# Advanced Encryption Standard Algorithm in Digital Watermark Images

# خوارزمية التشفير القياسية المتقدمة في صور العلامة المائية الرقمية

**Nawfal Abdullah Ramadhan** **نوفل عبدالله رمضان**
Computer Science Department, University of Technology, Baghdad - Iraq
nnnommm9863@gmail.com

**Prof. Dr. Abdul Monem S. Rahma** **أ.د. عبد المنعم صالح رحمة**
Computer Science Department, Al-Maarif University College, Anbar - Iraq
Monem.rahma@uoa.edu.iq

**Prof. Dr. Ahmad Ghandour** **أ.د. احمد غندور**
Computer and Communication Engineering Department / Islamic University of Lebanon, Wardanieh - Lebanon
ahmad.ghandour@iul.edu.lb

**تاريخ تقديم البحث: 2023/10/21**
**تاريخ قبول البحث: 2024/05/28**

**Abstract:**

Abundant amount of information was produced, stored, and shared digitally. This increase as well as validating the info of ownership information has been digitally watermarked.

The process of embedding confidential data into an original image is known as "watermarking" an image. In order to guarantee the system's security, Advanced Encryption Standard (AES) encrypt the logo image in this proposed paper.

The normalize root mean square error (NRMSE), peak to signal ratio (PSNR), root mean square (RMSE), mean square error (MSE), and structural similarity (SSIM) are utilized for evaluating the performance of embedding and decrypting watermark images.

The developments and findings from measurements supported the AES encryption method's reliability, and the histogram demonstrated the encrypted logo image's pixels' excellent distribution and showed how different the encrypted image is from the watermark image in terms of uniformity and bit depth. This indicates that the bit interleaves encryption image affected the level values and pixel positions, and the extracted and original logo images' excellent structural similarity (SSIM) scores are around 0.9.

**Keywords*: Logo image, Cover image, Watermark images, AES, LSB.***

**الخلاصة**

تم إنتاج كمية وفيرة من المعلومات وتخزينها ومشاركتها رقميًا. تم وضع علامة مائية رقمية على هذه الزيادة بالإضافة إلى التحقق من صحة معلومات معلومات الملكية.

تُعرف عملية تضمين البيانات السرية في الصورة الأصلية باسم "العلامة المائية" للصورة. من أجل ضمان أمان النظام، يقوم معيار التشفير المتقدم (AES) بتشفير صورة الشعار في هذه الورقة المقترحة.

يتم استخدام جذر متوسط مربع التطبيع (NRMSE)، ونسبة الذروة إلى الإشارة (PSNR)، وجذر متوسط مربع (RMSE)، ومتوسط خطأ مربع (MSE)، والتشابه الهيكلي (SSIM) لتقييم أداء تضمين وفك تشفير صور العلامات المائية.

دعمت التطورات والنتائج المستخلصة من القياسات موثوقية طريقة تشفير AES، وأظهر الرسم البياني التوزيع الممتاز لوحدات البكسل في صورة الشعار المشفرة وأظهر مدى اختلاف الصورة المشفرة عن صورة العلامة المائية من حيث التوحيد وعمق البت. يشير هذا إلى أن صورة التشفير ذات تشذير البت أثرت على قيم المستوى ومواضع البكسل، وأن درجات التشابه الهيكلي الممتاز (SSIM) لصور الشعار المستخرجة والأصلية تبلغ حوالي 0.9.

الكلمات المفتاحية: صورة الشعار, صورة الغلاف, صورة العلامة المائية, خوارزمية البت الاخير, التشفير AES.

## 1. Introduction

Data possession protection in the initial data (Text, Image, Video or Audio) represents the main goal of the digital watermarking system. Due to technology advancement, it is simpler to copy the material of a legitimate owner without their consent. This is due to knowledge of unauthorized parties' access to image processing and internet manipulation techniques. In order to prevent these illegal activities, numerous researchers from around the world have already proposed various types of effective watermarking schemes. However, they were unable to safeguard the power and imperceptibility, which are the (2) key characteristics of an effective system of watermarking [1].

Imperceptibility refers to the image of watermark or the data not being apparent in the cover image or host image. Robustness is the second quality. Attacks like noise, filtering, chopping, and rotation must not be successful against the concealed watermark image. The user will have to choose between these two attributes during design. Spatial domain approaches and domain transfer techniques make up the two groups that comprise all watermarking methods [2, 3].

Digital photographs have a modified value of pixel intensity in the spatial domain; however, the watermarking is not reliable. As more and more undetectable data and schema are added, the digital image coefficients are modulated in the frequency domain correspondingly [4].

In network communication, image security has grown to be a significant issue. Encryption is one method for keeping digital images safe, secure and difficult to violate and seize logo's images. With the exception of, image encryption techniques seek to change the original image into a new one that is challenging for anybody to interpret. Without a decryption key, only individuals with specialized knowledge should be able to decode the material [5, 6].

Data security using the AES algorithm is achieved. Both text and image data are encrypted using the AES technique that is currently available. With the use of Python software, the technique of AES for image encryption as well as the decryption is synthesized and simulated [7].

The AES contains the features and requirements of the system, including sensitivity to beginning circumstances, randomness, and unpredictability, etc. Several systems of AES image encryption have been proposed.

This research article describes a technique for creating digital watermarks that embeds a logo image into an image using encryption to create the watermark. The reverse of the AES encryption and embedding procedure may be used to get the concealed image.

The rest of such paper is split into the following Sections: Literature review, AES algorithm is briefly discussed in Section 3, The proposed schema of the proposed system discussed in details in section 4 with the processes for embedding and extracting the watermark, Performance measurement and investigational outcomes are shown in Section 5, The developments and findings consists of 2 tests discussed in section 6, Conclusion in section 7 and Future work in section.

## 2. Literature review

A variety of studies cover covers aspects of the watermarking processing chain. Most works focus mainly on the transformation techniques for embedding and extraction techniques and others. Many researchers worldwide already have suggested various types of efficient watermarking schemes in order to avoid illegal acts. In this section, some of the previous works are presented with a brief explanation for each of them:

Vijay Krishna Pallaw, et.al., "**A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications**", Digital watermarking is used to prove the authenticity of the medical images before diagnosis. In this paper, proposed a hybrid watermarking scheme using the Slantlet transform, randomized singular value decomposition, and optimization techniques inspired by nature (Firefly algorithm) then the WI is encrypted. Extensive testing reveals that our innovative approach outperforms the existing methods based on the NC, SSIM, and PSNR. The SSIM and NC values of watermarked image and extracted watermark are close to or equal to 1 at a scaling factor of 0.06, and the PSNR of the proposed scheme lies between 58 dB and 59 dB, which shows the better performance of the scheme [8].

Tianfu Li, et.al., "**Robust watermarking algorithm for medical images based on log polar transform**", Combined log-polar transform (LPT) and discrete cosine transform (DCT), a novel robust watermarking algorithm for medical images, is proposed. It realized the lossless embedding of patient information into medical images. In the process of feature extraction and watermark embedding, the proposed algorithm reflects the characteristics of LPT, scale invariance and rotation invariance, and retains the advantages of DCT's ability to resist conventional attacks and robustness. The good experimental results show the effectiveness of this algorithm and guaranteed the quality of medical images [9].

Chirag Sharma, et.al., "**A Robust Image Encrypted Watermarking Technique for Neurodegenerative Disorder Diagnosis and Its Applications**", A new method of watermarking is proposed on both standard and medical images. The paper addresses the use of digital rights management in medical field applications such as embedding the watermark in medical images related to neurodegenerative disorders, lung disorders, and heart issues. The various quality parameters are used to figure out the evaluation of the developed method. In addition, the testing of the watermarking scheme is done by applying various signal processing attacks. The results indicate the proposed technique's good performance. The proposed method is fast, and the addition of an optimization algorithm will improve the value of quality metrics [10].

Shankar A. et.al., "**A Hybrid of Watermark Scheme with Encryption to Improve Security of Medical Images**", In this work, both robust and reversible watermarking is done and a three-level security is provided. The medical image is divides into two major parts with giving importance to diagnose identification namely region of interest (ROI) and region of non-interest (RONI). Firstly, in ROI Reversible data embedding, which embeds payload data in reversible manner in to binary image, secondly in RONI, Robust watermarking is done, so that it can withstand various intentional and unintentional attacks. Later, both watermarked images are combined and a single watermarked image is obtained. Thirdly, the resultant image is further processed by using AES algorithm which makes output image in an unreadable form, thus providing high security. Further decryption process is done to retrieve the original image [11].

Sondes Ajili, et.al., "**Crypto-Watermarking Algorithm Using Weber's Law and AES: A View to Transfer Safe Medical Image**", Proposed a novel method for medical image watermarking in the DCT domain using the AES encryption algorithm. First, decompose the original medical image into subblocks of 8 × 8 and embed the patient's data into the corresponding medical image. To increase the robustness, we encrypt the watermarked medical images by using the AES algorithm based on chaotic technique. Arnold's cat map is used to shuffle the pixel values, and a chaotic Henon map is utilized to generate an aleatory sequence for the AES algorithm, the shuffled watermarked image is encrypted using the modified AES algorithm. The average peak signal-to-noise ratio (PSNR) of the medical images obtained is 61,7769 dB. Experimental results demonstrate the robustness of the proposed schema against various types of attacks [12].

## 3. AES Algorithm

The AES algorithm is a traditional symmetric encryption algorithm that was founded as the standard for encrypting digital data by the US National Institute for Standard and Technology (NIST). It is accepting input plain text block (128-bit) and using three different key length 128, 192, and 256 bits [13]. The key length specifies the number rounds of encryption and decryption which could be 10, 12, and 14 rounds for 128, 192, and 256-bit key-length, respectively. The strength of the algorithm security depends on the larger key length.

The security level is determined by the key size, and as the key size grows, so does the level of security. The round function used by the AES algorithm is made up of four separate byte-oriented

changes. The following table describe the rounds for encryption and decryption process, which includes the following steps [13]:

Table 1. Encryption and Decryption rounds.

| Encryption process | Decryption process |
|---|---|
| - Changing the byte | - Inversing the shift row |
| - Moving the row | - Inversing the replace byte |
| - Mixing the columns | - Adding the round key |
| - Adding the round key | - Inversing the mix columns |

Additionally, there's a no. of rounds that introduce the key as well as the block into the algorithm. And, the no. of rounds lies upon the key's length employed for encryption and decryption.

## 4. Proposed Scheme

The proposed scheme comprises (2) stages, the 1st one being for embedding, and the 2nd one being for extraction.

### 4.1 The embedding stage

The implementation technique steps of the embedding procedure of the proposed watermark image are shown in Figure 1.

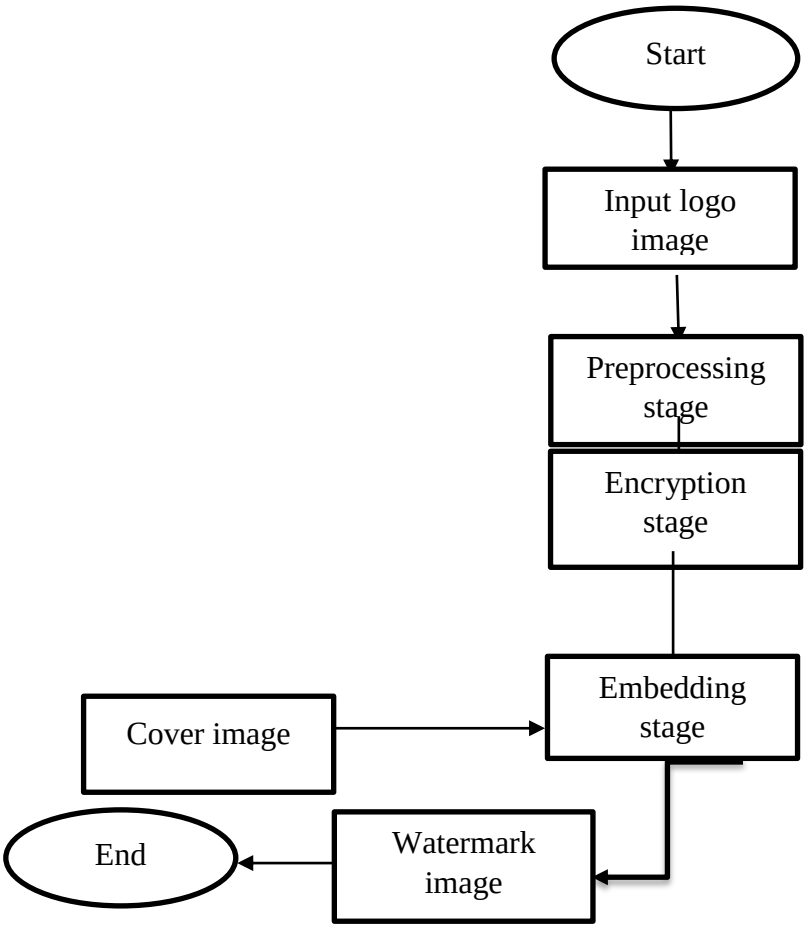



Fig. 1: General structure of the embedding schema

The present section will discuss the suggested embedding procedure of system algorithm (Figure 1):

Algorithm 1: Embedding procedure.
Input: Logo Image (LI) and Cover Image (CI)
Output: Watermark Image (WI)
Procedure:
Step 1: Loading the LI.
Step 2: Encrypting the LI by AES.
Step 3: Load the CI.
Step 4: Embedding the encrypted LI into CI.
Step 5: Obtaining WI.
End.

### 4.2 The extraction stage

In such stage, the extraction stage will debate exactly the embedding stage inverse.
Algorithm 2: Extraction procedure.

Input: Watermark Image (WI)

Output: Original Logo Image (CI)

Procedure:

Step 1: Loading WI.

Step 2: Utilizing XOR (inverse Least Significant Bit (LSB)).

Step 3: Obtaining (2) images: CI as well as the encrypted LI.

Step 4: Decrypting LI via implementing the inverse of AES.

Step 5: Obtaining the LI.

End.

## 5. Performance Measurement and Investigational Outcomes

The investigational findings were determined utilizing two images—CI and a LI—in two experiments. Test (1) used an image of a monkey as a logo as well as an image of flowers as a CI; and test (2) used as a Lenna image as a LI as well as a butterfly image as a CI.

The following metrics were employed to compare the two images, including the PSNR, MSE, NRMSE, and SSIM, and RMSE. Entropy was determined for the decrypted LI, as manifested in Tests 1 as well as Test 2.

The PSNR, which calculates the active info of the image to noise ratio, can indicate whether the image being distorted. And, the mathematical representation equation is [13]:

$$PSNR = \left(\frac{MAX^2}{MSE}\right) \quad \textbf{(1)}$$

*Where*, the MSE stands for mean square error and $MAX^2$ denotes the highest feasible pixel value for the image.

The range of values for the SSIM, which denotes structural similarity, is [-1,1]. The resulting value of SSIM in Tables 1 and 2 equals to one, which denotes the upper similarity degree as well as upper fusion quality level. The SSIM formula is:

$$SSIM(x,y) = \left(\frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)}\right) \quad \textbf{(2)}$$

*Where:*
c1, c2, and c3: Constants
$\mu_x$ & $\mu_y$: The Local Sample Means of (x) and (y), correspondingly
$\mu_x\mu_y$: The Coefficient of Local Sample Correlation between (x) and (y)
$\sigma_x$ & $\sigma_y$: The Local Sample Standard Deviation of (x) and (y)

The MSE, an objective assessment indicator of the image quality based on pixel error, displays the degree of disparity between the variables. It is used to measure the difference between the bonded image and the perfect reference image. And, the MSE being certainly not negative, as well as it has to be as minor as likely [14]. It is provided in this equation [15]:

$$MSE = \left(\frac{1}{mn}\right)\sum_{i=0}^{m-1} \quad \sum_{j=0}^{n-1} \quad [I(i,j) - K(i,j)]^2 \quad \textbf{(3)}$$

*Where:*

i & j: The row and the column pixels values of the (2) images I(i,j) and K(i,j), respectively

m & n: Number of the rows and the columns, respectively

According to Table 2, the MSE's lower value indicates a smaller difference between the two photos. By dividing the total number of pixels in the image by square root of squared error, thus RMSE is calculated [16].

$$RMSE = \sqrt{MSE} \quad \textbf{(4)}$$

The NRMSE mathematical equation is:

$$NRMSE = \left(\frac{\sqrt{MSE}}{\sum_{j=0}^{p} \frac{(d_j) - min(d_j)}{p}}\right) \quad \textbf{(5)}$$

*Where:*
$d_j$: The intended output at the treating element (j)
p: Number of the output treating elements
N: Number of the examples in data set.

An essential aspect of uncertainty and randomness is the info entropy (H) (Eq. 6), and the goal assessment index is counting the quantity of info present into an image. The quantity of info in the fused image increases with information entropy, and for a perfect random image, the info entropy number has to be near to (8).

And, the info entropy equation is given as:

$$H = \left(p_{(i,j)}\right) \quad \textbf{(6)}$$

*Where*, $P_{(i,j)}$ is the pixel gray level probability distribution with respect to (i, j), and n denotes the gray levels number (256 for 8-bit images).

## 6. The developments and findings

This section consists of two tests as follows:

**Test 1: Unencrypted and original logo images**

The measurement was done between the unencrypted and original versions of the logo, as seen in the Figures 2, 3, and 4.

The logo image underwent four rounds:

- Substituting the byte
- Shifting the row
- Mixing the columns
- Adding the round key

AES processing after encryption was applied, improving as well as bolstering the defenses of embedded watermark against the assaults.

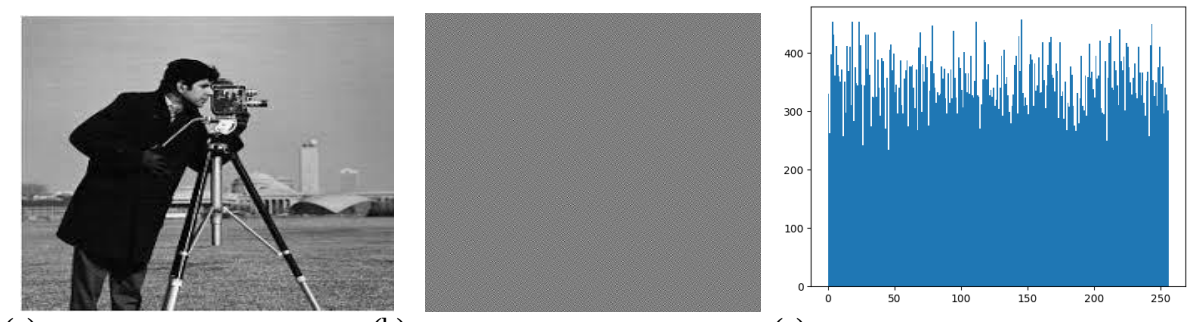
The experimental evaluation of performance results from the Table 2 that preceded it may be summed up as follows:

1. A better encryption scheme (must be as low as feasible) results from a lower PSNR value.
2. The highest MSE scores point to unpredictability and significant noise.
3. There is little and almost no difference between both of these images—the basic LI and the encrypted LI outlined in SSIM.
4. The entropy of the cypher logo (Entropy pic. 2) image is extremely near to the ideal value (8), which indicates that the proposed technique achieves high diffusion and substitution and has a reliable performance in addition to excellent security against entropy assaults.

The various MSE, PSNR, and SSIM resulting values demonstrated the potency of the suggested encryption scheme that was used to secure the logo image. The reasons for using encryption and the effectiveness of the encryption used to boost the security of the suggested method are all demonstrated by the aforementioned arguments.

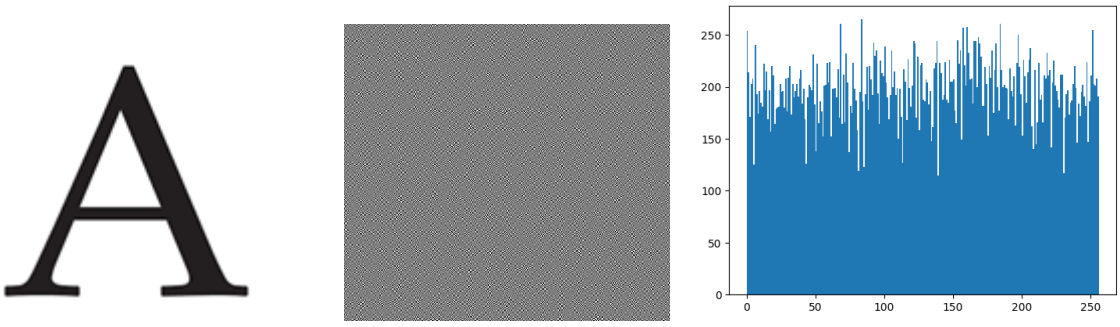

(a) (b) (c)

Fig. 2: Encryption and the histogram of “Monkey” LI; (a) The “Monkey” LI, (b) The encrypted LI, and (c) The histogram of (b).




(a) (b) (c)

Fig. 3: Encryption and the histogram of “Man” LI; (a) “Man” LI, (b) The encrypted LI, and (c) The histogram of (b).




(a) (b) (c)

Fig. 4: Encryption and the histogram of "A" LI; (a) Letter "A" LI, (b) The encrypted the LI, and (c) The histogram of (b)

Table 2: The quality measurements to test the strength of LI as well as encrypted LI for "Monkey", "Man", and "A" LIs.

| Results | PSNR | MSE | RMSE | SSIM | Entropy pic. 2 |
|---|---|---|---|---|---|
| Figure 2 | 27.90 | 105.44 | 10.23 | 0.01 | 7.90 |
| Figure 3 | 27.82 | 107.19 | 10.34 | 0.03 | 7.51 |
| Figure 4 | 33.32 | 152.22 | 12.33 | 0.05 | 7.01 |

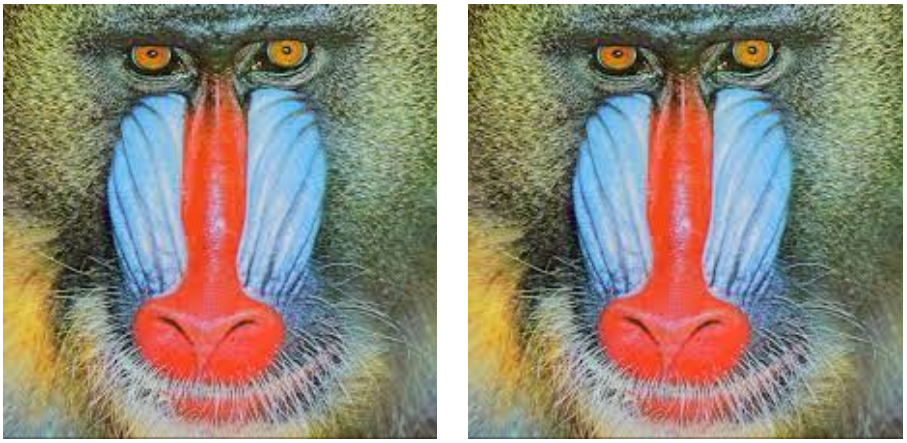
**Test 2: Original logo image and extracted LI**

The assessment metrics in Table 2 were implemented between the initial LI and the extracted LI, as displayed in the Figures 5, 6, and 7.

By looking at the Table 3, it can be notice that:

1. The greater PSNR value (higher than 60 dB) suggests a lower degree of variance between the two images and better reconstruction accuracy, as can be seen by glancing at the above table.
2. Lower MSE (roughly near to zero) indicates greater prediction accuracy since the real and reconstructed data sets would be a perfect match. Improvement in correlation as MSE approaches zero serves as an illustration of this.

The extracted logo image and the original image have a lot of similarities thanks to the greater value of SSIM, which is quite near to one. MSE and PSNR values are better from a human visual perspective.



(a) (b)

Fig. 5: "Monkey" image after and before embedding; (a) The original LI and (b) The extracted LI.

(a) (b)

Fig. 6: "Man" image after and before embedding; (a) The original LI and (b) The extracted LI.

(a) (b)

Fig. 7: Image of the letter "A" after and before embedding; (a) The original LI and (b) The extracted LI.

Table 3: The quality measurements to test the strength of LI after and before the embedding technique.

| Results | PSNR | MSE | SSIM |
|---|---|---|---|
| Figure 5 | 60.77 | 0.05 | 0.98 |
| Figure 6 | 65.01 | 0.03 | 0.79 |
| Figure 7 | 59.89 | 0.75 | 0.99 |

## 7. Future Works

Future applications might include:

- Increasing the usage of IoT (Internet of Things) and other healthcare-related applications and improve it to be used for real-time applications.
- It may be used to distinguish a 3D video and audio format from others by adding the ability to protect materials from loss and to encrypt images.

## 8. Conclusions

This study proposes a secure watermarking method based on AES encryption. The purpose of employing the encryption method for the logo image is to strengthen the security of the watermark algorithm by increasing the watermark data security, the information transmission safety, and the resilience of the watermark algorithm recovering. The quality of the fused image and excellent transparency improve with increasing PSNR values. The PSNR value is more than 60 which is mean good image quality. From this research, it is concluded that a high robustness of the watermark has been obtained.

**References**

[1] Aberna and Agilandeeswari "Digital image and video watermarking: methodologies, attacks, applications, and future directions", Multimedia Tools and Applications. 1-61. 10.1007/s11042-023-15806-y (2023).

[2] M. Saiful Islam, Muhammad Ahsan Ullah, and Jitu Prakash Dhar "An imperceptible & robust digital image watermarking scheme based on DWT, entropy and neural network", Karbala International Journal of Modern Science, Vol. 5 (2019).

[3] Begum M., Uddin M.S., "Digital Image Watermarking Techniques: A Review. Information", 11, 110. https://doi.org/10.3390/info11020110 (2020)

[4] Tipirneni Venugopal, and Vusthikayala Siva Kumar Reddy, "Image Watermarking Using Two Level Encryption Method Based on Chaotic Logistic Mapping and Rivest Shamir Adleman Algorithm", International Journal of Intelligent Engineering and Systems, Vol.11, No.6, 2018.

[5] Salim KG, Al-alak SMK, Jawad MJ., "Improved Image Security in Internet of Thing (IOT) Using Multiple Key AES" Baghdad Sci.J, 2021

[6] Nitin Kumar, Deepika, Divya Wadhwa, Deepak Tomer and S. Vijayalakshmi, "Review on Different Chaotic Based Image Encryption Techniques", International Journal of Information and Computation Technology, Volume 4, Number 2 (2014), pp. 197-206.

[7] Priya Deshmukh, "An Image Encryption and Decryption using AES Algorithm," International Journal of Scientific & Engineering Research, Vol. 7, Issue 2, February-2016.

[8] VK Pallaw, KU Singh, A Kumar, T Singh, C Swarup, A Goswami Electronics "A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications,", Electronics, 12(2), p.334.

[9] Li T, Li J, Liu J, Huang M, Chen YW, Bhatti UA. Robust watermarking algorithm for medical images based on log-polar transform. EURASIP Journal on Wireless Communications and Networking. 2022 Dec;2022(1):1-1.

[10] Sharma, Chirag, et al. "A robust image encrypted watermarking technique for neurodegenerative disorder diagnosis and its applications." Computational and Mathematical Methods in Medicine, 2021.

[11] A. Shankar and A. Kannammal, "A Hybrid Of Watermark Scheme With Encryption To Improve Security Of Medical Images," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 226-233, doi: 10.1109/ICICV50876.2021.9388616.

[12] Ajili, Sondes, Mohamed Ali Hajjaji, and Abdellatif Mtibaa. "Crypto-watermarking algorithm using weber's law and AES: a view to transfer safe medical image." Scientific Programming 2021 (2021): 1-22.

[13] D. M. Alsaffar et al., "Image Encryption Based on AES and RSA Algorithms," ICCAIS 2020 - 3rd Int. Conf. Comput. Appl. Inf. Secur., pp. 1–5, 2020, doi: 10.1109/ICCAIS48893.2020.9096809.

[14] Abeer Dawood Salman, and Hala Bahjat Abdulwahab, "Study Analysis to New Trend for 3D Video Watermark", 2019.

[15] Ahmad Abdulqadir Alrababah, Muasaad Alrasheedi, "Digital Image Encryption Implementations Based On AES", VFAST Transactions on Computer Sciences, Volume 5, Number 1, January-December, 2017.

[16] Hala Bahjat Abdulwahab, Khaldoun L. Hameed, and Nawaf Hazim Barnouti, "Video Authentication using PLEXUS Method", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 9, No. 11, December 2018.