International Journal of Engineering Inventions
ISSN: 2278-7461, www.ijeijournal.com
Volume 1, Issue 4 (September 2012) PP: 32-38

Content Based Hybrid Dwt-Dct Watermarking For Image Authentication in Color Images

S. Radharani[1], Dr. M.L. Valarmathi[2]
[1]*Assistant Professor, Department of Computer Applications, Sree Narayana Guru College, Coimbatore,*
[2]*Associate Professor, Department of Computer Science and Engineering, Government College of Technology, Coimbatore*

Abstract—The present work relates to a novel content based image authentication frame work. Here we take statistical based four methods for creating watermark. All these methods embed that statistical feature into the host image. In first method, Frobenius Norm of the host image is taken as watermark using ICA technique. The other methods used to create watermarks are namely, mean, standard deviation and combined mean and standard deviation of the host image. This hybrid method combines DCT and DWT to hide the watermark, so that imperceptibility will be maintained. The same statistical features are extracted as feature set which is embedded in the host image during embedding phase. In the watermark retrieval process, content modification is identified by correlation method with predefined threshold. The experimental results demonstrate that newly proposed DWT-DCT hybrid watermark embedding algorithm with HSV is robust for Compression, noise and other attacks.

Keywords—Discrete Cosine Transform, Discrete Wavelet Transform, Independent Component Analysis, Frobenius Norm, Human Visual System.

I. INTRODUCTION

Watermarking is the process of inserting predefined data into multimedia content in a way that the degradation of quality is minimized and remains at an imperceptible level. Some transformations such as DCT and DWT are used for watermarking in the frequency domain. A through comparison of the DCT and DWT is found in [1]. For content authentication, the embedded watermark can be extracted and used for verification purposes. The techniques used are classified into three main categories: robust, fragile and semi-fragile method. Robust techniques are primarily used in applications such as copyright protection and ownership, verification of digital media, because they can withstand nearly all attacks. Fragile methods are mainly applied to content authentication and integrity verification, because they are fragile to almost all modifications. By contrast, semi-fragile methods are robust against incidental modifications such as JPEG compression, but fragile to other modifications. The difference between the original watermark and the extracted watermark is compared by predefined threshold during authenticity verification. The applications of the watermark are Content Identification and management, Content protection for audio and video content, Forensics, Document and image security, Authentication of content and objects (includes government IDs), Broadcast monitoring, etc. The present work is applicable for Image authentication for color images. In this paper first the researchers utilize Frobenius norm as watermark, which is created using ICA technique and then the researchers also uses the other statistical measures such as mean, standard deviation and total value of both mean and standard deviation as watermark generation. To find the tampered location, random noise as tamper is applied on the watermarked image and it is located through coding. The advantage of this method is that it can tolerate the attacks such as, JPEG compression, Gamma Correction, Noise, Low pass filter, Sharpening, Histogram equalization and contrast stretching. The quality metrics used in this method are PSNR, Image Fidelity and Pearson Correlation Coefficient.

II. RELATED WORKS

In the area of robust watermarking techniques [2] proposes, quantization index modulation algorithm in the frequency domain to achieve copyright protection. In [3] a binary watermarked image is embedded in selected sub-bands of a 3-level DWT transformed of a host image. Further, DCT transformation of each selected DWT sub-band is computed and the PN-sequences of the watermark bits are embedded in the coefficients of the corresponding DCT middle frequencies. In extraction phase, the watermarked image, which may be attacked, is first preprocessed by sharpening Laplacian of Gaussian filters. Then the same method applied as the embedding process is used to extract the DCT middle frequencies of each sub-band. At last, correlation between mid-band coefficients and PN-sequences is calculated to determine watermarked bits. In the area of fragile watermarking techniques proposes [4] Secure fragile watermarking algorithm. In that scheme a signature is extracted from each block of the image and is inserted in that block. Extraction of the signature and appropriated parameters for computation of the signature were studied. In the paper [5] a novel fragile watermarking technique was proposed to increase accuracy of tamper localization by maintaining the dependence among blocks. In the method the watermark which is embedded in each block was composed of three digital signatures. This provides both security against vector quantization counterfeiting attack and increases accuracy of tamper localization. The earlier work on semi-fragile watermarking research [6], mostly focused on detecting whether an image was tampered with or not. However those techniques were not able to identify the tampered location. In this Journal Paper [7], the authors used random bias and nonuniform quantization, to improve the performance of the methods proposed by Lin and Chang. In 2000 [8] used the histogram of ‘value’ or ‘intensity’ component of HSV color space to find out most appropriate area to insert the watermark.

III. CONTENT BASED HYBRID DWT-DCT WATERMARKING

In the proposed method the researchers introduces the Human Visual system concepts in which the given RGB image is converted into HSV image and the embedding process is performed. Before embedding the image is resized into 256X256. During the extraction process, again the HSV image is converted into RGB image. It increases robustness. The proposed method is classified based on the watermark used to embed in the host image in combined DWT-DCT watermarking technique. The first method uses the watermark as frobenius norm of the host image. In the second method mean of the host is used as watermark. In the third method standard deviation is employed as watermark. In the last method combined value of mean and standard deviation of the host is used as watermark. For all these methods the comparative study is done based on time factor for both embedding and extraction of the watermark.

3.1. Watermark Generation

i. First the image is divided into blocks of size 16.
ii. For each block apply FastICA.
iii. Depends on choice (frobenius norm, mean, standard deviation, mean & standard deviation) , generate watermark.
   a. Compute frobenius norm of the block if the choice is 1.
      w =norm (A,’ fro')
   b. Compute mean of the block if the choice is 2.
      w =mean (mean (A))
   c. Compute standard deviation of the block if the choice is 3.
      w =std (std (A))
   d. Compute mean & standard deviation of the block if the choice is 4.
      w =std (mean (A))

3.2. Watermark Embedding

The embedding process follows the algorithm given below:

1. For each block apply DWT for 3 levels.
2. D=DCT(mid frequency of DWT 3rd level)
3. D=(sign(D))* □ * w(k)

Where □ isembedding strength, which is obtained by

□ = standard deviation of original watermark image / standard deviation of extracted watermark

In this work, after completing the experiments, average value of □ for frobenius norm is 0.247, for mean is 0.068, for standard deviation is 0.092 and for combined mean and standard deviation is 0.2021 .

4. Perform inverse DCT and inverse DWT.
5. Repeat the steps 2 – 4 for all the blocks.

The result is the watermarked image I*.

3.3 Watermark extraction

1. Perform steps 1 – 5 of the watermark generation procedure on the received image I’ and get the computed watermark.
2. Perform DWT of each block and then perform DCT of the same block.
3. Extract the embedded watermark from the chosen DCT coefficient.
4. w’ = abs (D) / □
5. This set forms the extracted watermark.

3.4 Authentication

1. Perform block wise percentage difference between the values w and w’

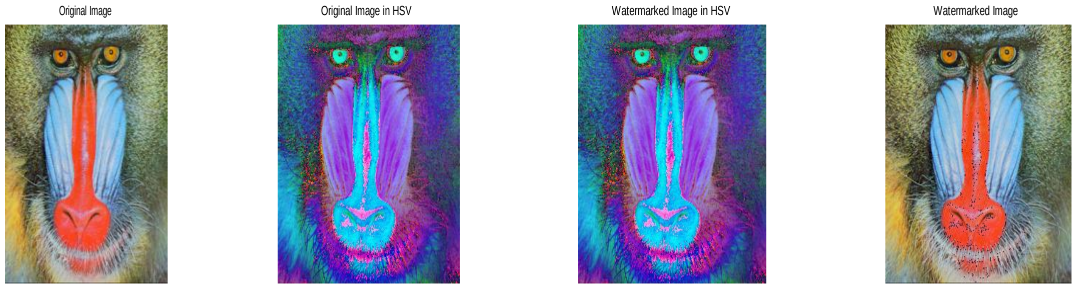
Block difference = $|w_i' – w_i| / \max (w_i) * 100$

Threshold for the percentage difference has been experimentally determined as 15%.

This block wise difference is used to verify any modifications in the block to check the authenticity. The threshold value is fixed by experimentation and if the difference is less than threshold value accepts it as authentic otherwise the image is unauthentic.

IV. EXPERIMENTAL RESULTS

The proposed scheme has been tested using Matlab. The scheme has been evaluated on the different set of images of size 256 X 256, 1920 X 1440, 1024 X 768 and 729 X 546. The block size chosen is 16 X 16 so that it resulted in better PSNR value. The alpha value is calculated based on the standard deviation of original image and watermarked image. For Frobenius norm as watermark method its value is 0.247, for mean as watermark method the value is 0.068, for standard deviation as watermark method the value is 0.92 and for the value combined mean and standard deviation its value is 0.2021. Threshold value of the calculation of percentage difference is chosen as 25%. The value below the threshold resulted as false negative and the value above the threshold indicates the method to be fragile. Middle-frequency coefficients are selected to embed the watermark. Embedding the watermark in low-frequency components, result in visual degradation of the host image. Similarly embedding the watermark data in high-frequency components results loss of data due to compression. Hence our method ensures robustness. The ICA algorithm adopted in this proposed method has been discussed in [9] [10]. To find out the quality of the watermarked image, the metrics PSNR, Pearson Normalized Cross Correlation Coefficient, Normalized Cross Correlation and Image Fidelity are used. These are calculated between host image and the watermarked image. The present work implemented in four different types of watermark generation techniques. Fig. 1 shows the Baboon image, before watermarking and after watermarking both in RGB and HSV formats in Frobenius Norm as watermark generation technique. Fig. 2 shows the Baboon image after JPEG Compression, Gamma Correction, noise, filter, histogram equalization and Contrast stretching attacks.



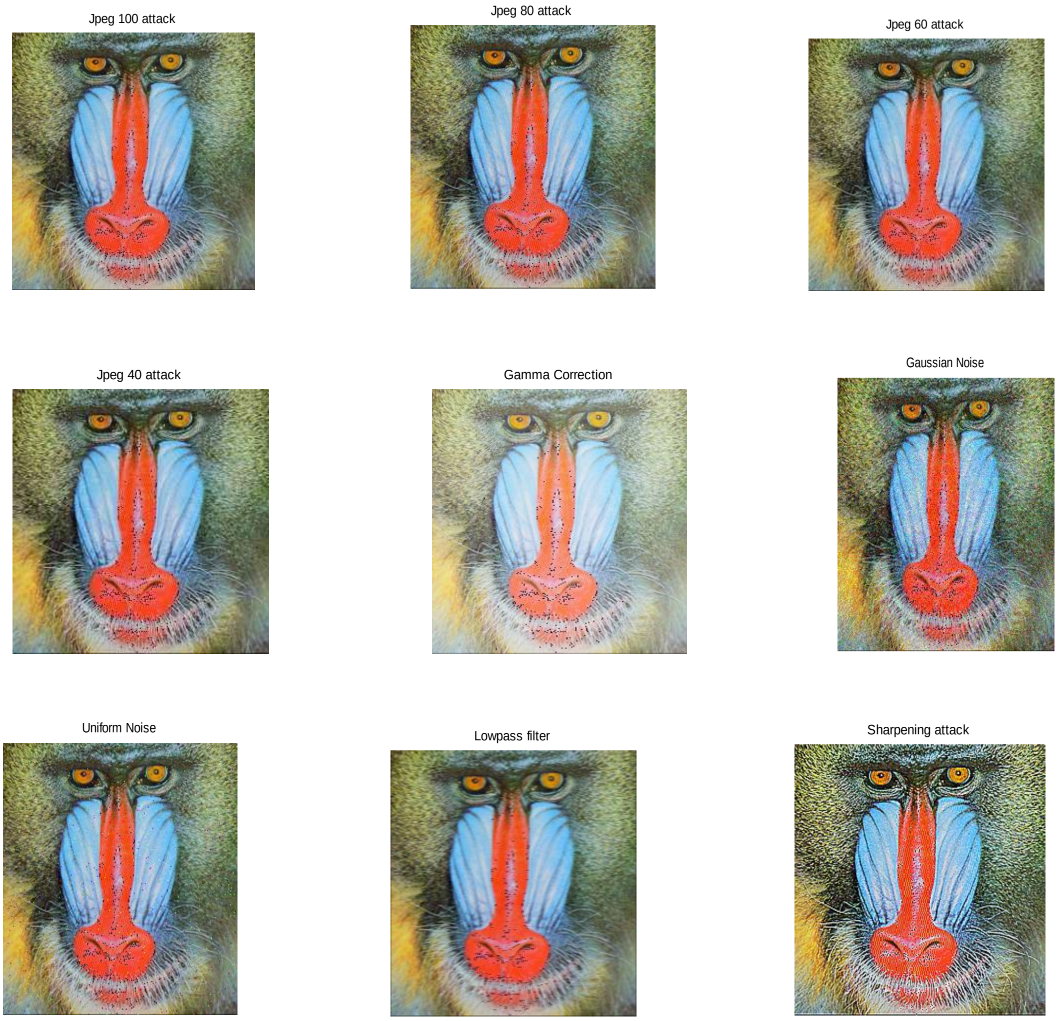
Original Image

Original Image in HSV

Watermarked Image in HSV

Watermarked Image

Figure 1. Original Image , Original Image in HSV, Watermarked image in HSV, Watermarked Image.



Jpeg 100 attack

Jpeg 80 attack

Jpeg 60 attack

Jpeg 40 attack

Gamma Correction

Gaussian Noise

Uniform Noise

Lowpass filter

Sharpening attack

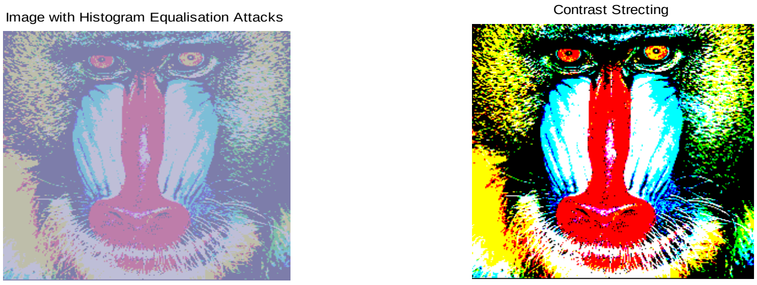


Figure 2. Watermarked Image after various attacks.

Figure 3 shows the tampered location identification for Baboon Image. Here the random noise is applied as tamper to the watermarked image. That tampered location was identified correctly.

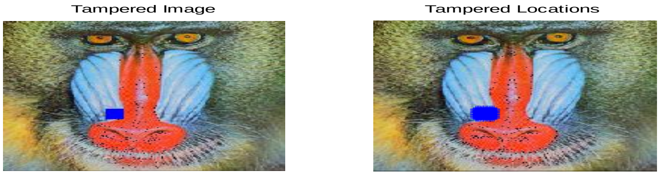


Figure 3. Detection of tampered location.

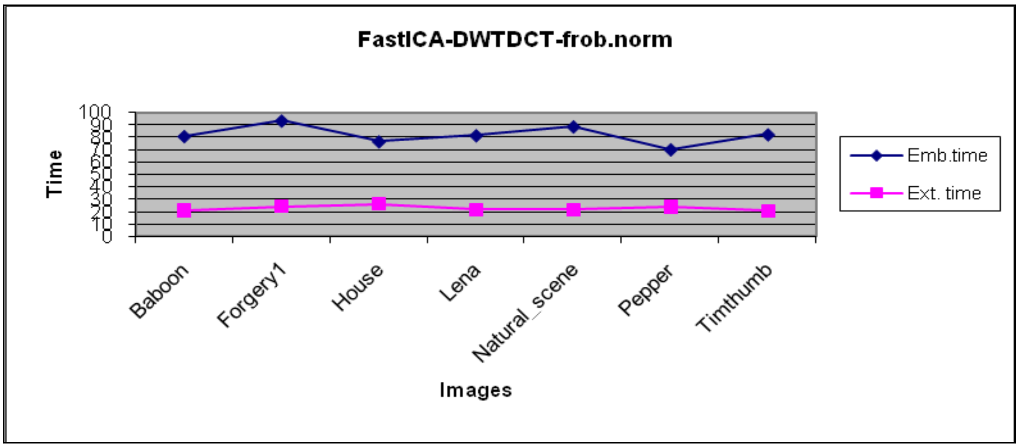


Figure 4. Embedding time and Extraction time for various test images.

From Fig. 4, Embedding time depends on the size of the image and extraction time almost same for all types of images.

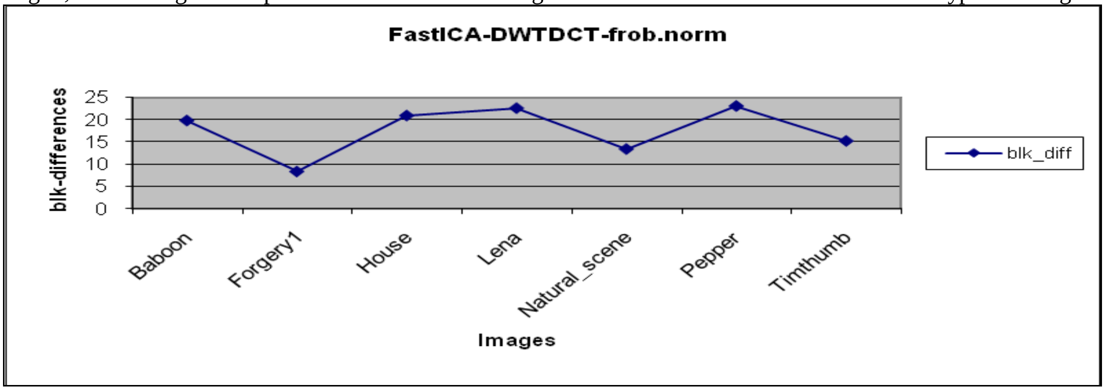


Figure 5. Percentage block difference between watermark extracted and the watermark for various test images.

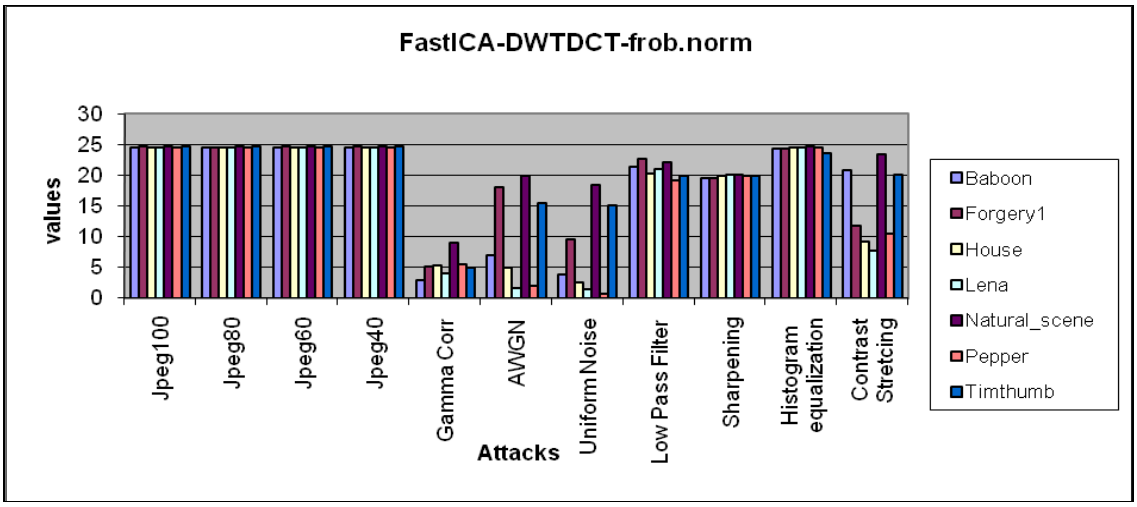


Figure 6. Percentage block differences for various test images after incidental image processing operations.

From Fig. 6 for the entire test image's block wise percentage difference is 25 for JPEG attack. For gamma correction the block wise percentage difference is approximately 5. For Noise attacks the value is negligible other than natural scenes. For low pass filter the value is above 20 for all images. For sharpening attack its value is almost equal to all types of images and it is 20. Histogram equalization attack the value is 25 and for contrast stretching it value depends on the type of image.

Table 1. Quality Metrics after Watermarking. Using Hybrid DCT and DWT Watermarking with Frobenius norm

Images	MSE	PSNR	IF	PCC	NC
Baboon	2.88E-05	93.539	1	0.99972	1
Forgery1	3.98E-06	102.1355	1	0.99984	1
House	2.13E-05	94.843	1	0.9998	1
Lena	6.23E-05	90.1869	1	0.99963	1
Natural_scene	9.00E-06	98.5898	1	0.99983	1
Pepper	4.00E-05	92.1122	1	0.99764	1
Timthumb	1.70E-05	95.8175	1	0.99966	1

From TABLE 1, the quality metric PSNR is approximately 95%. Mean Square Value is negligible. Image Fidelity, Pearson Correlation Coefficient and Normalized Correlation the value is approximately 1.

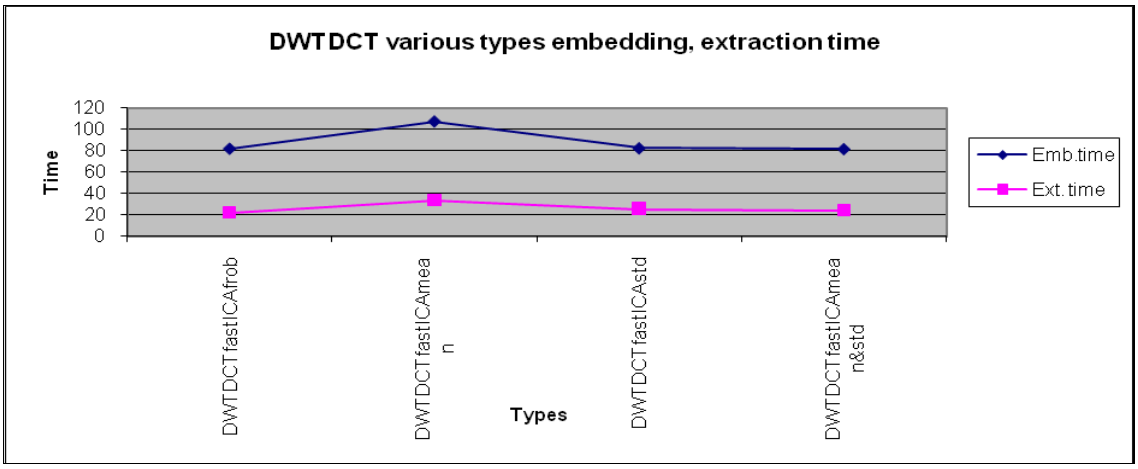


Figure 7. Embedding time and Extraction time for various test images in various watermark generation techniques.

From Fig. 7 Embedding time is same for the methods using Frobenius norm, Standard Deviation and Combined mean and standard deviation as watermark and their value is 80. The Embedding time for mean as watermark is 107. Similarly the extraction time is same for all the methods (20) except mean as watermark (33).

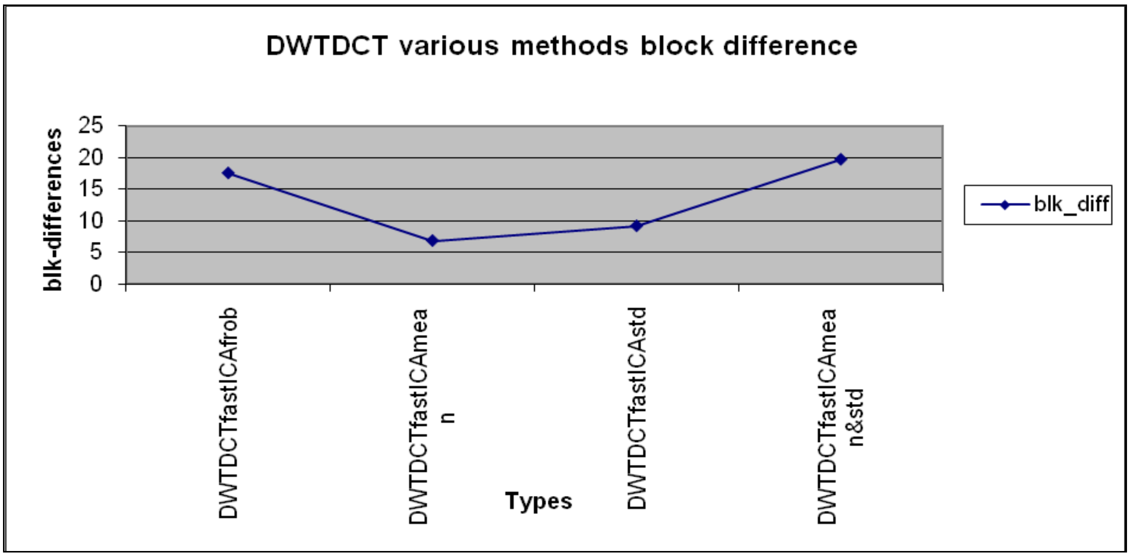


Figure 8. Percentage block difference between watermark extracted and the watermark for various test images in various watermark generation techniques.

From Fig. 8 Block wise difference is Less for mean as watermark and high for combined mean and standard deviation.

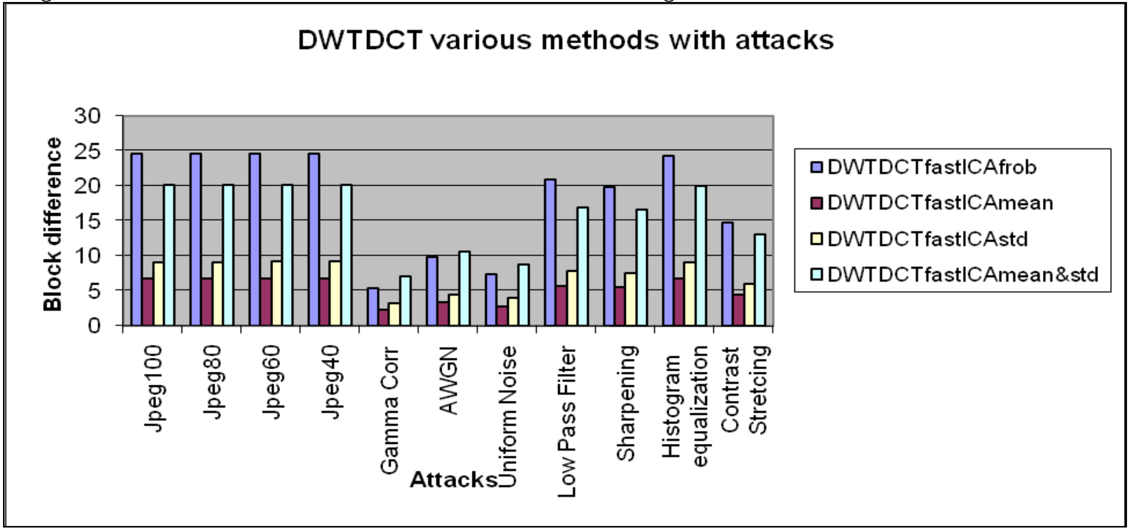


Figure 9. Percentage block differences for average test image values after incidental image processing operations. From Fig. 9 frobenius norm as watermark has high blockwise percentage difference for all attacks comparing to all other watermark techniques and mean as watermark has low blockwise percentage difference for all attacks comparing to all other watermark techniques.

Table 2. Quality Metrics after Watermarking. Using Hybrid DCT and DWT Watermarking with all watermark generation techniques.

Type	MSE	PSNR	IF	PCC	NC
DWTDCTfastICAfrob	2.61E-05	95.3177	1	0.999446	1
DWTDCTfastICAmean	2.13E-05	96.64904	0.999931	0.999813	0.9999
DWTDCTfastICAstd	2.1E-05	96.72099	0.999933	0.999814	0.999901
DWTDCTfastICAmean&std	1.51E-05	96.95161	0.999933	0.999851	0.999901

From TABLE 2, the PSNR value is almost same for all the methods and it is approximately 95%. IF, PCC, NC values are nearly same for all methods and it is 1. The MSE value is negligible for all methods.

V. CONCLUSION

This paper has discussed about content based watermarking of 4 different types of watermark generation schemes for image authentication using hybrid DWTDCT watermarking. The proposed system embeds the watermark in the HSV equivalent of the host image and changes it to RGB equivalent watermarked image. The attacks are applied on the RGB equivalent watermarked image. The proposed method correctly authenticates the image even under normal image processing operations and it correctly detects tampering and identifies the tampered regions of the image in all four watermark types. The quality of the watermarked image is better than the existing techniques. The average PSNR value in the proposed system is 95 % for all methods discussed in this paper. In terms of computation time mean watermark technique takes slightly greater time than other methods. Extensive experimentation demonstrates the efficiency of the standard deviation watermark method among the four methods developed.

REFERENCES

1. Abbasfard, M., Digital Image watermarking robustness: A comparative study, Master's Thesis, Delft, Netherlands (2009).

2. Chi-Hung Fan, Hui-Yu Huang and Wen-Hsing Hsu, Department of Electrical Engineering, A robust watermarking technique Resistant JPEG compression, Journal of Information Science and Engineering, 27, 163 – 180 (2011).

3. Kasmani, S.A, Naghsh –Nilchi , A, A new robust digital image watermarking technique based on Joint DWT-DCT transformation, Convergence and hybrid information technology, 2008, ICCIT '08 , Third international conference on 11-13 Nov. 2008 , Vol. 2 , Pages 539-544.

4. Raja' S. Alomari and Ahmed Al-Jaber, Computer Science Department, Jordan, A fragile watermarking algorithm for Content authentication, International Journal of Computing & Information Sciences, Vol. 2, No.1, Apr. 2004.

5. Bilgisayar Muhendisligi Bolumu, Firat Univ, Elazig Tatar, Y, A Novel fragile watermarking technique with high accuracy tamper localization, Signal Processing and Communications Applications , 2006 IEEE 14th, Pages 1-4.

6. Yeung, M.M. Mintzer, F, Invisible watermarking for image verification, ICIP (2)97, Pages 680-683.

7. Maeno, K, Qibin Sun, Shih-Fu Chang, Suto , M, New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization, IEEE transactions on Multimedia, Volume 8 , Issue 1, Pages 32-45.

8. Dinu Coltuc and Philippe Bolon , Color Image Watermarking in HIS Space, (0-7803-6297-7/00 2000 IEEE).

9. Dr. Latha Parameswaran, Dr. K. Anbumani, Content-Based watermarking for Image Authentication using Independent Component Analysis, Informatica 32 (2008) Pages 299 – 306.

10. Aapo Hyverinen, Survey on Independent Component Analysis, Neural Computing Surveys, Vol. 2, pp 04 – 128, 1999.