Image Watermarking Approach Using LSB and Laplacian Filter

N Imran¹, S Hameed¹, Z Hafeez², Z Faheem¹, M Waseem³, U Latif¹ and M S Amin²

¹Department of Computer Science, Government College University Faisalabad, Sahiwal, Pakistan.
²Department of Computer Engineering, University of Engineering & Technology, Taxila, Pakistan.
³School of Electrical Engineering, Zhejiang University Hangzhou, 310027, China.

Email: zaid_fahim@yahoo.com

Abstract. With the growth of information technologies, E-industry safety has recently become the mutual attention of education and business firms. Digital image watermarking is a technique that refers to the security of multimedia data. It is a process referred to the security and authentication of a digital image, video, and audio by embedding a watermark. Watermarking technique applies a number of variable editions to the host content, where the addition is related to embed information. In the past, researchers develop multiple simple watermarking techniques, today race is to find a region where the watermark is imperceptible and have a high payload. In this paper, an invisible image watermarking technique based on the least significant bit (LSB) and laplacian filter is proposed. The original image is divided into blocks and the laplacian filter is applied on each block. Laplacian is a derivative filter that uses the second derivate to find out the area of rapid changes in the image and the least significant bit is a technique to embed a watermark into the bit positions. Watermark is embedded on these regions which is favourable in achieving high desirable properties. This technique shows strong robustness against image processing and geometrical attacks. In evaluation with state of art methods, the proposed technique shows satisfactory progress.

1. Introduction

In today’s frequent advancement in the global world, the internet and communication technologies play a vital role in our daily life. It creates ease in multi-media transformation i.e. image, audio, and video from person to person. However, at the same time, digital data stealing, duplication, and modification have become easier. To solve these problems different techniques were proposed in recent years including watermarking and steganography, which refer to techniques of hiding a piece of information in digital media [1].

Watermarking is performed either in the spatial domain or in the frequency domain [2]. Spatial domain techniques are simple and have a high payload, work directly on the pixel level, but these are not robust against few attacks, it can be made robust by adding optimization. In contrast frequency domain techniques are complex and have a lesser amount of payload and work on the transform coefficient, but these are robust against attacks i.e., JPEG compression and noise attacks.
2. Types of watermarking

These are the two main types of watermarking, visible and invisible [3]. In visible watermarking, watermark i.e. logo or text is embedded in multimedia and these watermark signal are visible on original media. In invisible watermarking the data that is embedded in multimedia is invisible. Watermarking can be classified on the base of the robustness of the watermark:

2.1. Fragile
In fragile watermarking, the watermark that is used will modify or remove at the time of processing.

2.2. Robust
In robust watermarking, watermark resists various kinds of transformation such as filtering, compression, and distortion.

2.3. Semi Fragile
In semi fragile, watermarks are primarily used to locate the tempered area and can also be used to re-build them.

3. Techniques of watermarking

In spatial domain the information is added simply by just varying the pixel values of the host signal. The values of some colours or pixels are also directly editable in the spatial domain technique [4]. Spatial domain techniques are much simple as compare to frequency domain techniques.

3.1. Least significant bit watermarking:
In the least significant bit (LSB), the watermark is added in the least significant bit of each pixel. When the extraction of information is needed, the LSB of each pixel is read. LSB is one of the simplest strategies to implement. The degradation of the image is also less in LSB and also in LSB the watermarking insertion and extraction computational diversity of the least significant bit is easy. But the major disadvantage of least significant bit watermarking is that it is not robust again various attacks [5].

3.2. Patchwork technique:
Patchwork technique is simply based on the statistical property of the host image by inserting the patches of the watermark in the image. Two patches are randomly chosen both having the opposite property i.e. one patch has brightened information and the other patch has darkened information of the image. In the patchwork technique, the image becomes robust against various attacks but the amount of data that can be concealed is very small.

4. Requirements of watermarking

The basic requirements for the implementation of watermarking are discussing below [3]:

4.1. Imperceptibility:
One of the main property that is a must in non-evident watermarking is imperceptibility. This means that the watermark can’t be perceived by the senses of end users.

4.2. Robustness:
One more digital watermarking tested property, if the watermark is survived against image processing operations then this property is satisfied. Robust watermark must have the property to bear varieties of attacks.
4.3. Capacity:
There must be proper amount of data which is going to be inserted in the image. The inserted data is also known as payload. And there must be sufficient amount of data in order to get an imagined application.

4.4. Security:
The main purpose of watermarking is to make the data secure so there must be some secret key in a watermark. Without the knowledge of secret keys, the attacker or end user can’t change or steal the information.

5. Laplacian
Laplacian is a second derivative filter that uses the second derivative of the image. By using Laplacian filter on image find the rapidly changing areas of intensity and it is also used for edge detection. In laplacian input is given in image form and output also produces in image form. Laplacian of Gaussian is mostly used for this purpose; it is a type of laplacian filter.

Laplacian $L$ of $(x, y)$ with pixel intensity $I$ of $(x, y)$ of an image is as follow:

$$L(x, y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2}$$

(1)

6. Watermark Embedding
In this technique, watermark is embedded in grayscale image by using the steps describe below:
1) Read the grayscale image
2) Convert the grayscale image into the blocks of 16*16 for tamper localisation.
3) Apply laplacian filter on the blocked image.
4) Divide the pixel into LSB and MSB.
5) Pass the initial value to the chaotic map and generate the S-box.
6) Scramble the watermark logo using s-box and divide it into blocks and XOR with the original image.
7) Combine the LSB and MSB to generate the watermarked image.

Figure 1 shows the flow diagram of the watermark embedding procedure, the resultant is the watermarked image.

7. Watermark Extraction
Watermark from the image will be extracted in following steps:
1) Read the grayscale watermarked image
2) Convert the grayscale image into the blocks of 16*16.
3) Apply laplacian filter on each block
4) Divide the pixel into LSB and MSB.
5) The LSB is XOR with a scramble logo to perform inverse operations.
6) Combine the LSB and MSB to generate a watermark.
7) S-box is used to de-scramble the extracted watermark

8. Results
The performance of the proposed technique is experienced using different testing grayscale images i.e. Lena and baboon. The testing image of size 512x512 and binary watermark logo of size 32x32 is used to analyse the proposed approach. The binary watermark logo is the first scramble using an s-box that makes it more secure to predict. Then the scrambled logo is embedded in the host images. To evaluate performance most important parameters i.e. PSNR, SSIM, and NC are calculated. Structural similarity index (SSIM) and peak signal to noise ratio (PSNR) are used to measure the visual similarity between original and watermarked image. The PSNR greater than 28dB is acceptable, and in the same way, the value of SSIM is in the range [0 1] higher value give better results. Normalized correlation (NC) is a matrix to determine the level of robustness of watermark. The mathematical expression of PSNR is shown.

\[
\text{PSNR} = 10 \log_{10} \left( \frac{(255)^2}{\text{MSE}} \right)
\]

MSE is the mean squared error of the original host and watermarked image.

\[
\text{MSE} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} [I(m, n) - K(m, n)]^2
\]

MxN is the dimensions of the original host image and \([I(m, n) - K(m, n)]^2\) is the difference of two images i.e. host original image and watermarked image. The mathematical expression of SSIM is given.

\[
\text{SSIM} (x, y) = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{\mu_x^2 + \mu_y^2 + \sigma_x^2 \sigma_y^2 + C_1 (\sigma_x^2 + \sigma_y^2 + C_2)}
\]

\(
\mu_x \mu_y \) is the average of x and y. \(\sigma_x^2 \sigma_y^2 \) is the variance of x and y. \(\sigma_{xy}\) is the covariance of x and y.

\[
\text{NC} = \frac{\Sigma_i \Sigma_j W_{ij} W'_{ij}}{\Sigma_i (W_{ij})^2}
\]

where \(W_{ij}, W'_{ij}\) are original and extracted watermark values at \((i, j)\).

---

**Figure 2.** Original Lena Image  
**Figure 3.** Watermarked Lena Image

**Figure 4.** Watermark image
In Table 1, show the PSNR and SSIM values of Lena and Baboon images. The original Lena image and watermarked Lena image is shown in Figure 2 and Figure 3. The original watermark logo image which is to be embedded is shown in Figure 4 in the same way Baboon original and the watermarked image is shown in Figure 5 and Figure 6.

Image quality assessment (IQA) is part of the quality of experience measures. It is possible to determine image quality using two methods: subjective and objective. Subjective methods are focused on a human viewer's perceptual evaluation of the characteristics of an image or series of images, whereas objective methods are based on computer models that can predict the perceptual quality of the image.

| IQA   | Proposed Method (Lena) | Proposed Method (Baboon) |
|-------|------------------------|--------------------------|
| PSNR  | 55.7                   | 52.18                    |
| SSIM  | 1                      | 1                        |

In this division, compare results of the projected technique with other techniques, the technique used in [15] is the spatial domain in which the watermark is embedded in the blue component. The PSNR value of the proposed technique is larger than [15] which shows watermark is imperceptible in the proposed approach, in the same way, the SSIM value of both technique is equal and this is the maximum value, which shows no change in the watermarked image. The simulation result is listed in Table 2.

| Attack Type | Intensities | Proposed method | Method [15] |
|-------------|-------------|-----------------|-------------|
| SAP Noise   | 0.01        | NC = 0.9910     | NC = 0.9032 |
| Gaussian Noise | 0.05   | NC = 0.9895     | NC = 0.9977 |
| Gaussian Noise | 0.10   | NC = 0.9815     | NC = 0.9816 |
| JPEG        | 60%         | NC = 0.9875     | NC = 0.7512 |
In Table 4, compare to the resistance of the proposed technique against geometric attacks, geometric attacks is basically the displacement of pixels and it is difficult to handle, some of the geometric attacks results are presented here.

Table 4. NC Against Geometric Attacks

| Attacks          | Normalized Correlation |
|------------------|------------------------|
|                 | Proposed Method | Method [15] |
| Cropping 25%    | 0.9955            | 1.0        |
| Median Filter 3x3| 0.9890            | 0.8848     |

9. Conclusion
In this study, an invisible robust image watermarking technique using LSB and laplacian filter is proposed, which enhances the security of the watermark image by choosing suitable positions for watermark embedding. The original image is divided into sub-blocks and the laplacian filter is applied on each block to choose embedding positions. Therefore, the quality of the watermarked image depends on the bits substituted. In the spatial domain, the PSNR value is greater than the frequency domain because the operation is on the pixel level. Moreover, the experimental result on Lena and Baboon image is performed to compare the performance of the proposed technique. Experimental results show the imperceptibility and robustness of the proposed approach against different image processing and geometrical attacks.

References
[1] M. Barni and S. Katzenbeisser 2010 *Handbook of Financial Cryptography and Security*
[2] V. M. Potdar, H. Song, and C. Elizabeth 2005 *IEEE Int. Conf. on Ind. Info, INDIN* 1560462.
[3] A. Mooney 2009 *Handbook of Research on Secure Multimedia Distribution*
[4] N. Sruthi, A. V. Sheetal, and V. Elamaran 2014 *Int. Conf. on Computation of Power, Energy, Info. and Comm. 6915415*
[5] Y. Zhang 2009 *Int. Conf. on Future Comp. and Comm. 10* 76
[6] Y. Naderahmadian and S. Hosseini-Khayat 2014 *Multimed. Tools Appl. 10.1007*
[7] S. Liu, Z. Pan, and H. Song 2017 *IET Image Process. 10.1049*
[8] J. Li and C. Zhang 2020 *Multimed. Tools Appl. 10.1007*
[9] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat 2016 *Digit. Signal Process. A Rev. J*
[10] S. Roy and A. K. Pal 2017 *Multimed. Tools Appl. 10.1007*
[11] S. Roy and A. K. Pal 2017 *Int. J. Electron. Commun. 10.1016*
[12] A. K. Abdulrahman and S. Ozturk 2019 *Multimed. Tools Appl. 10.1007*
[13] S. Chandran and K. Bhattacharyya 2015 *Int. Conf. on Electrical, Electronics, Signals, Comm. and Opt. 10.1109*
[14] A. Bamatraf, R. Ibrahim, and M. N. B. M. Salleh 2010 *Int. Conf. on Comp. App. and Ind. Electronics, 10.1109*
[15] Q. Su and B. Chen 2018 *Soft Com 10.1007*