

New Watermark Algorithm support Based on Watermark Designing

Abdul MonemS.Rahma

Matheel E.Abdulmunim

Rana J.S. Al-Janabi

New Watermark Algorithm support Based on Watermark Designing

Abdul MonemS.Rahma

Matheel E.Abdulmunim

Rana J.S. Al-Janabi

Computer Science Department University of Technology, Baghdad, Iraq

Received 1 September 2015; Accepted 23 November 2015

Abstract

In this research, embedding process is done on RGB image by comparing pixel by pixel to embed watermark. This algorithm depends on embedding style that are less effect on RGB image through analyzing watermark and finding the most dominant bit and with using new techniques depends on probability principle for embedding process to ensure less change ratio on original image to provide high quality image. Image watermark are added to all parts of image to make watermark more robust. This algorithm give an excellent result when watermark with less thickness edge and it provides high security because of several reasons first it depends on probability embedding style; second, it uses keys to select compared pixels; third it gives less effect on original image. Therefore, the attacker didn't notice that there is watermark.

Keywords : RGB image watermark, copyright, watermark based on probability, image watermark.

خوارزمية علامة مائية جديدة تعتمد على تصميم العلامة المائية

رنا جمعة سريح

مثيل عماد الدين عبد المنعم

عبد المنعم صالح رحمة

قسم علوم الحاسبات - الجامعة التكنولوجية

الخلاصة

في هذا البحث، عملية التضمين تتم باستخدام صورة (RGB) من خلال مقارنة نقطة مع نقطة اخرى. هذه الخوارزمية تعتمد اسلوب تضمين يكون اقل تأثيرا على صورة ال (RGB) من خلال تحليل العلامة المائية وايجاد البت الاكثر سيادة، حيث انها تستخدم تقنية جديدة تعتمد مبدا الاحتمالية في عملية الاخفاء لضمان اقل نسبة تأثير على الصورة الاصلية لاعطاء صورة ذات نقاوة عالية. العلامة المائية اضيفت لكل اجزاء الصورة لجعل هذه العلامة اكثر قوة. هذه الخوارزمية تعطي نتائج ممتازة عندما تحوي العلامة المائية حافات حادة وتقدم امنية عالية لعدة اسباب اولا تعتمد اسلوب التضمين باستخدام الاحتمالية، ثانيا انها تستخدم المفاتيح في تحديد النقاط التي تتم مقارنتها، ثالثا انها اقل تأثير على الصورة الاصلية، لذلك المهاجم لن يلاحظ وجود علامة مائية.

كلمات مفتاحية: اضافة العلامة المائية في صور ال RGB، حق النشر، اضافة العلامة المائية اعتمادا على الاحتمالية، العلامة المائية للصور.

1.1 Review

Multimedia's author can distribute their media by web pages or any other public form. So anyone can copy author's media. So, copiers can claim that the media are their own. To solve this problem additional information are added to this media which can be author, license information or copyright protection. Digital watermarks may be visible or invisible to human vision [1]. Visible watermarks, are more intrusive to the media. Examples of such watermarks can be seen easily on most network television stations by the station's logo in the corner of the screen. Attackers have a clear goal and can remove the watermark [1].

New Watermark Algorithm support Based on Watermark Designing

Abdul Monem S. Rahma

Matheel E. Abdulmunim

Rana J.S. Al-Janabi

Digital Watermarks are potentially useful in many applications including:[2,3]

1. **Ownership Assertion:-** ownership assertion can be achieved by watermarking. So, the creator of a Multimedia wishes to prove his ownership.
2. **Fingerprinting:-** In applications where multimedia content is electronically distributed over a network, the content owner would like to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data.
3. **Copy Control: -** copy prevention and control can be achieved using watermarking.

1.2 Watermark Requirements

Because of the high trading data, including pictures on the Internet, the need to provide authenticity emerged. Watermark is one of the existing techniques for this purpose. Watermark should satisfy the following [4,5]:-

1. **Robustness:** if any attempt to remove watermark, the watermark should be robust to prevent that.
2. **Capacity:** the embedded information should be large enough to identify the owner of the multimedia.
3. **Security:** manipulations of watermark must be prevented.
4. **Imperceptibility:** The watermark should cause as little image degradation as possible, people can't notice it.

When designing a watermarking algorithm, three parameters exist: Capacity, imperceptibility, and robustness. Capacity is the number of bits that can be embedded in multimedia, the imperceptibility is the degradation introduced into the signal, and the robustness is the watermark ability to remain readable after innocent or malicious processing on the signal. These three parameters conflict to each other, and selection of these parameters according to the requirements of the application.

New Watermark Algorithm support Based on Watermark Designing

Abdul MonemS.Rahma

Matheel E.Abdulmunim

Rana J.S. Al-Janabi

1.3 Quality Metrics for Images

Visual Quality degradation of the image is measured using different metrics. In this paper, peak signal to noise ratio (PSNR) and mean square error (MSE) are used. PSNR is the ratio of the maximum signal power to the noise power that effect on it. PSNR is used to measure the reconstructed signal quality and usually measured in dB [6, 7]. Mean Squared Error (MSE):- is the average squared difference between a reference and a distorted image. It is calculated pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count [8].

2. Proposed Algorithm

2.1 Most Dominant bit Calculation Algorithm

The embedded watermark include {0, 1} bit:

Step1:-Calculates all Zeros Bit in watermark

Step2:-Calculates all ones Bit in watermark

Step3:-If No. ones > No. Zeros then Most Dominant bit =1

- Else Most Dominant Bit =0;

Step4:- Stop.

2.2 Embedded Process for Proposed Watermark Algorithm

Input: -RGB Image, Watermark

Output: - Watermark image

Step1:- Determine the most Dominant bit in Watermark.

Step2:- key generation process is initialized according to predefined formula and store keys in an array.

Step3:- in RGB image, use the first key to determine the first pixel which are used to embed the most dominant bit value in its LSB.

New Watermark Algorithm support Based on Watermark Designing

Abdul Monem S. Rahma Matheel E. Abdulmunim Rana J.S. Al-Janabi

Step4:- In RGB image, second pixel is determined by first pixel + one which is represent the first data embedding process.

Step5:- select new key from array of keys.

Step6:- The next pixels is determined by the new key which represent the distance between them.

Step7:- by take the LSB of two pixels (**Pixel_A** and **Pixel_B**). The embedding process is done according to the following tables (1 and 2):-

- **If Watermark Bit = Most Dominant Bit**

Table (1):- embedding process in case watermark bit is most dominant one

LSB of Pixel _A	LSB of Pixel _B	Embedding State
0	0	No_Change
1	1	No_Change
1	0	No_Change
0	1	Change LSB of Pixel_A to be (1)

If Watermark Bit = Least Dominant Bit

Table (2):- embedding process in case watermark bit is least dominant one

LSB of Pixel _A	LSB of Pixel _B	Embedding State
0	0	Change LSB of Pixel_B to be (1)
1	1	Change LSB of Pixel_A to be (0)
1	0	Change LSB of Pixel_B to be (1) & Change LSB of Pixel_A to be (0)
0	1	No_Change

New Watermark Algorithm support Based on Watermark Designing

Abdul Monem S. Rahma

Matheel E. Abdulmunim

Rana J.S. Al-Janabi

Step8:- if the generated key is equal to n, repeat that key n times to all pixels between these two.

Step9:- After repetition is complete and jump pixel count by n and if pixel count doesn't reach to end of image, then go to step5.

Step10:- stop.

2.3 Extracting Process of Proposed watermark Algorithm

Input: - Watermark Image Output: - Watermark

Step1:- use the first key to determine the first pixel to extract most dominant bit value

Step2:- according to predefined formula key is produced and store it in an array.

Step3:- in RGB image, use the first key to determine the first pixel which are used to extract the most dominant bit value in its LSB.

Step4:- In RGB image, second pixel is determined by first pixel + one which is represent the first data embedding process.

Step5:- select new key from array of keys.

Step6:- The next pixels is determined by the new key which represent the distance between them.

Step7:- by take the LSB of two pixels (**Pixel_A** and **Pixel_B**). The extracting process is done according to the following table (3):-

New Watermark Algorithm support Based on Watermark Designing

Abdul Monem S. Rahma

Matheel E. Abdulmunim

Rana J.S. Al-Janabi

Table (3):- extracted the watermark process

LSB of Pixel _A	LSB of Pixel _B	Bit Extraction Process
0	0	Most dominant bit
1	1	Most dominant bit
1	0	Most dominant bit
0	1	Least dominant bit

Step8:- if the generated key is equal to n, repeat that key n times to all pixels between these two.

Step9:- After repetition is complete and jump pixel count by n and if pixel count doesn't reach to end of image, then go to step5.

Step10:- stop.

2.4 Good Watermark Characteristics for Proposed Algorithm

According to the proposed algorithm, the greater the difference between the most dominant bit and least dominant one, the better results by this algorithm. Table (4) that contain several watermarks, explaining how to calculate probability of watermark bits that are embedded in image without change in it.

Table (4):- show how to calculate probability of watermark effect on image

Watermark	Ratio of the Most Dominant bit in image	Ratio of the Least Dominant Bit in image	Ratio of the watermark Bit That doesn't change image	Ratio of the watermark Bit That Make change
Watermark1	70%	30%	60%	40%
Watermark2	80%	20%	65%	35%
Watermark3	90%	10%	70%	30%

New Watermark Algorithm support Based on Watermark Designing

Abdul Monem S. Rahma

Matheel E. Abdulmunim

Rana J.S. Al-Janabi

According to this table, watermark2 give better result than watermark1 and watermark3 give better result that watermark 2. Figure (1) explain the watermark that are less thickness give less effect on the original image

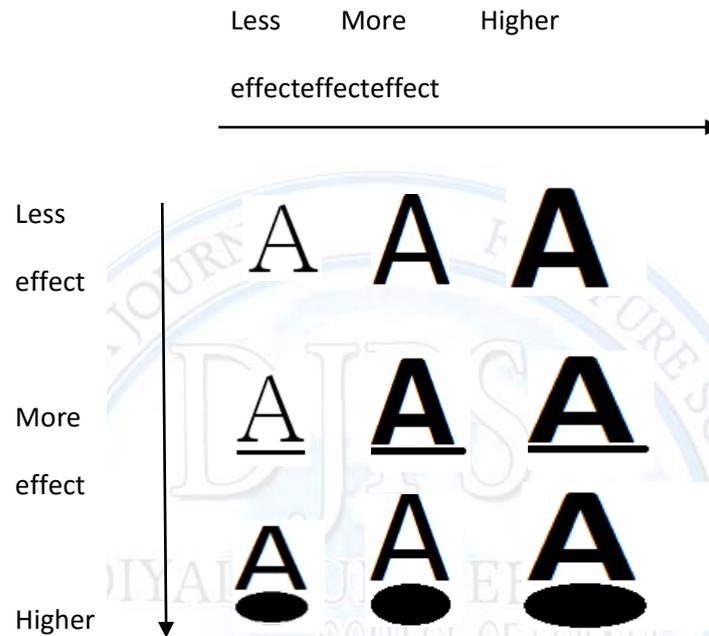


Fig. (1) Show that less thickness watermark is better for the proposed algorithm

3 Results and Discussion

Because the mechanism of embedding adopted, watermark specifications affect the watermarked image. Table (5) show the characteristics of watermark 1 and watermark 2.

Table (5):- Watermark characteristics

Watermark Name	No.zero bit in watermark	Zero bits ratio to watermark	No.one bit in watermark	One Bits ratio to watermark
Watermark ₁	881	0.108	7219	0.981
Watermark ₂	3785	0.467	4315	0.532

New Watermark Algorithm support Based on Watermark Designing

Abdul MonemS.Rahma

Matheel E.Abdulmunim

Rana J.S. Al-Janabi

Table (6) shows the result applied them on different RGB images which all gives higher result when there is (less thickness) high difference between two bits of {0,1} of watermark. Table 2 uses different images (A and B) with the same size and c with different size. Different watermark with the same size (different ratio for zero to one). From this table it can be concluded that when the watermark with less thickness give better result (low MSE and high PSNR) according to the proposed algorithm.

Table (6):- MSE and PSNR for different images

Image Name	Image size (Kb)	Watermark Name	Embedded Data (Bytes)	MSE	PSNR
Image (A)	2250	Watermark _{k1}	147456	0.165	55.93
Image (A)	2250	Watermark _{k2}	147456	0.300	53.35
Image (B)	2250	Watermark _{k1}	147456	0.189	55.34
Image (B)	2250	Watermark _{k2}	147456	0.314	53.149
Image (c)	393	Watermark _{k1}	25151	0.178	55.61
Image (c)	393	Watermark _{k2}	25151	0.308	53.233

Fig.(2), Fig.(3) and Fig.(4) shows the original and watermarked image that are used in table (6).

New Watermark Algorithm support Based on Watermark Designing

Abdul MonemS.Rahma

Matheel E.Abdulmunim

Rana J.S. Al-Janabi



Original Image (A) Watermarked Image (A)

Fig. (2) Show the original and watermarked image



Original Image (B) Watermarked Image (B)

Fig. (3) Show the original and watermarked image B



Original Image (c) Watermarked Image (c)

Fig. (4) Show the original and watermarked image C

Conclusion

The proposed algorithm provides high quality watermarked image, although the watermarked is repeated in all pixels of image and in every color of these pixels which provide robust watermark image. This algorithm depends on the probability, where the bits are embedded through making pattern of bits in image one pattern for most dominant bit and another for least dominant bit. This embedding process provide high security because of the following reasons:-changing of the original image is as less as possible so ensure watermarked image have a high quality second uses keys to choose pixels where these keys represent the distance between pixels.

References

1. Neil F. Johnson,” An Introduction to Watermark Recovery from Images”, SANS Intrusion Detection and Response Conference, February1999.
2. Sunesh, Harish Kumar,” Watermark attacks and applications in watermarking”, international journal of computer applications, 2011.
3. BorkoFurht and DarkoKirovski,” Multimedia Watermarking Techniques and Applications”, 2006.
4. Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom,” Watermarking applications and their properties”, Int. Conf. on Information Technology’2000, Las Vegas, 2000.
5. Hai Tao, Li Chongmin,JasniMohamad Zain, Ahmed N. Abdalla,” Robust Image Watermarking Theories and Techniques: A Review”, Journal of applied Research and technology, volume 12, 2014.
6. MeghaGoyal,Yashpal Lather and Vivek Lather, “ ANALYTICAL RELATION & COMPARISON OF PSNR AND SSIM ON BABBON IMAGE AND HUMAN EYE PERCEPTION USING MATLAB”, International Journal of Advanced Research in Engineering and Applied Sciences,2015.
7. AlbertusJokoSantoso, 3Dr. Lukito Edi Nugroho, 4Dr. GedeBayuSuparta, 3Dr. RisanuriHidayat, “Compression Ratio and Peak Signal to Noise Ratio in Grayscale Image Compression using Wavelet”, IJCST Vol. 2, Issue 2, June 2011.
8. Anu, Komal, ShipraKhurana, Amit Kumar ,” Comparative Analysis of Image Quality Assessment Using HVS Model”, Vol. 2, Issue 7, July 2014.