Implementation of Secret Information Hiding over Colour Image using Frequency Domain Technique

A.C.Suthar[1], C.B.Patel[2], Dr. Kulkarni G.R.[3], Dr. Shah D.J.[4]
[1]Research Scholar, Dept. of E.C.E., KSV University, Gandhinagar, Gujarat, India
[2,4]Department of E.C.E., L. C. Institute of Technology, GTU, Mehsana, Gujarat, India
[3] C. U. S. C. Engineering and Technology, GTU, Wadhwan, Gujarat, India
([1]acsuthar@ieee.org, [2]chiragkumar.patel.ec@lcit.org, [3] grkulkarni29264@rediffmail.com, [4]djshah@lcit.org)

Abstract - **Digital watermarking is used to defend the intellectual property privileges in the multimedia. Various algorithms are utilized to embed digital multimedia data such as video, image or audio using undetectable information of its proprietor. In this paper, we put into practice tenable model for colour image using frequency domain method. We use discrete cosine transform scheme for binary entrenched in red, green and blue components of colour image. The extraction is done from the secured colour image. Colour secured image has greater advantage due to three component planes of the image. Embedded message is damaged due to any intentional or unintentional attack in one component plane then it can be extracted effectively from the supplementary two component planes.**

Keywords - **digital image watermarking; spatial domain watermarking; frequency-domain watermarking; discrete cosine transform**

I. INTRODUCTION

Transmission and exposure of digital products like digital images, video, audio and multimedia applications is moderately apprehensive. Our aims to provide efficient solution for violate the intellectual property privileges in multimedia. Imperceptible watermarking of the digital media has been proposed as a particular solution to protect the copyright property of the legal owner or provider.

This effortlessness of digital multimedia allotment over the Internet, simultaneously with the prospect of unlimited duplication of this information, threatens the intellectual property privileges more than ever. Thus, property owners are willingly in the hunt for technology that guarantee to guard their privileges. Cryptography is probably the most frequent used technique for shielding digital property from the time when it has an entrenched theoretical foundation and developed very effectively as a science. The digital property is encrypted prior to delivery and a key is provided to the legitimate owner (who has paid for it). However, the vendor is incapable to determine how the product is handled after it is decrypted by the consumer. Encryption protects the content during the transmission only. When transmitted to the receiver, data must be decrypted in order to be important.

Once decrypted at the receiver, the data is no longer protected and it becomes vulnerable. The purchaser may turn out to be a reproduce distributing illegitimate copies of the decrypted content. Consequently, encryption obligation is complemented with a technology that can persist to shield the valuable content even after it is decrypted. This is the spot where watermarking is introduced for shielding of content.

Digital watermarking technology is getting escalating awareness in view of the fact that it presents an achievable elucidation for omission copyright contravention of the multimedia data in open, extremely uncontrolled environments where cryptography cannot be functional effectively. A digital watermark is a distinguishing portion of information that is adhered to the data (generally called host data) that it is projected to care for the digital content. Watermarking embeds (generally hides) a signal straightforwardly into the data and the signal becomes a connected part of the data, travelling with the data to its destination. This approach, the precious data is confined as long as the watermark is present (and detectable) in it. At some certain instant, the secret signal can be extracted to get the copyright-related information. Thus, the objectives of a watermark have to be to always stay behind in attendance in the host data. On the other hand, in practice the prerequisite is somewhat weaker than to facilitate, Depending on the relevance, a watermark is mandatory to endure all the achievable manipulations the host data may undergo as long as they do not corrupt too much the eminence of the document.

The most important divergence between watermarking and encryption is that encryption disguises the data and protects it by making it unreadable without the acceptable decryption key, while watermarking aims to make available defense in its original viewable/audible form. Watermarking is like cryptography that needs secret keys to recognize authorized owners. The key is used to entrench the watermark, and at the same time to extract or distinguish it. Only with an adequate key can the embedded signal can be exposed. While a single bit of information suggestive of that a given document is watermarked is sufficient sometimes, most applications insist extra information to be concealed in the imaginative data. This information may consist of ownership identifiers, operation dates, logo, consecutive numbers, etc., that play a key responsibility whilst prohibited providers are being tracked. Watermarking can be used principally for proprietor recognition (copyright protection), to discover the substance owner, fingerprinting, to identify the consumer of the content, for broadcast monitoring to conclude royalty expenditure,

978-1-61284-693-4/11/$26.00 ©2011 IEEE

authentication and to resolve whether the data has been misrepresented in any way from its original structure.

II. VARIOUS TECHNIQUES TO BE USED

Presently the various techniques are utilized for making safe image but according to the transform domain generally two techniques are used one is spatial domain and another frequency domain techniques.

A. The Spatial Domain Technique

We replacing the one least significant bit of each pixel of cover image with the data of a hidden image. Our human visual system is not extraordinarily accustomed to minute variations in color of images. The technique adjusts the diminutive differences between adjacent pixels leaving the consequence is practically unnoticeable.

The most straight-forward method of secures image embedding into the least-significant-bits of the cover image. Consider a M * N * 3 color image, where M indicates digit of rows and N indicates digit of columns. Here color image apiece pixel significance is represented by a decimal numeral in the assortment resolute by the number of bits used. In a color image, with 8 bit exactitude for every pixel, each pixel assumes a assessment in the range [0, 255] and each one positive number β_{10} can be represented by

$$\beta_{10} = b_0 + b_1 \times G^1 + b_2 \times G^2 + \ldots \qquad (1)$$

Where G = 2.

As a result of using the above properties, we can molder of an image into a set of binary images by separating the b_i into n bit planes. Figure 1 show, least significant bit (LSB) decomposition of the one pixel. The Most significant bit (MSB) that is bit plane 7 has maximum information while the LSB that is bit plane 0 has minimum information. So in our algorithm watermark is embed in LSB of red component plane, green component plane and blue component plane of an RGB color image. So the humiliation of original image is negligible and as far as human illustration system is apprehensive it is imperceptible to the human eye.

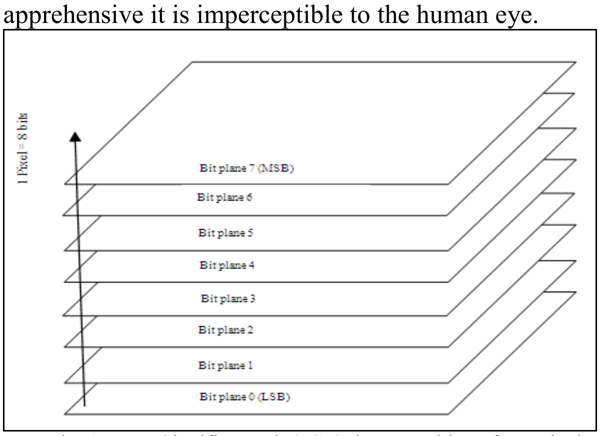

Fig. 1. Least Significant Bit (LSB) decomposition of one pixel

B. The Frequency Domain Technique

Generally frequency-domain transforms take account of the Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). The DCT and DWT transforms have been broadly used in various digital image processing applications.

B1.DCT Based Watermarking

Discrete cosine transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform. It concentrates the information energy in the bands with low frequency, and therefore shows its popularity in image compression techniques. Two dimensional DCT of an image with size M * N and its inverse DCT (IDCT) are defined in below equations, respectively,

$$F(u,v) = a(u)a(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u*pi}{2*M}\right]\cos\left[\frac{(2y+1)v*pi}{2*N}\right] \qquad (2)$$

Where, a (u) = $\sqrt{\frac{1}{M}}$ for u = 0 ; a(u) = $\sqrt{\frac{2}{M}}$ for u = 1,2,3…M-1 ;

$a(v) = \sqrt{\frac{1}{N}}$ for v = 0 ; $a(v) = \sqrt{\frac{2}{N}}$ for v = 1,2,3……N-1 ;

$$F(x,y) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} a(u)a(v)F(u,v)\cos\left[\frac{(2x+1)u*pi}{2*M}\right]\cos\left[\frac{(2y+1)v*pi}{2*N}\right] \qquad (3)$$

Where, x= 0,1,2.........M-1 y= 0,1,2..........N-1

This transform allows an image to be broken up into various frequency bands and making it easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are elected such a way, they have diminished to avoid the largest visual important parts of the image without over-exposing themselves to eliminate during compression and noise attacks. Different region in frequency domain shows in figure 2.

F_L	F_L	F_L	F_M	F_M	F_M	F_M	F_H
F_L	F_L	F_M	F_M	F_M	F_M	F_H	F_H
F_L	F_M	F_M	F_M	F_M	F_H	F_H	F_H
F_M	F_M	F_M	F_M	F_H	F_H	F_H	F_H
F_M	F_M	F_M	F_H	F_H	F_H	F_H	F_H
F_M	F_M	F_H	F_H	F_H	F_H	F_H	F_H
F_M	F_H	F_H	F_H	F_H	F_H	F_H	F_H
F_H	F_H	F_H	F_H	F_H	F_H	F_H	F_H

Fig. 2. Different regions in discrete cosine transform domain

F_L is used to signify the lowest frequency components of the block, while F_H is used to signify the higher frequency components. F_M is elected as the embedding section as to make available supplementary confrontation to lossy compression technique, despite the fact that avoid significant modification of the cover image.

B2. Comparison of Middle Band DCT Coefficients

In middle band two locations B_i (u_1, v_1) and B_i (u_2, v_2) are chosen from the F_M region for evaluation function rather than randomly choosing these locations, further toughness to compression can be achieved, if one bases the selection of coefficients on the recommended JPEG quantization table shown figure 3. We choose two locations have indistinguishable quantization values and we self-assured that any scaling of solitary coefficient will scale the other by the same aspect, preserving their comparative size.

As a result of examination of the quantization significance table, the coefficients (5,2) and (4,3) make appropriate candidates for evaluation and other quantization values are equal.

16	**11**	**10**	**26**	**24**	**40**	**51**	**61**
12	**12**	**14**	**19**	**26**	**58**	**60**	**55**
14	**13**	**16**	**24**	**40**	**57**	**69**	**56**
14	**17**	**22**	**29**	**51**	**87**	**80**	**62**
18	**22**	**37**	**56**	**68**	**109**	**103**	**77**
24	**35**	**55**	**64**	**81**	**104**	**113**	**92**
49	**64**	**78**	**87**	**103**	**121**	**120**	**101**
72	**92**	**95**	**98**	**112**	**100**	**103**	**99**

Fig. 3. Quantization values used in JPEG compression scheme

B3. Embedding Process

In the Embedding algorithm, when the message bit is a '1' then it is checked whether (5,2) is less then (4,3) or not. Stipulation answer is not then the two blocks are swapped so as to formulate (5,2) < (4,3). Likewise, whilst the message bit is a '0' then it is checked whether (5,2) is greater than (4,3) or not .Stipulation answer is not then the two blocks are swapped so as to make (5,2) > (4,3).The swapping of such coefficients should not alter the watermarked image extensively because generally assumed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be enhanced by strength constant k, such that (5,3) – (4,3) > k. Condition of the coefficient does not meet the criteria, then modified while the use of random noise when satisfy the relation. Increasing k consequently reduces the chance of detection errors at the expense of further image degradation.

B4. Extraction Process

During extraction process whole color image is broken down up into 8x8 alike blocks and discrete cosine transform performed on it. Each block is checked that whether the block (5,3) is greater than block (4,2). When (5,3) > (4,3) then '0' is detected otherwise '1' is detected.

B5. DCT Coefficients Characteristics

Magnitude of DC components of an 8*8 block DCT coefficient is directly proportional to the average gray level of the corresponding block. All the frequency components are in a sequential order with low to high frequency components. Appropriate components can be elected according to chronological way. Most of the high frequency components are zero then it represents a smooth blocks.

B6 .Coefficient selection in DCT

In discrete cosine transform superior perceptual criterion based coefficients used due to they allow stronger watermarks to be embedded and outcome is least perceptual distortion. These coefficients are least tainted by ordinary attacks like low pass filtering, noise addition etc. Most of the watermarking algorithms preferred low frequency ac component which is satisfies above criteria. While all the image processing operations are exaggerated the high frequency components. The ac components have low perceptual capacity but the magnitude of dc component is much larger than the ac component which means they have a very high perceptual capacity. This approach has a much better vigor than spatial domain. It is also more adaptive because ultimate resulted in the standard JPEG quantization table.

III. PROPOSED METHOD

A. Watermark Embedding

Step 1: Acquire the colour image.
Step 2: Detach red frame, green frame and blue frame from the colour image.
Step 3: Read the message image and which is to be embed in the respective red, green and blue frame.
Step 4: Take block discrete cosine transform of red, green and blue frame in isolation.
Step 5: Take the first block of the transformed red, green and blue frame.
Step 6: Ensure the message bit, if it is '1' then take values of (5,2) and (4,3) coefficients of a red frame, green frame and blue frame of a block , if values of (5,2) is greater than (4,3) then swap the values of blocks otherwise keep both values as it is. Now, analysed the difference (4,3) and (5,2). If difference is less than k, compute new values for the coefficients; otherwise keep values of the coefficients as it is.

New values of the coefficients are calculated as following.
(4,3) = (4,3) + k/2;
(5,2) = (5,2) - k/2;
If message bit is '0' then, Take values of (5,2) and (4,3) coefficients of a red frame, green frame and blue frame of a block , if values of (5,2) is less than (4,3) then swap the values of blocks otherwise keep both values as it is.
Now, analysed the difference (5,2) and (4,3). If difference is less than k, compute new values for the coefficients; otherwise keep values of the coefficients as it is. New values of the coefficients are calculated as following.

(5,2) = (5,2) + k/2;
(4,3) = (4,3) - k/2;

Step 7: Repeat this procedure for all the blocks of red, green and blue frame.
Step 8: Perform inverse discrete cosine transform of secured image.
Step 9: Determine performance parameters of image.

B. Watermark Extraction

Step 1: Acquire the secured image.
Step 2: Split red frame, green frame and blue frame from the secured image.
Step 3: Perform block discrete cosine transform for a red, green and blue frame
Step 4:Check the coefficients (5,2) and (4,3). If (5,2) is greater than (4,3) then save the message bit '0' and otherwise save message bit as a '1'.
Step 5: Repeat step 4 for all the blocks and finally display the message.

IV. EXPERIMENTAL RESULTS

We are taking a variety of images and observe the results, which is show in this section. Our results show, the effectiveness and success of secured information model for color in frequency domain. Various figures and table show the experimental results. Also check the image quality using peak signal to noise ratio and mean square error formula.

$$PSNR = 10 \log \frac{MAX_I^2}{\frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(x(m,n) - \hat{x}(m,n)\right)^2} \quad (4)$$

Where, MAX_I is the maximum possible pixel value of the color image.

The mean square error (MSE) of an image with 3 * m * n pixels is defined as,

$$MSE = \frac{1}{3mn}\sum_{i=o}^{m-1}\sum_{j=0}^{n-1}\left(I(i,j) - I'(i,j)\right)^2 \quad (5)$$

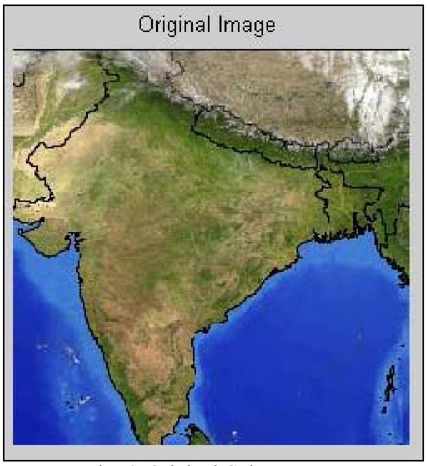

Fig. 4. Original Colour Image

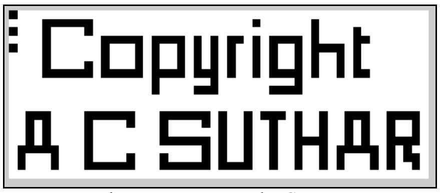

Fig. 5. Message to be Secure

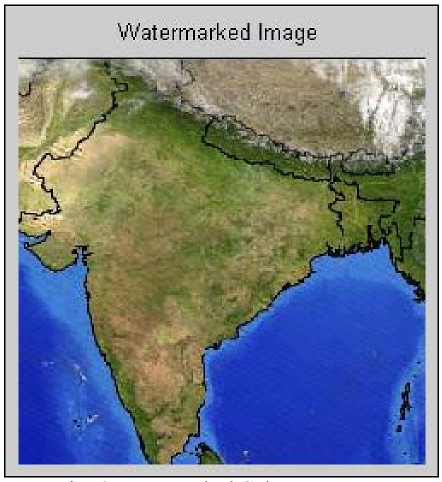

Fig. 6. Watermarked Colour Image

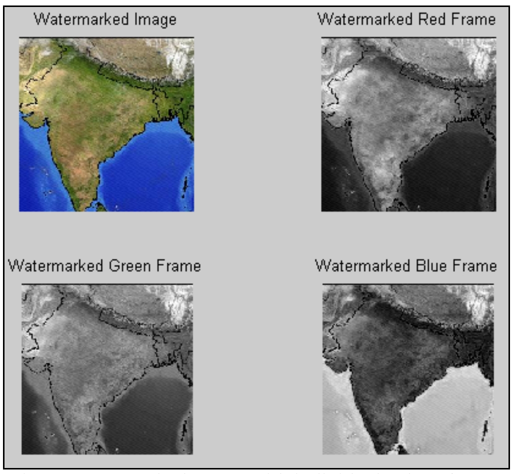

Fig. 7. Watermarked Image with individual colour frames

Fig. 8. Simulation Output for k=1,block size=8

Fig. 9. Simulation Output for k=25,block size=8

Fig. 10. Simulation Output for k=50,block size=8

TABLE I
VALUES OF VARIOUS PERFORMANCE PARAMETERS OF COMPARISON BASED ON MIDDLE BAND COEFFICIENT DCT METHOD

Performance Parameters (JPEG)	*Block Size=8*			*Block Size= 16*		
	K=1	*K=2*	*K=5*	*K=1*	*K=2*	*K=5*
PSNR(dB)	46.93	39.27	34.40	54.31	45.40	40.42
SNR(dB)	78.55	63.24	53.52	93.32	75.50	65.54
MSE(dB)	1.32	7.68	23.58	0.24	1.87	5.89
Execution Time(Sec.)	3.79	3.77	3.80	1.38	1.34	1.34

V. CONCLUSION

The benefit of embedding message in the color image is that, we can embed message into three components of an RGB image. Due to the any attack, if embedded message in any component is damaged then it can be successfully extracted from other two components. This method is vigorous then spatial domain technique. A variety of performance parameters like PSNR, MSE and SNR for watermarked image are shown in the table. We can see from the experimental results using discrete cosine transform based method, there is a deal between robustness and imperceptibility. We increase the strength of embedding factor ‘k’, the watermark increases but at the same time image is degraded as far as human visual system are concerned.

ACKNOWLEDGMENT

The authors would like to thank L. C. Institute of Technology, Bhandu and KSV University, Gandhinagar for their support in this work.

REFERENCES

[1] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "*Robust spatial watermarking technique for colour images via direct saturation adjustment*," Vision, Image and Signal Processing, *IEE Proceedings* -, vol.152, pp. 561574, 2005.

[2] S. Kimpan, A. Lasakul, and S. Chitwong, "*Variable block size based adaptive watermarking in spatial domain*," in *IEEE International Symposium on Communications and Information Technology*, vol. 1, pp. 374-377

[3] Nasir, I. Ying Weng Jianmin Jiang, Sch. of Inf., Univ. of Bradford, Bradford “*A New Robust Watermarking Scheme for Color Image in Spatial Domain*” This paper appears in: Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. *Third International IEEE Conference.*

[4] Soumik Das, Pradosh Bandyopadhyay, Shauvik Paul, Arindam Sinha Ray and Dr. Monalisa Banerjee “*A New Introduction towards Invisible Image Watermarking on Color Image*” 2009 *IEEE International Advance Computing Conference* (IACC 2009) Patiala, India, 6-7 March 2009.