University of Baghdad
College of Engineering
JE
JOURNAL OF ENGINEERING

Electrical, Electronics and communications, and Computer Engineering

Digital Color Image Watermarking Using Encoded Frequent Mark

Abdulkareem Mohammed Salih*
Assist Lecturer
Al-Dour Technical Institute-Northern Technical
University
abdulkreem86@gmail.com

Salih Hassan Mahmood
Assist Lecturer
Al-Dour Technical Institute-Northern Technical
University
saleh_hassan64@yahoo.com

ABSTRACT

With the increased development in digital media and communication, the need for methods to protection and security became very important factor, where the exchange and transmit date over communication channel led to make effort to protect these data from unauthentication access.
This paper present a new method to protect color image from unauthentication access using watermarking. The watermarking algorithm hide the encoded mark image in frequency domain using Discrete Cosine Transform. The main principle of the algorithm is encode frequent mark in cover color image. The watermark image bits are spread by repeat the mark and arrange in encoded method that provide algorithm more robustness and security. The proposed algorithm efficiency is measured by using many of measurement factors such as Peak Signal to Noise Ratio PSNR and Normalized Correlation Coefficient NC, the watermark robustness and feasibility are measured by using many types of attacks.
Key words: watermarking, security, robustness.

العلامة المائية للصور الرقمية الملونة باستخدام العلامة المشفرة المكررة

عبد الكريم محمد صالح
مدرس مساعد
المعهد التقني الدور-الجامعة التقنية الشمالية

صالح حسن محمود
مدرس مساعد
المعهد التقني الدور-الجامعة التقنية الشمالية

الخلاصة

مع زيادة التنمية في وسائل الإعلام والاتصالات الرقمية ، أصبحت الحاجة إلى أساليب الحماية والأمن عامل مهم جدا، حيث أدى تبادل وإرسال البيانات عبر قناة اتصال الى بذل الجهود لحماية هذه البيانات من الوصول بطريقة غير شرعية.
قدم البحث طريقة جديدة لحماية صورة الملونة من الوصول الغير مخول باستخدام العلامة المائية. الخوارزمية تتضمن إخفاء صورة علامة المشفرة في مجال التردد باستخدام دالة تحويل جيب التمام المتقطعة. المبدأ الرئيسي من الخوارزمية هو تشفير علامة متكررة في الصورة الملونة. حيث تنتشر بيانات العلامة المائية من خلال تكرار العلامة وترتيبها بطريقة مشفرة تعطي الخوارزمية أكثر وثوقية وسرية. يتم قياس كفاءة الخوارزمية المقترحة باستخدام العديد من العوامل مثل قياس الذروة نسبة الإشارة إلى الضوضاء PSNR ومعامل الارتباط الطبيعي NC، يتم قياس المتانة والجدوى باستخدام العديد من أنواع الهجمات.
كلمات رئيسية: العلامة المائية ٫ الأمنية ٫ متانة.

---

1. INTRODUCTION

The process of embedding invisible signal in an image called Digital Watermarking Image. This process consider a form of copyright Protection, **ElGamal, et al., 2013**. Watermarking classify according to many parameters, at first according to the domain of embedding and extraction where two domain are used spatial domain and frequency domain. The spatial domain used the cover image without convert it to frequency domain and it is characterized by simplicity and less immunity to attacks where as in frequency domain the cover image transfer to frequency domain using Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), the transform coefficients modified by the mark value, then to get the mar image, one should perform the transform inversely**, Hajjara , et al. , 2009**.The visibility is another parameter to classification where there are two types: visible watermarking and invisible watermarking, visible water mark is clearly detectable .While the invisible watermarking is used to identify the owner or the origin of the host image, **Giri ,et al. ,2015** . Many techniques for color image watermarking are presented, Some of these techniques focus on spatial domain as in **Dharwadkar,** and **Amberker, 1999,** where the paper focus on the average intensity which is estimated from the intensities of the R, G and B components. In **Abdallah,** and **Hammo , 2006,** deals with colored images in the biological color model, the Hue, Saturation, and Intensity (HSI), where the method robustness is tested against several attacks. Watermark security is increased by using the Hadamard transform matrix. .Another part of researches focus on the transform domain using (DCT) as in **Abraham, and Paul, 2016,** it uses Discrete Cosine Transform to transform the host image into frequency domain for selecting appropriate coefficients for watermark embedding. Wavelet transform is another type of the transform domain which provide the property of multi-Resolution analysis, many of searcher focus on this property as in **Sharma ,**and **Prashar, 2012** .There are papers merge more of transform as in **ElGamal , et al. , 2013**, the searchers joined between DCT and (DWT) which take advantage of the two frequency domains.

The main objective in the proposed paper is to present the hiding watermark in color cover image using encoded frequent mark embedded in frequency hopping since much than one frequency are used to embed the watermark in DCT blocks for get more security , then the watermark image is extracted at the receiver without need for origin image . The rest of this paper is organized as follows: In Section 2 Discrete cosine Transform explained. Section 3 discusses the Basic watermarking criterias.Watermark Embedding and Watermark Extraction respectively explained in section 4 and section 5. Error and Correction Ratio are explained in Section 6. Section 7 contain Encoded and Frequent Stage. Simulation Results are discussed in Section 8. Finally, Section 9 concludes the paper.

2. DISCRETE COSINE TRANSFORM

 Discrete Cosine Transform (DCT) can be defined is a transformation algorithm that converts images from spatial domain to frequency domain **ElGamal , et al. ,2013**.Carried out watermarking need to change the transform coefficients and the DCT watermarking is more robust compared to the spatial domain **Hajjara, et al. , 2009** .

3. BASICS WATERMARKING CRITERIAS

Watermarking algorithm to be efficient, many criterias should be obtained or saved as explained:-

1- Invisibility: which means the quality of cover image should not be effected and cannot be explained by users **Giri, et al., 2015**.

2- Robustness: Means the immunity to the various signal operation that can be obtain during transmit such as noise ,compression and resizing **Patel ,**and **Tahilramani ,2016**.

3- Security: can be defined as the ability to resist hacking attempts to remove the mark without modified cover image **Hui-fang, et al., 2010**.

4- Capacity: means amount of information bits can be inserted in cover image **ElGamal, et al. , 2013**.

4.   PROPOSED WATERMARK EMBEDDING

As shown in **Fig.1**, many stages are used in embedding side, these stages explained as:

1- Convert the color image from RGB components to YCbCr components.Since the Luminance (Y) is less sensitive for human.

2- The Luminance (Y) layer convert to (8*8) non-overlapped DCT domain.The size of (8*8) standard as in **Abraham, and Paul, 2016**.

3- For the mark, encoded frequent mark is used, where the binary image mark is used and the mark is encoded in way that depend on repeated the bits value of mark and reposition these bit in a sequence predefined at Extraction side. This step consider the main aim for this algorithm, where the criterias of watermarking image are saved. The number of repeated is commensurate extrusive with capacity criteria, where as directly proportional with security and robustness criterias.

4- The encode bits are insert in frequency domain layer of cover image, middle frequency positions are used for insertion and these positions selected using predefined secret key.

5- Convert the Luminance component (Y) from Frequency domain to spatial domain.
    Convert YCbCr components to RGB components to obtained watermarked image.

5. PROPOSED WATERMARK EXTRACTION

At the receiver side in **Fig.2** backward steps are used to recover mark image as explain:

1- Convert the watermarked color image from RGB components to YCbCr components.

2- Convert the Luminance component (Y) to Frequency domain to.

3- Select the position of insertion mark value, where the middle frequencies are used and these positions can be selected depend on secret key.

4- After extract the mark value, decode stage is used which include obtaining a one copy of mark image. The number of copy and rules of select sequence mark value are predefined in Embedding stage.

5- The value of the sequence is threshold to '1' or '0'.

6. ERROR AND CORRECTION RATIO

The quality of the watermarked image can be calculated by finding the value of Peak Signal to Noise Ratio PSNR **Sharma,** and **Prashar, 2012,** as shown:

$$PSNR = 10\log10\ 2552/RMSE \tag{1}$$

Where the RMSE is root mean square error and equal to:

$$RMES = 1/(M*N)\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N}[I(i,j) - f(i,j)]^2} \tag{2}$$

M and N are image dimensions (number of pixels) (M=N). The similarity between extracted mark and the origin mark can be calculated by finding the Normalized correlation coefficient NC as in Eq. (3):

$$NC = \sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j)w^*(i,j)\ /\sum_{i=1}^{M}\sum_{j=1}^{N} w(i.j)^2 \tag{3}$$

Where w (i , j) and w*(i , j) represent the origin and extracted watermark respectively. The value of NC equal to1 as maximum value **Zubair , et al. ,2009.**

7. ENCODED AND FREQUENT STAGE
This stage include two steps, the first step make numbers of copy of mark and this number is commensurate extrusive with security and robustness criteria where as inversely proportional with the Capacity and PSNR for the watermarked image. **Fig.3** show the ratio between the PSNR and the number of mark copies. Second step include redistribution the bits sequence of the copies in away predefined at embedding and extraction stage.

8. SIMULATION RESULTS
In order to test the proposed algorithm, color (512*512) pixels images are used. Lena, Peppers and Airplane image used as cover images.In other side binary images size (64x64) pixels is used as mark image.The size of (512*512) constribte in capacity criteria. PSNR calculated to depend it as criteria metrics (it calculated for Number of mark copy =2).**Table 1** show the value of PSNR While **Table 2** show Normal Correlation and how it effect during transmitted or attack by hackers and these process may changed or modified.

9. CONCLUSION
New proposed algorithm presented in this paper for watermarking digital color image. This algorithm focus on away where make the criterias of watermarking are most important properties. Color image cover has three layers of color and one of these layer is used. The number of copies that can be inserted in this layer may be one copy or more ,this depend on the value of PSNR for watermarked image where the PSNR will reduce when the number of copies increased as shown in the graphs in **Fig.3** and the property of capacity achived . The redistribution of these copies give a security form for algorithm since the position of bits injection are known only in the extraction stage and it will contibute in increasing the security criteria . Techniques are used such as the position of insertion in DCT domain and position of insertion in over all the image led to reduce the effect of attacks on the watermarked image and as a result the robutness became agood. These properties are explained in results obtain as shown in **Table 1 and 2**. Five types of attacks are used and the value of NC obtained from extracted mark used as factor for the good robustness of the algorithm as compared with **Imran**,and **Harvey , 2017** and other referenced mentied in with **Imran**,and **Harvey , 2017** as shown in **Table 3**.

10. REFERENCES

- ElGamal, A, F, Mosa, N.A. and ElSaid, W. K.   , 2013 ,*Block-based Watermarking for Color Images using DCT and DWT*, International Journal of Computer Applications,Vol. 66, No.15, PP. 0975 – 8887.

- Hajjara, S. ,   Abdallah, M. , and Hudaib , A.2009   ,*Digital Image Watermarking Using Localized Biorthogonal Wavelets*, European Journal of Scientific Research,Vol.26, No.4, PP.594-608.

- Giri, K. J., Peer, M.q A. and Nagabhushan , P. , 2015, *A Robust Color Image Watermarking Scheme Using Discrete Wavelet Transformation* , I.J. Image, Graphics and Signal Processing,Vol.7, No.1 , PP. 47-52.

- Patel, Sh. K.J. , Tahilramani, N. V. , 2016, *Information Hiding Techniques: Watermarking, Steganography: A Review*, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 4, No. 4, PP. 168-173.

- Hui-fang, LI, Ning, CH., and Xiao-ming, CH. ,2010, *A Study on Image Digital Watermarking Based on Wavelet Transform* ", The Journal of China Universities of Posts and Telecommunications, (Suppl.) ,Vol. 17,No. 1,PP. 122–126.

- Sharma, Ch., Prashar,D. , 2012, *DWT Based Robust Technique of Watermarking Applied on Digital Images* , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol. 2,No. 2 , PP. 399-402.

- Zubair , A. R. ,   Fakolujo , O. A. , and   Rajan, P.K. ,2009, *Digital Watermarking Of Still Images With Color Digital Watermarks*, EUROCON 2009, EUROCON '09. IEEE, Vol.64, No.1, PP.18-23.

- Abraham, J. and Paul, V.   , 2016, *A DCT Based Imperceptible Color Image Watermarking Scheme*, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.7, pp.137-146.

- Dharwadkar, N. V. and Amberker , B. B. ,1999 , *Secure Watermarking Scheme for Color Image Using Intensity of Pixel and LSB Substitution*, School of Information Technology and Engineering,Vol.1,No.1,PP. 1-6.

- Abdallah, D. M. , and B. Hammo , 2006, *Dual Domain Watermarking in the Biological Color Model*, IEEE InternationalConference on Information and Automation (ICIA), pp. 407-411.

- Imran,M. and Harvey,B.,A. ,2017, *A Blind Adaptive Color ImageWatermarking Scheme Based on Principal Component Analysis, Singular Value Decomposition and Human Visual System,* Radioengineering , Vol.26,No.3,PP. 823-834

NOMENCLATURE:
YCbCr=Luminance and Chrominance
NC=Normal Correlation Coefficient
PSNR= Peak Signal to Noise Ratio
RGB: Red, Green, and Blue
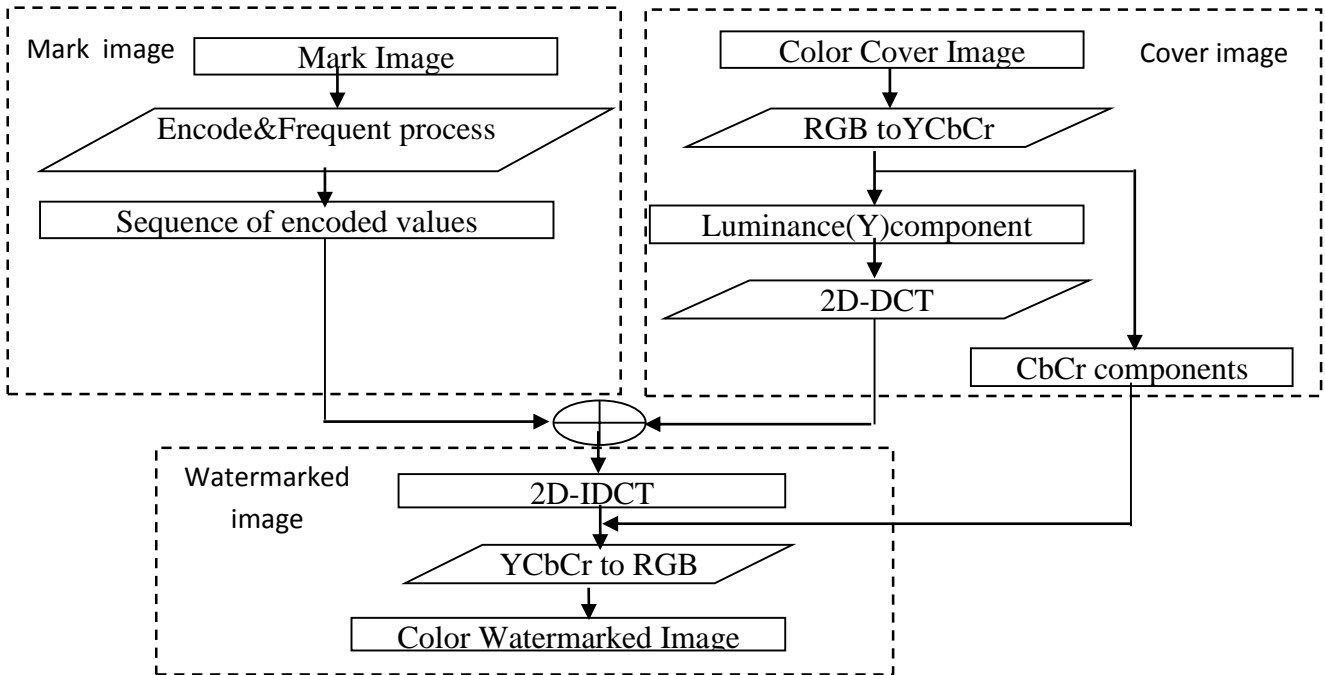
Figure 1. Proposed Algorithm for Watermark Embedded.
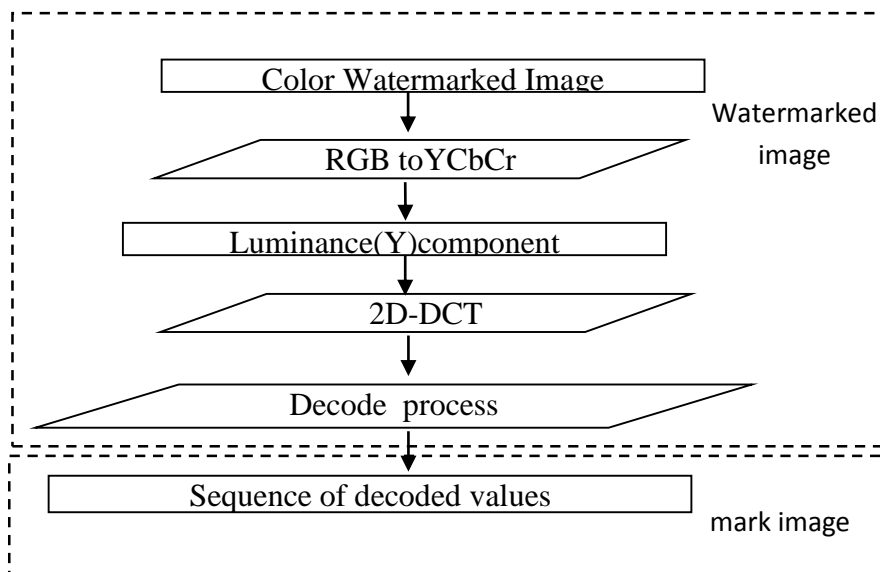
Figure 2. Proposed Algorithm for Watermark Extraction.
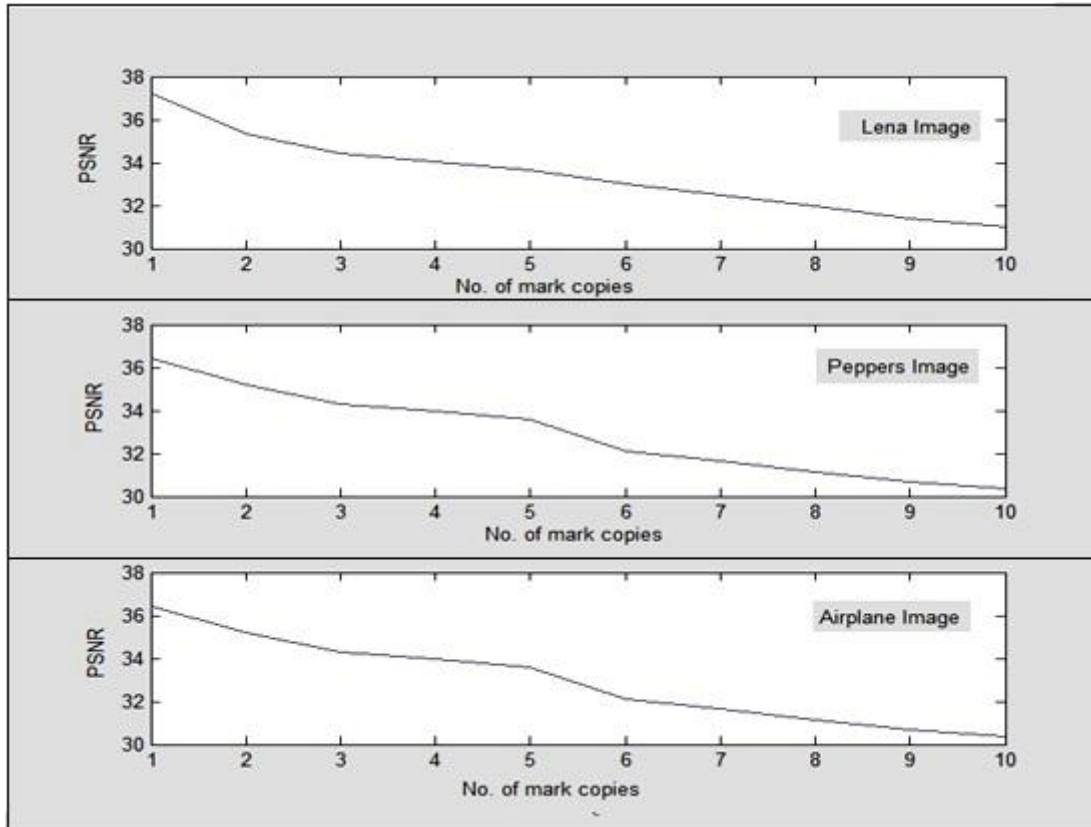
Figure 3. Ratio between PSNR and Number of Mark Copies.

Table 1. PSNR for Watermarked Color Image.

Lena Image	Peppers Image	Airplane Image
35.332 db	35.1734 db	34.7786 db

Table 2. NC for Extracted Mark Image.

Lena Image					
Type of Attacks	Without attack	Cut part from image	LPF	Salt and Peppers	Mean Filter	Gaussian Filter
NC	1	0.998	0.996	0.953	0.966	0.972
Extracted Mark Image						

Peppers Image					
Type of Attacks	Without attack	Cut part from image	LPF	Salt and Peppers	Mean Filter	Gaussian Filter
NC	1	0.999	0.952	0.946	0.9592	0.9743
Extracted Mark Image						

Airplane Image					
Type of Attacks	Without attack	Cut part from image	LPF	Salt and Peppers	Mean Filter	Gaussian Filter
NC	1	0.990	0.963	0.948	0.959	0.974
Extracted Mark Image						

Table 3. NC Comparsion(Lena Image) for Different Techniques.

Types of attack	Proposed Algorithm	Imran,and Harvey ,2017	[3] in Imran,and Harvey ,2017	[6] in Imran,and Harvey ,2017	[13] in Imran,and Harvey ,2017	[14] in Imran,and Harvey ,2017
Cut part from image	0.998	0.8570	0.6322	0.6825	0.7370	0.6216
LPF	0.996	-	-	-	-	-
Salt and Peppers	0.953	0.8656	0.5270	0.7406	0.7420	0.5436
Mean Filter	0.966	-	-	-	-	-
Gaussian Filter	0.974	0.8583	0.5797	0.7438	0.7896	0.5823