Open access Journal International Journal of Emerging Trends in Science and Technology

Randomized LSB Hiding Algorithm for Nested Image Watermarking

Authors

Mayuri Verma[1], Samta Gajbhiye[2]

[1]M.E (CTA) Scholar, Department of Computer Science & Engineering, FET, SSGI, SSTC, Bhilai, Chhattisgarh, India

Email: *mayuriverma27@gmail.com*

[2]Sr.Associate Professor, Department of Computer Science & Engineering, FET, SSGI, SSTC, Bhilai, Chhattisgarh, India

Email: *samta.gajbhiye@gmail.com*

Abstract

An image watermarking is process of embed an image with some parameter (secondary parameter) known as watermark image but without any degradation or deterioration in image quality to offer copyright protection. Copyright protection means protection from illegal copying for one's intellectual property. Here the method of nested digital image watermarking is used. Nesting of image watermarking means when a watermark is embedded into the other watermark. The Randomized Least Significant Bit (RLSB) hiding algorithm is used for the process embedding because it has the lesser complexity and also it is more robust to variations with the type of image. And the blowfish cryptographic algorithm is used for encryption. Here encryption done into watermark image before embedding with the cover image. Here the concept of encrypt the watermark image before embedded with the main image just to increase the level of security of the watermarked image.

Keywords: *Image Watermarking, RLSB, Blowfish Algorithm, Copyright Protection.*

1. Introduction

As Internet has become user friendly as it is an excellent sharing system for the digital media (electronic media in which data are stored in some digital form). Therefore, content owners see a high risk of piracy in it and also concerned about protection from illegal copying of their intellectual property. And thus copyright protection of such a data is become an important issue. The copyright protection of that multimedia data can be done by using cryptographic methods (which provides control over data accessing and also make data illegible from an unauthorized user). But cryptographic methods alone are not giving us the complete solution. Therefore, digital image watermarking was introduced, which resolves the problem of protection of one's intellectual property in digital media (identifies the rightful owner of that digital data).

The term 'watermark' was derived from 'wassermarke' (a German term) at around the end of 18th century. The name 'Watermark' has been put because these marks have a likeness towards upshot of water on the paper [1]. Watermarking is simply a pattern of bits inserted within a digital image, which identifies the copyright information (like author, rights, etc.) of the files. The actual bits which represent the watermark image must be sprinkled (scattered) throughout the file in such a manner that it cannot be easily identified and also manipulated. And also, the digital watermark should be robust towards changes into the file.

There are various hiding techniques used for embedding and extraction of the watermark image. LSB hiding technique is a simple method used for watermark embedding to embed the watermark into least significant bits of the main cover image. But the direct LSB hiding technique has some drawback

or disadvantage of having the higher complexity and also its dependency on image type. Thus here the randomized LSB hiding technique is used for embedding and extraction of watermark image into/from another image. And as compare to direct LSB hiding method, the RLSB hiding technique shows its robustness for variations in image type and have lesser complexity.

The quality of image is an important issue while working with images. The quality of image should remain unchanged while undergo through various processes. Two error metrics are used to measure the quality: PSNR and MSE. PSNR is Peak Signal to Noise Ratio which represents peak error calculation. And MSE is Mean Squared Error which represents cumulative square error between the original image and the compressed image. For the better quality watermarked image, the PSNR value should be as high as possible (tends to infinity) and value of MSE should be as low as possible (tends to zero).

The value of MSE will be calculated as follows:

$$\text{MSE} = \frac{1}{\text{m n}} \sum_{\text{i=0}}^{\text{m}-1} \sum_{\text{j=0}}^{\text{n}-1} [\text{I(i,j)} - \text{K(i,j)}]^2$$

It's given a noise free m x n image I and K its noisy estimation. And the value of PSNR is evaluated in terms of decibels and also it is inversely proportional to the MSE and is given as:

$$\text{PSNR} = 10 \,.\, \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

MAX_I is the maximum possible value of pixel of the image.

2. Related Work

In the field of Digital image watermarking there are lots of work has been proposed yet for the reason of getting proper security from illegal copying of digital data.

- Author P Gupta [2] uses the concept of Cryptography based digital image watermarking to enhance the security of watermarked data with the use of blind watermarking technique. The XOR operation is used for encryption and for embedding the watermarked watermark image into cover image, DWT based method is used.
- J S Bhalla and P Nagrath [3] used the concept of Nested Image Watermarking method using blowfish cryptographic algorithm. The main focus is on to enhancing the embedding capacity and improving the security of watermarks by using LSB hiding for embedding. One watermark image is encrypted and then embedded with another watermark (using LSB) and the nested watermark is again encrypted and embedded with main image.
- D Biswas et al. [4] suggests that the direct LSB hiding method has some disadvantage of having its complexity higher and also its dependency on image type when compare with Randomized LSB hiding which is having lesser complexity as well as is more robust towards variations in image type. The work done by considering their PSNR (Peak Signal to Noise Ratio) values.
- The research work by authors S P Singh and R Maini [5] shows a performance evaluation between the common encryption techniques that is DES, 3DES, Blowfish and AES. The result shows that Blowfish is having better performance as compare to other encryption cryptographic algorithms. Also and it has no security weak points so far which is known.
- Least Significant Bit based Lossless Image Watermarking using the polynomials for DRM in Spatial Domain by A. Siva Sankar et al. [6] suggests a new method of embedding in which it randomly hides the messages in Least Significant Bit of the chosen pixel (any component) using the polynomial thereby reducing the probability of determining correct coefficients.
- Authors Obaida Mohammad and Awad Al-Hazaimeh [7] introduce how to hide data in Images Using a New Random Technique. The message is inserted within the images in a random manner into pixels of the main

cover image and Least Significant Bit hides message in a manner that it becomes difficult to differentiate it.

- K M Singh et al. [8] suggests a least significant bit algorithm (for embedding) for hiding the encrypted messages in a non-adjacent and random pixel positions in an edges of the images.
- Authors M O Ali, R Rao [9] worked on the basics of image watermarking and also its implementation (hardware).
- Pia Singh [10] shows the blowfish cryptographic algorithm is safer towards illegal attacks and also how to fabricate and realize it using MATLAB. The result also shows that it runs faster when compared with other existing methods.

3. Security of Image

The main focus of digital image watermarking emphasizes on to improving the level of security for the watermark image by enhancing its embedding capacity. The main aim is to provide the proper protection to one's intellectual property from the illegal copying of image or data which is in a digital form.

The very common and simple method that is LSB hiding is mostly used for the embedding and also for extraction of the watermark image for digital image watermarking. But as the use of direct LSB hiding has some disadvantage of higher complexity and its dependency onto image type the Randomized LSB hiding technique is used here as it is having its complexity less and also shows its robustness towards variations in image type. And also if the process of encryption as well as embedding is done only on some of the selected pixels, then definitely it will provide higher security as when applied on to the whole image. And also the quality of image after completion of all the process as well as when undergo through various attacks is an important issue.

4. Methodology

The main methodology used here is the Randomized LSB hiding technique for the process of embedding and extraction of watermark image and Blowfish cryptographic algorithm for the process of encryption and decryption. Here the concept of nesting of image watermarking is used in which one watermark image is embedded with another watermark image so as to provide more security to the image. The process of encryption using blowfish algorithm is applied before the process of embedding so to enhance the level of security. All the processes are not applied on to the whole image but they are applied on only some of the selected pixels. Thus the probability of finding the exact pixel location correctly is quite difficult for the attackers. The step by step process followed by the embedding and then extraction of watermark image into/form the main cover image is as follows:

There are three images which are taking as an input that is Cover Image, Watermark Image1 and Watermark Image2.

<u>For the process of Embedding</u>

- Firstly the selected pixels of Watermark Image2 are encrypted using the blowfish algorithm.
- Then they are embedded using RLSB technique with the Watermark Image1. Only some selected pixels are embedded.
- The nested image generated above is now again encrypted using blowfish (some selected pixels).
- Now finally it gets embedded into the main cover image (again some randomly selected pixels) and generated the watermarked cover image.

<u>For the process of Extraction</u>

- Firstly the Extraction takes place from the watermarked cover image so as to retrieve the encrypted nested watermark image from the cover image.
- Then the decryption process being applied onto the above retrieved image and the

nested watermark image is being extracted from the encrypted nested watermark image.

- The retrieved nested watermark image is extracted using RLSB technique and Watermark Image1 is being retrieved from the image.
- Now finally the process of decryption is applied and final Watermark Image2 is retrieved from the above generated encrypted Watermark Image2.

5. Result and Discussions

The work is implemented and realized using MATLAB. Our main focus is onto improving the embedding capacity and also enhancing the level of security. The result has been obtained and evaluated on the basis of measurement of two quality metrics that is PSNR (Peak Signal to Noise Ratio calculation) and MSE (Mean Squared Error calculation). The result also is evaluated with various attacks when applied on the Original Image, Watermark Image1 and Watermark Image2 then their MSE and PSNR values are calculated according to it. There are three types of attacks are applied on the Original Image, Watermark Image1 and Watermark Image2 are Rotation attack, Noise attack and Cropping. And on the basis of that MSE and PSNR are calculated with every situation.

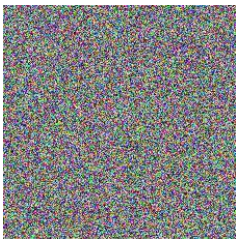
The work has also been evaluated for the Cover image of 900 x 900 pixels size, Watermark Image1 of 224 x 226 pixels size and Watermark Image2 of 56 x 56 pixels size. The following result is obtained after performing the various processes on each of the Original image, Watermark image1 and Watermark image2, and the various effects are shown below:

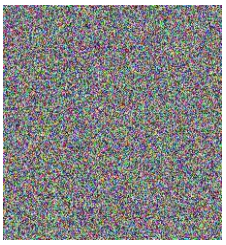
a) 

b)  c) 

Figure 1: a) Original Image b) Watermark 1 c) Watermark 2

a)  b) 

c)  d) 

e)  f) 

g)  h) 

Figure 2: a)Encryption-1 b)Embedding-1 c)Encryption-2 d)Embedding-2 e)Extraction-1 f)Decryption-1 g)Extraction-2 h)Decryption-2

COVER IMAGE	WATERMARK1	WATERMARK2	IMAGE	ATTACK	MSE	PSNR
900x900	224x226	56x56		Without attack	3.0033e-18	223.3888
900x900	224x226	56x56	Original Image	Rotation	3.0033e-18	223.3888
				Noise	3.0033e-18	223.3888
				Cropping	3.0033e-18	223.3888
900x900	224x226	56x56	Watermark1	Rotation	3.0033e-18	223.3888
				Noise	3.0033e-18	223.3888
				Cropping	3.0033e-18	223.3888
900x900	224x226	56x56	Watermark2	Rotation	0.22759	54.5934
				Noise	0.23652	54.2563
				Cropping	0.23652	54.2563

Table 1: Calculation of MSE & PSNR depending upon the types of attack on Original, Watermark1 and Watermark2 Image respectively

It has been observed from the above calculations or the result obtained that the values of both quality metrics that is MSE and PSNR are change according to the variations in the different from of attacks which are applied on to the Original Image which is the main Cover Image, the Watermark Image1 (means first watermark) and Watermark Image2 (means second watermark) respectively. The result obtain also shows that the value of MSE obtained is almost tends towards zero and the value of PSNR obtained is higher. And thus on the basis of result, we can conclude that the quality of the image which we get after going through all the processes is higher. The result also shows that the quality of image after all the processes is not degraded. Thus it is ensuring the better quality image with high security.

6. Conclusion and Scope of Further work

The work is carried out for Cover image, Watermark image1 and Watermark image2. Each image has different sizes and also obtained different values for PSNR and MSE. While going through three types of attacks that is Rotation, Noise and Cropping, the image retrieved is not degraded from its originality and thus we can say that the quality of the image has been less unaffected. In the methodology used the main concern is to get the more secured image without disturbance in the original image's quality.

The basic advantage of the technique used is that, the concept of nested image watermarking and Randomized LSB hiding method used for embedding process and process of extraction and the blowfish cryptographic algorithm for process of encryption and decryption are applied not into the whole image but applied only onto some selected pixels. Thus it provides high level of security as the probability of determining the exact value of randomly selected pixel is difficult. As encryption is performed before embedding process, thus it provides more security to the watermarked image. But the whole process took more time for the completion. So in future some other process will be used which provides maximum security as well as will take less time for the completion.

References

1. Cox, I., Miller, M., Bloom, J. Digital Watermarking, Morgan Kaufmann, Ch 1, p. 6, Web ISBN-13: 978-0-08-050459-9.
2. Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data", International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 ISSN 2229-5518.
3. Jasdeep Singh Bhalla, Preeti Nagrath, "Nested Digital Image Watermarking

Technique Using Blowfish Encryption Algorithm", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153.

4. D. Biswas, S. Biswas, P.P. Sarkar, D. Sarkar, S. Banerjee, A. Pal, "Comparison And Analysis Of Watermarking Algorithms In Color Images – Image Security Paradigm", International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.
5. Simar Preet Singh, and Raman Maini, "Comparison Of Data Encryption Algorithms", International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127.
6. Siva Sankar, T. Jayachandra Prasad, M. N. Giri Prasad, "LSB Based Lossless Digital Image Watermarking using Polynomials in Spatial Domain for DRM", 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011 Proceedings published by International Journal of Computer Applications (IJCA).
7. Obaida Mohammad and Awad Al-Hazaimeh, "Hiding Data in Images Using New Random Technique", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012, ISSN (Online): 1694-0814.
8. Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April 2007.
9. Mustafa Osman Ali and Rameshwar Rao, "Digital Image Watermarking Basics, and Hardware Implementation", International Journal of Modeling and Optimization, Vol. 2, No. 1, February 2012.
10. Pia Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 ISSN 2229-5518.