

## **New method for Increasing watermarked image quality and security**

**Rana J.S. Al-janabi**

**Shroouq J.S. Al-janabi**

**Zinah Hussein Toman**

**Rana.Aljanaby@qu.edu.iq**

**Shroouq.jumaa@qu.edu.iq**

**Zinah.hussein@qu.edu.iq**

**Collage of Computer Science & Information Technology**

**Al-Qadisiyah University**

**Recived : 24\8\2017**

**Revised : 7\9\2017**

**Accepted : 19\9\2017**

### **Abstract**

Recently, information transmission is done electronically, information can be stored and manipulated easily using computer, information transferring should be done in secure way. Watermark is a technique that can be used to secure data.

In this paper, a new watermark algorithm is proposed which depends on integer wavelet transform, arithmetic encoding and adaptive run length encoding. Adaptive run length encoding is used to compress watermark before embedding process. Arithmetic encoding can be used to compress data in original image that are needed to be retrieved from watermarked images to recover original image without any differences after watermark extraction process.

To avoid the problem of traditional Run Length Encoding Technique that may produce file that is larger than original one. Adaptive run length encoding is suggested which is used to compress watermark in cover image. The adaptive compression technique can be done several times on watermark using different number of bits to represent counts of runs and produce several vectors for number of runs, compare several results and select smallest vector from them. Surely, the smallest vector means that watermarked image will be high quality image; capacity will be better and adaptively ensure embedding process will be more secure.

## 1. Introduction

Wavelet transform allows us to hide information in regions that is less sensitive to human visual system. Those regions are (HL, LH and HH), hiding data in these bands can increase robustness and provide high image quality [1].

Integer wavelet transform convert integer data group into another integer data group, while in discrete wavelet transform, the wavelet filter that are used , produce floating point coefficients, therefore these coefficients are used to hide data and any truncation of these value will cause loss of hidden data which in turn leads problem in hide data system[1]. To avoid problems of floating point truncation, integer wavelet transform can be used. Integer wavelet transform can be performed using lifting scheme [2].

Arithmetic coding is a type of entropy encoding used in lossless compression. Arithmetic coding vary from different types of entropy encoding, like Huffman coding, in that instead of separating the data input into symbols and replacing each one with a code . Arithmetic coding depends on recursive; it encodes one data symbol per iteration. Arithmetic coding encodes the whole message into one number, a fraction  $q$  where  $0.0 \leq q < 1.0$  [3].

RLE (Run-length encoding) is a simple type of data compression scheme, where the count for the same data is stored as a single count and single data value. RLE is very useful for the image which contains many runs, huge number of same data value. The Run length encoding technique is a lossless compression for input images that is based on sequences of identical values (runs) [4]. Run Length Encoding may be effective for some types of image, but it is not commonly effective for text, because letter of the alphabet is rarely occurred more than twice successively [5].

## 2. Watermark characteristic and classification

Watermarking can be used in image/video copyright protection. There are several properties of a watermarking algorithm according to the application it was designed for. The following are the watermarking algorithm properties [6]:

- Imperceptibility: watermark is called imperceptible if the cover image and the watermarked image are perceptually indistinguishable. Watermark is called perceptible if its existence in the watermarked image is noticeable.
- Robustness – watermark is called robust if watermark is able to survive any reasonable processing impose on the carrier and is called fragile when it doesn't not pass to detect a minor modification.
- Security – indicate the watermarked image should not provide any information of the existence of the watermark to avoid un-authorized detection.
- Capacity- It means the size of information that can be embedded in original cover.

Digital image watermarking algorithms can be divided into two types according to the embedding domain: the first is spatial domain, second is transform domain. The spatial domain watermarking methods are easy to implement but they are less robust to different geometric and non geometric attacks. Transform domain methods can yield more information embedding and more robustness against many common attacks. But the computational cost is higher than spatial-domain watermarking methods [7].

## 3. Related Work

IEEE publish research addressed " Lossless Data Hiding Based on Integer Wavelet Transform" (2002), This paper proposes a new data hiding algorithm based on integer wavelet transform, which can recover the cover image without any distortion from the watermarked image after watermark has been extracted. It can embed much more data compared with the existing lossless data hiding techniques and satisfy the imperceptibility requirement [8].

S. KHAN, N. AHMAD, and M. NAEEM (2015). propose new method that compress stego image using Run Length Encoding without loss of secret message. A hiding capacity of this method is 50% has been achieved with PSNR greater than 30dB limit and a compression ratio of greater than 1 has been achieved [9].

To produce better results, the proposed algorithm suggest compressing watermark before embedding stage, compression is done using adaptive run length encoding. Adaptively, enhance security and avoid producing compressed data that are larger than original data which are one of run length encoding disadvantage when runs are little.

#### 4. The proposed algorithm

This method depends on compress part of cover image which are dedicated for embedding process and compress watermark using adaptive Run length encoding, Algorithm(1) explains the embedding algorithm. The proposed algorithm embed compressed watermark in HL,LH and HH sub bands.

Algorithm (1):- Proposed embedding Algorithm

**Proposed Embedding Algorithm**

---

Input:- grayscale image, Binary watermark image.

Output:- Watermarked Image.

---

Step1:- convert cover image into grayscale image if necessary.

Step2:- perform integer wavelet transform.

Step3:- compress integer wavelet coefficient (CH,CV and CD) using arithmetic coding.

Step4:- compress watermark bits using adaptive run length encoding.

Step5:-embedding process done for compressed watermark and wavelet coefficients.

Step6:- perform inverse integer wavelet transform to produce watermarked image.

In algorithm (1), step (4), watermark is compressed using adaptive run length encoding, this method produces smallest vector, and this vector is used to avoid produce

data that are larger than original file, generally in watermark image this method is work

effectively. Algorithm (2) explains adaptive run length encoding.

Algorithm (2):- Adaptive Run length encoding.

**Adaptive Run Length Encoding**

---

Input: Binary watermark image.

Output: Compressed watermark image

---

Step1: read binary watermark image.

Step2: Initialize number of bit to represent the same data value (n=3)

Step3: Produce vector of compressed image using number of bits (n).

Step4:  $n=n+1$

Step5: Produce vector of compressed image using New number of bits (n).

Step6: Calculate the size of both produced vectors

Step7: If the size of new vector is less than size of previous one then go to step3.

Step8: take the smallest vector as the best.

Step9:- make agreement between the sender and receiver on number of bits.

In fact, this algorithm gives vector always smaller than original file and it is very suitable for watermark (binary image).

Extraction algorithm is done exactly in reverse steps for embedding algorithm.

### 5. Embedding Example

This technique are used to compress the watermark at representation stage, compressing process is done using new proposed technique that is called (adaptive RLE). Using the following technique will be illustrated below:-

Assume the embedded stream is  
 (000000000000000000000000000000001111111  
 11111111111111111111111111111111 ) and table (1)  
 will explain how to represent vectors of run  
 length encoding

**Table (1):- explains vector length for each  
 number of bits according this example**

Number of bits to represent count value (n)	Count Value	Data Value	Vector Length for each (n)
3 bits	111	0	40 bits
	111	0	
	111	0	
	111	0	
	011	0	
	111	1	
	111	1	
	111	1	
	111	1	
	011	1	
4 bits	1111	0	30 bits
	1111	0	
	0001	0	
	1111	1	
	1111	1	
	0001	1	
5 bits	11111	0	12 bits
	11111	1	
6 bits	011111	0	14 bits
	011111	1	

In this example, 5 bits are selected to represent (n). because 5 bits produce smallest vector (12 bits). Therefore, it will be used between sender and receiver.

### 6. Result

Usually, values for the Peak Signal to Noise Ratio are around from 30 to 50 dB, in fact, higher is better. Figure (1), figure (2) and figure (3) show that there are no distortion in watermarked image. The compression for data will effect directly to imperceptibility and capacity



Lena A: original image



Lena B: Watermarked image

**Figure(1):- shows there are no visible differences between Lena (A) and (B)**



Baboon A: original image



Baboon B: Watermarked image

**Figure(2):- shows there are no visible differences between Baboon (A) and (B)**



Airplane A: original image












Airplane B: Watermarked image

**Figure(3):- shows there are no visible differences between Airplane (A) and (B)**

Table (2) shows that the result of watermark in this algorithm gives a high quality of watermarked image (PSNR is high). This is because watermark is compressed before embedding process. PSNR for compressed

watermark as well as capacity is increased because of using compression before embedding process. In fact, using of three type of lossless compression allow to receiver to extract watermark without any losing.

Image No. 512X512x8	Watermark size	Compressed Watermark size	Watermark	Embedded data in Bits (compressed data: original data+ watermark)	PSNR
Lena	27547	1610		55516	44.77
Baboon	27547	1610		89378	43.23
Airplane	27547	1610		65105	44.23
Lena	58000	30700		84606	42.80
Baboon	58000	30700		118468	41.84
Airplane	58000	30700		94195	42.44
Lena	58750	19360		73266	43.37
Baboon	58750	19360		107128	42.29
Airplane	58750	19360		82855	42.99

Also, it can be noticed that the first watermark has a high sequence of identical value, so, it compressed and give PSNR higher than others

## A

In fact, when comparing our proposed method and previous one mentioned in [8], it can be noticed that PSNR in proposed method is higher than previous study. Increasing in PSNR may reach to (12 db). For example, baboon image in previous study is (32 db) while in proposed algorithm is (44 db). On the other hand, clearly capacity is also increased.

### 7. Conclusion

There are several advantages that can be result from this method:

1. Capacity will be increased because the data are compressed before embedding process.
2. This algorithm is suitable for medical application because of Bit plane of the original image that are used for embedding operation is compressed and stored, so, the original image will be completely retrieved.
3. Because compression is done adaptively, smallest vector will be produced which means less effect on cover image as a result high PSNR will be produced.
4. Because of embedding process is done in transformation domain, so watermark will be more robust.
5. The watermark will be more secure for the following reasons:-

- Attacker doesn't know there is compression.
- The compression method is done adaptively which mean the number of bits that are used to represent vector (number of zero or one in watermark) will be different for each watermark.
- The compressed watermark will be embedded after storing compressed data of original image for retrieving purpose, so the location of compressed watermark will be difficult to determine by attacker.

### References

1. R. Indra Gandhi and K. P. Kaliyamurthie," An Adaptive Data Hiding Scheme for Domain Based Secret Data in Random Order to Increase Steganography Using IWT", Int. J. Advanced Networking and Applications, Volume: 6 Issue: 5 Pages: 2464-2467, (2015).
2. Swati Goel, Pramod Kumar and Rekha Saraswat, "High Capacity Image Steganography Method Using LZW, IWT and Modified Pixel Indicator Technique", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 3759-3763,(2014).
3. G. G. Langdon," An Introduction to Arithmetic Coding", IBM Journal of Research and Development, Volume: 28, Issue (2), (1984).
4. Kamalpreet Kaur, Jyoti Saxena and Sukhjinder Singh, " Image Compression Using Run Length Encoding", International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 5, Issue (5),(2017).



5. Roberto Togneri and Christopher J.S. Desilva, "Fundamentals of information Theory and Coding Design", A CRC Press Company, (2002).
6. HaiTao LiChongmin JasniMohamad ZainAhmed N.Abdalla , " Robust Image Watermarking Theories and Techniques: A Review ", Journal of Applied Research and Technology, Volume 12, Issue 1,( 2014).
7. Anumol Joseph and K. Anusudha," Robust watermarking based on DWT SVD", International Journal of Signal & Image Processing, Issue. 1, Vol. 1, ( 2013).
8. Guorong Xuan, Jiang Zhu, Jidong Chen, Shi Y.Q., Zhicheng Ni, Wei Su, "Lossless data hiding based on integer wavelet transform" IEEE, Volume: 38, Issue 25, (2002).
9. S. KHAN, T. KHAN, M. NAEEM, N. AHMAD," Run -Length Encoding Based Lossless Compressed Image Steganography", Sindh University Research Journal, Vol.47 (3), 541-544 (2015).

## طريقة جديدة لزيادة درجة الدقة والامنية للصورة المحتوية على العلامة المائية

زينة حسين تومان

شروق جمعة سريح  
جامعة القادسية

رنا جمعة سريح

كلية علوم الحاسبات وتكنولوجيا المعلومات

Zinah.hussein@qu.edu.iq

Shroouq.jumaa@qu.edu.iq

Rana.Aljanaby@qu.edu.iq

### المستخلص :

في الوقت الحالي، يتم تناقل المعلومات بشكل الكتروني. خلال عملية النقل يمكن ان يتم التلاعب بالمعلومات بسهولة. لذلك يجب ان تتم عملية النقل بشكل امن. لجعل البيانات اكثر امانا يتم استخدام العلامة المائية.

في هذا البحث، تم اقتراح خوارزمية جديدة لاضافة العلامة المائية، والتي تحوي ثلاث طرق والتي تضم التحويل الموجي الرقمي، الترميز الرياضي و الترميز المعتمد على عدد التكرارات. تم استخدام الترميز المتكيف المعتمد على طول التكرارات لضغط العلامة المائية المراد تضمينها. وتم استخدام الترميز الرياضي لضغط البيانات في الصورة الاصلية و خزنها وذلك لاستعادة الصورة الاصلية بدون اي تغيير بعد استخراج العلامة المائية.

لتجنب مشكلة الترميز التقليدي المعتمد على التكرارات والتي من الممكن ان يولد ملف اكبر من حجم الملف الاصل. تم اقتراح طريقة الترميز المتكيف المعتمد على عدد التكرارات والتي سيتم استخدامها لضغط لعلامة المائية في الصورة الاصلية وسوف يتم تكرارها عدد من المرات باستخدام عدد مختلف من البتات لتمثيل التكرارات على العلامة المائية ومن ثم توليد عدد من المصفوفات الاحادية ومقارنة النتائج المختلفة واختيار المصفوفة الاحادية الاصغر منهم. بالتاكيد اختيار المصفوفة الاحادية الاصغر يعني انه الصورة الجديدة المحتوية على العلامة المائية سوف تكون ذات درجة دقة عالية بالاضافة الى سعة التضمين للصورة الاصلية افضل، الاسلوب المتكيف يعني ان عملية التضمين سوف تكون اكثر امانا.