Iraqi Journal of Information Technology. V.9 N.4. 2019

Digital Watermarking Under DCT Domain According to Image Types

Assist lecturer: Hussein A.Hilal
University of Mustansiriyah – Computer Center
Baghdad – Iraq
Email: husseinabed342@gmail.com

Abstract

The massive development of information hiding and data security consists of several and communications technology has made it difficult to maintain the security and confidentiality of information, it is necessary to find new ways through which information can be preserved in a safe manner that enables users to retrieve it later and exchange information at any time. Information hiding is one of the most common and important techniques to use to achieve security and data confidentiality. Moreover; with the different multimedia it has no way to deal with it in the process of data concealment. Our proposed method aimed to hide the binary image bits inside the transformed image under DCT, after converting these coefficients from decimal to the binary form taking into consideration the type of image. The image type is defined by using the fuzzy c-men function, If the image is gray, then the optimal hiding site is block (32) that will used to hide the binary bits for the logo, each binary bits will be exchanging with the corresponding bit of the host under DCT domain, otherwise, if the host is color image, then the optimal hiding site is block (1) that will used to hide the binary bits for the logo, each binary bits will be exchanging with the corresponding bit of the host under DCT domain. The results has approved that our proposed method has ability and flexibility in dealing with different types of images while preserving the quality of the image after the concealment process, the proposed method has the ability to retrieve the binary image with the diaper on the quality and also the resulting image after the concealment is a high-quality image, the security aspect of the proposed method good and safe Because we do not deal with all the images in the same style of concealment, but the contrast is clear from the color image to the gray image as each image has a special place to hide.

Keyword: information hiding, color image, gray image, watermark, security.

العلامه المائيه المرقمه تحت نطاق (DCT) وفقا لنوع الصورة

المدرس المساعد:حسين عبد هلال

المستخلص

إن التطور الهائل في تكنولوجيا المعلومات والاتصالات جعل من الصعب الحفاظ على أمن وسرية المعلومات ، ومن الضروري إيجاد طرق جديدة يمكن من خلالها الحفاظ على المعلومات بطريقة آمنة تمكن المستخدمين من استعادتها في وقت لاحق وتبادل المعلومات في أي وقت. تعد تقانة اخاء المعلومات واحدة من أكثر الأساليب شيوعًا وأهمية وذلك لاستخدامها لتحقيق الأمان وسرية البيانات ، وعلى الرغم من الاختلاف في الهائل في الوسائط المتعددة فان هنالك طريقة محددة للتعامل معها في عملية إخفاء البيانات. ان الطريقة المقترحة تعمل على اخفاء بتات الصورة الثنائية في معاملات الصورة بعد تطبيق دالة DCT عليها وبعد تحويل تلك المعاملات من صيغة البيانات العشرية الى الثنائية مع الاخذ بعين الاعتبار نوع الصورة, نوع الصورة يتم تحديدة من خلال استخدام دالة fuzzy c-men , فاذا كانت الصورة ملونة فسوف يكون موقع الافاء الامثل لها هو block(1) لانة يعتبر الموقع الامثل للاخفاء مع الصورة الملونة اذا ما تم التعامل معها بدالة DCT واذا كانت الصورة رمادية فسوف يكون الموقع الامثل للاخفاء هو block (32) باعتبارة الموقع الامثل للصورة الرمادية اذا ما تم التعامل معها بدالة DCT, النتائج التي حصلنا عليها اثبت القدرة العالية والمرونة في التعامل مع الانواع المختلفة للصور مع الحفاظ على جودة الصورة بعد عملية الاخفاء, الطريقة المقترحة لها القدرة على استرجاع الصورة الثنائية مع الحفاض على جودتها وايضا فان الصورة الناتجة بعد عملية الاخفاء هي صورة عالية الجودة, الجانب الامني للطريقة المقترحة جيد وامن لاننا لا نتعامل مع كل الصور بنفس اسلوب الاخفاء ولكن التباين واضح من الصورة الملونة الى الصورة الرمادية اذ ان لكل صورة مكان خاص للاخفاء.

1. Introduction

With the increasing security issues in society, it is necessary to provide a sophisticated mechanism to deal with this kind of important issues. On the other hand, we note the great assistance that provided by the development of the Internet technology and digital information, which has become interrelated and connected with a wide network despite the huge amount of Information and interaction between them and despite the distance, but it has become an effective way to deal with information through access to the information required from anywhere in the world and as soon as possible, so; the need for a technology to help us secure this goal was solved, by hiding the secret information inside an multimedia such as: still image, sound, or video clip, that it is important to maintain its confidentiality without affecting the quality of that incubator environment with easy retrieval to the other beneficiary. Our proposed method aimed to hide confidential data in the binary format (text or logo) within the image, taking into account the type of image that used. If the host is colored, then the hiding site is different from whether the image is gray.

1. Related Work

The first attempts in this field begin to hide the data in binary form in the gray image and then evolved to deal with the grayscale image. With the development of the digital technology, it is possible to deal with the color images. As is known, the color image has a special character that differs from one to another, furthermore; the image nature which varies from one image to another and each color image gives results may differ from other images after embedding process, as the effect can be clear in the quality of the resulting image after the process of concealment. While we can avoid this by choosing a picture that is ideal in the embedding

process, or find a way to hide the binary bits without effeteness to the resulting image. The process of hiding the confidential data in the host is different in the terms of data. Hidden data may be logo in the binary form, and may be a text message, we will address the digital watermark in the current paper because of it is important to protect copyrights for important publications. Most of the attempts that have dealt with this field are working to hide binary data in the gray image, while there are few attempts to hide a gray image inside the host of gray scale image, some of these attempts are found in [1], while in [2]; the watermark in grayscale was divided into 8 binary bits, while some of these bits are hidden in middle band after applying Discrete Cosine Transform (DCT) to the whole original image. In the case of dealing with images of a special nature such as critical medical images, it is not possible to allow any change in the image quality, so; it must be used special lossless watermarking techniques, some of these method are used in [3; 4]. Another attempts aimed to embed a color watermark in color host, [5] developed a dithering method that consume a various color spaces like RGB, HSV, and CMY. In [6], a method for blind digital watermarking based on anti-geometric algorithm of color image watermarking and scale-invariant feature transformation (SIFT) under Discrete Wavelet Transform (DWT) is presented.

2. Watermarking Domain

The domain that used in dealing with the watermark bits varies from one method to another, there is a method that depends on the direct change of the pixel values of the original image, so that the process of embedding the binary bits of the watermark in the original image, this type of techniques is called spatial domain. On the other hand, converts these pixel from their natural state to other format called coefficients; these transactions will be dealt with in order to hide binary bits of the logo inside the host under transform domain. This method is called frequency domain. Embedding the watermark bits in the original image within the frequency domain has many benefits and is intended to increase the robustness. There are three main transform methods generally used, discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT). Our proposed method used the DCT for inclusion in the frequency domain; the chosen because of it is simple and related with JPEG, BMP coding standard.

3. The Proposed Method

Our proposed method depends on the type of original image in order to determine the optimal hiding site of the binary bits. This is done through the use of the fuzzy C-Men function, through which we can determine the type of image. After selecting the image 256×256 Bit Map Image file format BMP it is divided into non-overlapping 8 x 8 blocks size, the logo will be with size of 32×32 (binary BMP-32 bits), here we have 64 blocks and each block contains 64 coefficients after executing DCT on the each block for the whole original image, these transactions will be hide the logo bits in the least

two bytes in the far left for each reduction of the percentage of distortion in the image as a result of the process of concealment. After the completion of the process of dividing image under DCT domain and get transactions we will convert each coefficients form decimal to the binary form, then each bits form the logo will be embedded inside the corresponding bit of the host. If the image is color, the hiding site will be in block (1) of the low frequency domain, and the binary image bits are embedded as shown in step 7 of the algorithm1. Otherwise, if the image is gray, the hiding location will be in block (32) in the high frequency domain. After embedding process completed, the binary form of the host image will be converted to the decimal format, and then applied IDCT to obtain a watermarked image. The following figure shows a general outline of the proposed method, while figure (2) illustrated the general flowchart for the proposed method:

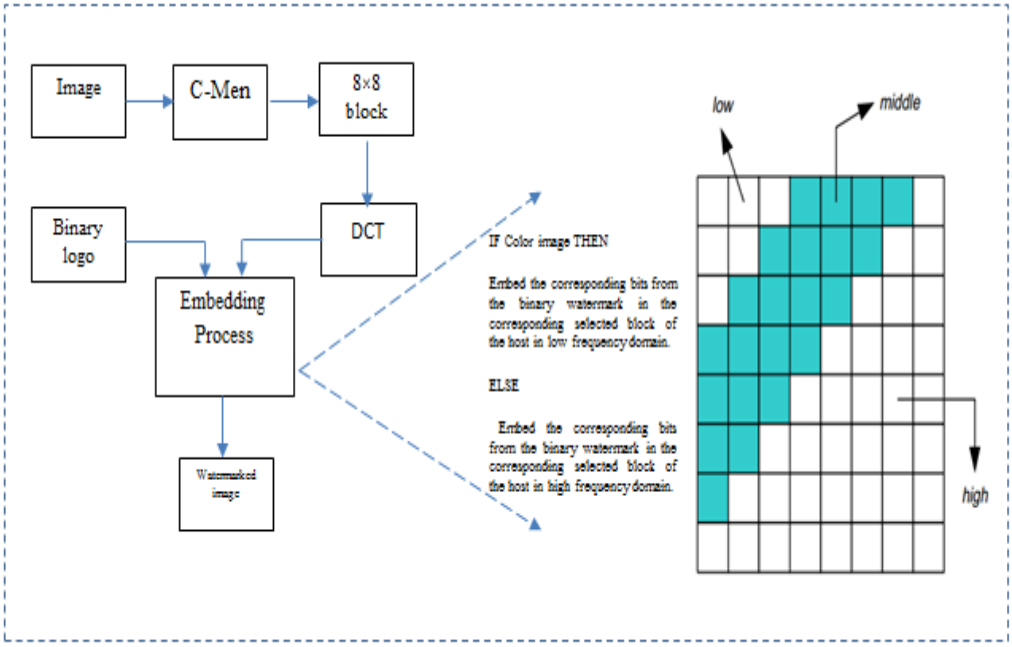

Figure (1): General Diagram for The Proposed Method

The Proposed method consists of following proses:

- Embedding Process.
- Extraction Process.

3.1 Embedding Process

After reading the original image with size of 256 x 256 BMP, as well as reading the binary logo with size of 32 x 32 (24 bit- BMP) , then C-Men function applied the on the original image to determine its type, then divide

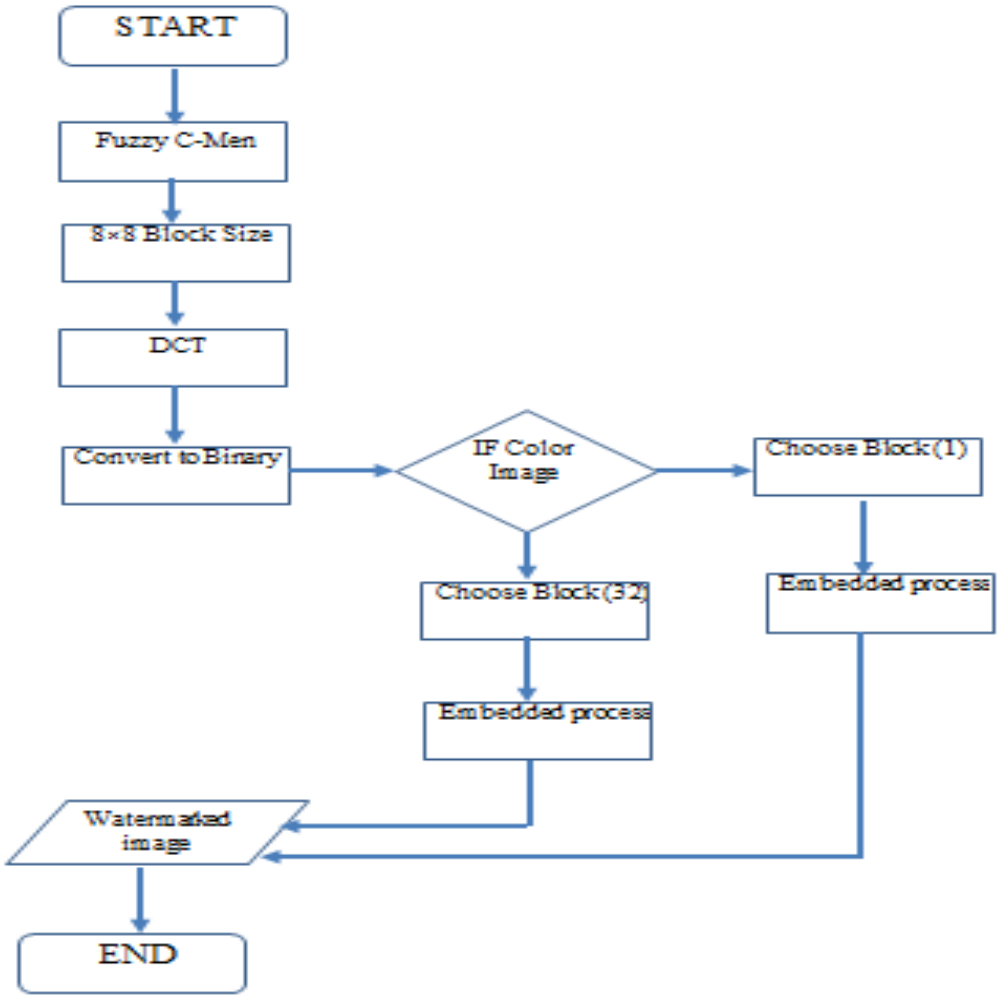

Figure (2): Flowchart for The Proposed Method

the original image into 8 x 8 non-overlapping blocks. Execute the DCT on all image blocks in order to Converting image values from pixels to coefficients, then convert these coefficients for the specified plots to the binary format, if the original image is colored, each bit of the logo will be hidden in the corresponding site in the selected block within the low frequency band of DCT domain, if the original image is gray, each bit of the logo will be hidden on the corresponding site for the selected block within the high frequency domain. This is because the color image has a large amount of extra information, unlike the gray image, which has less information about the color image. Therefore, the high frequency domain is selected in the proposed method to hide the extra bits if the image is gray, and the extra bit will be hide in the low frequency domain if the selected image is color, the contrast In the concealment site came because of the contrast in the type of image as well as to increase the security aspect of the proposed method, after completion of the embedding process for the entire

binary bits inside the host under DCT domain. We process the conversion of all transactions of the host from the binary to the decimal format and then apply the IDCT function on the entire host for the production of Watermarked Image which is the image that carries the watermark inside. The following algorithm illustrates our method of embedding:

Algorithm 1: Embedding Stage.

Input: Original Image, Binary Image

Output: Watermarked image

1. Read the original image O.
2. Read the binary image B.
3. Apply fuzzy C-Men to the O to check image type.
4. Divide O into 8×8 block size to produce $O_{b(i)}$, where i={1, 2, …. 64}.
5. Apply DCT for each $O_{b(i)}$ of the whole O to produce DCT coefficients as $O'_{b(i)}$.
6. Convert each $O'_{b(i)}$ to the binary form to produce $O''_{b(i)}$.
7. IF color image THEN
   Select $O''_{b(1)}$, and perform embedding process to the logo bits inside the corresponding binary sequence (least two significant bits 7, 8) of the selected block of low frequency domain.
   Else
   Select $O''_{b(32)}$, and perform embedding process to the logo bits inside the corresponding binary sequence (least two significant bits 7, 8) of the selected block.
8. Convert each $O''_{b(1)}$ to the decimal form of high frequency domain.
9. Apply IDCT.
10. Produce watermarked image as W_i.
    END.

3.2 Extraction Process

The extraction process of retrieving the binary logo from the watermarked image is done by applying the same steps that were handled in the embedding process, which begins with the application of Fuzzy C-Men to determine the image type and then divide the watermarked image into 8×8 non-overlapping blocks to produce the corresponding blocks, apply the DCT for each block of the whole image to produce the DCT coefficients and then convert those transactions to the binary form. If the received image is colored, the last two bits from the left side of the selected block from the low frequency domain, each bits will collected to recovered watermark. Otherwise choose the last two bits from the high frequency domain to retrieve the watermark image to be so convert those binary values to the decimal format and then apply IDCT to retrieve the binary image. The following algorithm shows us the embedding process:

Algorithm 2: Extraction Stage.

Input: Watermarked Image.

Output: Original Image, Recovered Watermark.

1. Read W_i.
2. Apply fuzzy C-Men to the O to check image type.

3. Divide W_i into 8×8 block size to produce $W_{b(i)}$, where i={1, 2, …. 32}.
4. Apply DCT for each $W_{b(i)}$of the whole W_i to produce DCT coefficients as $W'_{b(i)}$.
5. Convert each $W'_{b(i)}$ to the binary form to produce $W''_{b(i)}$.
6. IF color image THEN
   Select the least two significant bits (7, 8) from the selected block $O''_{b(1)}$ and perform extraction process.
   Else
   Select the least two significant bits (7, 8) from the selected block $O''_{b(32)}$, and perform extraction process.
7. Convert to the decimal form.
8. Apply IDCT.
9. The watermark extracted, and the original image recovered.
10. END.

4. Performance Measure

In our proposed method, the PSNR operation used to computes the value of peak signal-to-noise ratio in decibels units, between the original image and watermarked image to assess the quality of the watermarked image after embedding proses. PSNR computed by using equation 1:

$$PSNR = 10 \log_{10} \frac{(R)^2}{MSE} \quad 1$$

While Mean Square Error MSE that computed form equation 2, used to evaluate the quality for the recovered watermark after extraction process, MSE computed between the original watermark and the recovered watermark:

$$MSE = \frac{\sum_{x,y} [O(x,y) - R(x,y)]^2}{W*H} \quad 2$$

Another function that used to measure the difference ratio between the original watermark and the recovered watermark illustrated in equation 3:

$$AR = CP / NP$$

5. Result

The original color BMP images with size of 256×256 that used in the proposed method are illustrated in the following figure (3), while the gray images with the same properties are illustrated in figure (4), while figure (5) shows the color watermarked image, figure (6) shows the gray watermarked image. The color watermarked image that exposed to Salt&Peppers noise shows in figure (7), furthermore; the gray watermarked image that exposed to Salt&Peppers noise illustrated in figure (8). Filtered color watermarked image shows in figure (9), while the filtered gray watermarked image shows in figure (10). The original binary BMP logo with size of 32×32 of 24-bit that used in our proposed method illustrated in figure (11), and the recovered watermark from the color watermarked image shows

Figure (3): Original Image

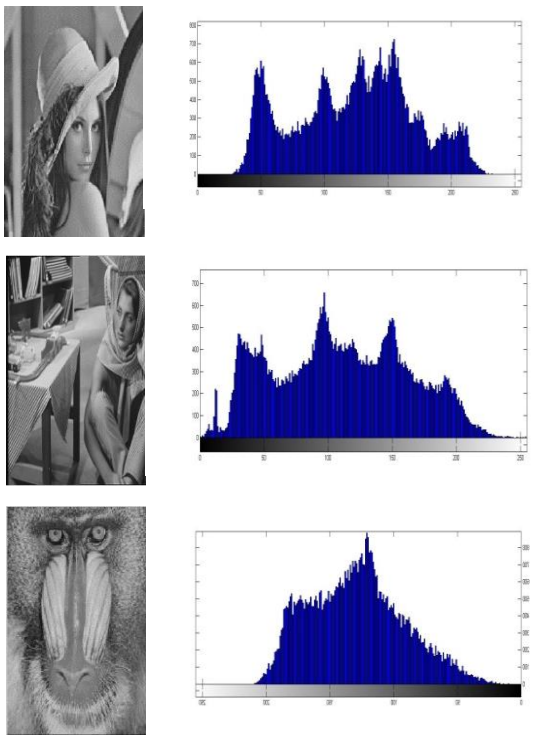

Figure (4): Gray Image

Figure (5): Color Watermarked Image

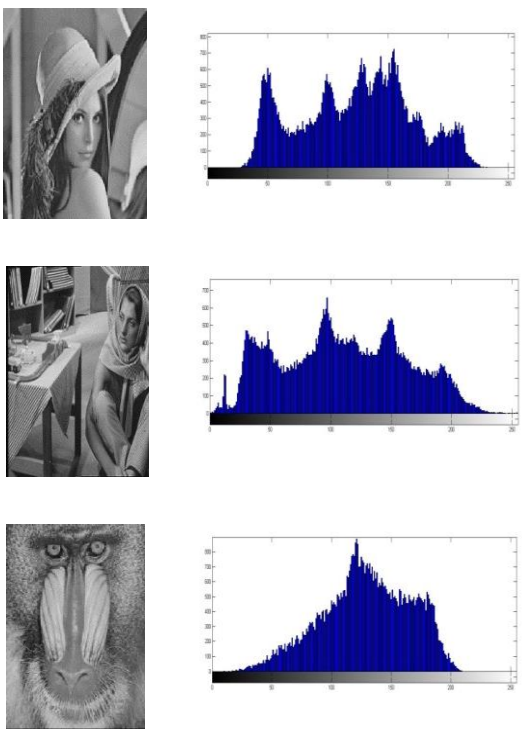

Figure (6): Gray Watermarked

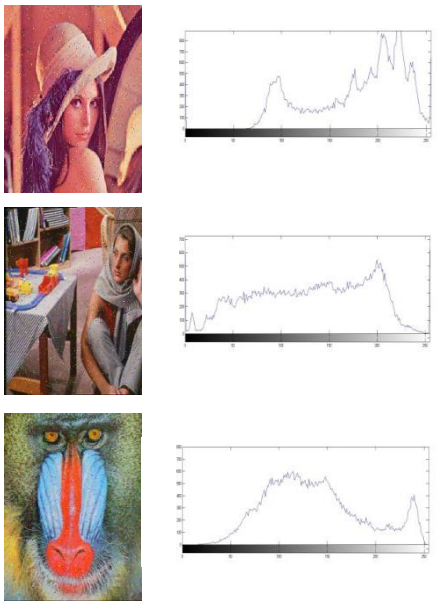

Figure (7): Color Watermarked Image After Salt&Peppers Noise

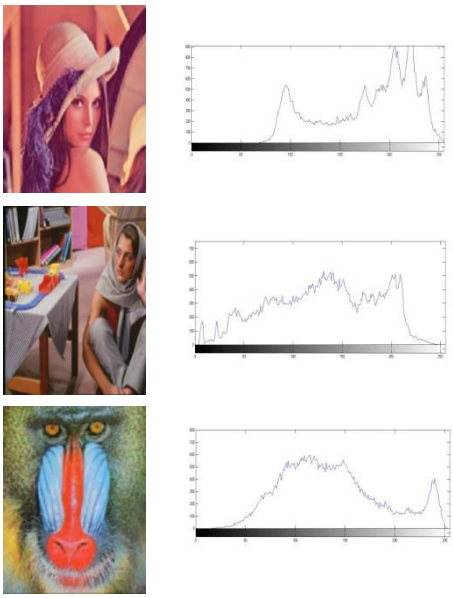

Figure (8): Color Filtered Watermarked Image

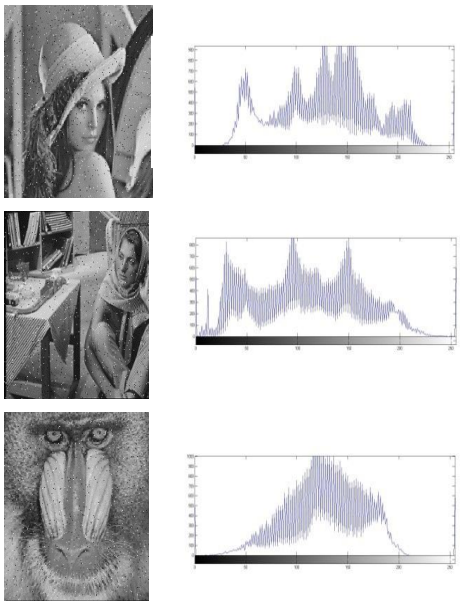

Figure (9): Gray Watermarked Image After Salt&Peppers Noise

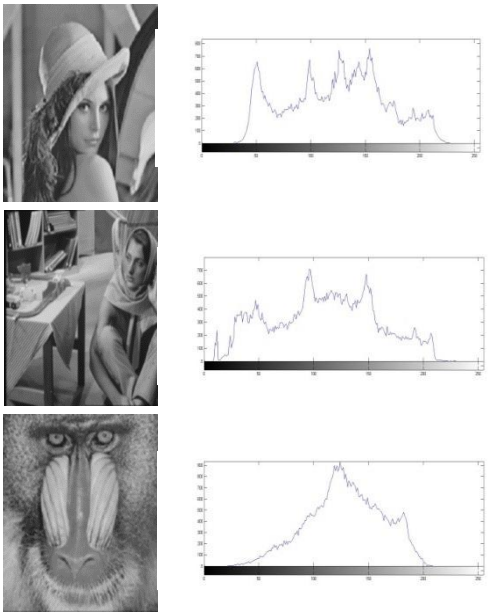

Figure (10): Gray Filtered Watermarked Image

The recovered watermark from color noised watermarked image illustrated in figure (14), and the recovered watermark from the filtered color watermarked image shows in figure (15). The recovered watermark from gray noised watermarked image illustrated in figure (16), and the recovered watermark from the filtered gray watermarked image shows in figure (17).

Figure (11): Original Binary Image

Figure (12): Recovered Watermark From

Figure (13): Recovered Watermark From

Figure (14): Recovered Watermark From Noised

Figure (15): Recovered Watermark From Filtered

Figure (16): Recovered Watermark From Noised

Figure (17): Recovered Watermark From Filtered

After objective evaluation side that showed in the above figures, the following tables illustrates the subjective side of the proposed method after embedding process, extraction process, noised process, and filtered process:

Table 1: The subjective Evaluation of The Color Image

Color Image	PSNR	MSE	AR
Original Watermarked	51.7645	0.99765	0.9943
Noised Watermarked	48.6452	0.4232	0.6534
Filtered Watermarked	49.3121	0.7645	0.8756

Table 2: The subjective Evaluation of The Gray Image

Gray Image	PSNR	MSE	AR
Original Watermarked	50.8678	0.8761	0.8821
Noised Watermarked	45.7754	0.4432	0.3421
Filtered Watermarked	47.4348	0.6544	0.6623

Table 3: The subjective Evaluation of The Binary Watermark

Watermark	MSE	AR
Recovered After Color Watermarked Image	0.9856	0.9941
Recovered After Gray Watermarked Image	0.9776	0.8934
Recovered After Noised Color Watermarked Image	0.7645	0.7388
Recovered After Filtered Color Watermarked Image	0.7581	0.8501
Recovered After Noised Gray Watermarked Image	0.9512	0.8113
Recovered After Filtered Gray Watermarked Image	0.9334	0.8011

The variation in the results for our proposed method between color image and gray images is not great, but the disparity in the values that shown in the previous tables comes from the field of embedding process that used, we explained that the color images will be handled with the low frequency domain, while the binary bits image will be hide in the high frequency domain with the gray image. Therefor the quality for the recovered watermark of color watermarked image is better than the recovered watermark from the gray watermarked image, which was supposed to give better results than the color images because of their color nature and the embedding process done within the range of high frequencies gave less results than the color image, although it is acceptable in terms of quality. If try to deal with the color image within the high frequency domain, the resulting watermarked images will be as shown in the following figure, noting that the watermark cannot be retrieved:

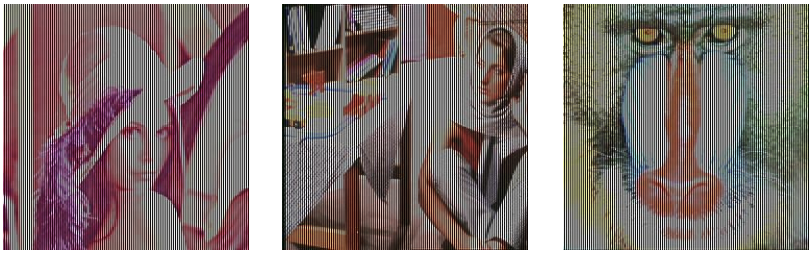

Figure (18): Color Watermarked Image with High Frequency Domain

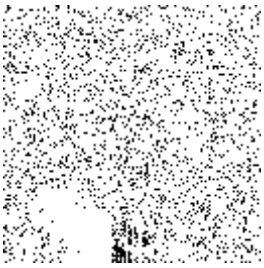

Figure (18): The Recovered Watermark with High Frequency Domain

6. Conclusion

In this paper, a digital watermarking block based a cording to the image types is presented. Our proposed method deal with still standard test image with different texture, the binary watermark bits will be embedded in the host under DCT domain, if the host is color the binary bits will be embedded in the corresponding selected block of low frequency domain, otherwise; the binary bits will be embedded in the selected block of high frequency domain. The watermarked images for both color and gray are exposed to some type of intended attack such as Salt&Peppers noise, it was found that the watermarked image survive this type of attack and the binary watermark is recovered. Different evaluation measures used to measure the quality for the watermarked image and the recovered watermark after embedding process. Experiments results indicate that the proposed method revealed a good quality for the objective side and good value in the subjective side.

7. References

[1] S. P. Mohanty, B. K. Bhargava., "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks." ACM Transactions on Multimedia Computing, Communications and Applications, November 2008, Issue 2, Vol. 5.

[2] X. M. Niu, Z. M. Lu, S. H. Sun., "Digital watermarking of still images with gray-level digital watermarks." IEEE Transactions on Consumer Electronics, 2000, Issue I, Vol. 46, pp. 137-145.

[3] W. B. Lee, T. H. Chen., "A public verifiable copy protection technique for still images." The Journal of Systems and Software, 2002, Issue 3, Vol. 62, pp. 195-204.

[4] J. M. Shieh, D. C. Lou, M. C. Chang., "A semi-blind digital watermarking scheme based on singular value decomposition." Computer Standards & Interfaces, 2006, Issue 4, Vol. 28, pp. 428- 440.

[5] N.Vinay, A.Venkat, C.Sunil and V.Raghavendra," An Enhanced invisible Digital Watermarking Method for Image Authentication "International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12016-12022.

[6] C.G. Thorat, B.D. Jadhav, "A Blind Digital Watermark Technique for Color Image Based on Integer Wavelet Transform and SIFT", Procardia Computer Science 2 (2010) 236–241, 1877-0509© 2010 Published by Elsevier Ltd.