Introduction

In the field of digital art, especially digital images, every work represents the unique creative expression of the creator [1]. This digital image art is not only a medium of artistic expression but also a valuable asset that can be easily accessed through various online platforms. However, this ease of access also brings serious challenges, such as the risk of copyright infringement, plagiarism, and counterfeiting. In this context, it is important to develop effective approaches to protect the authenticity and value of digital image artworks.

Watermarking allows embedding an image, text, PDF, audio, or video within a multimedia entity to prevent misuse and protect copyright [2]. Steganography, also known as hidden watermarking, is one of the reliable techniques to overcome these challenges. Steganography is the art of hiding some secret data by embedding it into an unclassified host medium [3]. This technique allows the insertion of secret information, such as copyright metadata or ownership marks, directly into a digital image while maintaining its visual quality. This is particularly relevant in the world of digital art, where the aesthetic and artistic value of the work must be maintained. One method of steganography is reversible data hiding (RDH). This method allows information to be inserted into digital media without damaging the original visual elements. RDH typically utilizes approaches such as lossless compression [4]–[8] difference expansion [9]–[11], histogram shifting [12]–[14], prediction error expansion [15]–[17]. With these features, RDH becomes an ideal solution for protecting digital image art while ensuring its artistic integrity is preserved.

Huang et al. [18] proposed a new method for RDH in encrypted domains that uses stream encryption and permutation algorithms to maintain the correlation between neighboring pixels. The dataset used consists of twelve images of 512 x 512 pixels. The experimental results show varying embedding capacities, with high PSNR values reaching over 48 dB. Fadlan et al. [19] proposed a modified RDH method using dynamic permutation to increase security against known plaintext attacks, by applying the difference histogram shifting (DHS) algorithm to encrypted medical images. The dataset used consists of twelve medical images measuring 1024 x 1024 pixels. Tiwa et al. [20] proposed a digital diploma validation system using the RDH method with histogram shifting and random sub-block insertion techniques. The dataset used consists of 20 digital diplomas of 1122 x 792 pixels in PNG format, designed with various colors and patterns to test the compatibility of the system. The experimental results show good EC and high PSNR values, with PSNR values over 48 dB and SSIM above 0.99, indicating excellent image quality after data insertion.

This research develops a data insertion method in digital images with a histogram shifting-based approach to maintain visual quality and data integrity. The process begins with the division of the image into sub-blocks, where the sub-blocks used for data insertion are randomly selected using a PIN as input to enhance security. Histogram shifting is used to modify the pixel values in certain blocks to enable binary data insertion without damaging the image. Pixels equal to 0 or 255 can cause overflow/underflow [18], and this approach includes mechanisms to handle distortions such as overflow and underflow. The validation stage is performed using the extracted image to obtain the index list S, which is then compared with the original image. If the index maps of the extracted image and the original image are identical, the method is considered successful in maintaining the integrity of the inserted data.

This method seeks to enhance the security and integrity of the hidden information by guaranteeing that only authorized persons can access and extract the embedded message. By integrating these two methodologies, we aim to build a robust architecture that provides secure embedding of data within the obfuscation medium while authenticating the identity of individuals who wish to access the data.