employing the "detection theory" if the verification is necessary. Restated, the selective coefficients of the image in question are subtracted from those of the referenced image. Then, the similarity between the difference image and the specific watermark is evaluated on the basis of a pre – defined threshold to determine whether (or) not the image in question contains the specific water mark.

A residual mask is used to perform the embedding procedure. Restated, the watermark is not embedded as an additive noise. Instead, the watermarks are embedded into the 'neighboring relationship' within the transformed images. The procedure as follows.

Initially, compute the residual polarity between the neighboring pixels according to the specified residual mask. For each marked pixels of the water mark, swap the relevant coefficients of the host image such that the residual polarity of the modified sequence becomes the reverse of the original polarity (i.e. the "NOT" operation for binary sequence). For instance, according to fig. 5., A = B = C = 0; D = –1; E = l;, that is, the residual polarity is set as "1" if the coefficient of the current pixel exceeds that of the former one and is set as "0" otherwise. For each marked pixel, modify the associated host coefficient so that the residual polarity becomes the the reverse of the original polarity. During the extraction procedure, perform the exclusive –or (XOR) operation upon the polarities from the original and modified sequences to obtain the extracted outcome.

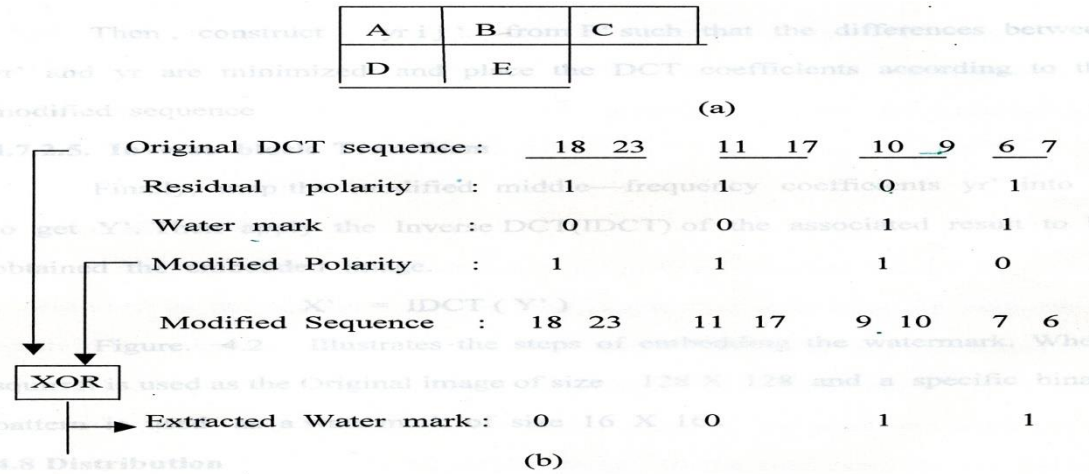

Figure 5 : (a) The residual mask, Where each square includes a pixel and position 'E' denotes the current pixel, 'D' represents the former pixel, and so on. (b) An example of embedding and extraction based on the reversal of polarity

In this example, we set A = B = C = 0, D = –1, E = 1, that is, if the transformed coefficient of current pixel exceeds that of the former one, then the residual polarity is set as "one ", otherwise, the polarity is set as "zero".

$$P = \text{Polarity } (y_{rij})$$

$$\text{And } P' = XOR(P, W_b)$$

Then, construct yr i j 'from P' such that the differences between yr' and yr are minimized and place the DCT coefficients according to the modified sequence

1.3.1. Inverse block Transform

Finally, map the modified middle—frequency coefficients yr' into Y to get Y'. Then apply the Inverse DCT(IDCT) of the associated result to be obtained the embedded image.

$$X' = IDCT(Y')$$

Fig.2 Illustrates the steps of embedding the watermark. Where squirrel is used as the Original image of size 128X 128 and a specific binary pattern is used as a watermark of size 16 × 16.

1.4 Distribution

The watermarked image is then distributed –for example published on a web server (or) sold to a customer. During transmission and distribution of the watermarked image, not only adds distortion to the host image but also transmission errors and common image processing tasks, such as, enhancement, re – sampling, etc., contribute errors to the watermarked image. Especially geometric image manipulation like scaling, rotation, has been proved to be very harmful to the embedded watermark. All manipulation of the watermarked image data has to seen as an attack on the embedded information. Modification that occur during normal image processing are called coincidental attack, while attack that attempt to weaken, remove (or) alter the watermark itself are termed intentional attacks. We characterize a number of attacks and describe counter – measures that can be taken by the watermarking system.

1.5 Extraction stage

Eventually, after the watermarked image has undergone severe distortion as described in the previous section, one would like to extract the embedded signature from the host data. This can be done by the party that embedded the watermark, the customer that received the image, a designated party – such as a Web crawler that scan the Internet for illegal copies of the protected work or a legal prosecution official – or by a third party. In the first case, the secret key used to embed the watermark as well as the original image might

be available. This tremendously facilitates the watermarking system and makes watermark detection relatively straightforward. We call detection systems that have access to the secret (private) key and original image non–oblivious, non–blind or private watermarking systems.

The other extreme is the case where neither the private key nor the original image is available during the extraction process. These watermarking systems are called public key watermarking systems. However, no reliable public –key watermarking system is known to work and it is likely that no such system can ever be built. Recently, also asymmetric watermarking schemes have been proposed that use different keys for embedding and detecting the watermark

A watermarking scheme that allows to extract the signature data without reference to the original, unwatermarked, image (host) is dubbed blind or oblivious watermarking scheme. There are also detection or extraction methods that rely on some data or features derived from the original host image. These schemes have been named semi–blind or semi–oblivious watermarking algorithms.

To summarize these important distinctions based on the availability of the original image, there are

- Blind or oblivious (public watermarking)
- Semi–blind (semi – private) and
- Non–blind or non–oblivious (private watermarking)

1.5.1. Watermarking extracting Procedures

The extraction of watermark requires the original image. Fig. 6 will give complete idea of watermark extraction. The extraction steps are described as follows

1.5.2. Block Transformation

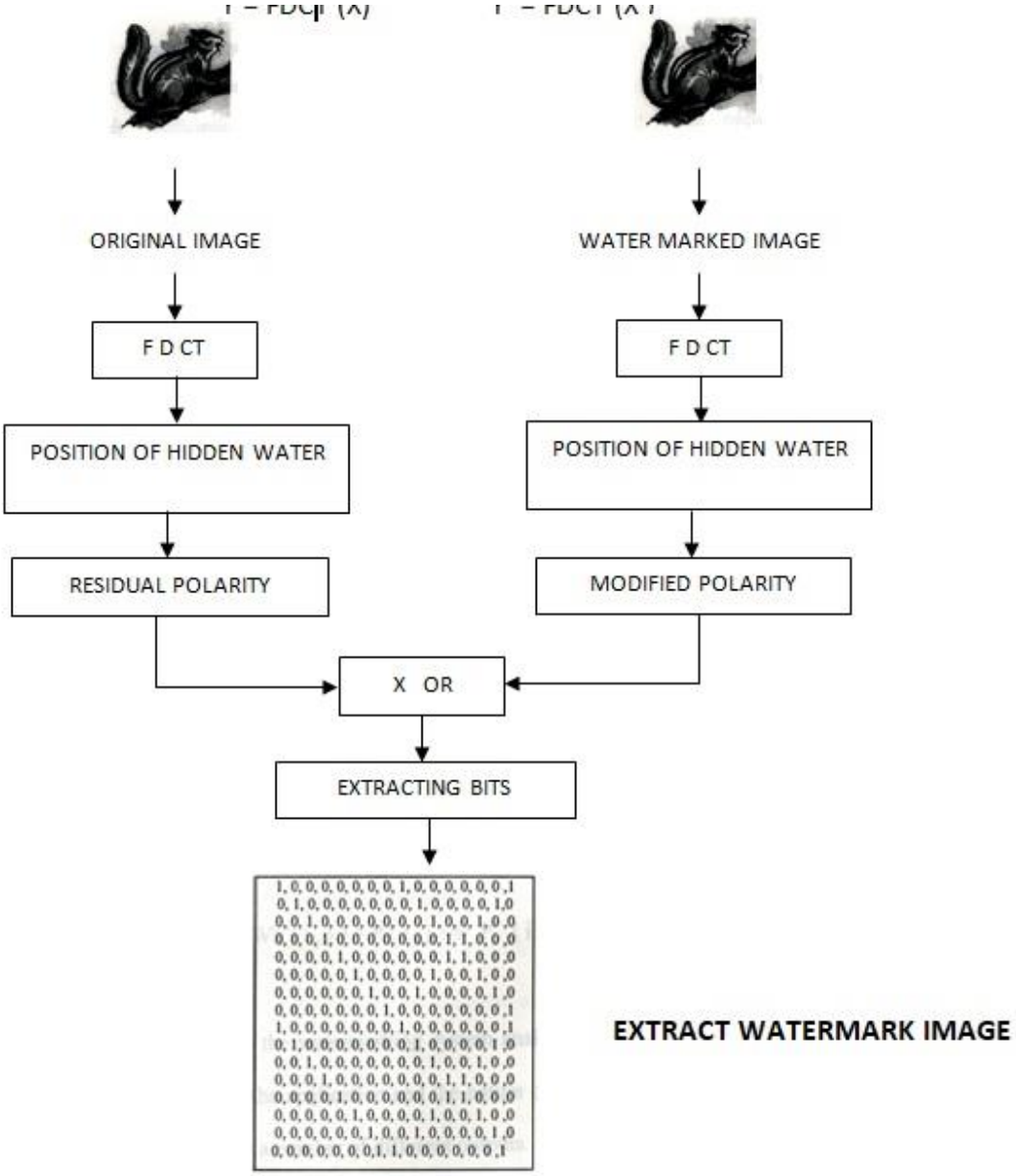

Figure.6. WATERMARK EXTRACTING PHASE

1.5.3. Extract the data

Perform Exclusive – OR (XOR) operation on these two polarity patterns to obtain a binary data i.e.

$$W = XOR (P, P')$$

Where

$$Wb' (i,j) = P(i, j) \oplus P' (i, j)$$

1.6 CONCLUSION

In the decision stage, the watermarking system analyzes the extracted data. Depending on the type of the application and the nature of the signature data, the decision stage can produce a number of different outputs. for image copy protection applications, the output of the watermarking system can range from simple to more complicated answers. In the simplest case, the result is just a yes/no decision indicating if the copyright holder's mark has been found in the received image data. More complex systems return the embedded logo image or the textual copyright information that was placed into the host image data. A widely used similarity measure between the original, W, and the extracted watermark sequence, W* is the normalized correlation. Image labeling and data hiding applications will typically try return the message originally embedded. Since message corruption can not be tolerated, the use of error–correcting codes is mandatory for this type of application.

References:

1. M. Alghoniemy, A.H. Tewfik Geometric distortion correction in image watermarking Proc. SPIE Security and Watermarking of Multimedia Contents II, 3971 (2000), pp. 82-89
2. D. Kundur and D.Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition," Speech and Signal Processing Proceedings, Acoustics, pp. 2969-2972.
3. L. Rajab, T. Khatib and A. Haj, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science, Vol. 3, 2002, pp. 740-749.
4. M. Jiansheng and L. Sukang, "A Digital Watermarking Algorithm Based on DCT and DWT," International Sym- posium on Web Information System and Application (WISA), 2009, pp. 104-107.
5. Bender W, Gruhl D, Morimoto N, Lu A. Technique for data hiding.*IBM Systems Journal*, 1996, 35(3&4): 313–335.
6. .Swanson D, Tewfik H. Multimedia data—Embedding and watermarking technologies. In*Proc. the IEEE*, 1998, 86(6): 1064–1087.

Authors

Dr.T.BhaskaraReddy is a Professor in the department of Computer Science and Technology at S.K University, Anantapur A.P. He holds the post of Deputy Director of Distance education at S.K.University and He also the CSE Coordinator of Engineering at S.K.University. He has completed hisM.Sc and Ph.D in computer science from S.K.University. He has acquired M.Tech from Nagarjuna University. He has been continuously imparting his knowledge to several students from the last 17years. He has published 55 National and International publications.10 International conferences.13 National conferences. One UGC Major ResearchProject. Attended several seminars in 3 countries. He has completed major research project (UGC).

E-Mail:bhaskarreddy_sku@yahoo.co.in

Mr. Kesava Reddy is a research scholar in SK.university. He completed M.C.A in sri krishnadevaraya university. He joined as research scholar in 2011 and he has research experience of nearly 7 years.