International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.9, No.7 (2016), pp.137-146
http://dx.doi.org/10.14257/ijsip.2016.9.7.13

A DCT Based Imperceptible Color Image Watermarking Scheme

Jobin Abraham[1*] and Varghese Paul[2]

[1] *Mahatma Gandhi University, India*
[2] *Cochin University of Science & Technology, Kochi, India*
[1]*jnabpc@gmail.com*, [2]*vp.itcusat@gmail.com*

Abstract

The paper proposes a novel scheme for watermarking color images. Majority of the papers published on color image watermarking consider color image watermarking process as a normal extension to grayscale image watermarking techniques without attending to the specific characteristics of color images. In color image watermarking, the host color image is embedded using a unique mark with the sole intention of making the host image identifiable. The objective of this work is to find suitable regions in a color image where the watermark embedding could be effected robustly without significantly degrading the image and at same time ensuring the impact of embedding will remain imperceptible. The proposed algorithm uses Discrete Cosine Transform to transform the host image into frequency domain for selecting appropriate coefficients for watermark embedding. Also, instead of resorting to global embedding of watermark over host image, safer regions that are oblivious to watermark embedding are selected for watermark integration. The measures discussed ensures that the watermarking process do not introduce visible distortions. A new metric, named as GEI (Global Embedding Impact), is also defined for measuring the impact of embedded watermark information over each host image pixel.

Keyboard*: color image watermarking, discrete cosine transform (DCT), watermark embedding, extraction, Global Embedding Impact, GEI*

1. Introduction

With wider popularity and increasing use of Internet as a medium for publishing digital resources, digital images are exposed to the risk of being downloaded and reused without proper permissions. Such unauthorized uses have to be controlled effectively to avoid misuses and other possible losses in terms of resources and revenues. Digital watermarking is envisaged as a mechanism that can be used for copyright protection. Watermarking proclaims the owners identity with the help of a hidden watermark.

The process of embedding a watermark signal in a host image is known as digital image watermarking. Watermark is the unique signature that unambiguously refers to the owner. The watermark thus can be a logo image or a message text or even a slogan. The watermark is embedded within the host image so that the source contents permanently carry the signature of the creator owner. The three main requirements of an image watermarking scheme are transparency, robustness and payload capacity [1]. The watermarking process should not significantly distort the source file. In fact adding any kind of external data with image is equivalent to noise addition. So the biggest challenge is in integrating the watermark signal without making its presence visible to an extent that damages quality of the source image. Another important objective to be met is that the hidden watermark should not be easily destroyable or removable. Robustness of an embedding scheme depends on the embedding strength used for integrating the

*Corresponding Author

ISSN: 2005-4254 IJSIP

watermark. Hence watermarking robustness is contradictory to the requirement of watermark imperceptibility. Higher the embedding strength, greater the robustness of watermarking scheme. However, the side effect is that employment of larger embedding strength significantly degrades the image.

The proposed method attempts to achieve the above narrated objectives by selecting suitable areas in the image that are insensitive to human eyes and strongly embedding watermark in those regions. Thus the scheme presented is successful in embedding watermark robustly as well as imperceptibly.

Literature survey describes two broad class of watermark embedding methods namely, spatial domain methods [2-3] and frequency domain methods [4-6]. Spatial domain methods operate at image pixel level. Least significant bits (LSB) in the host image are modified in accordance with the watermark to hide the identification information. On the other hand, frequency domain methods transform the pixel values to a convenient domain and perform watermark embedding. After embedding, the modified contents are transformed back to the spatial domain to generate the watermarked image. It is found that the frequency domain methods are more robust to attacks that are targeted at erasing the embedded identification watermark. Most commonly used transform operations are FFT (Fast Fourier Transform) [7], DST (Discrete Sine Transform) [8], DCT (Discrete Cosine Transform) [9] and DWT (Discrete Wavelet Transform) [10].

The following sections are organized as follows. Section 2 describes some related works. Section 3 presents the proposed algorithm for watermarking color image. The algorithm is coded and tested in section 4. Finally, section 5 concludes the paper.

2. Related Work

Majority of the works in image watermarking is on grayscale images. Many researchers extend these algorithms to color images. However a color image has three channels and more information per pixel, it is a different problem to design a robust color image watermarking scheme that is oblivious to human eyes. Few research works based on color image watermarking are described in this section. [7] suggest the Y component from the YST equivalent of the RGB image can be employed for embedding the watermark signal.

Watermarking scheme proposed in [11] operates in spatial domain. The average intensity is estimated from the intensities of the R, G and B channels. The color channel that has intensity greater than the average intensity is used for embedding the watermark bit. In the selected channel, three bits on least significant side are substituted with the watermark bits. The method is found to be highly susceptible to compression attacks. When compressed beyond a quality factor of 50, the watermark extracted becomes non-recognizable.

In [12] original image is decomposed into R, G, B channels and the B component of the image is selected for watermark embedding. DWT of B channel is computed and the watermark is embedded by modifying the coefficients of mid-frequency bands, i.e. LH and HL bands. A binary watermark is added to these DWT coefficients with gain k transforming them to an embedded coefficient value. Whenever the pixel in the watermark vector is zero, then a PN sequence with an appropriate gain is added. Though the authors claim to be a blind method, the extraction stage uses the key for generating the PN sequence. After watermark extraction correlation between the generated PN sequence and the watermarked sub-band coefficients is computed. If the correlation between extracted bit and the original bit is above a threshold, the watermark is declared to be detected successfully. The method adopts global processing of source image for watermark embedding instead of considering the local image characteristics for safer and oblivious embedding. The paper discusses the impact of only two attacks, Salt & pepper

and Gaussian noise. Such noise addition attacks are less common compared to compression or filtering attacks.

[13] proposes a method for watermarking color images after transforming to YIQ format. The RGB channels in color image are transformed into YIQ channels. Further, DWT is applied on Y channel. The mid-frequency and high frequency components LH, HL and HH of Y are then modified to embed the watermark. The locations of modified frequency bands are stored into an array called key array. Later at the time of extraction, the DWT of the Y channel of the watermarked image is computed. The locations used for embedding the watermark are identified using a key array generated during the embedding stage. Thus at the time of extraction there is the overhead of requiring the original image and the key array.

[14] proposes another method for color image watermarking using SVD (Singular Value Decomposition) transformation. RGB components in the original image are portioned into 4x4 non-overlapping blocks. This is followed by SVD decomposition of each block. This results in two orthogonal matrices U and V and a singular diagonal matrix D. The relation between two elements in U matrix, $U_{2,1}$ and $U_{3,1}$ is used to represent the watermark bit. For representing the watermark bit 1, the value of ($U_{2,1}$ –$U_{3,1}$) should be negative and for watermark bit 0, the value of ($U_{2,1}$ –$U_{3,1}$) is to be positive.

3. The Method

The proposed algorithm takes into consideration certain specific features of the color image to minimize the impact of watermark embedding. The sensitivity of human visual system (HVS) to variations in blue channel is lesser compared to the red and green channels. To ensure that only the most insensitive regions in image are used for embedding the watermark, appropriate regions that satisfy certain criteria are selected embedding in blue channel rather than adopting global embedding.

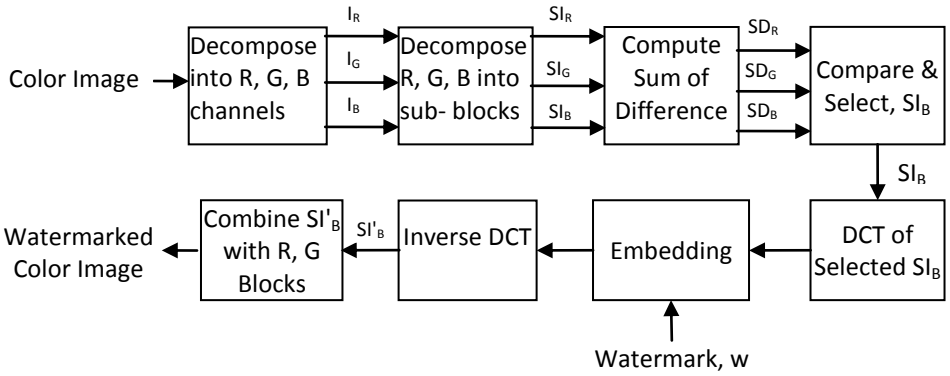

Figure 1. Watermark Embedding Process

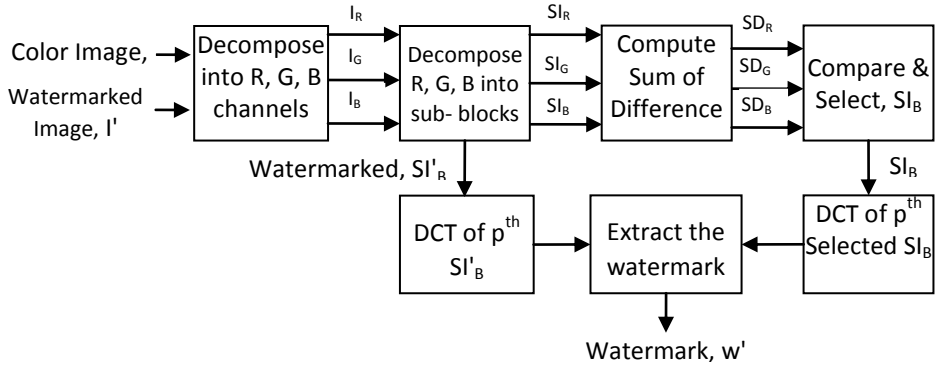

Figure 2. Watermark Extraction Process

The method has two stages, embedding stage and extraction stage. Embedding process integrates the identification watermark within the host color image. The embedding algorithm starts with decomposing the host image into composite R, G and B channels. The three color channels are further decomposed into non-overlapping 8x8 blocks. Then a set of computations and comparisons are performed to identify appropriate sub-blocks (SI_B) from blue channel for integrating the watermark. DCT is applied on all selected SI_B blocks and watermark bit is embedded to the transformed domain coefficients. After embedding the watermark bits, all host image sub-blocks are merged with embedded SI'_B to output the watermarked color image. Second stage is the extraction process for retrieving the hidden code from the watermarked image. Figure.1 shows the block diagram of the embedding process. Extraction need not always follow the embedding stage. Extraction process is operated only when the ownership of the image is to be ascertained. Figure.2 shows the block diagram of the extraction process.

3.1. Embedding Algorithm

The steps for embedding the watermark are as described below.

1. Input a color image, I and the watermark, W. Let the images be of sizes MxN and XxY respectively.
2. Decompose the color image I into constituent R (I_R), G (I_G) and B (I_B) channels.
3. Decompose the three channels into sub-blocks (SI_R, SI_G, SI_B) of size 8x8. The number of resulting sub- blocks, t=1 to (M*N/64).
4. Select v number of sub-blocks from (I_B) that satisfies the criteria below. Here v= X*Y
5. For the sub-blocks, find sum of difference, $SD_{xt} = \sum |(P_{i,j} - P_{avg})|$. Here x = 1, 2 or 3 (where 1 is for SI_R, 2 for SI_G and 3 for SI_B), $P_{i,j}$ is the pixel value in the sub-block and P_{avg} is the average of all pixel intensities in the sub-block under consideration and t is the sub-block number that varies from t=1 to (M*N/64).
6. Compare the three SD_{xt} values and whenever SD_{xt} is found to be larger for a SI_B compared to the other two (SI_R and SI_G), embed the watermark bit in the blue channel sub-block.
7. Compute DCT of selected SI_B. Modulate a DCT coefficient term in accordance to the watermark bit.

   if (W_r ==1), f' = α_1 * f, else f' = α_2 * f. Here $\alpha_1 > 1$ and $\alpha_2 < 1$.

   Here α_1, α_2 are the strength factors, f is the selected DCT coefficient and r =1 to v.

8. Perform inverse transform to generate the watermarked sub-block, SI'_B.

9. Increment t, r and continue from step 5 until v. If (t== (M*N/64)) && (v < t)), execute from step 5 by opting for the green channel sub-blocks (SI_G) to embed the remaining watermark bits in W.

10. Combine the three channels and output the watermarked color image, I_w.

3.2. Extraction Algorithm

Extraction process is meant for ensuring the presence of the embedded mark. The output of this stage is the identification watermark that was hidden in the host image by the previous embedding stage. The steps for watermark extraction are as follows.

1. Input the watermarked image, I_w and color image, I.

2. Decompose the color image I and I_w into constituent color channels.

3. Decompose the color channels in I and I_w into sub-blocks. Let the sub-blocks be (SI_R,SI_G, SI_B) and (SI'_R,SI'_G, SI'_B) respectively.

4. For the sub-blocks from I, find sum of difference, $SD_{xt} = \sum |(P_{i,j} – P_{avg})|$. Here x=1, 2 or 3 and indicates the color channel (1 is R, 2 is G and 3 is B). Compare the three SD_x values. Whenever SD_x is found larger for SI_B compared to the sub-blocks from other two channels, extract the watermark bit as follows.

5. Compute DCT of SI_B and also the DCT of corresponding SI'_B .

6. Let the DCT coefficient f be the embedded term. Compare the corresponding terms in SI_B and SI'_B to generate the hidden code as:

   If ($f_{SI'B} > f_{SIB}$), W_t =1; else W_t = 0.

7. Increment t and continue from step 4 until t==v. If sufficient blue sub-blocks are not formed, repeat further from step 4 after selecting eligible sub-blocks from green channel.

8. Output the watermark image. W'.

4. Testing and Analysis

The proposed algorithm is implemented and tested on several color images. A binary watermark of size 32x32 is used for embedding in host color images. The host image used is of size 512x512. DCT of the blocks selected from the B channel as per the embedding algorithm discussed in the previous section is used for embedding the watermark bits. For improved robustness a low frequency coefficient from the selected sub-block is modified. Extraction process for decoding the hidden signal from the watermarked images is also tested. The results obtained after watermark embedding and watermark extraction on three of the test images used are given in the figure.3 and figure.4.

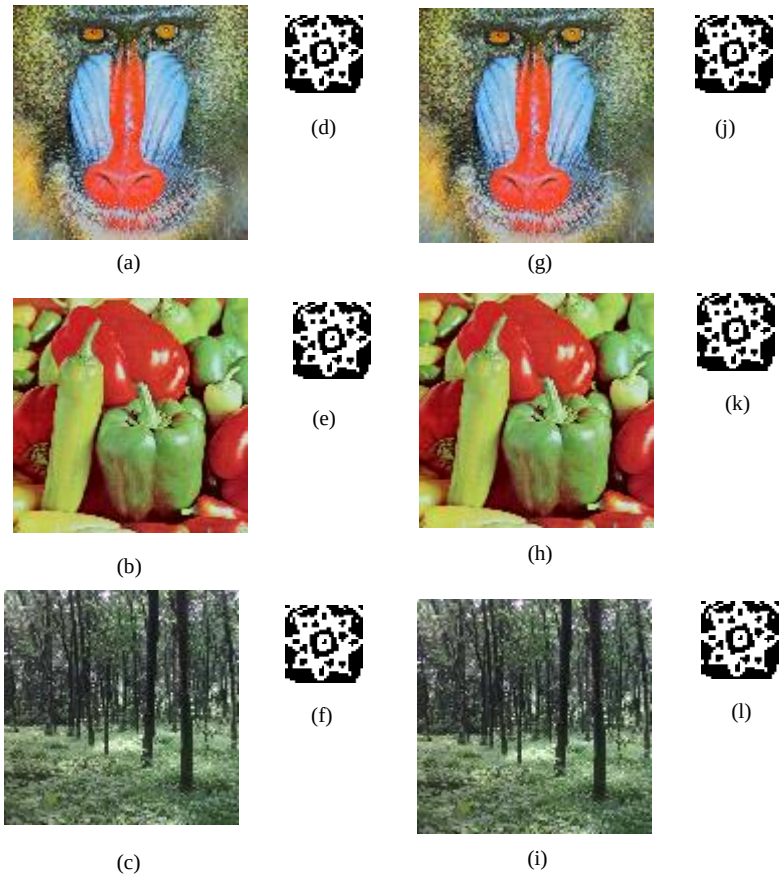

Figure 3. Host and Watermarked Images, (a) Baboon (b) Peppers (c) Trees, (d) – (f) Watermark, (g), (h), (i) Watermarked Images of (a), (b) and (c) Respectively, (j), (k), (i) Extracted Watermark from (g), (h) and (l) Respectively

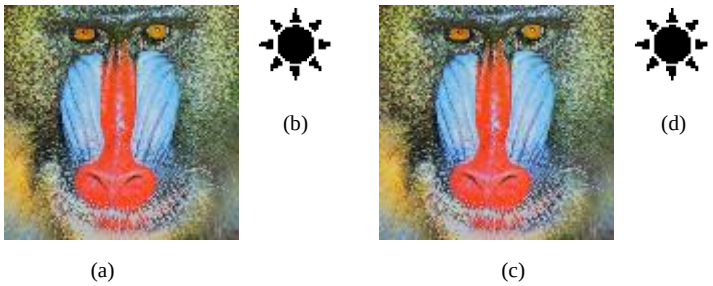

Figure 4. Host Image Watermarked using a Star Logo

Peak Signal to Noise (PSNR) Ratio and Normalized Cross Correlation (NCC) values are used to measure the quality and robustness of the watermarked image [6]. PSNR compares the original image and its watermarked version using the equation 1. Higher the PSNR value, better the quality of the watermarked image. A lower PSNR value means that that larger error is introduced during the watermark embedding process. Table 1 shows the observed PSNR values for different images.

$$PSNR = 10\log_{10}\frac{R^2}{MSE} \tag{1}$$

$$MSE = \sum_{k=1i=1}^{3}\sum^{M}\sum_{j=1}^{N}\frac{[I(i,j)-W(i,j)]^2}{3*M*N} \tag{2}$$

Table 1. Peak Signal to Noise Ratio

Image	PSNR
Peppers	37.29
Lena	35.26
Baboon	34.49
Trees	37.62

Global Embedding Impact (GEI) is a measure that indicates the depth or net impact of watermarking over a host image pixel. Global Embedding Impact, GEI, is defined as the ratio of sum of the difference between the original and modified version of the image by the number of pixels in the host image. GEI is computed using the equation 3. This measure portrays the average impact of the embedding process over each pixel in the host image.

$$GEI = \frac{\sum_{k=1i=1}^{3}\sum^{M}\sum_{j=1}^{N}|(W(i,j)-I(i,j))|}{3*MxN} \tag{3}$$

Here, I is the host image and W is the modified or watermarked image. M and N denotes the size of the image. Smaller the GEI value, lesser the impact of the embedded watermark bits over the original host image pixels. A larger value indicates that the pixels were subject to a greater variation during the process of watermark embedding. Table.2 shows the GEI values measured on the pixels of few test images. This shows that each pixel is subjected to a variation in the range of 0.7 to 1.2 after the process of watermarking.

Table 2. Global Embedding Impact on Image Pixels

Image	GEI
Peppers	0.71
Lena	1.04
Baboon	1.27
Trees	0.76

The extraction process decodes the hidden watermark. Extracted watermark is to be identical to the actual watermark used at the time of embedding. Normalized cross-correlation (NCC) is used here for comparing similarity between the two signals. NCC between the original versus the watermarked image is computed using equation 4. NCC measures the amount of variation between the original watermark and the extracted watermark. NCC ratio varies in the range 0 to 1. A value close to 1 indicates that the extracted signal is identical to the actual signal. As the NCC value astray from 1 it means that the extracted signal is less identical to the actual version and implies that the

embedded watermark was broken either due to attack or due to the failure of the scheme to correctly extract the watermark.

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[\, I(i,j).W(i,j)\,]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[W(i,j)]^2}} \quad (4)$$

A watermarking scheme should be robust to various intentional or unintentional attacks. This ability to withstand attacks is essential for proving the ownership right of a resource whenever illegal uses of digital contents is reported [15]. Hence, the images watermarked using the proposed scheme is subjected to several known attacks for testing their robustness to attacks. The watermark extracted is compared against the actual using NCC. The figure 5 shows the degraded watermarked images after noise addition. And figure 6 shows the compressed watermarked image at different quality factors and the corresponding extracted watermark.

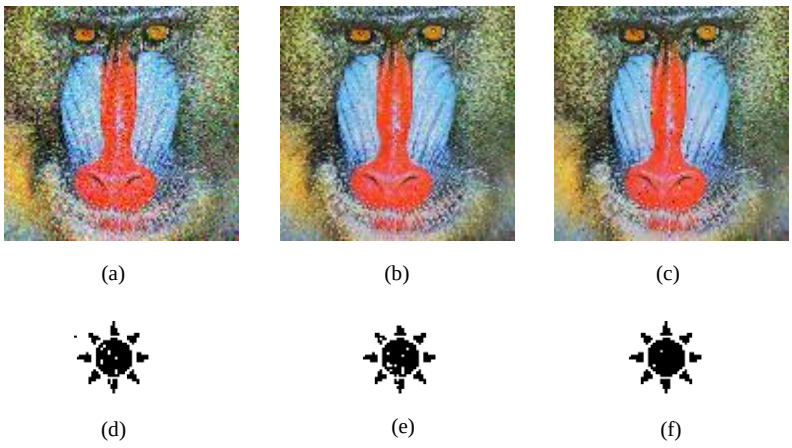

Figure 5. Watermarked Image Mixed with (a) Gaussian (b) Poisson (c) Salt & Pepper Noise. (d) – (f) Corresponding Extracted Watermarks

The proposed scheme is found to be extremely robust against noise addition. Table 3 shows the NCC values of the extracted watermark under different cases in Figure.5 and Figure.6. It may be observed that the hidden watermark extracts has not undergone massive deformations. Similar is the case with JPEG compression. The image was compressed with quality factor as low as 15 and yet yielded a meaningful extract.

Table 3. Normalized Cross Correlation Values

Attack	NCC
No Attack	1
Gaussian	0.9896
Poisson	0.9892
Salt & Pepper	0.9993
Compression (QF =60)	0.9986
Compression (QF =40)	0.9944
Compression (QF =30)	0.9831

Compression (QF =20)	0.9436
Compression (QF =15)	0.9035

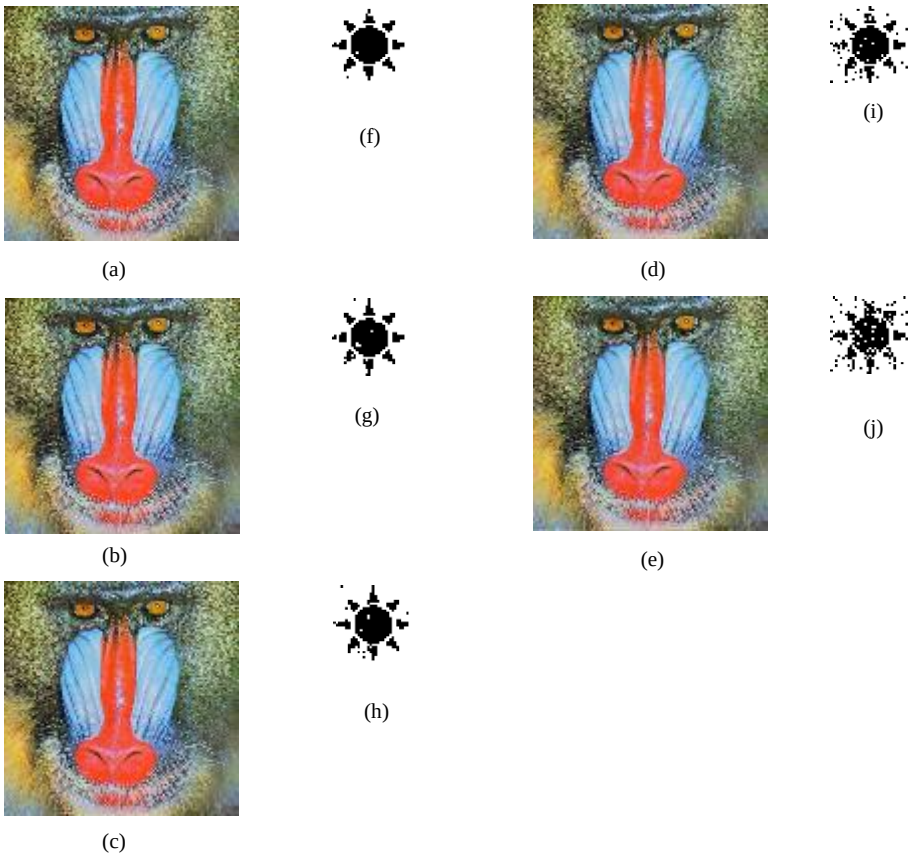

Figure 6. (a) – (e) Compressed Watermarked Images with QF 60,40,30,20 and 15, (f) – (j) Corresponding Extracted Watermarks

The proposed method is compared with peer algorithm presented in [8-11]. The comparison is made with respect to imperceptibility, robustness to attacks, watermarking domain etc. Table 4 lists the important outcomes.

Table 4. Prominent Features and Performance Comparison with [11, 14]

Feature	Nagaraj et al [11]	Shao-li Jia[14]	Proposed Scheme
Imperceptibility	Good	Good	Good
Watermark Payload	Good	Reasonable	Reasonable
Watermark Security	Reasonable	Good	Good
Watermarking Domain	Spatial	SVD	Frequency (DCT)
JPEG Compression Survival	Low	Good	High

5. Conclusion

A scheme for watermarking color images is proposed. Frequency domain techniques using DCT is used for embedding watermark bit over selected host image pixels. The experimental results from PSNR and NCC measurement deliver fair outcomes. During the testing stage of the algorithm most common attacks such as signal addition and compression were experimented. The extraction stage successfully decoded the hidden watermark from attacked images. Thus the proposed algorithm succeeded in embedding the watermark imperceptibly as well as robustly. Compression is one of the most common forms of attack. Our method survived jpg compression at different quality factor. For instance the actual size of Baboon image used is 611KB. This is compressed with a quality factor as low as 15% reducing the image size to 22KB. Still the extraction algorithm was able to detect the watermark with a certainty of NCC=0.90. These results prove beyond doubt that the proposed method is robust to compression, which incidentally is the most common kind of attack on the Internet resources.

References

[1] V. M. Potder, S. Van and E. Chang, "A Survey of Digital Image Watermarking Techniques", Third International Conference on Industrial Infomatics, **(2005)**, pp 709-716.
[2] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible Data Hiding", IEEE Transactions on Circuits and Systems for Video Technology, vol.16, no. 3, **(2006)**.
[3] P. L. Lin, C. K. Hsieh and P. W. Huang, "A Hierarchical digital watermarking method for image tamper detection and recovery", Pattern Recognition, vol. 38, **(2005)**, pp. 2519-2529
[4] M. Ali, C. W. Ahn and M. Pant, "A Robust Image Watermarking Technique using SVD and Differential Evolution in DCT Domain", Optik 125, **(2014)**, pp. 428-434.
[5] C. H. Chen, Y. L. Tang, C. P. Wang and W. S. Hsieh, "A Robust Watermarking Algorithm based on Salient Image Features", Optik, vol. 125, **(2014)**, pp. 1134-1140.
[6] R. Keshavarzian and A. Aghagolzadh, "ROI based Robust and Secure Image Watermarking using DWT and Arnold map", International Journal of Electronics and Communication, vol. 70, **(2016)**, pp. 278-288.
[7] C. W. Tang and H. M. Hang, "A Feature based Robust Digital Image Watermarking Scheme", IEEE Transactions on Signal Processing, vol. 51, no. 4, **(2003)**.
[8] H. Yassine, B. Bachir and K. Aziz, "A Secure and High Robust Audio Watermarking System for Copyright Protection", International Journal of Computer Applications, vol. 53, no. 17, **(2013)**.
[9] C. H. Chen, Y. L. Tang, C. P. Wang and W. S. Hsieh, "A Robust Watermarking Algorithm based on Salient Image Features", Optik 125, **(2014)**, pp. 1134-1140.
[10] B. Surekha and G. N. Swamy, "Sensitive Digital Image Watermarking for Copyright Protection", International Journal of network Security, vol. 15, no. 1, **(2013)**.
[11] N.V. Dharwadkar and B. B. Amberkar, "Secure Watermarking Scheme for Color Image using Intensity of Pixel and LSB Substitution", Journal of Computing, **(2009)**.
[12] P. Ramana Reddy, V. N. K Prasad and D. S. Rao, "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent trends in Engineering, **(2009)**.
[13] N. V. Dharwadkar and B. B. Amberker, "An Efficient Non-blind Watermarking Scheme for Color Images using Discrete Wavelet Transformation", International Journal of Computer Applications, **(2010)**.
[14] S. L. Jia, "A Novel Blind Color Image Watermarking based on SVD", Optik, vol. 125, **(2014)**, pp. 2868-2874.
[15] Dr. S. Sherekar, Dr. V. M. Thakare and Dr. S. Jain, "Attacks and Countermeasure on Digital Waters: Classification", Implications, Benchmarks, International Journal of Computer Science and Applications, vol. 4, no. 2, **(2011)**.

