International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 28th April 2023. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-4

DOI: 10.48047/IJIEMR/V12/ISSUE 04/182

Title **Providing Authentication for Digital Images Using Innovative Invisible Watermarking Technique**

Volume 12, Issue 4, Pages: 1417-1421

Paper Authors
G. Anushya Kirthy, R. Sai Laxmi, J. Vandana, B. Vyshnavi, Dr. B. Vijaya Kumar

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Providing Authentication for Digital Images Using Innovative Invisible Watermarking Technique

G. Anushya Kirthy[1] , R. Sai Laxmi[2] , J. Vandana[3], B. Vyshnavi[4], Dr. B. Vijaya Kumar[5]
[1,2,3,4] B.Tech CSE Scholars, [5] Professor CSE, Department of Computer Science and Engineering,
Vidya Jyothi Institute of Technology

Abstract
The increased use of the internet in daily life necessitates the use of watermarking. Data security issues are common due to the rapid growth in the use of digital content. Different techniques can be used to watermark content. One of these is the Least Significant Bit Watermarking (LSBW) technique. The spatial domain method called LSB is known as least significant bit. The suggested procedure comprises two steps. In order to implant the watermark into the original image, it first chooses the region of interest (RI). The pixels in the chosen RI are then all sorted before the watermark bits are embedded using the LSB method. As a result, the original image can be authenticated with two levels of protection.

Introduction

A logo, line of text, or signature used as a watermark is placed over a picture. Using invisible watermarks, you can cover up text or images inside of pictures. This is most frequently employed as a means of preventing photo piracy. Watermarks have historically been 'stamps' used by photographers to identify their work in an image. These stamps are typically placed on the bottom right and are either overlaid as a pattern on the image or are slightly transparent. Introduction Digital photos are frequently distributed and shared online and through other channels like email, social media, and the internet. However, the problem of the legitimacy and dependability of these photos arises along with the convenience of sharing.[1] Digital photographs can be altered or utilised inappropriately, resulting in the fake or misleading information. Therefore, reliable and effective means of authenticating digital images is needed. Invisible watermarking technique is one such techniques that can be used for images authentication.

Literature Survey

Digital images have progressively assimilated into our daily lives. People post photographs online regularly now that social media and other digital platforms are available. The ease of sharing has brought about an upsurge in image manipulation and unauthorised use, though. Consequently, a reliable digital image authentication system that can confirm an image's validity is required.[1] One of the most promising methods for digital image authentication is the invisible watermarking technique. This method involves hiding a watermark in a picture so that it cannot be seen by the human eye. Information that can be used to confirm the legitimacy of the image is contained in this watermark. Several scholars have put forth several approaches to invisible watermarking for the authentication of digital images. In their research, Kanchan Kumari et al. suggested a technique for inserting the watermark in the image's low frequency DCT coefficients. To boost security, they scrambled the watermark using Arnold Transform. In terms of security and robustness, the suggested method produced positive results. A technique for embedding the watermark in the high-frequency wavelet coefficients of the image was suggested in a different paper by Gangling Shi et al. They employed a watermarking method that is rather fragile and may identify both tampering and innocent image alteration. The outcomes of the suggested technique in terms of robustness and forgery detection were good. Similar to this, J.M. Rodrigues et al.'s paper suggested a technique for

inserting watermarks in the image's colour planes. To strengthen the method's security, they used a chaotic map for watermark insertion and extraction. In terms of security, tamper detection, and robustness, the suggested solution performed well. In conclusion, testing of current invisible watermarking methods for digital image authentication yielded encouraging results. For their robustness, security, and forgery detection skills, various approaches have been put out and evaluated. Researchers must still investigate the shortcomings and weaknesses of these approaches in order to create more reliable and secure methods.

Feasibility Study

An examination of the viability of a proposed project or solution is known as a feasibility study. It seeks to establish the viability of the suggested or proposed solution from a technical, financial, and operational standpoint. [2]A feasibility study would involve evaluating the technology, calculating the costs and benefits of implementing the solution, and determining whether it is feasible to implement it within the constraints of the organisation's resources, capabilities, and objectives in the context of providing authentication for digital images using invisible watermarking technique. The feasibility assessment would also take into account elements including the solution's market demand, legislative requirements, and potential risks and difficulties. The study's conclusions would be taken into consideration when deciding whether to move forward with the solution's implementation. In order to determine whether invisible watermarking for digital photographs is technically feasible, it would be necessary to assess how well the technology serves as an authentication method and how well it works with current tools and systems. The expertise and resources needed to develop and maintain the solution would also be evaluated. In order to determine whether the solution is financially feasible, it would also be necessary to assess any prospective benefits, such as decreased litigation expenses and elevated customer confidence.

Methodology

Literature Review

The use of digital watermarking techniques has become increasingly important in ensuring the authenticity and integrity of digital images. Invisible watermarking techniques, such as the LSB technique used , provide a non-intrusive method of embedding information into an image without significantly altering its appearance. Such techniques have been used in various applications, including copyright protection, image authentication, and tamper detection.

Case study analysis

Several case studies have been conducted to evaluate the effectiveness of invisible watermarking techniques. One study evaluated the robustness of watermarking techniques against image processing operations, such as noise addition and compression. The results showed that the LSB technique, along with other techniques, was able to withstand these operations without significant degradation in image quality.

Technical assessment

The above implementation uses the LSB technique to embed a watermark image into a region of interest in the original image. The watermark is extracted from the watermarked image by iterating over each pixel in the RI and extracting its LSB. The PSNR and NCC metrics are used to evaluate the quality and similarity of the original and watermarked images.

Verification Process:

To verify the authenticity and integrity of the watermarked image, the extracted watermark can be compared with the original watermark using metrics such as PSNR and NCC. If the metrics indicate a high similarity between the extracted and original watermarks, it can be concluded that the watermarked image has not been tampered with and is authentic.

These procedures can be used to develop an efficient and secure authentication mechanism for digital picture invisible watermarking techniques.

Proposed Invisible Watermarking Technique on Sorted Pixel Values in Region of Interest (ROI) Using LSB Technique

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

The suggested approach for adding a watermark on the source image involves two steps:
The distinct digital code is inserted into each of the little blocks of pixels that make up the original image in step 1.
Step 2: Digital photographs with invisible watermarks can be authenticated using the LSB (Least Significant Bit) approach. This method embeds a watermark without altering the appearance of the image by changing the least significant bit of each pixel in the image.

Sorting the Selected Pixles

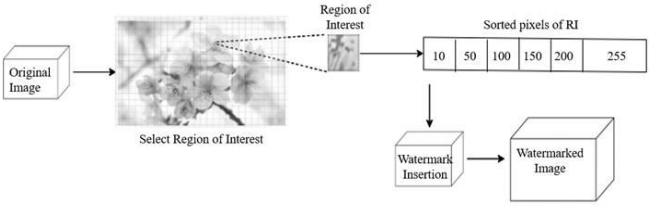
By encoding a special digital code into the image, the technique of invisible watermarking allows users to authenticate digital photos. Although this code cannot be seen with the human eye, it can be found with the aid of specialized software. The image is first transformed into a digital format and then sorted into pixels for invisible watermarking. The distinctive digital code (watermark bits) is encoded into each of the image's discrete blocks of pixels. Since the watermark is injected into the pixels' Least Significant Bits (LSB), it is essentially undetectable and has no impact on the image's quality.

After the watermark has been added, it can be checked using a technique called reverse watermarking, which can retrieve the watermark's unique code and confirm the image's legitimacy. The image can be regarded as suspect or fraudulent if the expected watermark is absent if the watermark does not match the expected code. Digital image authentication using invisible watermarking is safe, dependable, and popular in fields including photography, fine art, and digital media.

Insertion of Watermark Bits into Selected Sorted Pixles

To implement this technique, the following steps can be followed:
1. Select a unique watermark for the image.
2. Convert the watermark into a binary format.
3. Modify the Least Significant Bit of each pixel in the image to contain the watermark information.
4. Save the modified image as a new file.

To verify the authenticity of the image, the following steps can be taken:
1. Extract the watermark from the modified image.
2. Compare the extracted watermark with the original watermark.
3. If the watermarks match, then the image is authentic. If not, then the image may have been tampered with.
The invisible watermarking technique using LSB technique provides a simple and effective way to authenticate digital images without visibly altering them. It can be used in applications such as copyright protection, digital forensics, and document authentication.



Results

Original image

Watermarked Image

Watermark

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Extracted Watermark

Original Image

Watermarked Image

Watermark

Extracted Watermark

5.1 Performance Measures

PSNR

The PSNR (in dB) is defined as

$$PSNR = 20 \cdot \log_{10}\left(MAX_I\right) - 10 \cdot \log_{10}\left(MSE\right)$$

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with B bits per sample, MAXI is 2B − 1.

NCC

The formula for Normalized Cross-Correlation (NCC) between two grayscale images A and B can be expressed as:

$$NCC(A,B) = \frac{\sum(i,j)\left[\left(A(i,j)-\mu A\right)\left(B(i,j)-\mu B\right)\right]}{\sqrt{\sum\left[(A(i,j)-\mu A)^2\right] \times \sum\left[(B(i,j)-\mu B)^2\right]}}$$

Here, (i, j) are the pixel coordinates, A(i,j) and B(i,j) are the pixel values of images A and B at position (i,j), μA and μB are the mean pixel intensities of images A and B, respectively

Conclusion

In today's digital world, when photographs are traded and shared across various platforms, providing authentication for digital images is essential. An efficient method of guaranteeing the authenticity, integrity, and confidentiality of digital photographs without sacrificing their aesthetic quality is the use of invisible watermarking. [4]It makes it possible to incorporate distinctive identification codes, like digital signatures, into photographs that may be used to confirm their authenticity at any time.

Additionally, this method improves the integrity of information sharing, offers solid copyright protection, and prohibits

unauthorised use or altering of photos. Invisible watermarking has become an essential tool for many industries, including medical imaging, law enforcement, and data privacy, because to the growing demand for secure and trustworthy techniques to verify digital images. In conclusion, invisible watermarking is a reliable method that represents an important step in guaranteeing the secrecy and integrity of digital images.

To calculate the accuracy of the present work PSNR and NCC are used. The value for PSNR was above 80 dB and for NCC value is 0.9. Results shows that Watermark Image is embedded more securely and it is robust for attackers

References

[1]. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital watermarking. San Francisco, CA: Morgan Kaufmann Publishers.
[2]. Delgado-Fernandez, M., & Perea-Ortega, J. M. (2018). An overview of invisible watermarking techniques. International Journal of Computer Applications, 179(28), 35-40.
[3]. Kaur, R., & Singh, H. (2017). Robust and invisible digital watermarking using DCT and SVD. International Journal of Computer Applications, 160(8), 1-6.
[4].Li, X., & Yang, Y. (2019). An improved invisible watermarking algorithm based on singular value decomposition. Journal of Ambient Intelligence and Humanized Computing, 10(2), 431-436.