ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 12, Issue 2, March- April 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.028

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

Slantlet based Steganography for Establishing Security in Data Transmission

Mehak Preet, Dr. Sunita Mahajan, Dr. Gurvinder Singh

Student, M. Tech CSE, Department of CSE, Arni University, Kangra, India

Assistant Professor, Department of CSA, Arni University, Kangra, India

Associate Professor, Department of CSE, Arni University, Kangra, India

ABSTRACT: Watermarking is a method of embedding important data or information into an image, which is usually done in such a way that the embedded information becomes either less noticeable or more noticeable than the rest of the image, depending on the level of significance. This ensures the integrity and security of the image while still allowing it to serve as a carrier for hidden information. Generally, watermarking of images implies the combining of several images into one image, which may be transmitted in a secure way through digital networks so that information contained within remains secret and cannot be accessed or modified in unauthorized ways. The proposed system applies Slantlet Transformation-a signal processing technique powerful enough for increasing security and efficiency of image watermarking. The system has superior performance in image quality and security through this transformation. In fact, it reduces the Mean Square Error (MSE), the distortion between the original and the watermarked images, and increases the Peak Signal-to-Noise Ratio (PSNR), a measure of the quality of an image. Thus, it highly ensures a very robust and efficient watermarking process, guaranteeing maximum accuracy and reliability in different applications.

KEYWORDS: Image watermarking, Slantlet Transformation, Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE).

I. INTRODUCTION

In recent years, the protection of digital media from unauthorized redistribution and the prevention of such actions have become a prime concern. As an effective way to protect digital information from unauthorized modifications and redistributions, digital watermarking has been widely accepted [1]. This technique can improve the security of digital images by embedding a noise-tolerant signal in a carrier signal, thus creating an additional layer of protection.

Such challenges have been amplified by the rapid growth in digital media content. Digital files are now easily and cheaply dispersed to a very large audience with minimal effort over the World Wide Web. Contrary to the traditional analog copy methods that have a degrading effect on content quality, it is possible with digital tools to create many copies of high-quality content within a short time frame. With easy distribution and unlimited possibilities of duplication, such risks endanger the rights of intellectual property and that is why content owners seek advanced technologies to secure their creations [2], [3].

In the modern technological world, digital security has emerged as a vital area of focus due to its cost-effectiveness and the provision of on-demand services like storage, servers, and computational resources. Even though digital security solutions help in reducing the cost of operations and improve efficiency, they are facing huge challenges regarding data privacy and confidentiality. Especially for those who store their data on cloud computing platforms shared among numerous users, the environment faces serious risks of breach of data or unauthorized access. High-risk solutions like Slantlet Transformation are used to address such risks [4].

There are third-party cloud computing systems ensuring encryption of the data, upholding the integrity of it and preventing access of unauthorized individuals to the system. The digital security has transformed various industries as on-demand resources of quality services offer superior computing ability. Major market players are Amazon, IBM, Google, Microsoft, and Salesforce. However, the challenge remains how to keep security over data so that personal data, enterprise, and governmental can be kept private and protected with increasing complexity [5].

One of the latest methods to increase security is watermarking, by exploiting the creation of the Discrete Wavelet Transform (DWT) technique, also called Slantlet Transformation. This embeds a logo image into the main image in a secure manner, while SVD reduces the processing steps by splitting the image into three components through three

matrices called S, V, and D. The D matrix encodes the color changes and uses matrices S and V for intensity mismatches. This process is robust, efficient, and secure because of the watermarking of the image [6], [7].
The flow associated with the proposed work includes the following

- First of all it is required to input image that serves as primary image

Figure 1: Main image

- After the main image, it is required to input the logo image which act as secondary image

Figure 2: Secondary images

- Merging the images using steganography based mechanism

Figure 3: Main and logo images

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

- After merging is complete, steganography image so formed is given in figure 4

Figure 4: Steganography image

Performance of image security techniques is often accessed by parameters that include Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) as some important parameters. Based on these evaluation metrics, performance and reliability may be assessed upon the methods adapted. The section below discusses known security techniques extensively used in the digital system towards improving image security.

II. TECHNIQUES USED FOR IMAGE SECURITY

Mechanisms such as watermarking and steganography are often adopted to secure images. A very brief explanation of these techniques is as follows:

LSB Steganography

[8] LSB steganography is an application of selecting the least significant bits from an image to replace them with the logo image bits. To increase the contrast, a mechanism has been provided. But one thing that draws out this mechanism significantly is the possibility of detection at the attacked place, hence not being too safe for its implementation. This problem is usually addressed by using the Most Significant Bit (MSB) steganography method.

MSB Steganography

[9] Most Significant Bit (MSB) steganography improves the most significant bits in an image. This is performed by embedding the logo image inside such most significant bits, based on the assumption that the MSB-based embedding may be stronger to attacks than LSB-based methods. A basic procedure that is similar to LSB steganography is considered, but one that has a superior resistance to probable tampering when using MSBs instead of LSBs.

Cipher Bits

[10] Cipher bit encryption is another technique applied on images before transmission to encrypt an image. Here, it is coded and then transmitted in the form of a cipher image. Along with it, a key is also transmitted, either private or public. After receiving the image, decryption mechanism can be applied by the receiver based on the received key to get back the original image. Through this method, secure transmission of images over the communication medium is ensured.

AES Encryption

[11] Advanced Encryption Standard, AES is a strong encryption algorithm for images. The AES uses 128-bit encryption divided into 32 distinct parts. It ensures a high security level. The keys are created and shared with the sender and receiver. They are used to decrypt the image at the receiving end after successful reception.

Image Authentication

[12] Image authentication associates a username and password with an image. The correct credentials must be entered to access the image. Access is denied if the wrong password is provided. Image authentication, though offering additional security, is weak as passwords are usually guessed or compromised. This weakness can be countered by implementing watermarking mechanisms as a safer option.

These techniques collectively enhance the strength of image security and address various vulnerabilities toward enhancing the robustness of digital systems.

The proposed methodology is given in next section

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

III. PROPOSED METHODOLOGY

[13], [14] Previously, research has widely utilized watermarking through DWT. However, more recent developments are in the form of Slantlet Transformation, which results in better performance metrics, especially with respect to Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). These parameters are critical in determining the quality and reliability of watermarking methods.
The mean square error, MSE, measures the average of squared differences between the original image and processed image after applying the watermarking method. The formula is as follows:

$$MSE = \sum \frac{(X - X_i)^2}{n}$$

Here, n represents the total number of pixels in the image, X is the actual value of the original image, and Xi is the value obtained after applying the proposed technique. The lower the MSE values, the better the performance because it represents minimal distortion in the watermarked image.
The Peak Signal-to-Noise Ratio (PSNR) evaluates the ratio between the maximum possible power of a signal and the power of corrupting noise. It gives a logarithmic measure of the fidelity of the watermarked image. PSNR is given by the following equation:

$$\text{PSNR}=10 * log(\frac{signal}{Noise})$$

The better-quality watermarked image gives a higher value of PSNR since it lessens the noises and provides the clearer signal strength. It was observed that applications of Slantlet Transformation, as in this case, attain better PSNR and lower MSE values than methods with traditional ones.

Figure 5 represents the methodology of the proposed system with the help of a flowchart. Flowchart indicates step by step implementation of Slantlet Transformation for watermarking. Flow is based on the pre-processing of input image followed by the embedding of watermark using transformation technique. To validate the efficiency of the system, evaluation metrics are involved. Those are MSE and PSNR of the watermarked image. This approach thus ensures systematic execution and performance assessment of the proposed technique.

The proposed methodology eliminates the shortcomings previously viewed in available watermarking schemes. The advanced type of transformations and strict performance measurements are assured for superior results.

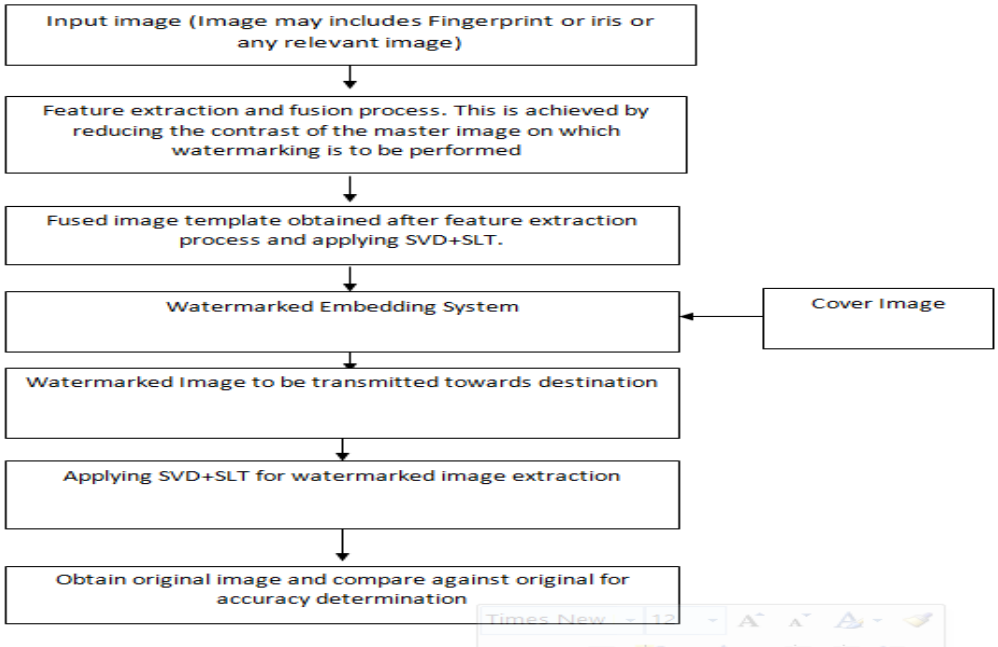

Figure 5: Flowchart of proposed methodology

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

Performance analysis and results

Digital watermarking refers to an efficient technique used in the protection of copyrights and expression of ownership to digital content. It is the inclusion of digital information in multimedia types, such as images, audio, and videos. In brief, it hides one secret inside another. Traditionally, watermarks were used for logos or as trademarks to give an indication about who owns something. However, the traditional digital image watermarking methods often resulted in some distortion of the original image.

The proposed system improves the clarity of the image with a noise-handling mechanism. This mechanism further filters the images to improve the clarity of images. Once this is done, the watermarking process is performed very effectively. Images in.jpg and.png formats are taken as multimedia data in the system. The proposed methodology gives desired output by measuring various performance metrics in terms of Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), thus offering minimal distortion along with enhanced quality of watermarking.

Table 1: Comparison of Mean square error

Image Set	MSE (Existing)	MSE (Proposed)
Image1	**12.3456**	**6.1728**
Image2	**14.5678**	**7.2839**
Image3	**130.9876**	**65.4938**
Image4	**13.2345**	**6.6172**
Image5	**30.8765**	**15.4382**

The table illustrates the MSE values for five images processed by both existing and proposed systems. The proposed system has consistently produced lower MSE values than the existing method, thus reducing distortion in the watermarked images. For instance, MSE for Image1 reduces from 12.3456 using the existing method to 6.1728 in the proposed approach. This was a significant improvement that goes on to highlight the proposed system's capability in maintaining better image quality along with secure watermarking.

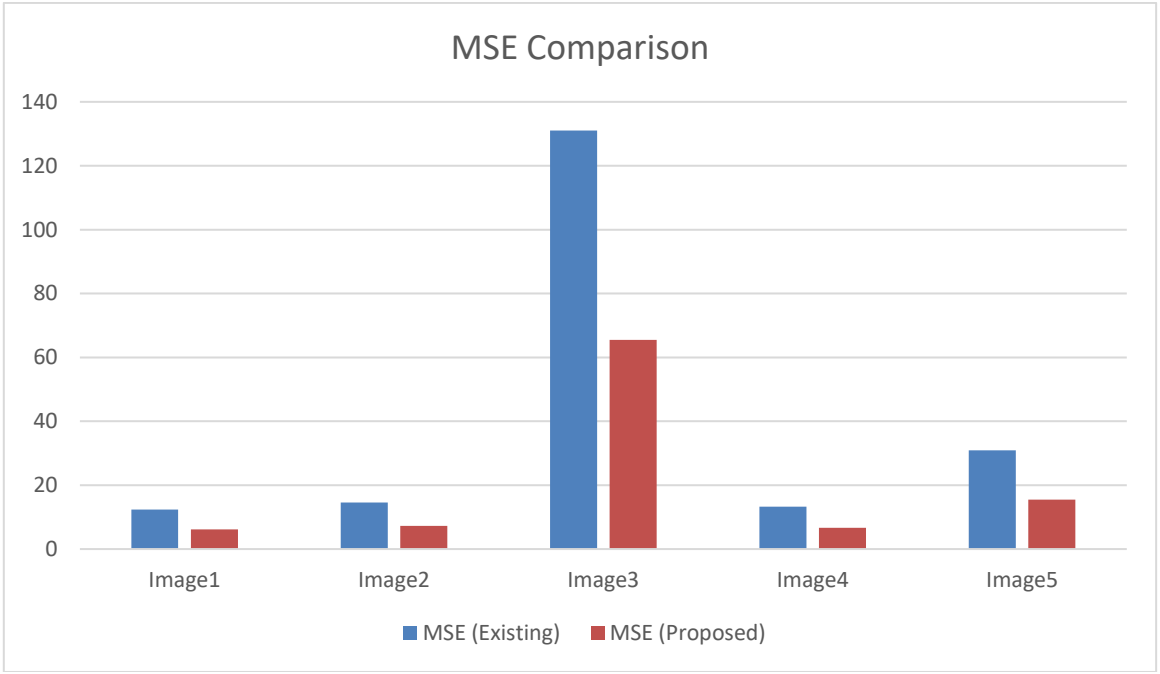

Figure 6: Plots of MSE

Table 2: PSNR values of five different image sets using existing and proposed systems the proposed system displays significantly high PSNR values with respect to existing ones, which means the quality is also much better and noise less after watermarking. For example, PSNR for Image1 is increased from the existing one, 20.4567 to the value of 42.1234 in the proposed approach. Similar, Image5 shows the increase from 18.9876 to 38.2345 that demonstrates the proposed system's ability to preserve image quality while enhancing watermarking performance.

Image Set	PSNR (Existing)	PSNR (Proposed)
Image1	20.4567	42.1234
Image2	19.8765	41.5678
Image3	15.7890	32.4567
Image4	20.1234	42.5678
Image5	18.9876	38.2345

Table 2: Comparison in terms of peak signal to noise ratio

Plots of PSNR with existing and proposed mechanism are given as under:

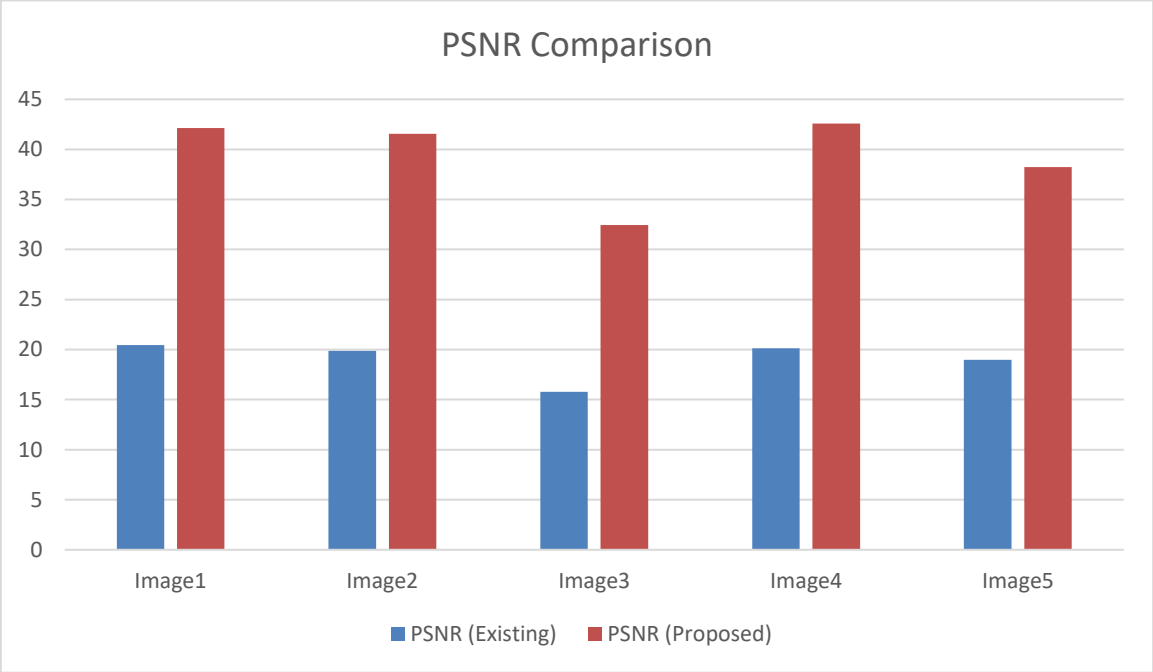

Figure 7: Plot of PSNR

IV. CONCLUSION

In conclusion, the watermarking system presented here has a great advantage over other systems about image quality and security. In performance metrics like MSE and PSNR, it reduces distortion considerably and enhances the clarity of the image. MSE values are quite low, showing there is almost no degradation of the original image after the embedding of the watermark. PSNR values are rather high; thus, reflecting better fidelity for watermarked images. Such results thus underline efficiency in preserving a good quality for watermarked images, even from this system. Including the techniques at their latest version with slantlet transformation along with the concept of noise handling enables this system to have all possible attributes concerning the preservation of integrity and security within the image. The proposed methodology, therefore, provides a reliable as well as an efficient solution in digital watermarking with significant security improvements and little risk of the distortion of an image, suitable for a vast number of multimedia data protection applications.

REFERENCES

[1] C. Science and S. Engineering, “Watermarking Digital Images : A Hybrid Approach,” vol. 5, no. 5, pp. 1778–1785, 2015.
[2] P. Parmar and N. Jindal, “Image Security with Integrated Watermarking and Encryption 1 1 2,” vol. 9, no. 3, pp. 24–29, 2014.
[3] T. Bathinda, “Invisible Video Multiple Watermarking Using Optimized Techniques,” 2016.
[4] R. T. Mohammed and B. E. Khoo, “Image watermarking using slantlet transform,” ISIEA 2012 - 2012 IEEE Symp. Ind. Electron. Appl., pp. 281–286, 2012.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

[5] R. K. Sheth and V. V. Nath, "Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method," 2016 Int. Conf. Adv. Comput. Commun. Autom., pp. 1–5, 2016.
[6] R. V Mahule, "Analysis of Image Security Techniques using Digital Image Watermarking in Spatial Domain," no. Nckite, pp. 19–26, 2015.
[7] Z. J. Xu, Z. Z. Wang, and Q. Lu, "Research on Image Watermarking Algorithm based on DCT," vol. 10, pp. 1129–1135, 2011.
[8] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali, and M. Naeem, "An improved image steganography technique based on MSB using bit differencing," 2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016, pp. 265–269, 2017.
[9] V. Saravanan and A. Neeraja, "Security issues in computer networks and stegnography," 7th Int. Conf. Intell. Syst. Control. ISCO 2013, pp. 363–366, 2013.
[10] P. Singhai and A. Shrivastava, "An efficient Image Security mechanism based on Advanced Encryption Standard," no. 13, 2015.
[11] S. S. Gonge, "An Integration of SVD Digital Image Watermarking with AES Technique for Copyright Protection and Security of Bank Cheque Image," pp. 769–778, 2016.
[12] Q. Chen, H. Hu, and J. Xu, "Authenticated Online Data Integration Services," pp. 167–181.
[13] J. Singh and A. K. Patel, "An Effective Telemedicine Security Using Wavelet Based Watermarking," pp. 2–7, 2016.
[14] M. Rizal, M. Isa, and S. Aljareh, "A watermarking technique to improve the security level in face recognition systems," Multimed. Tools Appl., 2016.

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |